

Draft Recommendation for
Space Data System Standards

|  |
| --- |
|  |

AUTHORITY

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  | Issue: | ,  |  |
|  | Date: |  |  |
|  | 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

STATEMENT OF INTENT

**(WHEN THIS RECOMMENDED STANDARD 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 **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:

o 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.

o 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.

o 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 document describes a protocol for applying security services to the CCSDS Space Data Link Protocols used by space missions over a space link.

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

Through the process of normal evolution, it is expected that expansion, deletion, or modification of this document may occur. This Recommended Standard is therefore subject to CCSDS document management and change control procedures, which are defined in 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.
* Federal Space Agency (FSA)/Russian Federation.
* Instituto Nacional de Pesquisas Espaciais (INPE)/Brazil.
* Japan Aerospace Exploration Agency (JAXA)/Japan.
* National Aeronautics and Space Administration (NASA)/USA.
* UK Space Agency/United Kingdom.

Observer Agencies

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

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.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

DOCUMENT CONTROL

|  |  |  |  |
| --- | --- | --- | --- |
| **Document** | **Title** | **Date** | **Status** |
| CCSDS 355.0-R-1 | , , Issue 1 | May 2011 | Original (superseded) |
|  | , ,  |  | Current draft:* Adds a PICS annex
* Adds SANA registry and patent considerations
* Adds the use of an authentication bit mask
* Removes the option to transmit only a partial anti-replay sequence number
 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

CONTENTS

Section Page

1 Introduction 1-1

1.1 Purpose 1-1

1.2 Scope 1-1

1.3 Applicability 1-1

1.4 Rationale 1-2

1.5 Document Structure 1-2

1.6 Definitions 1-3

1.7 Conventions 1-4

1.8 References 1-5

2 Overview 2-1

2.1 Concept of Security Protocol 2-1

2.2 Features of Security Protocol 2-2

2.3 Service Functions 2-6

3 SERVICE DEFINITION 3-1

3.1 OVERVIEW 3-1

3.2 SOURCE DATA 3-1

3.3 Security Association Management Service 3-4

3.4 Encryption Service 3-7

3.5 Authentication Service 3-9

4 Protocol Specification 4-1

4.1 Protocol Data Units 4-1

4.2 Security Protocol Procedures 4-3

5 use of the serviceS with CCSDS Protocols 5-1

5.1 TM Protocol 5-1

5.2 TC Protocol 5-2

5.3 AOS Protocol 5-3

5.4 Summary of Protocol Services 5-4

6 MANAGED PARAMETERS 6-1

ANNEX A Protocol Implementation Conformance Statement (PICS) Proforma (normative) A-1

ANNEX B SECURITY (Informative) B-1

ANNEX C Patents and Registries (Informative) C-1

ANNEX D Abbreviations and Acronyms (Informative) D-1

ANNEX E Informative References (Informative) E-1

ANNEX F Baseline Implementation Mode (Informative) F-1

Figure

2-1Security Protocol within OSI Model 2-1

2-2Conceptual Order of Processing within TM 2-3

2-3Conceptual Order of Processing within TC 2-4

2-4Conceptual Order of Processing within AOS 2-5

4-1Security Header 4-1

4-2Security Trailer 4-3

4-3Abstract Model of Authentication Function in TM 4-7

4-4Abstract Model of Authentication Function in TC or AOS 4-8

4-5Abstract Model of Encryption Function 4-9

5-1TM Transfer Frame Using the Security Protocol 5-2

5-2TC Transfer Frame Using the Security Protocol 5-3

5-3AOS Transfer Frame Using the Security Protocol 5-4

D-1Security Header (TM Baseline) F-1

D-2Security Trailer (TM Baseline) F-2

D-3Security Header (TC Baseline) F-3

D-4Security Trailer (TC Baseline) F-3

D-5Security Header (AOS Baseline) F-4

D-6Security Trailer (AOS Baseline) F-4

Table

5-1Summary of Protocol and Services Support 5-4

6-1Managed Parameters for Security Protocol 6-1

# Introduction

## Purpose

The purpose of this Recommended Standard is to specify the Space Data Link Security Protocol (hereafter referred as the Security Protocol) for CCSDS data links. This protocol provides a security header and trailer along with associated procedures that may be used with the CCSDS Telemetry, Telecommand, and Advanced Orbiting Systems Space Data Link Protocols (references [1]-[3]) to provide a structured method for applying data authentication and/or data confidentiality at the Data Link Layer.

## Scope

This Recommended Standard defines the Security Protocol in terms of:

1. the protocol data units employed by the service provider; and
2. the procedures performed by the service provider.

It does not specify:

1. individual implementations or products;
2. the implementation of service interfaces within real systems;
3. the methods or technologies required to perform the procedures; or
4. the management activities required to configure and control the service.

This Recommended Standard does not mandate the use of any particular cryptographic algorithm with the Security Protocol. Reference [7] provides a listing of algorithms recommended by CCSDS; any organization should conduct a risk assessment before choosing to substitute other algorithms. Annex F (non-normative) defines baseline implementations suitable for a large range of space missions.

## Applicability

This Recommended Standard applies to the creation of Agency standards and to the future data communications over space links between CCSDS Agencies in cross-support situations. The Recommended Standard includes comprehensive specification of the service for inter-Agency cross support. It is neither a specification of, nor a design for, real systems that may be implemented for existing or future missions.

The Recommended Standard specified in this document is to be invoked through the normal standards programs of each CCSDS Agency, and is applicable to those missions for which cross support based on capabilities described in this Recommended Standard is anticipated. Where mandatory capabilities are clearly indicated in sections of the Recommended Standard, they must be implemented when this document is used as a basis for cross support. Where options are allowed or implied, implementation of these options is subject to specific bilateral cross support agreements between the Agencies involved.

## Rationale

The goals of this Recommended Standard are to:

1. provide a standard method of applying security at the Data Link Layer, independent of the underlying cryptographic algorithms employed by any particular space mission;
2. preserve compatibility with existing CCSDS Space Data Link Protocol Transfer Frame Header and Trailer formats and frame processing implementations so that, where appropriate, legacy frame processing infrastructure may continue to be used without modification;
3. preserve compatibility with the CCSDS Space Link Extension (SLE) forward and return services; and
4. facilitate the development of common commercial implementations to improve interoperability across agencies.

More discussion of the Security Protocol’s goals and design choices, including its interaction with other CCSDS services, may be found in reference [E3].

## Document Structure

This document is organized as follows:

Section 1 presents the purpose, scope, applicability and rationale of this Recommended Standard and lists the conventions, definitions, and references used throughout the document.

Section 2 (informative) provides an overview of the Security Protocol.

Section 3 (normative) defines the services provided by the protocol entity.

Section 4 (normative) specifies the protocol data units provided for this service and the procedures employed by the service provider.

Section 5 (normative) specifies the Transfer Frame formats and constraints associated with this service for each of the supported Space Data Link Protocols.

Section 6 (normative) lists the managed parameters associated with this service.

Annex A (normative) provides a Protocol Implementation Conformance Statement (PICS) proforma for the Security Protocol.

Annex B (informative) provides an overview of security considerations with using the Security Protocol.

Annex C (informative) provides an overview of patent and registry considerations with using the Security Protocol.

Annex D (informative) provides a glossary of abbreviations and acronyms that appear in the document.

Annex E (informative) provides a list of informative references.

Annex F (informative) defines baseline implementations suitable for a large range of space missions.

## Definitions

Generic definitions for the security terminology applicable to this and other CCSDS documents are provided in [8]. For any terms not defined therein, the following definitions apply for the purposes of this document.

**Authentication**: The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data. [E8] See also peer entity authentication. See also data origin authentication.

**Cipher text**: Data produced through the use of encipherment. The semantic content of the resulting data is not available. [E2]

**Confidentiality**: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. [E2]

**Data Integrity**: The property that data has not been altered or destroyed in an unauthorized manner. [E2]

**Data Origin Authentication**: The corroboration that the source of data received is as claimed. [E2]

**Denial of Service**: The prevention of authorized access to resources or the delaying of time-critical operations. [E2]

**Encipherment**: see encryption.

**Encryption:** The cryptographic transformation of data (see cryptography) to produce ciphertext. [E2]

**Encryption Algorithm**: A set of mathematically expressed rules for rendering data unintelligible by executing a series of conversions controlled by a key. [E8]

**Initialization Vector**: A vector used in defining the starting point of a cryptographic process. [E10]

**Message Authentication Code** (MAC): A cryptographic checksum that results from passing data through a message authentication algorithm. [E9]

**Padding**: Fill data required by certain cipher modes.

**Peer-entity Authentication**: The corroboration that a peer entity in an association is the one claimed. [E2]

**Plaintext**: Unencrypted information. [E8]

**Risk**: Possibility that a particular threat will adversely impact an information system by exploiting a particular vulnerability. [E8]

**Security Policy**: The set of criteria for the provision of security services (see also identity-based and rule-based security policy). [E2]

**Threat**: A potential violation of security. [E2]

## Conventions

### NOMENCLATURE

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

1. the words ‘shall’ and ‘must’ imply a binding and verifiable specification;
2. the word ‘should’ implies an optional, but desirable, specification;
3. the word ‘may’ implies an optional specification;
4. 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.

### 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.

## 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.

[] *TM Space Data Link Protocol*. Recommendation for Space Data System Standards, CCSDS 132.0-B-1. Blue Book. Issue 1. Washington, D.C.: CCSDS, September 2003.

[] *TC Space Data Link Protocol*. Recommendation for Space Data System Standards, CCSDS 232.0-B-2. Blue Book. Issue 2. Washington, D.C.: CCSDS, September 2010.

[] *AOS Space Data Link Protocol*. Recommendation for Space Data System Standards, CCSDS 732.0-B-2. Blue Book. Issue 2. Washington, D.C.: CCSDS, July 2006.

[] *TM Synchronization and Channel Coding*. Recommendation for Space Data System Standards, CCSDS 131.0-B-2. Blue Book. Issue 2. Washington, D.C.: CCSDS, August 2011.

[] *TC Synchronization and Channel Coding*. Recommendation for Space Data System Standards, CCSDS 231.0-B-2. Blue Book. Issue 2. Washington, D.C.: CCSDS, September 2010.

[] *Space Link Identifiers*. Recommendation for Space Data System Standards, CCSDS 135.0-B-4. Blue Book. Issue 4. Washington, D.C.: CCSDS, October 2009.

[] *CCSDS Security Algorithms*. Proposed Recommendation for Space Data System Standards, CCSDS 353.0-R-1. Red Book. Under development.

[] *Information Security Glossary of Terms*. Report Concerning Space Data System Standards, CCSDS 000.0-G-0. Green Book. Issue 1. Washington, D.C.: CCSDS, forthcoming.

[] *Information Technology—Open Systems Interconnection—Conformance testing methodology and framework—Part 7: Implementation Conformance Statements*. International Standard, ISO/IEC 9646-7: 1995. Geneva: ISO, 1995.

NOTE – Informative references are listed in annex E.

# Overview

## Concept of Security Protocol

The Space Data Link Security Protocol is a data processing method for space missions that need to apply authentication and/or confidentiality to the contents of Transfer Frames used by Space Data Link Protocols over a space link. The Security Protocol is provided at the Data Link Layer (Layer 2) of the OSI Basic Reference Model (reference [E1]), as illustrated in figure 2‑1. It is an extra service of the Space Data Link Protocols defined in references [1]-[3], and therefore is to be used together with one of these references.

NOTE – The Security Protocol is **not** associated with the Space Packet Protocol, which operates at a higher layer within the OSI Reference Model.



Figure 2‑1 : Security Protocol within OSI Model

## Features of Security Protocol

The purpose of the Security Protocol is to provide a secure standard method, with associated data structures, for performing security functions on octet-aligned user data within Space Data Link Protocol Transfer Frames over a space link. The maximum length of input data that can be accommodated is not limited by the Security Protocol, but is an attribute of the underlying Space Data Link Protocol. Both Security Header and Trailer are provided for delimiting the protected data and conveying the necessary cryptographic parameters within Transfer Frames. The size of the Security Header and Trailer used will reduce the maximum size of the input data unit byte-for-byte below the maximum allowed by the underlying Space Data Link Protocol.

The Security Protocol provides only the quality of service that is provided by the underlying Space Data Link Protocol. The Security Protocol is scalable to operate across any number of Virtual Channels supported by the underlying Space Data Link Protocols. The use of a Security Header for a given Virtual Channel is a managed parameter which remains constant for a given Mission Phase.

### Internal Organization of Protocol Entity

Two sublayers of the Data Link Layer are defined for CCSDS space link protocols as shown in reference [E7]. Each of the three supported Space Data Link Protocols – Telemetry (TM), Telecommand (TC), and Advanced Orbiting Systems (AOS) – correspond to the Data Link Protocol Sublayer. Operation of the Security Protocol is unaffected by the Synchronization and Channel Coding Sublayer.

### placement of the service in TM

The conceptual order of processing of the Security Protocol’s functions with respect to other functions of the TM Protocol is shown in figure 2‑2. Depending on the security services actually used, not all of the functions may be present in a real system.



Figure 2‑2 : Conceptual Order of Processing within TM

All Security Protocol functions (authentication, encryption, and authenticated encryption) can be used with TM to protect the Packet and Virtual Channel (VC) Access Services. They can be used with the Virtual Channel Frame Secondary Header (VC\_FSH) and Master Channel Frame Secondary Header (MC\_FSH) Services for authentication only. They have no effect on the Virtual Channel Operational Control Field (VC\_OCF), VC Frame, Master Channel Operational Control Field (MC\_OCF), and Master Channel (MC) Frame Services.

### placement of the service in TC

The conceptual order of processing of the Security Protocol’s functions with respect to other functions of the TC Protocol is shown in figure 2‑3. Depending on the services actually used, not all of the functions may be present in a real system.



Figure 2‑3 : Conceptual Order of Processing within TC

All Security Protocol functions (authentication, encryption, and authenticated encryption) can be used with TC to protect the Multiplexer Access Point (MAP) Packet, MAP Access, VC Packet, and VC Access Services. They have no effect on the Communications Operation Procedure (COP) Management, VC Frame, and MC Frame Services.

### placement of the service in AOS

The conceptual order of processing of the Security Protocol’s functions with respect to other functions of the AOS Protocol is shown in figure 2‑4. Depending on the services actually used, not all of the functions may be present in a real system.



Figure 2‑4 : Conceptual Order of Processing within AOS

All Security Protocol functions (authentication, encryption, and authenticated encryption) can be used with AOS to protect the Packet, Bitstream, and VC Access Services. They have no effect on the VC\_OCF, VC Frame, MC Frame, and Insert Services.

## Service Functions

### Security AssociationS

#### General

The Security Protocol provides *security associations* for defining the cryptographic communications parameters to be used by both the sending and receiving ends of a communications session, and for maintaining state information for the duration of the session. A Security Association (SA) defines a simplex (one-way), stateful cryptographic session for providing authentication, data integrity, replay protection, and/or data confidentiality.

#### Security Association Context

All Transfer Frames that share the same SA on a physical channel constitute a Secure Channel. A Secure Channel consists of one or more Global Virtual Channels or Global MAP IDs (TC only) assigned to an SA at the time of its creation.

The Security Parameter Index (SPI) is a transmitted value that uniquely identifies the SA applicable to a Transfer Frame. All Transfer Frames having the same SPI on a physical channel share a single SA. The SPI can be considered as a table index key to an SA data base that stores all of the managed information required by each of the SAs on a physical channel.

#### Security Association Service Types

When an SA is created, one of the following cryptographic functions is selected to be applied on specified fields for all Transfer Frames using that SA:

1. authentication;
2. encryption;
3. authenticated encryption.

Once an SA is created, the authentication and/or encryption algorithms specified, along with their modes of operation, are fixed and cannot be changed for the duration of the SA.

#### Security Header and Trailer

All Transfer Frames using an SA on a physical channel include a Security Header and Trailer surrounding the Frame Data area of the Transfer Frame. The Security Header carries the SPI, initialization vector, anti-replay sequence number, length of any encryption block padding used (where necessary); the Security Trailer carries a Message Authentication Code (MAC).

Once an SA is created, the lengths of the managed fields in the Security Header and Trailer are fixed for the duration of that SA.

#### Security Association Management

Both the sender and the receiver must create an SA, associate it with cryptographic key(s), and activate it before the SA may be used to secure Transfer Frames on a channel.

SAs may be statically preloaded prior to the start of a mission. SAs may also be created dynamically as needed, even while other existing SAs are active. The mechanism for switching from one active SA to another is an Application Layer function.

NOTE – Over-the-air negotiation of SA parameters is a (currently undefined) Application Layer function.

### Authentication

#### General

The Security Protocol provides for the use of authentication algorithms to ensure the *integrity* of transmitted data and the *authenticity* of the data source. The Security Protocol also provides for the use of sequence numbering to detect the unauthorized *replay* of previously transmitted data.

#### Message Authentication and Integrity

When the Security Protocol is used for authentication, a MAC is computed over the specified Transfer Frame fields, which are the Frame Header, the optional Frame Secondary Header (TM only), the optional Segment Header (TC only), the Security Header (as part of this security protocol), and the Frame Data Field. An SA providing authentication also manages an authentication bit mask for that SA, enabling the sender and receiver to ‘mask out’ (i.e., substitute zeros in place of) certain bit fields within the headers from the input to the MAC computation. Transfer frame fields always excluded from MAC computation are the optional Insert Zone (AOS only), optional Operational Control Field (OCF), optional Error Control Field (ECF), and the MAC field itself within the Security Trailer. Transfer frame header fields always included for MAC computation are the Virtual Channel ID, Segment Header (TC only), Security Header, and Frame Data Field.

NOTE – The channel coding synchronization marker prepended to a transfer frame prior to transmission – the Attached Sync Mark (ASM) in TM and AOS, or the Communications Link Transmission Unit (CLTU) Start Sequence in TC – is always excluded from MAC computation.

#### Replay Protection

##### General

When the Security Protocol is used for authentication, a sequence number is also transmitted in the Transfer Frame. As part of an SA providing authentication, both the sender and receiver manage the following information:

1. a sequence number value (current value for the sender, expected value for the receiver);
2. a sequence number window for comparison by the receiver;
3. the location within the Transfer Frame of the sequence number.

##### Sequence Number

The sender increments its managed sequence number by one with each transmitted frame belonging to that SA. The receiver compares each received frame’s Sequence Number to its own stored sequence number. With each valid received frame belonging to that SA, the receiver will replace its stored sequence number with the received value and will increment its stored sequence number by one. If the received Sequence Number differs from the expected value by more than a defined window, the receiver discards the frame, and neither replaces nor increments its stored sequence number.

NOTE – The interpretation of a sequence number rollover (to zero) is mission-specific. Rollover of the sequence number could be used to signal to both the sender and the receiver when the acceptable lifetime of a cryptographic key will end, in order that a key change may be commanded programmatically.

##### Sequence Number Window

The sequence number window is a fixed delta value, specified in the SA, for the receiver to use in comparing the sequence number received to the expected value. A received frame whose sequence number falls outside this window should be discarded. The size of the selected window should account for predicted delays and gaps in RF transmission.

##### Sequence Number Location

The location of the transmitted Sequence Number in the Transfer Frame is specified in the SA. Two options are provided:

1. The Sequence Number may be located in the Sequence Number field of the Security Header. In this case, its length is a managed SA parameter.
2. For systems that implement authenticated encryption using a simple incrementing counter as an initialization vector (i.e., as in Galois/Counter-Mode algorithms), the Initialization Vector field of the Security Header may serve also as the Sequence Number. In this case, the Sequence Number field in the Security Header is zero octets in length.

### Encryption

The Security Protocol provides for the use of encryption algorithms to ensure the *confidentiality* of transmitted data.

When the Security Protocol is used for encryption, the data area of the frame (the ‘plaintext’) is replaced with an encrypted version of the same data (the ‘ciphertext’). An initialization vector should be used as an input to the encryption process. Depending upon the encryption algorithm and mode used, additional fill data may be needed to pad any undersized encryption blocks.

NOTE – Encryption used without authentication may provide a false sense of security, depending upon the specific implementation. Selection of security services should be done carefully after considering a mission-specific threat & risk analysis.

### Authenticated Encryption

The Security Protocol provides for the use of authentication and encryption as one combined (“encrypt-then-MAC”) procedure.

When the Security Protocol is used for authenticated encryption, the frame data supplied by the user is first encrypted as described in 2.3.3, a current anti-replay sequence number is applied to the Transfer Frame, and lastly a MAC is computed over the resultant Transfer Frame as described in 2.3.2.

# SERVICE DEFINITION

## OVERVIEW

This section provides service definition in the form of primitives, which present an abstract model of the logical exchange of data and control information between the protocol entity and the service user. The definitions of primitives are independent of specific implementation approaches.

The parameters of the primitives are specified in an abstract sense and specify the information to be made available to the user of the primitives. The way in which a specific implementation makes this information available is not constrained by this specification. In addition to the parameters specified in this section, an implementation may provide other parameters to the service user (e.g., parameters for controlling the service, monitoring performance, facilitating diagnosis, and so on).

## SOURCE DATA

### Overview

This subsection specifies the service data units that are transferred from sending users to receiving users by the Security Protocol.

### SOURCE DATA for Encryption

#### General

The service data units encrypted by the Security Protocol on a physical channel are one of the following types of service data units, according to the Space Data Link Protocol used on the channel:

1. TM Encryption Payload;
2. TC Encryption Payload;
3. AOS Encryption Payload.

#### TM Encryption Payload

The TM Encryption Payload shall consist of a TM Transfer Frame Data Field.

NOTES

1. The TM Transfer Frame Data Field is the data field of the fixed-length protocol data unit of the TM Space Data Link Protocol whose format is defined in reference [1]. The TM Transfer Frame Data Field is provided to the Security Protocol either by the Packet processing function of the TM Space Data Link Protocol or by the Virtual Channel Access (VCA) Service user.
2. The length of the TM Transfer Frame Data Field Unit is reduced with respect to the maximum size defined in the TM Space Data Link Protocol by the sizes of the Security Header and Trailer.

#### TC Encryption Payload

The TC Encryption Payload shall consist of one of the following types of frame data for the TC Space Data Link Protocol defined in reference [2]:

1. a TC Segment provided by the MAP processing function of the TC Space Data Link Protocol, ***excluding*** the Segment Header;
2. a TC Transfer Frame Data Field consisting of an integral number of Virtual Channel Packets provided by the Virtual Channel Packet processing function of the TC Space Data Link Protocol; or
3. a Virtual Channel Access Service Data Unit (VCA\_SDU) provided by a VCA service user.

Only one of these Encryption Payload types shall exist on a Virtual Channel.

NOTES

1. The TC Segment is the variable-length protocol data unit of the TC Space Data Link Protocol when the Segment Header ***is*** used on the Virtual Channel. The TC Segment contains an integral number of octets of user data corresponding to one Frame Data Unit (for a Type-D Transfer Frame), ***not*** including the Segment Header. Its format is defined in reference [2].
2. The Virtual Channel Packet is the variable-length protocol data unit of the TC Space Data Link Protocol when the Segment Header ***is not*** used on the Virtual Channel. The TC Transfer Frame Data Field contains an integral number of Virtual Channel Packets corresponding to one Frame Data Unit for a Type-D Transfer Frame. Its format is defined in reference [2].
3. The VCA\_SDU is a fixed-length, octet-aligned data unit, the format of which is unknown to the service provider. Its length is established by management. VCA\_SDUs are transferred over a space link with the VCA Service.

#### AOS Encryption Payload

The AOS Encryption Payload shall consist of a Multiplexing Protocol Data Unit (M\_PDU), a Bitstream Protocol Data Unit (B\_PDU), or a VCA\_SDU.

NOTES

1. The M\_PDU is the fixed-length protocol data unit of the AOS Multiplexing Service. Its format is defined in reference [3].
2. The B\_PDU is the fixed-length protocol data unit of the AOS Bitstream Service. Its format is defined in reference [3].
3. The VCA\_SDU is a fixed-length, octet-aligned data unit, the format of which is unknown to the service provider. Its length is established by management. VCA\_SDUs are transferred over a space link with the VCA Service.
4. The length of the M\_PDU, B\_PDU, or VCA\_SDU is reduced with respect to the maximum size defined in the AOS Space Data Link Protocol by the sizes of the Security Header and Trailer.

### SOURCE DATA for Authentication

#### General

The service data units authenticated by the Security Protocol on a physical channel are one, and only one, of the following types of partially formatted Transfer Frame data, according to the Space Data Link Protocol used on the channel:

1. TM Authentication Payload;
2. TC Authentication Payload;
3. AOS Authentication Payload.

#### TM Authentication Payload

The TM Authentication Payload shall consist of the portion of the TM Transfer Frame from the first octet of the Transfer Frame Primary Header to the last octet of the Transfer Frame Data Field immediately preceding the MAC field in the Security Trailer, filtered by the SA authentication mask, and ***excluding*** the optional OCF and ECF.

NOTE – The TM Transfer Frame is the fixed-length protocol data unit of the TM Space Data Link Protocol. Its format is defined in reference [1]. The length of any Transfer Frame transferred on a physical channel must be constant, and is established by management.

#### TC Authentication Payload

The TC Authentication Payload shall consist of the portion of the TC Transfer Frame from the first octet of the Transfer Frame Primary Header to the last octet of the Transfer Frame Data Field immediately preceding the MAC field in the Security Trailer, filtered by the SA authentication mask, and ***excluding*** the optional ECF.

NOTE – The TC Transfer Frame is the variable-length protocol data unit of the TC Space Data Link Protocol. Its format is defined in reference [2].

#### AOS Authentication Payload

The AOS Authentication Payload shall consist of the portion of the AOS Transfer Frame from the first octet of the Transfer Frame Primary Header to the last octet of the Transfer Frame Data Field immediately preceding the MAC field in the Security Trailer, filtered by the SA authentication mask, ***masking out*** the optional Insert Zone, and ***excluding*** the optional OCF and ECF.

NOTE – The AOS Transfer Frame is the fixed-length protocol data unit of the AOS Space Data Link Protocol. Its format is defined in reference [3]. The length of any Transfer Frame transferred on a physical channel must be constant, and is established by management.

## Security Association Management Service

### Overview

The Security Association Management Service establishes the context of an SA for a particular Global Virtual Channel and/or MAP ID. Implementation of the services necessary to manage the parameters contained in the SA data base is a mission-specific function.

### SA Management Service PARAMETERS

#### Overview

Each SA is composed of the commonly applicable parameters listed in 3.3.2.2 below, as well as those parameters in 3.3.2.3 and 3.3.2.4 applicable to the cryptographic function(s) specified in the SA.

#### Security Association Parameters required by all SAs

##### Global Virtual Channel ID

The Global Virtual Channel ID (GVCID) parameter shall contain the ID of the Global Virtual Channel applicable to the SA.

NOTE – The GVCID consists of a Master Channel ID and a Virtual Channel ID.

##### Global Multiplexer Access Point ID

The Global Multiplexer Access Point ID (GMAP\_ID) parameter shall contain a TC MAP ID that indicates the MAP Channel (within the Virtual Channel specified by GVCID) applicable to the SA.

NOTE – The GMAP\_ID consists of a GVCID and a TC MAP ID, and is applicable only if the TC Space Data Link Protocol is used on the channel.

##### Security Parameter Index

The Security Parameter Index parameter shall contain an index identifying the SA applicable to a Frame.

NOTE – Each SA on a physical channel is identified by a unique SPI.

##### SA\_service\_type

The SA\_service\_type parameter indicates the cryptographic function(s) specified for the SA: one of authentication, encryption, or authenticated encryption.

##### SA\_length\_SN

The SA\_length\_SN parameter indicates the length of the Sequence Number field in the Security Header.

##### SA\_length\_IV

The SA\_length\_IV parameter indicates the length of the Initialization Vector field in the Security Header.

##### SA\_length\_PL

The SA\_length\_PL parameter indicates the length of the Pad Length field in the Security Header.

##### SA\_length\_MAC

The SA\_length\_MAC parameter indicates the length of the MAC field in the Security Trailer.

#### Security Association Parameters Specific to Authentication

NOTE – The parameters under this sub-section are applicable only if the SA\_service\_type parameter is Authentication or Authenticated Encryption.

##### SA\_authentication\_algorithm

The SA\_authentication\_algorithm parameter indicates the applicable authentication algorithm and mode of operation.

##### SA\_authentication\_key

The SA\_authentication\_key parameter indicates the value of a provided authentication key, or of an index that refers to the actual key.

##### SA\_authentication\_mask

The SA\_authentication\_mask parameter indicates the value of a provided bit mask that is applied against the transfer frame in a bitwise-AND operation to generate an Authentication Payload.

##### SA\_sequence\_number

The SA\_sequence\_number parameter indicates the present value of a managed anti-replay sequence number.

##### SA\_sequence\_window

The SA\_sequence\_window parameter indicates the amount of deviation the receiving end will accept between the expected anti-replay sequence number and the sequence number in the received frame.

#### Security Association Parameters Specific to Encryption

##### SA\_encryption\_algorithm

NOTE – The parameters under this sub-section are applicable only if the SA\_service\_type parameter is Encryption or Authenticated Encryption.

The SA\_encryption\_algorithm parameter indicates the applicable encryption algorithm and mode of operation.

##### SA\_encryption\_key

The SA\_encryption\_key parameter indicates the value of a provided encryption key, or of an index that refers to the actual key.

##### SA\_initialization\_vector

The SA\_initialization\_vector parameter indicates the present value of a managed initialization vector.

### SA Management SERVICE Primitives

NOTE – At present, this Recommended Standard does not define any service primitives for the Security Association Management Service. Specific directives may be defined in a future revision of this Recommended Standard.

## Encryption Service

### Overview

The Encryption Service transfers Encryption Payloads as applicable to the Space Data Link Protocol in use on the channel. Encryption Payloads, preformatted by the service user according to the specification given in 3.2.2 of this Recommended Standard, are transferred by the service provider according to the SA parameters for the applicable Global Virtual Channel.

### Encryption SERVICE PARAMETERS

#### Encryption Payload

The Encryption Payload parameter shall contain an Encryption Payload of the applicable Space Data Link Protocol (TM, TC, or AOS) to be transferred on the Virtual Channel / Multiplexer Access Point identified by GVCID / GMAP\_ID.

#### GVCID

The GVCID parameter shall contain the ID of the Global Virtual Channel on which the Encryption Payload is to be transferred.

NOTE – The GVCID consists of a Master Channel ID and a Virtual Channel ID.

#### GMAP\_ID

The GMAP\_ID parameter shall contain the ID of the Global Multiplexer Access Point on which the Encryption Payload is to be transferred.

NOTE – The GMAP\_ID consists of a GVCID and a TC MAP ID, and is applicable only if the TC Space Data Link Protocol is used on the channel.

### Encryption SERVICE Primitives

#### General

The service primitives associated with this service are:

1. ENCRYPT.request;
2. ENCRYPT.indication.

#### ENCRYPT.request

##### Function

At the sending end, the Encryption Service user shall pass an ENCRYPT.request primitive to the service provider in order to encrypt and transfer the Encryption Payload through the specified channel.

##### Semantics

The ENCRYPT.request primitive shall provide parameters as follows:

ENCRYPT.request (Encryption Payload, GVCID | GMAP\_ID)

#### ENCRYPT.indication

##### Function

At the receiving end, the service provider shall pass an ENCRYPT.indication primitive to the Encryption Service user in order to transfer the decrypted Payload.

##### Semantics

The ENCRYPT.indication primitive shall provide parameters as follows:

ENCRYPT.indication (Encryption Payload, GVCID | GMAP\_ID)

## Authentication Service

### Overview

The Authentication Service transfers Authentication Payloads as applicable to the Space Data Link Protocol in use on the channel. Authentication Payloads, preformatted by the service user according to the specification given in 3.2.3 of this Recommended Standard, are transferred by the service provider according to the SA for the applicable Global Virtual Channel.

### Authentication SERVICE PARAMETERS

#### Authentication Payload

The Authentication Payload parameter shall contain an Authentication Payload of the applicable Space Data Link Protocol (TM, TC, or AOS) to be transferred on the Virtual Channel / Multiplexer Access Point identified by GVCID / GMAP\_ID.

#### GVCID

The GVCID parameter shall contain the ID of the Global Virtual Channel on which the Frame is to be transferred.

NOTE – The GVCID consists of an Master Channel ID and a Virtual Channel ID.

#### GMAP\_ID

The GMAP\_ID parameter shall contain the ID of the Global Multiplexer Access Point on which the Encryption Payload is to be transferred.

NOTE – The GMAP\_ID consists of a GVCID and a TC MAP ID, and is applicable only if the TC Space Data Link Protocol is used on the channel.

#### Exception

The Exception parameter shall contain a message or status code for the service user to indicate the reason for an authentication failure (e.g., MAC mismatch, sequence number mismatch).

### Authentication SERVICE Primitives

#### General

The service primitives associated with this service are:

1. AUTHENTICATE.request;
2. AUTHENTICATE.indication.
3. AUTHENTICATE.exception.

#### AUTHENTICATE.request

##### Function

At the sending end, the Authentication Service user shall pass an AUTHENTICATE.request primitive to the service provider in order to perform authentication processing on the Authentication Payload supplied by the service user and transfer the Authentication Payload through the specified channel.

##### Semantics

The AUTHENTICATE.request primitive shall provide parameters as follows:

AUTHENTICATE.request (Authentication Payload, GVCID | GMAP\_ID)

#### AUTHENTICATE.indication

##### Function

At the receiving end, the service provider shall pass an AUTHENTICATE.indication primitive to the Authentication Service user to deliver an Authentication Payload after the service has successfully verified the MAC and sequence number of the received Authentication Payload.

##### Semantics

The AUTHENTICATE.indication primitive shall provide parameters as follows:

AUTHENTICATE.indication (Authentication Payload, GVCID | GMAP\_ID)

#### AUTHENTICATE.exception

##### Function

At the receiving end, the service provider shall pass an AUTHENTICATE.exception primitive to the Authentication Service user to notify the user that the service has received an Authentication Payload but the Authentication Payload’s MAC or sequence number has failed verification.

##### Semantics

The AUTHENTICATE.exception primitive shall provide parameters as follows:

AUTHENTICATE.exception (Exception, Authentication Payload,
GVCID | GMAP\_ID)

# Protocol Specification

## Protocol Data Units

### Security Header

#### General

The Security Header is mandatory and shall consist of one mandatory field and three optional fields, positioned contiguously, in the following sequence:

1. Security Parameter Index (16 bits; mandatory);
2. Initialization Vector (octet-aligned, fixed-length for the duration of the SA; optional);
3. Sequence Number (octet-aligned, fixed-length for the duration of the SA; optional);
4. Pad Length (octet-aligned, fixed-length for the duration of the SA; optional).

A Security Header shall consist of at most 64 octets.

The presence or absence of a Security Header on a Virtual Channel shall remain constant throughout a Mission Phase.

NOTES

1. The receiver will determine the presence and length of optional fields in the Security Header by using the SPI to reference the corresponding SA.
2. The format of the Security Header is shown in figure 4‑1.



Figure 4‑1 : Security Header

#### Security Parameter Index

Bits 0-15 of the Security Header shall contain the SPI.

This 16-bit field shall be used as an index to identify an SA.

There can be up to 65534 SAs per Master Channel.

A value of all zeros (‘0’) or all ones (‘65535’) for this field is reserved by CCSDS for future use.

#### Initialization Vector

The Initialization Vector field shall follow the Security Parameter Index field, without gap.

This field shall contain the transmitted portion of the initialization vector, consisting of an integral number of octets.

The Initialization Vector field length is managed and is fixed for the duration of the SA.

If encryption is not selected for an SA, this field shall be zero octets in length.

#### Sequence Number

The Sequence Number field shall follow the Initialization Vector field, without gap.

This field, if authentication or authenticated encryption is selected for an SA, shall contain the anti-replay sequence number, consisting of an integral number of octets.

NOTE – For systems which implement authenticated encryption using a simple incrementing counter as an initialization vector (i.e., as in Galois/Counter-Mode algorithms), the Initialization Vector field of the Security Header may serve also as the Sequence Number. In this case, the Sequence Number field in the Security Header is zero octets in length.

The Sequence Number field length is managed and is fixed for the duration of the SA.

If authentication or authenticated encryption is not selected for an SA, this field shall be zero octets in length.

#### Pad Length

The Pad Length field shall follow the Sequence Number field, without gap.

This field shall contain the number of fill bytes used in the encryption process, consisting of an integral number of octets.

If encryption is not selected for an SA, this field shall be zero octets in length.

### Security Trailer

The Security Trailer is optional and shall consist of a MAC (octet-aligned, fixed-length for the duration of the SA).

If authentication is not selected for an SA, this field should be zero octets in length.

NOTES

1. This field may be present and unused where it is envisioned that the service user may switch between using authentication SA(s) and not using them. In this scenario, it may be preferable to keep the field lengths constant across all operational configurations.
2. The format of the Security Trailer is shown in figure 4‑2.



Figure 4‑2 : Security Trailer

## Security Protocol Procedures

### General

The following procedures shall be carried out to perform the operations of the active SA.

Prior to operation of the Security Protocol, the sending and receiving ends shall initialize a common SA data base containing all the parameters of the SAs to be used on the link.

Synchronization of the contents of the sender’s and receiver’s SA data bases should be maintained during operation.

NOTE – Initialization, modification, and maintenance procedures for those SA data bases are not part of this Security Protocol but are planned to be developed later by CCSDS.

### Security Association Management Procedures

#### General

In order to use an SA to secure Transfer Frames on a channel, each end (both sending and receiving end) of an SA shall:

1. create the SA;
2. associate it with cryptographic key(s); and
3. associate it with the Global Virtual Channel(s) or Global MAP IDs with which it is to be used.

NOTES

1. It is expected that some missions will choose to define SAs statically and preload/pre-activate them prior to the start of the mission.
2. Specifying the successful implementation of cryptographic key management is beyond the scope of this document.

#### Security Association Context

##### General

Every SA shall specify one or more Global Virtual Channels or Global MAP IDs (TC only) with which the SA is to be used.

NOTES

1. The GVCID consists of a Master Channel ID and a Virtual Channel ID.
2. The GMAP\_ID parameter is applicable only if the TC Space Data Link Protocol is used on the channel. In all other cases it is invalid.

##### Idle Transfer Frame Virtual Channels

SAs shall not be created for use with Virtual Channels reserved by CCSDS for carrying only ‘fill’ or ‘idle’ data (i.e., Idle Transfer Frames as defined in references [1] and [3]).

#### Security Parameter Index

Every SA shall be associated with an SPI. The SPI is a transmitted value that uniquely identifies the SA applicable to a Transfer Frame. All Transfer Frames having the same SPI on a Master Channel share a single SA.

#### Security Association Service Type

Every SA shall specify one and only one of the following cryptographic functions to perform:

1. authentication;
2. encryption;
3. authenticated encryption.

NOTE – It is possible to create a ‘clear mode’ SA using one of the defined service types by specifying the algorithm as a ‘no-op’ function (no actual cryptographic operation to be performed). Such an SA might be used, e.g., during development testing of other aspects of data link processing before cryptographic capabilities are available for integrated testing. To avoid inducing a false perception of secure communications, and the problems described in Annex , the use of such an SA is not recommended in normal operation. It is also possible to activate a ‘clear mode’ by designating one or more Virtual Channels to use the underlying Space Data Link Protocol without the Security Protocol’s protections.

#### Parameters Common to All SAs

Every SA shall also specify the following:

1. SPI;
2. length of Initialization Vector field in Security Header;
3. length of Sequence Number field in Security Header;
4. length of Pad Length field in Security Header;
5. length of MAC field in Security Trailer.

#### Parameters for Authentication SAs

Every SA providing authentication shall also specify the following:

1. authentication algorithm and mode of operation;
2. authentication bit mask;
3. managed anti-replay sequence number;
4. managed anti-replay sequence number window.

##### Authentication Bit Mask

Every SA providing authentication shall initialize its authentication bit mask as follows:

1. the mask to be applied shall be equal in length to the data extending from the first octet of the Transfer Frame Primary Header to the last octet of the Transfer Frame Data Field immediately preceding the MAC field in the Security Trailer;
2. the mask bits corresponding to the Virtual Channel ID field of the Transfer Frame Primary Header shall contain all ones;
3. the mask bits corresponding to the Segment Header (TC only) shall contain all ones;
4. the mask bits corresponding to the Security Header shall contain all ones;
5. the mask bits corresponding to the Frame Data Field shall contain all ones;
6. the mask bits corresponding to the Insert Zone (AOS only) shall contain all zeros (i.e., the field shall be ***excluded*** from the authenticated data);
7. the mask bits corresponding to all other Transfer Frame header fields should contain all zeros, unless otherwise specified according to mission requirements.

NOTE – Missions desiring to authenticate other fields (e.g., Spacecraft ID, TM Frame Secondary Header) can include them among the authenticated data merely by selecting an authentication mask that overrides the defaults listed in paragraph g) above.

#### Parameters for Encryption SAs

Every SA providing encryption shall also specify the following:

1. encryption algorithm and mode of operation;

NOTE – The chosen algorithm and mode also imply other attributes such as the required encryption block size and the corresponding need to pad undersized data blocks.

1. managed initialization vector.

#### Parameters for Authenticated Encryption SAs

Every SA providing authenticated encryption shall specify everything required in both 4.2.2.6 and 4.2.2.7 above.

### Sending Procedures

#### Overview

This subsection describes procedures at the sending end associated with each of the functions shown in figures 2‑2, 2‑3, and 2‑4. These figures identify data-handling functions performed by the protocol entity and show logical relationships among these functions. These figures are not intended to imply any hardware or software configuration in a real system. Depending on the services actually used for a real system, not all of the functions may be present in the protocol entity. The procedures described in this subsection are defined in an abstract sense and are not intended to imply any particular implementation approach of a protocol entity.

#### Authentication Operations

If authentication is selected for an SA, then for each transmitted frame belonging to that SA, the sender shall:

1. increment the SA’s managed sequence number by one;

NOTE – The interpretation of a sequence number rollover (to zero) is mission-specific. Rollover of the sequence number may be used to signal the end of the acceptable lifetime of a cryptographic key, in order that a key change may be commanded programmatically.

1. place the managed sequence number in the Sequence Number field of the Security Header, unless that SA specifies to use the Initialization Vector field of the Security Header instead;
2. copy into a temporary buffer the portion of the Transfer Frame extending from the first octet of the Transfer Frame Primary Header to the last octet of the Transfer Frame Data Field immediately preceding the MAC field in the Security Trailer, excluding the optional OCF (TM, AOS only), and optional ECF;
3. apply the SA’s authentication bit mask in a bitwise-AND operation against the temporary buffer, resulting in the Authentication Payload;
4. compute a MAC over the Authentication Payload;
5. (if necessary) truncate the least-significant bits of the computed MAC, such that the result is of identical length to the MAC field in the Security Trailer;
6. place the computed MAC in the Security Trailer.

NOTE – An abstract model of the authentication function is illustrated in figure 4‑3 for the TM protocol, and in figure 4‑4 for the TC and AOS protocols. While the operation of the authentication function is substantially the same across TM, TC, and AOS, its execution is deferred in TM until after Master Channel Generation because of the placement of the Master Channel Frame Count in the TM Primary Header.



Figure 4‑3 : Abstract Model of Authentication Function in TM



Figure 4‑4 : Abstract Model of Authentication Function in TC or AOS

#### Encryption Operations

If encryption is selected for an SA, then for each transmitted frame belonging to that SA, the sender shall:

1. encrypt the Frame Data Field.
2. (optionally) if the encryption algorithm and mode selected for the SA require the use of fill padding, place the number of fill bytes used in the encryption process into the Pad Length field of the Security Header.

NOTE – An abstract model of the encryption function is illustrated in figure 4‑5.



Figure 4‑5 : Abstract Model of Encryption Function

#### Authenticated Encryption Operations

If authenticated encryption is selected for an SA, the sender shall:

1. carry out the encryption operations described in 4.2.3.3; then,
2. carry out the authentication operations described in 4.2.3.2.

### Receiving Procedures

#### Overview

This subsection describes procedures at the receiving end associated with each of the functions shown in figures 2‑2, 2‑3, and 2‑4. These figures identify data-handling functions performed by the protocol entity and show logical relationships among these functions. These figures are not intended to imply any hardware or software configuration in a real system. Depending on the services actually used for a real system, not all of the functions may be present in the protocol entity. The procedures described in this subsection are defined in an abstract sense and are not intended to imply any particular implementation approach of a protocol entity.

#### Security Association Management Operations

##### General

For all frames received over a Global Virtual Channel, the receiver shall:

1. if the received frame has a Security Header, verify that the SA referenced in its SPI is associated with that Global Virtual Channel and/or GMAP ID;
2. report an exception to the service user for frames in which the received frame fails SA verification, and discard those frames.

NOTE – Discarded frames can be archived for forensic investigation if desired.

##### Order of Operations

Each receiver shall enforce the policy described in section 4.2.4.2.1 above ***prior***to performing the specific SA operations described in 4.2.4.3, 4.2.4.4, and 4.2.4.5.

#### Authentication Operations

If authentication is selected for an SA, then for each received frame belonging to that SA, the receiver shall:

1. copy into a temporary buffer the portion of the Transfer Frame extending from the first octet of the Transfer Frame Primary Header to the last octet of the Transfer Frame Data Field immediately preceding the MAC field in the Security Trailer, excluding the optional OCF (TM, AOS only), and optional ECF;
2. apply the SA’s authentication bit mask in a bitwise-AND operation against the temporary buffer, resulting in the Authentication Payload;
3. compute a MAC over the Authentication Payload;
4. (if necessary) truncate the least-significant bits of the computed MAC, such that the result is of identical length to the MAC field in the Security Trailer;
5. verify that the computed MAC matches the MAC received in the Security Trailer;
6. report an exception to the service user for frames in which the received frame fails MAC verification, and discard those frames;

NOTE – Discarded frames can be archived for forensic investigation if desired.

1. extract the received sequence number from either the Sequence Number field or the Initialization Vector field of the Security Header, according to the options specified for that SA;
2. compare the received sequence number to the managed sequence number;
3. report an exception to the service user for frames in which the received sequence number deviates from the managed sequence number (i.e., the expected value) by more than the window defined for that SA, and discard those frames;

NOTE – Discarded frames can be archived for forensic investigation if desired.

1. only upon receipt of frames that pass the verification operations a) - i) above, replace the managed sequence number with the received sequence number and increment it;

NOTE – The interpretation of a sequence number rollover (to zero) is mission-specific. Rollover of the sequence number may be used to signal the end of the acceptable lifetime of a cryptographic key, in order that a key change may be commanded programmatically.

1. remove the Security Trailer from the Frame Data Field to be returned to the service user;
2. if authentication only is specified for the SA, remove the Security Header from the Frame Data Field to be returned to the service user.

#### Encryption Operations

If encryption is selected for an SA, then for each received frame belonging to that SA, the receiver shall:

1. decrypt the Frame Data Field;
2. remove the Security Header from the Frame Data Field to be returned to the service user.

#### Authenticated Encryption Operations

If authenticated encryption is selected for an SA, then for each received frame belonging to that SA, the receiver shall:

1. carry out the authentication operations described in 4.2.4.3; then,
2. carry out the encryption operations described in 4.2.4.4.

# use of the services with CCSDS Protocols

## TM Protocol

### General

The following restrictions apply to use of the Security Protocol with TM:

1. the Packet and VC Access Services may be used on a Global Virtual Channel with the Authentication, Encryption, or Authenticated-Encryption Service, and are protected by each of these services;
2. the VC\_FSH and MC\_FSH Services may be used on a Global Virtual Channel with the Authentication, Encryption, or Authenticated-Encryption Service, and may be protected by authentication but are **not** protected by encryption;
3. the VC\_OCF, VC Frame, MC\_OCF, and MC Frame Services are **not** protected by the Authentication, Encryption, or Authenticated-Encryption Services, but may be used on the same Master Channel.

### TM Transfer Frame Procedures

NOTE – The format of the TM Transfer Frame is defined in reference [1].

The following rules on the format of the TM Transfer Frame shall be applied when the Security Header is present:

1. the TM Frame Secondary Header, if present, shall follow the TM Transfer Frame Primary Header;
2. the Security Header shall follow the TM Frame Secondary Header, if present;
3. the Transfer Frame Data Field shall follow the Security Header;
4. the Security Trailer (MAC), if present, shall follow the Transfer Frame Data Field;
5. the OCF, if present, shall follow the Security Trailer (MAC);
6. the Frame ECF, if present, shall follow the OCF.

NOTE – The format of a TM Transfer Frame using the Security Protocol is shown in figure 5‑1.



Figure 5‑1 : TM Transfer Frame Using the Security Protocol

## TC Protocol

### General

The following restrictions apply to use of the Security Protocol with TC:

1. the MAP Packet, MAP Access, VC Packet, and VC Access Services may be used on a Global Virtual Channel with the Authentication, Encryption, or Authenticated-Encryption Service, and are protected by each of these services;
2. the COP Management, VC Frame, and MC Frame Services are **not** protected by the Authentication, Encryption, or Authenticated-Encryption Services, but may be used on the same Master Channel.

### TC Transfer Frame Procedures

NOTE – The format of the TC Transfer Frame is defined in reference [2].

The following rules on the format of the TC Transfer Frame shall be applied when the Security Header is present:

1. the TC Segment Header, if present, shall follow the TC Transfer Frame Primary Header;
2. the Security Header shall follow the TC Segment Header, if present;
3. the Transfer Frame Data Field shall follow the Security Header;
4. the Security Trailer (MAC), if present, shall follow the Transfer Frame Data Field.
5. the Frame ECF, if present, shall follow the Security Trailer (MAC).

NOTE – The format of a TC Transfer Frame using the Security Protocol is shown in figure 5‑2.



Figure 5‑2 : TC Transfer Frame Using the Security Protocol

## AOS Protocol

### General

The following restrictions apply to use of the Security Protocol with AOS:

1. the Packet, Bitstream, and VC Access Services may be used on a Global Virtual Channel with the Authentication, Encryption, or Authenticated-Encryption Services, and are protected by each of these services;
2. the VC\_OCF Service, VC Frame, MC Frame, and Insert Services are **not** protected by the Authentication, Encryption, or Authenticated-Encryption Services, but may be used on the same Master Channel.

### AOS Transfer Frame Procedures

NOTE – The format of the AOS Transfer Frame is defined in reference [3].

The following rules on the format of the AOS Transfer Frame shall be applied when the Security Header is present:

1. the Insert Zone, if present, shall follow the AOS Transfer Frame Primary Header;
2. the Security Header shall follow the Insert Zone, if present;
3. the Transfer Frame Data Field shall follow the Security Header;
4. the Security Trailer (MAC), if present, shall follow the Transfer Frame Data Field;
5. the OCF, if present, shall follow the Security Trailer (MAC);
6. the Frame ECF, if present, shall follow the OCF.

NOTE – The format of an AOS Transfer Frame using the Security Protocol is shown in figure 5‑3.



Figure 5‑3 : AOS Transfer Frame Using the Security Protocol

## Summary of Protocol Services

Table 5‑1 provides a summary of which services of the supported Space Data Link Protocols may be protected using the service functions of the Security Protocol.

Table 5‑1 : Summary of Protocol and Services Support

| Space Data Link Protocol | Service | Authentication | Encryption | Authenticated Encryption |
| --- | --- | --- | --- | --- |
| TM | Packet | Protected | Protected | Protected |
| VC Access | Protected | Protected | Protected |
| VC\_FSH | Protected | Not protected | authentication only |
| VC\_OCF | Not protected | Not protected | Not protected |
| VC Frame | Not protected | Not protected | Not protected |
| MC\_FSH | Protected | Not protected | authentication only |
| MC\_OCF | Not protected | Not protected | Not protected |
| MC Frame | Not protected | Not protected | Not protected |
| TC | MAP Packet | Protected | Protected | Protected |
| MAP Access | Protected | Protected | Protected |
| VC Packet | Protected | Protected | Protected |
| VC Access | Protected | Protected | Protected |
| COP Management | Not protected | Not protected | Not protected |
| VC Frame | Not protected | Not protected | Not protected |
| MC Frame | Not protected | Not protected | Not protected |
| AOS | Packet | Protected | Protected | Protected |
| Bitstream | Protected | Protected | Protected |
| VC Access | Protected | Protected | Protected |
| VC\_OCF | Not protected | Not protected | Not protected |
| VC Frame | Not protected | Not protected | Not protected |
| MC Frame | Not protected | Not protected | Not protected |
| Insert | Not protected | Not protected | Not protected |

# MANAGED PARAMETERS

In order to conserve bandwidth on the space link, certain parameters associated with the Security Protocol are handled by management rather than by inline communications protocol. The managed parameters are generally those which tend to be static for long periods of time, and whose change signifies a major reconfiguration of the service provider associated with a particular mission. Through the use of a management system, management conveys the required information to the service provider.

The managed parameters used for the Security Protocol are listed in table 6‑1. These parameters are defined in an abstract sense, and are not intended to imply any particular implementation of a management system.

The majority of managed parameters are the parameters of the SA data base managed by both the sending and receiving ends, which must match one another in order to operate correctly.

Table 6‑1 : Managed Parameters for Security Protocol

| **Managed Parameter** | **Allowed Values** | **Defined In** |
| --- | --- | --- |
| **Managed Parameters taken from underlying Space Data Link Protocol:** |
| Minimum TM/TC/AOS Frame Data Unit length (octets) | Integer | Reference [6] |
| Maximum TM/TC/AOS Frame Data Unit length (octets) | Integer | Reference [6] |
| **Security Association Data Base Parameters held staticfor the duration of the applicable SA:** |
| Security Parameter Index (SPI) | 1-65534 |  |
| Security Association Service Type(indicates which cryptographic operations are performed for an SA) | AuthenticationEncryptionAuthenticated Encryption |  |
| Security Association Context(identifies the GVCIDs or Global MAP IDs with which an SA is used) | GVCIDGlobal MAP ID | References [1], [2], [3]Reference [2]  |
| Transmitted length of Initialization Vector (if used) | 0-32 octets |  |
| Transmitted length of Sequence Number (if used) | 2-8 octets |  |
| Transmitted length of Pad Length (if used) | 0-2 octets |  |
| Transmitted length of MAC (if used) | 8-64 octets |  |
| Authentication algorithm |  | Reference [7]  |
| Authentication mask | Bit mask |  |
| Anti-replay sequence number window(± current Sequence Number) | Integer  |  |
| Encryption algorithm |  | Reference [7]  |
| **Security Association Data Base Parameters held static while the applicable SA is active on the channel:** |
| Authentication key | Algorithm-specific |  |
| Encryption key | Algorithm-specific |  |
| **Security Association Data Base Parameters that vary** **dynamically while the applicable SA is active on the channel:** |
| Anti-replay sequence number(sender’s current value, receiver’s expected value). | Integer |  |
| Encryption initialization vector(sender’s current value) | Algorithm-specific |  |

1. Protocol Implementation Conformance Statement (PICS) Proforma

(Normative)
	1. Introduction

To evaluate conformance of a particular implementation, it is necessary to have a statement of which capabilities and options have been implemented for a given protocol specification. Such a statement is called a Protocol Implementation Conformance Statement (PICS). This Annex provides the PICS proforma for the Space Data Link Security Protocol in compliance with the relevant requirements, and in accordance with the relevant guidance given in ISO/IEC 9646-7.

* + 1. Conformance

If it is claimed to conform to this Recommendation, the actual PICS proforma to be filled in by a supplier shall be technically equivalent to the text of the PICS proforma in this Annex, and shall preserve the numbering/naming and ordering of the PICS proforma items. A PICS which conforms to this Recommendation shall be a conforming PICS proforma completed in accordance with the instructions for completion given in section A2.

* + 1. Copyright

Users of this Recommendation may freely reproduce this PICS proforma so that it can be used for its intended purpose and may further publish the completed PICS.

* 1. Instructions for completing the PICS proforma

In order to reduce the size of tables in the PICS proforma, notations have been introduced that have allowed the use of a multi-column layout, where the columns are headed ‘Status’, and ‘Support’. The definition of each of these follows.

* + 1. Status column

The ‘Status’ column indicates the level of support required for conformance to the standard. The values are as follows:

**M** Mandatory support is required.

**O** Optional support is permitted for conformance to the standard. If implemented, it must conform to the specifications and restrictions contained in the standard. These restrictions may affect the optionality of other items.

**O.*n*** The item is optional, but support of at least one of the options labeled with the same number *n* is mandatory. The definitions for the qualification statements used in this annex are written under the tables in which they appear..

**C.*n*** The item is conditional (where *n* is the number which identifies the applicable condition). The definitions for the conditional statements used in this annex are written under the tables in which they appear.

**n/a** The item is not applicable.

* + 1. Support column

The ‘Support’ column shall be completed by the supplier or implementer to indicate the level of implementation of each feature. The proforma has been designed such that the only entries required in the ‘Support’ column are:

**Y** Yes, the feature has been implemented.

**N** No, the feature has not been implemented.

**–** The item is not applicable.

* + 1. Item reference numbers

Each line within the PICS proforma which requires implementation detail to be entered is numbered at the left hand edge of the line. This numbering is included as a means of uniquely identifying all possible implementation details within the PICS proforma. The need for such unique referencing has been identified by the testing bodies.

The means of referencing individual responses should be to specify the following sequence:

1. a reference to the smallest subclause enclosing the relevant item;
2. a solidus character, ‘/‘;
3. the reference number of the row in which the response appears;
4. if, and only if, more than one response occurs in the row identified by the reference number, then each possible entry is implicitly labelled a, b, c, etc., from left to right, and this letter is appended to the sequence.

An example of the use of this notation would be A4/1, which refers to the SDLS implementation’s support for the TM Space Data Link Protocol.

* + 1. Completion of the PICS

The implementer shall complete all entries in the column marked ‘Support’. In certain clauses of the PICS proforma further guidance for completion may be necessary. Such guidance shall supplement the guidance given in this clause and shall have a scope restricted to the clause in which it appears. In addition, other specifically identified information shall be provided by the implementer where requested. No changes shall be made to the proforma except the completion as required. Recognizing that the level of detail required may, in some instances, exceed the space available for responses, a number of responses specifically allow for the addition of appendices to the PICS.

* 1. GENERAL INFORMATION
		1. Referenced Base Standards

The Space Data Link Security (SDLS) Protocol (this Recommendation) is the only base standard referenced in this PICS proforma. In the tables below, numbers in the Reference column refer to applicable subsections within this document.

* + 1. IDENTIFICATION OF the PICS

|  |  |
| --- | --- |
| Date of statement (yyyy-mm-dd) |  |
| PICS version |  |
| System Conformance Statement cross-reference |  |
| Other information |  |

NOTE – The System Conformance Statement is identified in ISO/IEC 9646-7 (reference [9]). It contains a declaration of the layers of the Reference Model covered by the implementation to be tested.

* + 1. Identification of the system supplier and/or
		test laboratory client

|  |  |
| --- | --- |
| Organization name |  |
| Contact name |  |
| Address |  |
| Telephone |  |
| E-mail |  |
| Other information |  |

* + 1. IDENTIFICATION OF the IMPLEMENTATION UNDER TEST

|  |  |
| --- | --- |
| Implementation name |  |
| Implementation version |  |
| Machine name |  |
| Machine version |  |
| Operating system name |  |
| Operating system version |  |
| Special configuration |  |
| Other information |  |

* + 1. IDENTIFICATION OF the protocol

|  |  |
| --- | --- |
| Protocol specification / version |  |
| Technical corrigenda implemented |  |
| Other amendments implemented (explain) |  |

* + 1. Global statement of conformance

|  |  |
| --- | --- |
| Are all mandatory features implemented? (Yes or No) |  |

NOTE – If a ‘No’ answer is given to this question, then the implementation does not conform to the SDLS standard. Non-supported mandatory capabilities are to be identified in the PICS, with an explanation of why the implementation is non-conforming.

|  |  |
| --- | --- |
| Non-conforming capabilities (explain) |  |

* 1. Supported Space Data Link Protocols

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Protocol Feature | Reference | Status | Support |
|  | TM Space Data Link Protocol | Reference  | O.1 |  |
|  | TC Space Data Link Protocol | Reference  | O.1 |  |
|  | AOS Space Data Link Protocol | Reference  | O.1 |  |
|  | O.1: Support for at least one of [ A4/1 | A4/2 | A4/3 ] is M |

* 1. Supported Security Services

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Protocol Feature | Reference | Status | Support |
|  | Encryption | 4.2.2.4 | O.2 |  |
|  | Authentication | 4.2.2.4 | O.2 |  |
|  | Authenticated Encryption | 4.2.2.4 | O.2 |  |
|  | O.2: Support for at least one of [ A5/1 | A5/2 | A5/3 ] is M |

* 1. Security Association Management Data

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Protocol Feature | Reference | Status | Support |
|  | GVCID | 3.3.2.2.14.2.2.2.1 | M |  |
|  | GMAP\_ID | 3.3.2.2.24.2.2.2.1 | C.1 |  |
|  | SPI | 3.3.2.2.34.2.2.3 | M |  |
|  | SA\_service\_type | 3.3.2.2.44.2.2.4 | M |  |
|  | SA\_length\_SN | 3.3.2.2.54.2.2.5 c) | M |  |
|  | SA\_length\_IV | 3.3.2.2.64.2.2.5 b) | M |  |
|  | SA\_length\_PL | 3.3.2.2.74.2.2.5 d) | M |  |
|  | SA\_length\_MAC | 3.3.2.2.84.2.2.5 e) | M |  |
|  | SA\_authentication\_algorithm | 3.3.2.3.14.2.2.6 a) | C.2 |  |
|  | SA\_authentication\_key | 3.3.2.3.2 | C.2 |  |
|  | SA\_authentication\_mask | 3.3.2.3.34.2.2.6 b) | C.2 |  |
|  | SA\_sequence\_number | 3.3.2.3.44.2.2.6 c) | C.2 |  |
|  | SA\_sequence\_window | 3.3.2.3.54.2.2.6 d) | C.2 |  |
|  | SA\_encryption\_algorithm | 3.3.2.4.10 a) | C.3 |  |
|  | SA\_encryption\_key | 3.3.2.4.2 | C.3 |  |
|  | SA\_initialization\_vector | 3.3.2.4.34.2.2.7 b) | C.4 |  |
|  | C.1: if [ A4/2 ] is supported then M, else n/a C.2: if [ A5/2 | A5/3 ] is supported then M, else n/aC.3: if [ A5/1 | A5/3 ] is supported then M, else n/aC.4: if [ A5/1 | A5/3 ] is supported then M, else O |

* 1. Service Primitives

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Protocol Feature | Reference | Sender | Receiver |
| Status | Support | Status | Support |
|  | ENCRYPT.request | 3.4.3.2 | C.3 |  | n/a |  |
|  | ENCRYPT.indication | 3.4.3.3 | n/a |  | C.3 |  |
|  | AUTHENTICATE.request | 3.5.3.2 | C.2 |  | n/a |  |
|  | AUTHENTICATE.indication  | 3.5.3.3 | n/a |  | C.2 |  |
|  | AUTHENTICATE.exception  | 3.5.3.4 | n/a |  | C.2 |  |
|  | C.2: if [ A5/2 | A5/3 ] is supported then M, else n/aC.3: if [ A5/1 | A5/3 ] is supported then M, else n/a |

* + 1. Encryption Procedures
			1. ENCRYPT.request (Sending)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Protocol Feature | Reference | Status | Support |
|  | TM Encryption Payload |  | C.5 |  |
|  | TC Encryption Payload |  | C.1 |  |
|  | AOS Encryption Payload |  | C.6 |  |
|  | GVCID |  | M |  |
|  | GMAP\_ID |  | C.1 |  |
|  | Encrypt frame data |   | M |  |
|  | Put length of pad in header |   | O |  |
|  | C.1: if [ A4/2 ] is supported then M, else n/a C.5: if [ A4/1 ] is supported then M, else n/aC.6: if [ A4/3 ] is supported then M, else n/a |

* + - 1. ENCRYPT.indication (Receiving)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Protocol Feature | Reference | Status | Support |
|  | TM Encryption Payload |  | C.5 |  |
|  | TC Encryption Payload |  | C.1 |  |
|  | AOS Encryption Payload |  | C.6 |  |
|  | GVCID |  | M |  |
|  | GMAP\_ID |  | C.1 |  |
|  | Discard frames with wrong SA |  | M |  |
|  | Decrypt frame data |   | M |  |
|  | Remove header |   | M |  |
|  | C.1: if [ A4/2 ] is supported then M, else n/a C.5: if [ A4/1 ] is supported then M, else n/aC.6: if [ A4/3 ] is supported then M, else n/a |

* + 1. Authentication Procedures
			1. AUTHENTICATE.request (Sending)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Protocol Feature | Reference | Status | Support |
|  | TM Authentication Payload |  | C.5 |  |
|  | TC Authentication Payload |  | C.1 |  |
|  | AOS Authentication Payload |  | C.6 |  |
|  | GVCID |  | M |  |
|  | GMAP\_ID |  | C.1 |  |
|  | Increment SN |   | M |  |
|  | Put SN in header |   | M |  |
|  | Get authentication payload data |  c) | M |  |
|  | Apply mask |  d) | M |  |
|  | Compute MAC |  e) | M |  |
|  | Truncate MAC |   | O |  |
|  | Put MAC in trailer |   | M |  |
|  | C.1: if [ A4/2 ] is supported then M, else n/a C.5: if [ A4/1 ] is supported then M, else n/aC.6: if [ A4/3 ] is supported then M, else n/a |

* + - 1. AUTHENTICATE.indication (Receiving)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Protocol Feature | Reference | Status | Support |
|  | TM Authentication Payload |  | C.5 |  |
|  | TC Authentication Payload |  | C.1 |  |
|  | AOS Authentication Payload |  | C.6 |  |
|  | GVCID |  | M |  |
|  | GMAP\_ID |  | C.1 |  |
|  | Discard frames with wrong SA |  | M |  |
|  | Get authentication payload data |   | M |  |
|  | Apply mask |  b) | M |  |
|  | Compute MAC |  c) | M |  |
|  | Truncate computed MAC |   | O |  |
|  | Compare to received MAC |   | M |  |
|  | Read received SN |   | M |  |
|  | Compare to managed SN |   | M |  |
|  | Update managed SN |   | M |  |
|  | Remove trailer |   | M |  |
|  | Remove header |   | M |  |
|  | C.1: if [ A4/2 ] is supported then M, else n/a C.5: if [ A4/1 ] is supported then M, else n/aC.6: if [ A4/3 ] is supported then M, else n/a |

* + - 1. AUTHENTICATE.exception (Receiving)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Protocol Feature | Reference | Status | Support |
|  | TM Authentication Payload |  | C.5 |  |
|  | TC Authentication Payload |  | C.1 |  |
|  | AOS Authentication Payload |  | C.6 |  |
|  | GVCID |  | M |  |
|  | GMAP\_ID |  | C.1 |  |
|  | Exception |  | M |  |
|  | Report MAC exceptions |   | M |  |
|  | Discard frames with bad MAC |   | M |  |
|  | Archive rejected-MAC frames |   | O |  |
|  | Report SN exceptions |   | M |  |
|  | Discard frames with bad SN |   | M |  |
|  | Archive rejected-SN frames |   | O |  |
|  | C.1: if [ A4/2 ] is supported then M, else n/a C.5: if [ A4/1 ] is supported then M, else n/aC.6: if [ A4/3 ] is supported then M, else n/a |

* + 1. Authenticated Encryption Procedures
			1. Authenticated Encryption (Sending)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Protocol Feature | Reference | Status | Support |
|  | First perform encryption | 4.2.3.4 a) | M |  |
|  | Then perform authentication | 4.2.3.4 b) | M |  |
|  |  |

* + - 1. Authenticated Encryption (Receiving)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Protocol Feature | Reference | Status | Support |
|  | First verify authentication |   | M |  |
|  | Then perform decryption |   | M |  |
|  |  |

* 1. Protocol Data Units
		1. Security Header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Protocol Feature | Reference | Status | Support |
|  | SPI |   | M |  |
|  | IV |   | C.4 |  |
|  | SN |   | C.2 |  |
|  | PL |   | C.3 |  |
|  | Max length |  | M |  |
|  | C.2: if [ A5/2 | A5/3 ] is supported then M, else n/aC.3: if [ A5/1 | A5/3 ] is supported then M, else n/aC.4: if [ A5/1 | A5/3 ] is supported then M, else O |

* + 1. Security Trailer

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Protocol Feature | Reference | Status | Support |
|  | MAC | 4.1.2.1 | C.7 |  |
|  | C.7: if [ A5/2 | A5/3 ] is supported then M, else O |

* + 1. TM Frame Structure Using SDLS

NOTE – If [ A4/1 ] is not supported, then this section is n/a.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Protocol Feature | Reference | Status | Support |
|  | TM Primary Header | 5.1.2  | M |  |
|  | Frame Secondary Header | 5.1.2 a) | O |  |
|  | Security Header | 5.1.2 b) | M |  |
|  | Frame Data | 5.1.2 c) | M |  |
|  | Security Trailer | 5.1.2 d) | C.2 |  |
|  | OCF | 5.1.2 e) | O |  |
|  | ECF | 5.1.2 f) | O |  |
|  | C.2: if [ A5/2 | A5/3 ] is supported then M, else n/a |

* + 1. TC Frame Structure Using SDLS

NOTE – If [ A4/2 ] is not supported, then this section is n/a.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Protocol Feature | Reference | Status | Support |
|  | TC Primary Header | 5.2.2  | M |  |
|  | Segment Header | 5.2.2 a) | O |  |
|  | Security Header | 5.2.2 b) | M |  |
|  | Frame Data | 5.2.2 c) | M |  |
|  | Security Trailer | 5.2.2 d) | C.2 |  |
|  | ECF | 5.2.2 e) | O |  |
|  | C.2: if [ A5/2 | A5/3 ] is supported then M, else n/a |

* + 1. AOS Frame Structure Using SDLS

NOTE – If [ A4/3 ] is not supported, then this section is n/a.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Protocol Feature | Reference | Status | Support |
|  | AOS Primary Header | 5.3.2  | M |  |
|  | Insert Zone | 5.3.2 a) | O |  |
|  | Security Header | 5.3.2 b)  | M |  |
|  | Frame Data | 5.3.2 c) | M |  |
|  | Security Trailer | 5.3.2 d)  | C.2 |  |
|  | OCF | 5.3.2 e) | O |  |
|  | ECF | 5.3.2 f) | O |  |
|  | C.2: if [ A5/2 | A5/3 ] is supported then M, else n/a |

1. SECURITY

(Informative)
	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 payload is not disclosed, not altered, and not spoofed.

* 1. Security concerns

Security concerns specific to the Security Protocol design are addressed in more detail in reference [E2].

It may be necessary to apply security services at multiple layers within the protocol stack, to account for distributed processing and cross-support, to account for different classes of data or end users, or to account for protection of data during unprotected portions of the complete end-to-end transmission (e.g., across ground networks). The specification of security services at other layers is outside the scope of this document.

References [E4] and [E5] contain more information regarding the choice of services and where they can be implemented. Reference [7] contains more information regarding the choice of particular cryptographic algorithms.

* 1. Potential threats and attack scenarios

The Security Protocol provides no protection against denial-of-service attacks against the communications channel, such as radio-frequency jamming.

The Security Protocol provides no protection against traffic flow analysis. Where encryption is used, a careful choice of algorithm and mode will provide protection to the user-supplied data unit, but an attacker can use the Spacecraft ID, Virtual Channel ID, TC MAP ID, OCF, or COP control directives as metadata for inferring information about the parties communicating and possibly the nature or status of their communications.

The Security Protocol provides no cryptographic key management protocol. Specifying the successful implementation of cryptographic key management is beyond the scope of this document. (See reference [E6] for more information.)

The Security Protocol provides no protection to TC COP control commands nor to COP CLCW status information returned in the OCF; an attacker could use false COP control directives or OCF contents to interfere with a communications session.

The Security Protocol foresees the existence of a ‘clear’ mode for certain VCs. If a clear mode is implemented, the conditions under which, and by which, it is activated should be carefully analyzed, as those might introduce major security vulnerabilities.

If encryption is implemented without authentication, the Security Protocol provides no protection against data substitution attacks. In addition, it may be possible for an attacker to reverse-engineer the encryption key and compromise data confidentiality, if portions of the original plaintext are predictable.

Specific potential threats and attack scenarios are addressed in more detail in reference [E2].

* 1. Consequences of not applying security

Without authentication, unauthorized commands or software might be uploaded to a spacecraft or data received from a source masquerading as the spacecraft. Without data integrity, corrupted commands or software might be uploaded to a spacecraft potentially resulting in the loss of the mission, harm to people and property, or loss of life (especially in the case of a manned mission). Without data integrity, corrupted telemetry might be retrieved from a spacecraft which could result in an incorrect course of action being taken. If confidentiality is not implemented, data flowing to or from a spacecraft might be visible to unauthorized entities resulting in disclosure of sensitive or private information.

1. Patents and Registries

(Informative)
	1. Patent COnsiderations

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

At the time of publication, CCSDS was not aware of any claimed patent rights applicable to implementing the provisions of this Recommendation.

* 1. Space Assigned Numbers Authority (SANA) COnsiderations

This Recommendation defines no new information registries. The recommendations of this document do not require any action from SANA.

1. Abbreviations and Acronyms

(Informative)

AES Advanced Encryption Standard

AOS Advanced Orbiting Systems

ASM Attached Sync Mark

B\_PDU Bitstream Protocol Data Unit

CLCW Communications Link Control Word

CLTU Communications Link Transmission Unit

CMAC Cipher-based Message Authentication Code

COP Communications Operation Procedure

ECF Error Control Field

FSH Frame Secondary Header

GCM Galois/Counter Mode

GVCID Global Virtual Channel ID

M\_PDU Multiplexing Protocol Data Unit

MAC Message Authentication Code

MAP Multiplexer Access Point

GMAP\_ID Global Multiplexer Access Point ID

MC Master Channel

OCF Operational Control Field

RF Radio Frequency

SA Security Association

SANA Space Assigned Numbers Authority

SLE Space Link Extension

SPI Security Parameter Index

TC Telecommand

TM Telemetry

VC Virtual Channel

VCA Virtual Channel Access

VCA\_SDU Virtual Channel Access Service Data Unit

1. Informative References

(Informative)

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

[] *Information Processing Systems—Open Systems Interconnection—Basic Reference Model—Part 2: Security Architecture*; International Standard, ISO 7498-2:1989(E); February 1989.

[] *Space Data Link Security Protocol*. Report Concerning Space Data System Standards, CCSDS 350.5-G-0. Green Book. Issue 1. Washington, D.C.: CCSDS, forthcoming.

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

[] *Security Architecture for Space Data Systems*. Draft Recommendation for Space Data System Standards, CCSDS 351.0-R-1. Red Book. Issue 1. Washington, D.C.: CCSDS, forthcoming.

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

[] *Overview of Space Communications Protocols*. Report Concerning Space Data System Standards, CCSDS 130.0-G-2. Green Book. Issue 2. Washington, D.C.: CCSDS, December 2007.

[] Committee on National Security Systems; *National Information Assurance (IA) Glossary*; CNSS Instruction No. 4009; April 2010.

[] National Institute of Standards and Technology (NIST); *Glossary of Key Information Security Terms*; NIST IR 7298 revision 1; February 2011.

[] National Institute of Standards and Technology (NIST); *Recommendation for Key Management – Part 1: General*; NIST SP 800-57, March 2007.

NOTE – Normative references are listed in 1.8.

1. Baseline Implementation Mode

(Informative)
	1. Baseline Mode for use with TM
		1. 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 [7]. In addition:

1. the key is 128 bits in total length;
2. 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;
3. the output MAC is 128 bits in total length.
	* 1. Security Header

The baseline implementation uses a Security Header of 14 octets in length. The format of the Security Header is shown in figure F‑1.

NOTES

1. GCM normally uses a simple incrementing counter as its initialization vector. A separate anti-replay Sequence Number is unnecessary; therefore the Sequence Number field shown in figure F‑1 is zero octets in length. (See 4.1.1.3.)
2. GCM does not require padding; therefore the length of the Pad Length field shown in figure F‑1 is zero octets.



Figure F‑1 : Security Header (TM Baseline)

* + 1. Security Trailer

The baseline implementation uses a Security Trailer of 16 octets in length. The format of the Security Trailer is shown in figure F‑2.



Figure F‑2 : Security Trailer (TM Baseline)

* + 1. Authentication Bit Mask

The baseline implementation uses an authentication mask in which all of the mask bits corresponding to Transfer Frame header fields not otherwise specified in section 4.2.2.6.1 contain zeros.

* 1. Baseline Mode for use with TC
		1. Algorithm

The baseline implementation to be used for interoperability testing and operation is authentication, using the AES algorithm used in the Cipher-based Message Authentication Code (CMAC) mode as defined in reference [7]. In addition:

1. the key is 128 bits in total length;
2. the anti-replay sequence number is 32 bits in total length, where all 32 bits are transmitted in-line in the Sequence Number field of the Security Header;
3. the output MAC is 128 bits in total length.
	* 1. Security Header

The baseline implementation uses a Security Header of 6 octets in length. The format of the Security Header is shown in figure F‑3.

NOTE – The CMAC mode of operation performs no encryption and does not require an initialization vector nor padding; therefore the length of the Initialization Vector and Pad Length fields shown in figure F‑3 are zero octets each.



Figure F‑3 : Security Header (TC Baseline)

* + 1. Security Trailer

The baseline implementation uses a Security Trailer of 16 octets in length. The format of the Security Trailer is shown in figure F‑4.



Figure F‑4 : Security Trailer (TC Baseline)

* + 1. Authentication Bit Mask

The baseline implementation uses an authentication mask in which all of the mask bits corresponding to Transfer Frame header fields not otherwise specified in section 4.2.2.6.1 contain zeros.

* 1. Baseline Mode for use with AOS
		1. Algorithm

The baseline implementation to be used for interoperability testing and operation is authenticated encryption, using the AES algorithm used in the GCM as defined in reference [7]. In addition:

1. the key is 128 bits in total length;
2. 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;
3. the output MAC is 128 bits in total length.
	* 1. Security Header

The baseline implementation uses a Security Header of 14 octets in length. The format of the Security Header is shown in figure F‑5.

NOTES

1. GCM normally uses a simple incrementing counter as its initialization vector. A separate anti-replay Sequence Number is unnecessary; therefore the Sequence Number field shown in figure F‑5 is zero octets in length. (See 4.1.1.3.)
2. GCM does not require padding; therefore the length of the Pad Length field shown in figure F‑5 is zero octets.



Figure F‑5 : Security Header (AOS Baseline)

* + 1. Security Trailer

The baseline implementation uses a Security Trailer of 16 octets in length. The format of the Security Trailer is shown in figure F‑6.



Figure F‑6 : Security Trailer (AOS Baseline)

* + 1. Authentication Bit Mask

The baseline implementation uses an authentication mask in which all of the mask bits corresponding to Transfer Frame header fields not otherwise specified in section 4.2.2.6.1 contain zeros.