The Consultative Committee for Space Data Systems

Recommendation for Space Data System Standards

NETWORK LAYER SECURITY ADAPTATION PROFILE

RECOMMENDED STANDARD

CCSDS 356.0-B-1

BLUE BOOK

June 2018

The Consultative Committee for Space Data Systems

Recommendation for Space Data System Standards

NETWORK LAYER SECURITY ADAPTATION PROFILE

RECOMMENDED STANDARD

CCSDS 356.0-B-1

BLUE BOOK

June 2018

AUTHORITY

Issue:	Recommended Standard, Issue 1
Date:	June 2018
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 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

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

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

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

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

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

FOREWORD

This CCSDS Recommended Standard 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.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CCSDS has processes for identifying patent issues and for securing from the patent holder agreement that all licensing policies are reasonable and non-discriminatory. However, CCSDS does not have a patent law staff, and CCSDS shall not be held responsible for identifying any or all such patent rights.

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

DOCUMENT CONTROL

Document	Title	Date	Status
CCSDS 356.0-B-1	Network Layer Security Adaptation Profile, Recommended Standard, Issue 1	June 2018	Original issue

CONTENTS

1 INTRODUCTION

1.1 PURPOSE

This CCSDS Recommended Standard provides the basis for Network Layer security for space missions utilizing the Internet Protocol (IP) and complying with *IP over CCSDS Space Links* (reference [D2]).

1.2 SCOPE

This Recommended Standard specifies the manner in which the Internet Engineering Task Force's IP Security Protocol (IPsec) should be implemented and used for CCSDS missions.

1.3 APPLICABILITY

This Recommended Standard 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. The end-points of the secure flow could be the originating source and the final recipient of the data, or they might be security gateways at the network perimeters. It is assumed that the CCSDS space links have been established, that connectivity to an IP-based network is in place, and that the network is available for use.

The Recommended Standard is to be used in suitable space communications scenarios where unprotected IP may be used. The document provides for a standardized way to protect such IP traffic over CCSDS or non-CCSDS links in an end-to-end fashion. Suitable space communications scenarios may be found in reference [D5].

1.4 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 may utilize Data Link Layer security services such as the Space Data Link Security (SDLS) Protocol (reference [D3]) 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 IPsec protocol could be used. This document specifies a CCSDS 'profile' of IPsec for use by CCSDS missions.

1.5 NOMENCLATURE

1.5.1 NORMATIVE TEXT

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

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

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

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

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

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

1.5.2 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.

1.6 REFERENCES

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

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

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

[3] C. Kaufman, et al. *Internet Key Exchange Protocol Version 2 (IKEv2)*. STD 79. Reston, Virginia: ISOC, October 2014.

[4] *CCSDS Cryptographic Algorithms*. Issue 1. Recommendation for Space Data System Standards (Blue Book), CCSDS 352.0-B-1. Washington, D.C.: CCSDS, November 2012.

2 OVERVIEW

2.1 GENERAL CONCEPTS

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

As can be seen in *The Application of CCSDS Protocols to Secure Systems* (reference [D4]), security services may be applied at various protocol layers. Below the Network Layer, security services that operate on a hop-by-hop basis across a link must be used, because these link layer protocols only operate on a hop-by-hop basis. Figure 2-1 illustrates the use of hop-by-hop security across a network.

When operating at or above the Network Layer, security can be provided on an end-to-end basis, and 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.

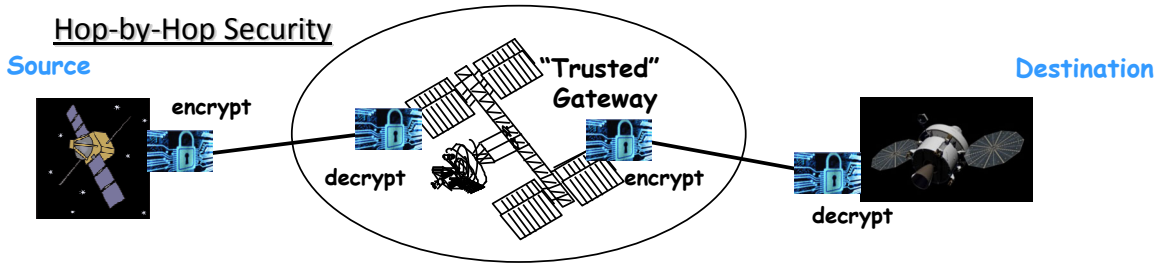

Figure 2-1: Illustration of Hop-by-Hop Security across a Network

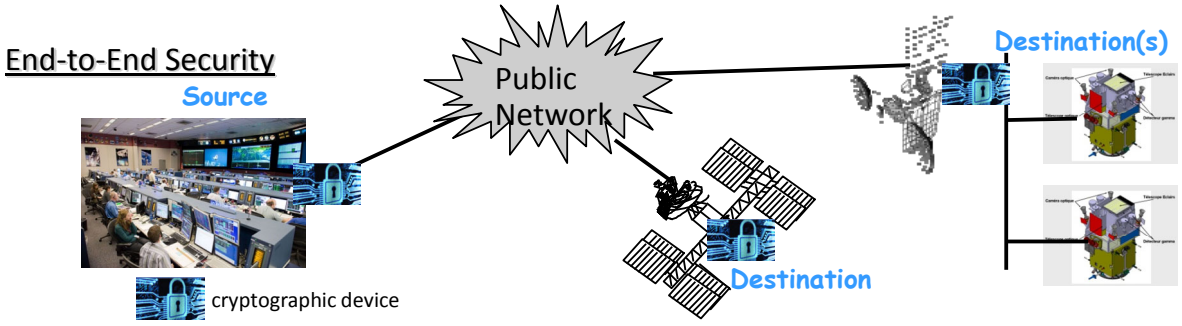

Figure 2-2: Illustration of End-to-End Security across a Network

2.2 SERVICE OVERVIEW

When Internet Protocols are used in the flight system to provide networking services, then security services can be applied at the Network Layer in the form of the 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 utilized without change (e.g., using *IP over CCSDS Space Links*, reference [D2]), requiring no changes to the existing communications infrastructure.

IPsec consists of two protocols, the Authentication Header (AH) (reference [D1]) and the Encapsulating Security Payload (ESP) (reference [2]). 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 also be used to provide an authentication-only service with the use of a null encryption algorithm.

CCSDS only supports ESP as the IPsec protocol. AH is not required, because ESP can provide an authentication-only service. Section 3 of this document specifies which ESP options are supported and which are not.

3 CCSDS IPSEC PROFILE

3.1 GENERAL

This profile adopts RFC 4301 (reference [1]) and RFC 4303 (reference [2]) except as specified in 3.2 through 3.9, below.

3.2 SUPPORTED PROTOCOLS

For CCSDS implementations, IPsec shall support only ESP (reference [2]).

3.3 ESP MODE

For CCSDS implementations, IPsec shall support only ESP tunnel mode.

3.4 ESP AUTHENTICATED ENCRYPTION SERVICE

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

3.5 ESP INTEGRITY SERVICE

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

3.6 ESP NON-AUTHENTICATED ENCRYPTION

For CCSDS implementations, only authenticated encryption shall be used.

3.7 ESP MANUAL KEY MANAGEMENT

For CCSDS implementations, IPsec shall support manual key management.

3.8 ESP AUTOMATIC KEY MANAGEMENT

For CCSDS implementations, IPsec shall support automated key management as described in RFC 4306 (reference [3]) 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.

3.9 ESP CIPHER SUITE

For CCSDS implementations, IPsec shall employ the algorithms described in the CCSDS Cryptographic Algorithms Recommended Standard (reference [4]).

ANNEX A

IMPLEMENTATION CONFORMANCE STATEMENT PROFORMA

(NORMATIVE)

A1 INTRODUCTION

A1.1 OVERVIEW

This annex provides the Implementation Conformance Statement (ICS) Requirements List (RL) for an implementation of Network Layer Security (CCSDS 356.0). The ICS for an implementation is generated by completing the RL in accordance with the instructions below. An implementation shall satisfy the mandatory conformance requirements referenced in the RL.

The RL in this annex is blank. An implementation's completed RL is called the ICS. The ICS states which capabilities and options have been implemented. The following can use the ICS:

- the implementer, as a checklist to reduce the risk of failure to conform to the standard through oversight;
- a supplier or potential acquirer of the implementation, as a detailed indication of the capabilities of the implementation, stated relative to the common basis for understanding provided by the standard ICS proforma;
- a user or potential user of the implementation, as a basis for initially checking the possibility of interworking with another implementation (it should be noted that, while interworking can never be guaranteed, failure to interwork can often be predicted from incompatible ICSes);
- a tester, as the basis for selecting appropriate tests against which to assess the claim for conformance of the implementation.

A1.2 ABBREVIATIONS AND CONVENTIONS

The RL consists of information in tabular form. The status of features is indicated using the abbreviations and conventions described below.

Item Column

The item column contains sequential numbers for items in the table.

Feature Column

The feature column contains a brief descriptive name for a feature. It implicitly means, ‘Is this feature supported by the implementation?’

Keyword Column

The keyword column contains, where applicable, the keyword associated with the feature.

Reference Column

The reference column indicates the relevant subsection or table in Network Layer Security Adaptation Profile (CCSDS 356.0) (this document).

Status Column

The status column uses the following notations:

M mandatory.

O optional.

Support Column Symbols

The support column is to be used by the implementer to state whether a feature is supported by entering Y, N, or N/A, indicating:

Y Yes, supported by the implementation.

N No, not supported by the implementation.

N/A Not applicable.

The support column should also be used, when appropriate, to enter values supported for a given capability.

A1.3 INSTRUCTIONS FOR COMPLETING THE RL

An implementer shows the extent of compliance to the Recommended Standard by completing the RL; that is, the state of compliance with all mandatory requirements and the options supported are shown. The resulting completed RL is called an ICS. The implementer shall complete the RL by entering appropriate responses in the support or values supported column, using the notation described in A1.2. If a conditional requirement is inapplicable, N/A should be used. If a mandatory requirement is not satisfied, exception information must be supplied by entering a reference X*i*, where *i* is a unique identifier, to an accompanying rationale for the noncompliance.

A2 ICS PROFORMA FOR NETWORK LAYER SECURITY

A2.1 GENERAL INFORMATION

A2.1.1 Identification of ICS

Date of Statement (DD/MM/YYY)	
ICS serial number	
System Conformance statement cross-reference	

A2.1.2 Identification of Implementation Under Test (IUT)

Implementation name	
Implementation version	
Special Configuration	
Other Information	

A2.1.3 Identification of Supplier

Supplier	
Contact Point for Queries	
Implementation Name(s) and Versions	
Other information necessary for full identification, e.g., name(s) and version(s) for machines and/or operating systems; System Name(s)	

A2.1.4 Document Version

CCSDS 356.0-B-1	
Have any exceptions been required? NOTE – A YES answer means that the implementation does not conform to the Recommended Standard. Non-supported mandatory capabilities are to be identified in the PICS, with an explanation of why the implementation is non-conforming.	Yes [ ] No [ ]

A2.1.5 Requirements List

Item	Feature	Keyword	Reference	Status	Support
1	Supported Protocols	ESP	3.2	M	
2	ESP Mode	Tunnel	3.3	M	
3	ESP Authenticated Encryption	Authenticated Encryption	3.4	M	
4	ESP Integrity	Integrity	3.5	M	
5	ESP Non-authenticated encryption	Non-authenticated Encryption	3.6	M	
6	ESP Manual Key Management	Manual key management	3.7	M	
7	ESP Automatic Key Management	Automatic Key Management	3.8	M	
8	ESP Cipher Suite	Cipher suite	3.9	M	

ANNEX B

SECURITY, SANA, AND PATENT CONSIDERATIONS

(INFORMATIVE)

B1 SECURITY CONSIDERATIONS

B1.1 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.

B1.2 SECURITY CONCERNS WITH RESPECT TO THE CCSDS DOCUMENT

B1.2.1 Data Privacy

The use of IPsec, specified in references [1] and [2] provides end-to-end data privacy through the use of encryption. Without the use of encryption, any data transmitted over ground networks or RF links could be obtained, examined, and potentially, altered or replaced, by those not authorized to access these data. This might include the upload of spacecraft software or spacecraft commands, or access to and modification of spacecraft telemetry or spacecraft payload/science data.

B1.2.2 Data Integrity

The use of IPsec, specified in references [1] and [2] provides end-to-end data integrity through the use of Integrity Check Values (ICVs), which may also be known as Message Authentication Codes (MACs). 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.

B1.2.3 Authentication of Communicating Entities

The use of IPsec, specified in references [1] and [2], provides end-to-end data authentication through the use of integrity check values, which may also be known as MACs. The use of the authentication service provides assurance of the authenticity of the sender of the data. This service is critical for software uploads and commands sent to a spacecraft.

B1.2.4 Control of Access to Resources

The use of IPsec, specified in references [1] and [2], provides end-to-end control of unauthorized access to data and resources. The use of IPsec encryption allows only authorized entities to access system data and resources.

B1.2.5 Availability of Resources

The use of IPsec, specified in references [1] and [2], provides end-to-end 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.

B1.2.6 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.

B1.3 POTENTIAL THREATS AND ATTACK SCENARIOS

Without the use of IPsec, specified in references [1] and [2], CCSDS missions may have their data stolen, substituted, or modified 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 that 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.

B1.4 CONSEQUENCES OF NOT APPLYING SECURITY TO THE TECHNOLOGY

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

B2 SANA CONSIDERATIONS

The specifications of this document do not require action from SANA.

B3 PATENT CONSIDERATIONS

The specifications of this document are not known to be covered under any patent claims.

ANNEX C

BASELINE IMPLEMENTATION MODE

(INFORMATIVE)

C1 ALGORITHM

The baseline implementation to be used for interoperability testing and operation is authenticated encryption, using the Advanced Encryption Standard (AES) algorithm in the Galois/Counter Mode (GCM) as defined in reference [4]. In addition:

a) the key is 256 bits in total length;

b) the input initialization vector is 96 bits in total length, where all 96 bits are transmitted in-line in the Initialization Vector field of the Security Header;

c) the output MAC is 128 bits in total length.

C2 MANUAL KEYING

There are critical aspects of space missions where automated re-keying might result in a catastrophic event occurring. Therefore, the baseline mode should be capable of employing pre-shared keys with deterministic key lifetimes and with the ability to prohibit re-keying during critical periods of the flight.

ANNEX D

INFORMATIVE REFERENCES

(INFORMATIVE)

[D1] S. Kent. *IP Authentication Header*. RFC 4302. Reston, Virginia: ISOC, December 2005.

[D2] *IP over CCSDS Space Links*. Issue 1. Recommendation for Space Data System Standards (Blue Book), CCSDS 702.1-B-1. Washington, D.C.: CCSDS, September 2012.

[D3] *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.

[D4] *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.

[D5] *Recommendations on a Strategy for Space Internetworking*. Report of the Interagency Operations Advisory Group Space Internetworking Strategy Group, IOAG.T.RC.002.V1. Washington, D.C.: IOAG, August 2010.

ANNEX E

ABBREVIATIONS AND ACRONYMS

(INFORMATIVE)

Term	Meaning
AES	Advanced Encryption Standard
AH	authentication header
ESP	encapsulating security payload
GCM	Galois/Counter Mode
ICV	integrity check value
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPsec	Internet Protocol Security
MAC	Message Authentication Code
SDLS	Space Data Link Security