INTERNATIONAL STANDARD

ISO 21324

First edition
2016-11-15

Space data and information transfer systems — Space data link security protocol

Systèmes de transfert des données et informations spatiales — Protocole de sécurité de liaison de données spatiales

Reference number
ISO 21324:2016(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
copyright@iso.org
Web www.iso.org

Published in Switzerland

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2. www.iso.org/directives

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received. www.iso.org/patents

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

ISO 21324 was prepared by the Consultative Committee for Space Data Systems (CCSDS) (as CCSDS 355.0-B-1, September 2015) and was adopted (without modifications except those stated in clause 2 of this International Standard) by Technical Committee ISO/TC 20, *Aircraft and space vehicles*, Subcommittee SC 13, *Space data and information transfer systems*.

STATEMENT OF INTENT

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

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

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

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

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

FOREWORD

This 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 has processes for identifying patent issues and for securing from the patent holder agreement that all licensing policies are reasonable and non-discriminatory. However, CCSDS does not have a patent law staff, and CCSDS shall not be held responsible for identifying any or all such patent rights.

Through the process of normal evolution, it is expected that expansion, deletion, or modification of this document may occur. This Recommended Standard is therefore subject to CCSDS document management and change control procedures, which are defined in *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-4). Current versions of CCSDS documents are maintained at the CCSDS Web site:

http://www.ccsds.org/

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

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

Member Agencies

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

Observer Agencies

- Austrian Space Agency (ASA)/Austria.
- Belgian Federal Science Policy Office (BFSPO)/Belgium.
- Central Research Institute of Machine Building (TsNIIMash)/Russian Federation.
- China Satellite Launch and Tracking Control General, Beijing Institute of Tracking and Telecommunications Technology (CLTC/BITTT)/China.
- Chinese Academy of Sciences (CAS)/China.
- Chinese Academy of Space Technology (CAST)/China.
- Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
- Danish National Space Center (DNSC)/Denmark.
- Departamento de Ciência e Tecnologia Aeroespacial (DCTA)/Brazil.
- Electronics and Telecommunications Research Institute (ETRI)/Korea.
- European Organization for the Exploitation of Meteorological Satellites (EUMETSAT)/Europe.
- European Telecommunications Satellite Organization (EUTELSAT)/Europe.
- Geo-Informatics and Space Technology Development Agency (GISTDA)/Thailand.
- Hellenic National Space Committee (HNSC)/Greece.
- Indian Space Research Organization (ISRO)/India.
- Institute of Space Research (IKI)/Russian Federation.
- 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.
- South African National Space Agency (SANSA)/Republic of South Africa.
- Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
- Swedish Space Corporation (SSC)/Sweden.
- Swiss Space Office (SSO)/Switzerland.
- United States Geological Survey (USGS)/USA.

DOCUMENT CONTROL

Document	Title	Date	Status
CCSDS 355.0-B-1	Space Data Link Security Protocol, Recommended Standard, Issue 1	September 2015	Original issue

CONTENTS

CONTENTS (continued)

Section Page

Figure

Table

1 INTRODUCTION

1.1 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.

1.2 SCOPE

This Recommended Standard defines the Security Protocol in terms of:

a) the protocol data units employed by the service provider; and

b) the procedures performed by the service provider.

It does not specify:

a) individual implementations or products;

b) the implementation of service interfaces within real systems;

c) the methods or technologies required to perform the procedures; or

d) 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 [4] provides a listing of algorithms recommended by CCSDS; any organization should conduct a risk assessment before choosing to substitute other algorithms. Annex E (non-normative) defines baseline implementations suitable for a large range of space missions.

1.3 APPLICABILITY

This Recommended Standard applies to the creation of Agency standards and for secure 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 interoperability and 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 interoperability and cross support. Where options are allowed or implied, implementation of these options is subject to specific bilateral cross support agreements between the Agencies involved.

1.4 RATIONALE

The goals of this Recommended Standard are to:

a) provide a standard method of applying security at the Data Link Layer, independent of the underlying cryptographic algorithms employed by any particular space mission;

b) 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;

c) preserve compatibility with the CCSDS Space Link Extension (SLE) forward and return services; and

d) 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 [D3].

1.5 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 these services and the procedures employed by the service provider.

Section 5 (normative) specifies the constraints associated with these services for each of the supported Space Data Link Protocols.

Section 6 (normative) lists the managed parameters associated with these services.

Section 7 (normative) specifies how to verify an implementation's conformance with the Security Protocol.

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

Annex B (informative) provides an overview of security, SANA registry, and patent considerations related to this Recommended Standard.

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

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

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

1.6 DEFINITIONS

For the purposes of this document, the following definitions apply.

NOTE – Generic definitions for the security terminology applicable to this and other CCSDS documents are provided in reference [D5].

Payload: Data input to be processed by a Security Protocol function.

ApplySecurity Payload: Payload to the ApplySecurity function.

ProcessSecurity Payload: Payload to the ProcessSecurity function.

Authentication Payload: Part of the Transfer Frame to be authenticated.

1.7 CONVENTIONS

1.7.1 NOMENCLATURE

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

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

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

c) the word 'may' implies an optional specification;

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

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

1.7.2 INFORMATIVE TEXT

In the normative sections of this document, informative text is set off from the normative specifications either in notes or under one of the following subsection headings:

– Overview;

– Background;

– Rationale;

– Discussion.

1.8 REFERENCES

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

[1] *TM Space Data Link Protocol*. Issue 2. Recommendation for Space Data System Standards (Blue Book), CCSDS 132.0-B-2. Washington, D.C.: CCSDS, September 2015.

[2] *TC Space Data Link Protocol*. Issue 3. Recommendation for Space Data System Standards (Blue Book), CCSDS 232.0-B-3. Washington, D.C.: CCSDS, September 2015.

[3] *AOS Space Data Link Protocol*. Issue 3. Recommendation for Space Data System Standards (Blue Book), CCSDS 732.0-B-3. Washington, D.C.: CCSDS, September 2015.

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

NOTE – Informative references are listed in annex D.

2 OVERVIEW

2.1 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 only at the Data Link Layer (Layer 2) of the OSI Basic Reference Model (reference [D1]), 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. (The Security Protocol is *not* applicable for use with the Proximity-1 Space Data Link Protocol.)

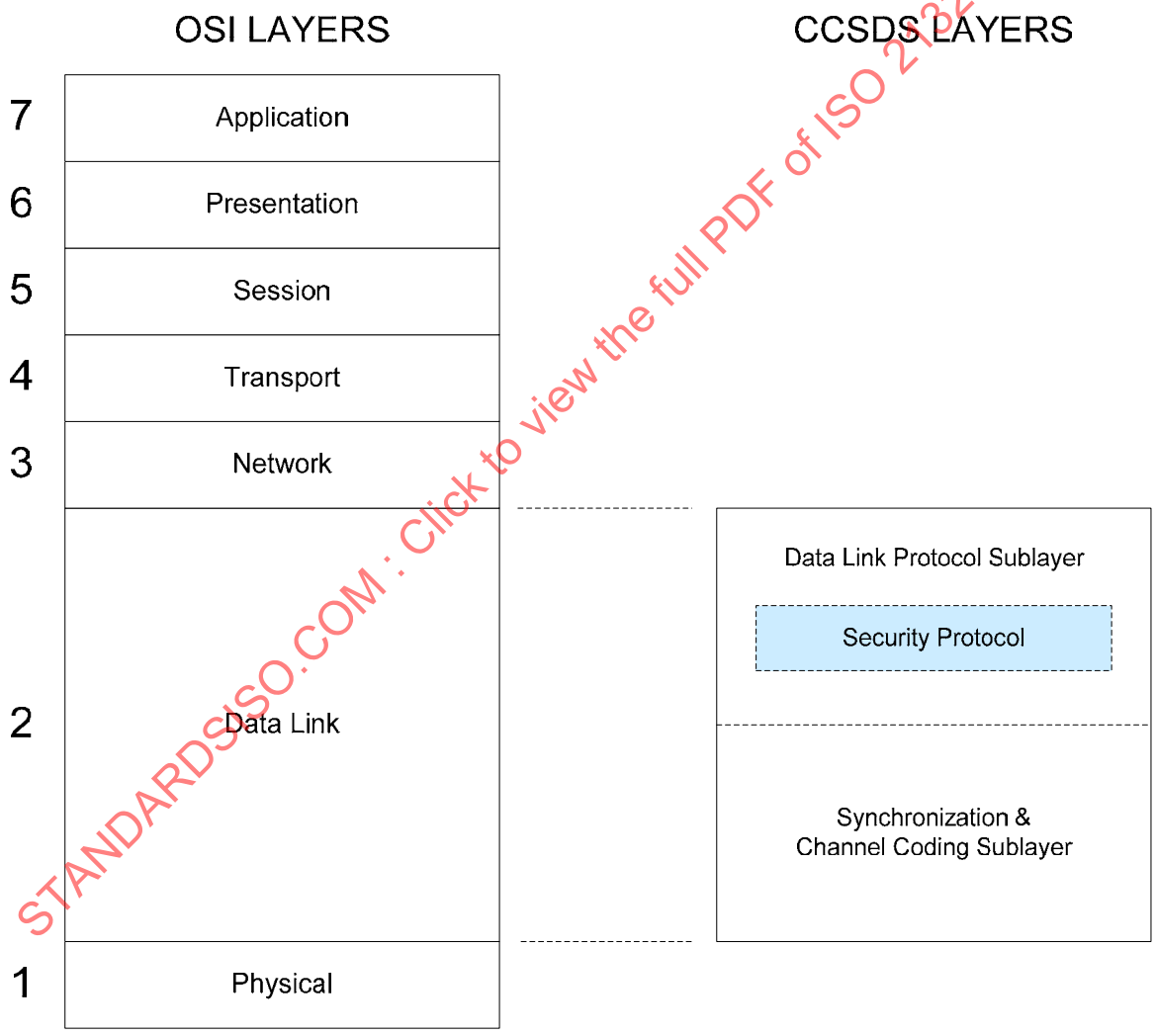

Figure 2-1: Security Protocol within OSI Model

2.2 FEATURES OF SECURITY PROTOCOL

2.2.1 GENERAL

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 related 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 reduces the maximum size of the Transfer Frame Data Field allowed by the underlying Space Data Link Protocol.

The Security Protocol preserves the quality of service that is provided by the Space Data Link Protocol. The Security Protocol is scalable to operate across any number of Virtual Channels supported by the Space Data Link Protocols. The use and sizes of a Security Header and a Security Trailer for a given Global Virtual Channel or Global Multiplexer Access Point are managed parameters which remain constant for a given mission.

2.2.2 DATA LINK LAYER PROTOCOLS

Two sublayers of the Data Link Layer are defined for CCSDS space link protocols as shown in reference [D4]. 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.

Figure 2-2 shows a simplified representation of Space Data Link Protocol frames and the effect of the Security Protocol's inserting header and optional trailer fields to surround the frame data supplied by higher layers. The detailed structure of the TM, TC, and AOS Transfer Frames with the Security Protocol is given in references [1], [2], and [3], respectively, and repeated below in figures 5-1, 5-2, and 5-3 for reference.

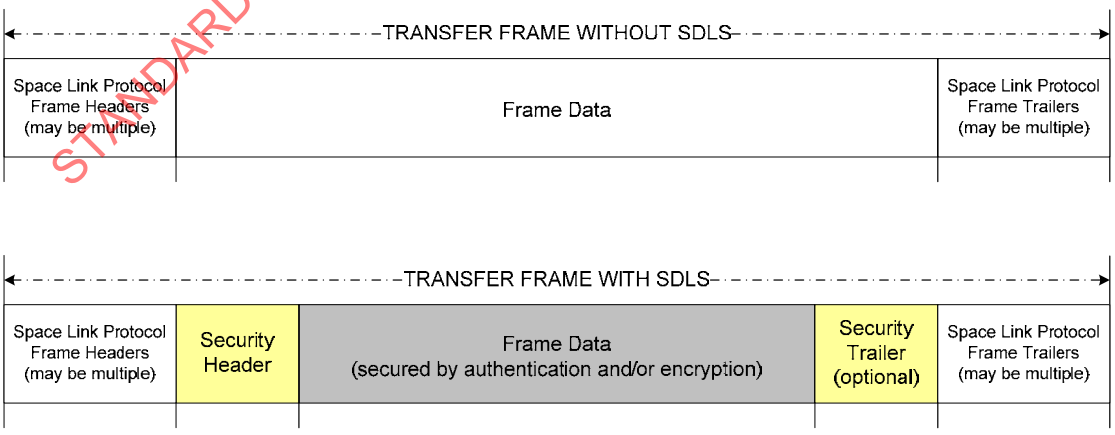

Figure 2-2: Security Protocol Interaction with Space Link Frames

2.2.3 SECURITY SERVICE FOR TM

The relationship of the Security Protocol's functions to the TM Protocol is shown in figure 2-3. The figure shows the sending end of a physical channel.

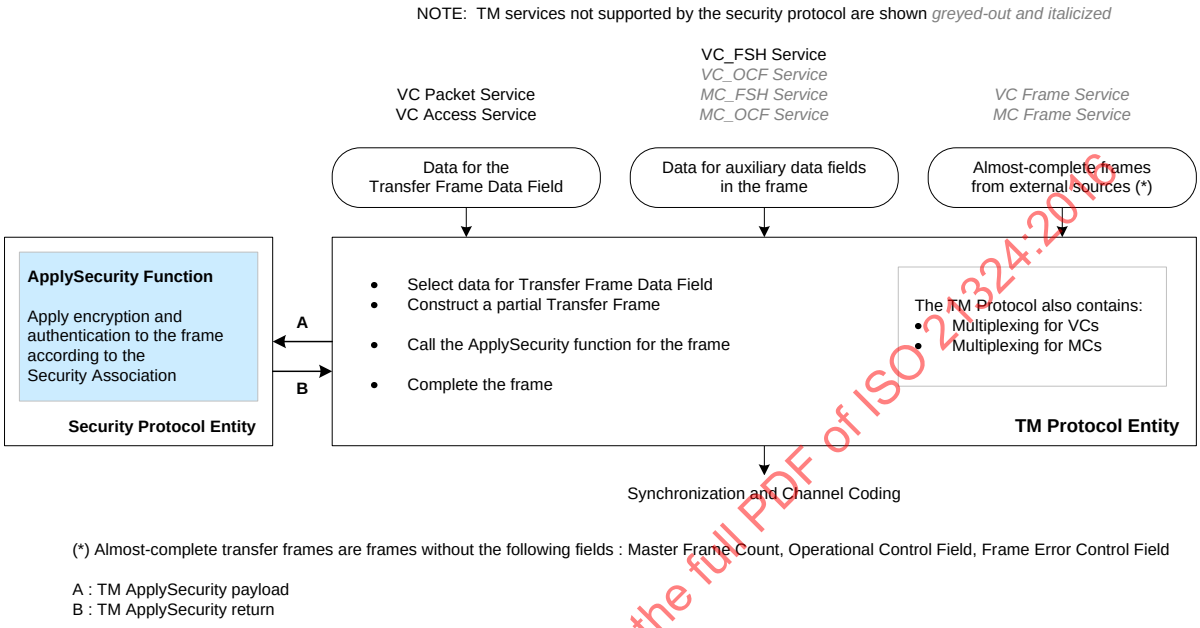

Figure 2-3: Security Protocol Support for TM Services

The Security Protocol provides all its functions (authentication, encryption, and authenticated encryption) for the data in the Transfer Frame Data Field of a TM Transfer Frame. It therefore provides full protection for the service data of the following TM Services: the Virtual Channel Packet (VCP) Service and the Virtual Channel Access (VCA) Service.

The Security Protocol provides authentication for some fields in the Transfer Frame Primary Header and for some auxiliary data fields in a TM Transfer Frame. It does not provide encryption for these fields. The Security Protocol can provide authentication protection for the service data of the Virtual Channel Frame Secondary Header (VC_FSH) Service.

The Security Protocol provides no protection for data of the other TM Services that use auxiliary data fields in a TM Transfer Frame: the Virtual Channel Operational Control Field (VC_OCF) Service, the Master Channel Frame Secondary Header (MC_FSH) Service, and the Master Channel Operational Control Field (MC_OCF) Service. The Security Protocol also provides no protection for the frames supplied to the TM Protocol by external sources on the following services: the Virtual Channel Frame (VC Frame) Service and the Master Channel Frame (MC Frame) Service.

2.2.4 SECURITY SERVICE FOR TC

The relationship of the Security Protocol's functions to the TC Protocol is shown in figure 2-4. The figure shows the sending end of a physical channel.

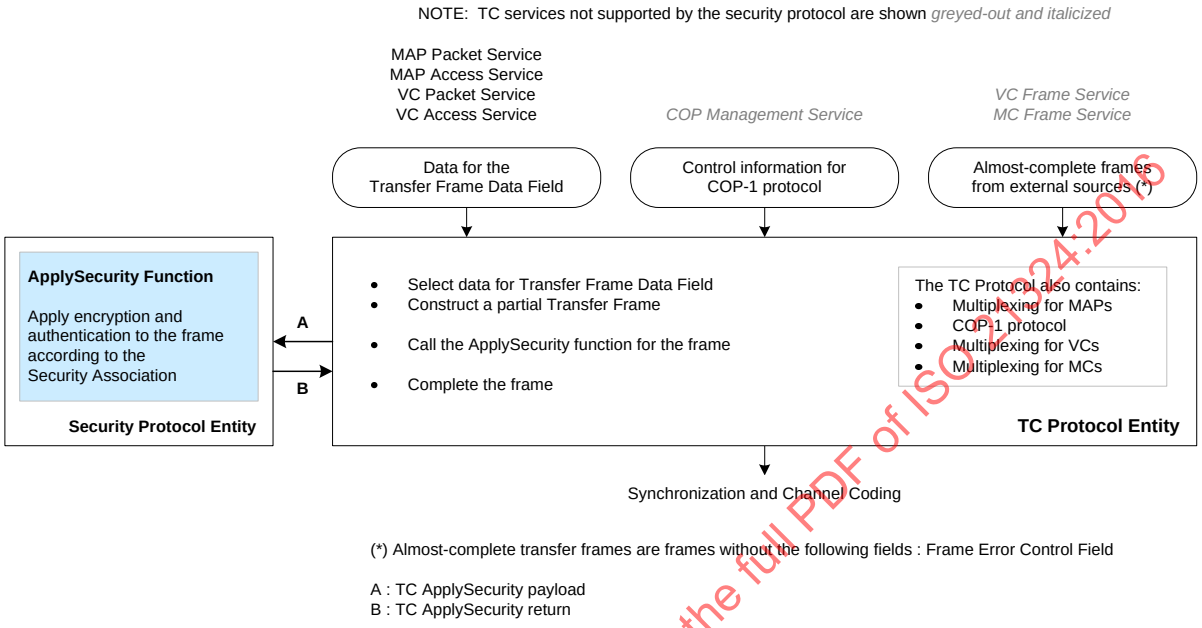

Figure 2-4: Security Protocol Support for TC Services

The Security Protocol provides all its functions (authentication, encryption, and authenticated encryption) for the data in the Transfer Frame Data Field of a TC Transfer Frame. It therefore provides full protection for the service data of the following TC Services: the MAP (Multiplexer Access Point) Packet Service, the MAP Access Service, the Virtual Channel Packet (VCP) Service, and the Virtual Channel Access (VCA) Service.

The Security Protocol provides authentication for some fields in the Transfer Frame Primary Header in a TC Transfer Frame. It does not provide encryption for these fields.

There are no auxiliary data fields in a TC Transfer Frame. The Security Protocol provides no protection for the control frames generated for the COP (Communications Operation Procedure) Management Service. The Security Protocol also provides no protection for the frames supplied to the TC Protocol by external sources on the following services: the Virtual Channel Frame (VC Frame) Service and the Master Channel Frame (MC Frame) Service.

2.2.5 SECURITY SERVICE FOR AOS

The relationship of the Security Protocol's functions to the AOS Protocol is shown in figure 2-5. The figure shows the sending end of a physical channel.

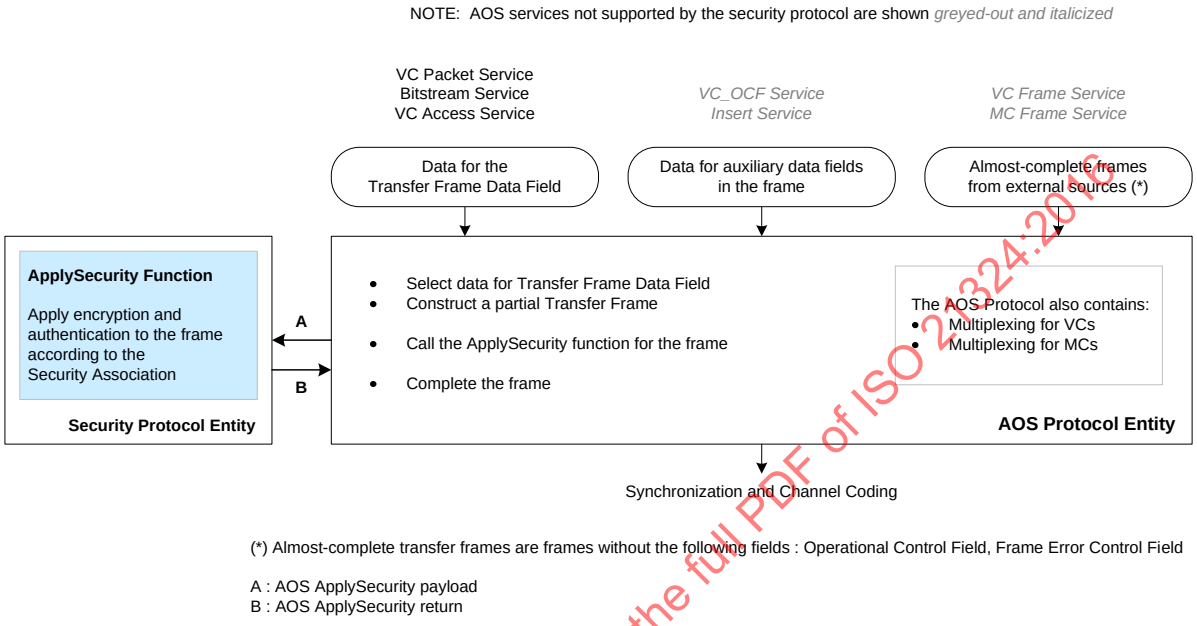

Figure 2-5: Security Protocol Support for AOS Services

The Security Protocol provides all its functions (authentication, encryption, and authenticated encryption) for the data in the Transfer Frame Data Field of an AOS Transfer Frame. It therefore provides full protection for the service data of the following AOS Services: the Virtual Channel Packet (VCP) Service, the Bitstream Service, and the Virtual Channel Access (VCA) Service.

The Security Protocol provides authentication for some fields in the Transfer Frame Primary Header in an AOS Transfer Frame. It does not provide encryption for these fields.

The Security Protocol provides no protection for data of the AOS Services that use auxiliary data fields in an AOS Transfer Frame: the Virtual Channel Operational Control Field (VC_OCF) Service and the Insert Service. The Security Protocol also provides no protection for the frames supplied to the AOS Protocol by external sources on the following services: the Virtual Channel Frame (VC Frame) Service and the Master Channel Frame (MC Frame) Service.

2.3 SERVICE FUNCTIONS

2.3.1 SECURITY ASSOCIATIONS

2.3.1.1 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.

2.3.1.2 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.

2.3.1.3 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:

a) authentication;

b) encryption;

c) 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.

2.3.1.4 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 block padding used (where necessary); the Security Trailer carries a Message Authentication Code (MAC).

The detailed structure of the TM, TC, and AOS Transfer Frames with the Security Protocol is given in references [1], [2], and [3], respectively, and repeated below in figures 5-1, 5-2, and 5-3 for reference.

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.

2.3.1.5 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.

2.3.2 AUTHENTICATION

2.3.2.1 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.

2.3.2.2 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 fields always included for MAC computation are the Virtual Channel ID, Segment Header (TC only), Security Header (except for the Initialization Vector), 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.

2.3.2.3 Replay Protection

2.3.2.3.1 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:

a) a sequence number value (current value for the sender, expected value for the receiver);

b) a sequence number window for comparison by the receiver;

c) the location within the Transfer Frame of the sequence number.

2.3.2.3.2 Sequence Number

The sender increments its managed sequence number by one with each transmitted frame belonging to that SA. With each valid received frame belonging to that SA, the receiver will replace its stored sequence number with the received value on the condition that the received sequence number is higher than the stored sequence number. Additionally, if the received Sequence Number differs from the expected value by more than a defined positive value called the Sequence Number 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. Possible interpretations and problems linked with this rollover are discussed in reference [D3].

2.3.2.3.3 Sequence Number Window

The sequence number window is a fixed positive 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 is discarded. The size of the selected window accounts for predicted delays and gaps in RF transmission.

2.3.2.3.4 Sequence Number Location

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

a) The Sequence Number can be located in the Sequence Number field of the Security Header. In this case, its length is a managed SA parameter.

b) For systems that implement authenticated encryption using a simple incrementing counter as an initialization vector (i.e., as in counter-mode cryptographic algorithms), the Initialization Vector field of the Security Header can serve also as the Sequence Number. In this case, the Sequence Number field in the Security Header is zero octets in length.

2.3.3 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 is often used as an input to the encryption process. Depending upon the cryptographic algorithm and mode used, additional fill data may be needed to pad any undersized blocks.

NOTE – Encryption used without authentication can 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 and risk analysis.

2.3.4 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.

3 SERVICE DEFINITION

3.1 OVERVIEW

This section provides the service definition for the Security Protocol.

The services that the Security Protocol provides to the Space Data Link Protocols are defined as functions. The ApplySecurity Function is defined for the sending end of a physical channel and the ProcessSecurity Function is defined for the receiving end. The definitions of the functions are independent of specific implementation approaches.

The parameters of the functions are specified in an abstract sense and specify the information passed in either direction between the Space Data Link Protocol entity that calls the function and the Security Protocol entity that executes the function. 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 on the function interface (e.g., parameters for controlling the service, monitoring performance, facilitating diagnosis, and so on).

This section also defines the Security Association Management Service.

3.2 FUNCTION AT THE SENDING END

3.2.1 OVERVIEW

The ApplySecurity Function is defined for the sending end of a physical channel. The function processes a Transfer Frame to apply security features to the frame. The Transfer Frame is a protocol (TM, TC, or AOS) data structure that is in use on the physical channel.

The input parameters of the function include the ApplySecurity Payload, containing the partially formatted frame, and the identifiers of the Virtual Channel and the MAP channel (for TC only). When the function is called, the Security Protocol applies encryption and/or authentication to the data supplied in the ApplySecurity Payload. In any given call to the ApplySecurity Function, the processing depends on the settings for the Security Association of the applicable Virtual Channel or MAP.

When the ApplySecurity Function has completed the processing, it returns the resulting data to the caller in the return parameter, the ApplySecurity Return.

3.2.2 INPUT PARAMETERS

3.2.2.1 Discussion—ApplySecurity Payload

The ApplySecurity Function applies security processing to a partially formatted Transfer Frame of the Space Data Link Protocol used on the physical channel.

The input parameter provided by the Space Data Link Protocol consists of an ApplySecurity Payload, which is one of the following types:

a) TM ApplySecurity Payload;

b) TC ApplySecurity Payload;

c) AOS ApplySecurity Payload.

3.2.2.2 TM ApplySecurity Payload

The TM ApplySecurity Payload shall consist of the portion of the TM Transfer Frame (see reference [1]) from the first octet of the Transfer Frame Primary Header to the last octet of the Transfer Frame Data Field.

NOTES

1 The TM Transfer Frame is the fixed-length protocol data unit of the TM Space Data Link Protocol. The length of any Transfer Frame transferred on a physical channel is constant, and is established by management.

2 The portion of the TM Transfer Frame contained in the TM ApplySecurity Payload parameter includes the Security Header field. When the ApplySecurity Function is called, the Security Header field is empty; i.e., the caller has not set any values in the Security Header.

3.2.2.3 TC ApplySecurity Payload

The TC ApplySecurity Payload shall consist of the portion of the TC Transfer Frame (see reference [2]) from the first octet of the Transfer Frame Primary Header to the last octet of the Transfer Frame Data Field.

NOTES

1 The TC Transfer Frame is the variable-length protocol data unit of the TC Space Data Link Protocol.

2 The portion of the TC Transfer Frame contained in the TC ApplySecurity Payload parameter includes the Security Header field. When the ApplySecurity Function is called, the Security Header field is empty; i.e., the caller has not set any values in the Security Header.

3.2.2.4 AOS ApplySecurity Payload

The AOS ApplySecurity Payload shall consist of the portion of the AOS Transfer Frame (see reference [3]) from the first octet of the Transfer Frame Primary Header to the last octet of the Transfer Frame Data Field.

NOTES

1 The AOS Transfer Frame is the fixed-length protocol data unit of the AOS Space Data Link Protocol. The length of any Transfer Frame transferred on a physical channel is constant, and is established by management.

2 The portion of the AOS Transfer Frame contained in the AOS ApplySecurity Payload parameter includes the Security Header field. When the ApplySecurity Function is called, the Security Header field is empty; i.e., the caller has not set any values in the Security Header.

3.2.2.5 GLOBAL VIRTUAL CHANNEL (GVCID) ID

The GVCID parameter shall contain the ID of the Global Virtual Channel (see references [1]–[3]) of the partially formatted Transfer Frame contained in the ApplySecurity Payload.

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

3.2.2.6 GLOBAL MULTIPLEXER ACCESS POINT (GMAP) ID

The GMAP_ID parameter shall contain the ID of the Global Multiplexer Access Point (see reference [2]) of the partially formatted TC Transfer Frame contained in the TC ApplySecurity Payload.

NOTES

1 The GMAP_ID consists of a GVCID and a TC MAP ID that indicates a MAP Channel within the Virtual Channel specified by GVCID.

2 The GMAP_ID is applicable only if the ApplySecurity Payload is a TC ApplySecurity Payload and the Virtual Channel specified by the GVCID is using Segment Headers.

3.2.3 RETURN PARAMETER—ApplySecurity Return

The ApplySecurity Return shall consist of the portion of the Transfer Frame starting at the first octet of the Security Header and ending at the last octet of the Security Trailer, if present, or the last octet of the Transfer Frame Data Field, if the Security Trailer is not present.

NOTE – When the ApplySecurity function has completed the processing for the frame that was input in the ApplySecurity Payload parameter, it returns part of the processed frame in the ApplySecurity Return parameter.

3.3 FUNCTION AT THE RECEIVING END

3.3.1 OVERVIEW

The ProcessSecurity Function is defined for the receiving end of a physical channel. The function provides the receiving end security processing for a Transfer Frame belonging to the underlying protocol (TM, TC, or AOS) that is in use on the physical channel.

The input parameters include the ProcessSecurity Payload, containing the frame, and the identifiers of the Virtual Channel and the MAP channel (TC only). When the function is called, the Security Protocol always applies verification and may apply decryption to the data supplied in the ProcessSecurity Payload. In any given call to the ProcessSecurity Function, the processing depends on the settings for the Security Association of the applicable Virtual Channel or MAP.

When the ProcessSecurity Function has completed the processing, it returns the results to the caller in the return parameters, which include status indicators and the ProcessSecurity Return.

3.3.2 INPUT PARAMETERS

3.3.2.1 Discussion—ProcessSecurity Payload

The ProcessSecurity Function applies security processing to a Transfer Frame of the Space Data Link Protocol used on the physical channel.

The input parameter provided by the Space Data Link Protocol consists of a ProcessSecurity Payload, which is one of the following types:

a) TM ProcessSecurity Payload;

b) TC ProcessSecurity Payload;

c) AOS ProcessSecurity Payload.

3.3.2.2 TM ProcessSecurity Payload

The TM ProcessSecurity Payload shall consist of the portion of the TM Transfer Frame (see reference [1]) from the first octet of the Transfer Frame Primary Header to the last octet of the Security Trailer, if present, or the last octet of the Transfer Frame Data Field, if the Security Trailer is not present.

NOTE – The TM Transfer Frame is the fixed-length protocol data unit of the TM Space Data Link Protocol. The length is constrained by the TM Synchronization and Channel Coding Blue Book (reference [D6]). The length of any Transfer Frame transferred on a physical channel is constant, and is established by management.

3.3.2.3 TC ProcessSecurity Payload

The TC ProcessSecurity Payload shall consist of the portion of the TC Transfer Frame (see reference [2]) from the first octet of the Transfer Frame Primary Header to the last octet of the Security Trailer, if present, or the last octet of the Transfer Frame Data Field, if the Security Trailer is not present.

NOTE – The TC Transfer Frame is the variable-length protocol data unit of the TC Space Data Link Protocol.

3.3.2.4 AOS ProcessSecurity Payload

The AOS ProcessSecurity Payload shall consist of the portion of the AOS Transfer Frame (see reference [3]) from the first octet of the Transfer Frame Primary Header to the last octet of the Security Trailer, if present, or the last octet of the Transfer Frame Data Field, if the Security Trailer is not present.

NOTE – The AOS Transfer Frame is the fixed-length protocol data unit of the AOS Space Data Link Protocol. The length is constrained by the TM Synchronization and Channel Coding Blue Book (reference [D6]). The length of any Transfer Frame transferred on a physical channel is constant, and is established by management.

3.3.2.5 GVCID

The GVCID parameter shall contain the ID of the Global Virtual Channel (see references [1]–[3]) of the partial Transfer Frame contained in the ProcessSecurity Payload.

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

3.3.2.6 GMAP ID

The GMAP_ID parameter shall contain the ID of the Global Multiplexer Access Point (see reference [2]) of the partial TC Transfer Frame contained in the TC ProcessSecurity Payload.

NOTES

1 The GMAP_ID consists of a GVCID and a TC MAP ID that indicates a MAP Channel within the Virtual Channel specified by GVCID.

2 The GMAP_ID is applicable only if the ProcessSecurity Payload is a TC ProcessSecurity Payload and the Virtual Channel specified by the GVCID is using Segment Headers.

3.3.3 RETURN PARAMETERS

3.3.3.1 Verification Status

The Verification Status parameter supplied by the Security Protocol shall indicate one of the following:

– no failures were detected; or

– the ProcessSecurity function has detected a failure.

NOTE – In addition to authentication failures, the ProcessSecurity function can detect additional failures such as an invalid Security Association identification in the Security Header. If no failure was detected, then the ProcessSecurity function has performed successful authentication or the SA does not include authentication.

3.3.3.2 Verification Status Code

If the Verification Status parameter indicates a failure, then the Verification Status Code parameter shall contain a status code to indicate the type of failure. At a minimum, the following failure conditions shall be supported:

– no failure;

– invalid Security Parameter Index (SPI);

– MAC verification failure;

– anti-replay sequence number failure;

– padding error.

3.3.3.3 ProcessSecurity Return

The ProcessSecurity Return shall consist of the portion of the Transfer Frame corresponding to the ProcessSecurity Payload, starting at the first octet following the Security Header and ending at the last octet of the Transfer Frame Data Field.

NOTES

1 When the ProcessSecurity function has finished processing the frame that was input in the ProcessSecurity Payload parameter, it returns part of the processed frame in the ProcessSecurity Return parameter. If the function has performed decryption then the ProcessSecurity Return contains the decrypted data.

2 If the SA does not include encryption then the ProcessSecurity function does not perform decryption. Also, the ProcessSecurity function does not perform decryption following a verification failure.

3.4 SECURITY ASSOCIATION MANAGEMENT SERVICE

3.4.1 OVERVIEW

The Security Association Management Service establishes the context of an SA for a particular Global Virtual Channel and/or MAP ID. This Recommended Standard specifies only the service parameters contained in the Security Association data base. Implementation of the services necessary to manage the parameters contained in the SA data base is a mission-specific function. Service directives for managing the SA parameters in-line are specified in the CCSDS SDLS Extended Procedures Recommended Standard (reference [D14]). At the time of publication of this document, the SDLS Extended Procedures book is still under development.

3.4.2 SA MANAGEMENT SERVICE PARAMETERS

3.4.2.1 Overview

Each SA is composed of the commonly applicable parameters listed in 3.4.2.2 below, as well as those parameters in 3.4.2.3 and 3.4.2.4 applicable to the cryptographic function(s) specified in the SA.

3.4.2.2 Security Association Parameters required by all SAs

3.4.2.2.1 Global Virtual Channel ID

The Global Virtual Channel ID (GVCID) parameter shall contain the ID of the Global Virtual Channel(s) (see references [1]–[3]) applicable to the SA.

NOTE – The GVCID consists of a Master Channel ID and a Virtual Channel ID. If the TC Space Data Link Protocol is used on the physical channel, a single Global Virtual Channel is applicable to the SA (see requirement 5.2 c)).

3.4.2.2.2 Global Multiplexer Access Point ID

The Global Multiplexer Access Point ID (GMAP_ID) parameter shall contain the ID of the Global Multiplexer Access Point(s) (see reference [2]) applicable to the SA.

NOTE – The GMAP_ID consists of a GVCID and a TC MAP ID that indicates a MAP Channel within the Virtual Channel specified by GVCID. The GMAP_ID is applicable only if the TC Space Data Link Protocol is used on the physical channel and Segment Headers are used on the TC Virtual Channel. In all other cases it is not applicable.

3.4.2.2.3 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.

3.4.2.2.4 SA_service_type

The SA_service_type parameter shall indicate the cryptographic function(s) specified for the SA: one of authentication, encryption, or authenticated encryption.

3.4.2.2.5 SA_length_SN

The SA_length_SN parameter shall indicate the length of the Sequence Number field in the Security Header.

3.4.2.2.6 SA_length_IV

The SA_length_IV parameter shall indicate the length of the Initialization Vector field in the Security Header.

3.4.2.2.7 SA_length_PL

The SA_length_PL parameter shall indicate the length of the Pad Length field in the Security Header.

3.4.2.2.8 SA_length_MAC

The SA_length_MAC parameter shall indicate the length of the MAC field in the Security Trailer.

3.4.2.3 Security Association Parameters Specific to Authentication

NOTE – The parameters under this subsection are applicable only if the SA_service_type parameter is Authentication or Authenticated Encryption.

3.4.2.3.1 SA_authentication_algorithm

The SA_authentication_algorithm parameter shall indicate the applicable authentication algorithm and mode of operation.

3.4.2.3.2 SA_authentication_key

The SA_authentication_key parameter shall indicate the value of a provided authentication key, or of an index that refers to the actual key.

3.4.2.3.3 SA_authentication_mask

The SA_authentication_mask parameter shall indicate the value of a provided bit mask that is applied against the Transfer Frame in a bitwise-AND operation to generate an Authentication Payload.

3.4.2.3.4 SA_sequence_number

The SA_sequence_number parameter shall indicate the present value of a managed anti-replay sequence number.

3.4.2.3.5 SA_sequence_window

The SA_sequence_window parameter shall indicate the amount of deviation the receiving end will accept between the expected anti-replay sequence number and the sequence number in the received frame.

3.4.2.4 Security Association Parameters Specific to Encryption

NOTE – The parameters under this subsection are applicable only if the SA_service_type parameter is Encryption or Authenticated Encryption.

3.4.2.4.1 SA_encryption_algorithm

The SA_encryption_algorithm parameter shall indicate the applicable encryption algorithm and mode of operation.

3.4.2.4.2 SA_encryption_key

The SA_encryption_key parameter shall indicate the value of a provided encryption key, or of an index that refers to the actual key.

3.4.2.4.3 SA_initialization_vector

The SA_initialization_vector parameter shall indicate the present value of a managed initialization vector.

3.4.3 DISCUSSION—SA MANAGEMENT SERVICE PRIMITIVES

This Recommended Standard specifies only the service parameters contained in the Security Association data base and does not define specific management services or data structures for implementation. Service directives for managing the SA parameters in-line are specified in the CCSDS SDLS Extended Procedures Recommended Standard (reference [D14]). At the time of publication of this document, the SDLS Extended Procedures book is still under development.

4 PROTOCOL SPECIFICATION

4.1 PROTOCOL DATA UNITS

4.1.1 SECURITY HEADER

4.1.1.1 General

4.1.1.1.1 The presence or absence of a Security Header on a Virtual Channel or MAP shall remain constant throughout a mission.

4.1.1.1.2 The Security Header is mandatory on a Virtual Channel or MAP whenever authentication, encryption, or authenticated encryption is applied on that Virtual Channel or MAP.

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

a) Security Parameter Index (16 bits; mandatory);

b) Initialization Vector (octet-aligned, fixed-length for the duration of the SA; optional);

c) Sequence Number (octet-aligned, fixed-length for the duration of the SA; optional);

d) Pad Length (octet-aligned, fixed-length for the duration of the SA; optional).

4.1.1.1.4 A Security Header shall consist of less than or equal to 64 octets.

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.

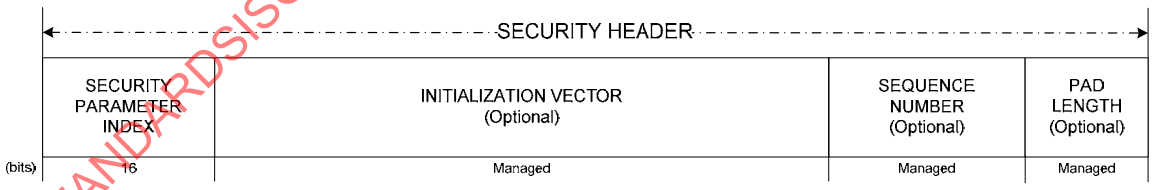

Figure 4-1: Security Header

4.1.1.2 Security Parameter Index

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

4.1.1.2.2 The SPI shall be used as an index to identify an SA.

4.1.1.2.3 The values of ‘all zeros’ (0) and ‘all ones’ (65535) for this field are reserved by CCSDS for future use.

4.1.1.3 Initialization Vector

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

4.1.1.3.2 The Initialization Vector field shall contain the initialization vector, or an agreed-upon portion of it, consisting of an integral number of octets.

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

4.1.1.3.4 If an initialization vector is not required for an SA, the Initialization Vector field shall be zero octets in length.

4.1.1.4 Sequence Number

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

4.1.1.4.2 The Sequence Number 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 counter-mode cryptographic 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.

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

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

4.1.1.5 Pad Length

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

4.1.1.5.2 The Pad Length field shall contain the count of fill bytes used in the cryptographic process, consisting of an integral number of octets.

4.1.1.5.3 If padding is not required for an SA, the Pad Length field shall be zero octets in length.

4.1.2 SECURITY TRAILER

4.1.2.1 The presence or absence of a Security Trailer on a Virtual Channel or MAP shall remain constant throughout a mission.

4.1.2.2 The Security Trailer shall be present on a Virtual Channel or MAP whenever authentication or authenticated encryption is applied on that Virtual Channel.

4.1.2.3 The Security Trailer, if present, shall consist of a MAC (octet-aligned, fixed-length for the duration of the SA).

NOTES

1 The length of the Security Trailer is a Managed Parameter (see section 6).

2 This field may be present and unused where it is envisioned that the service user may switch between using authenticated SA(s) and not using them on a given Virtual Channel (e.g., if a 'clear mode' SA is supported). In this scenario, it may be preferable to keep the field lengths constant across all supported operational configurations.

3 The format of the Security Trailer is shown in figure 4-2.

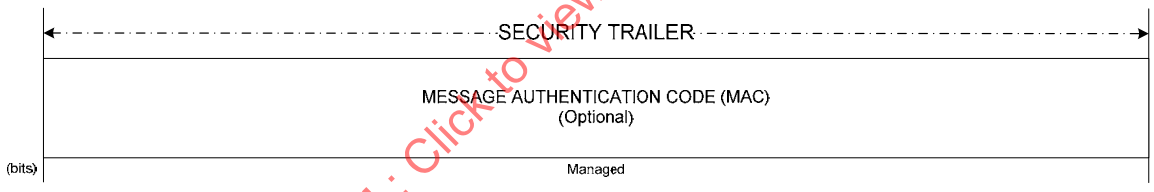

Figure 4-2: Security Trailer

4.2 SECURITY PROTOCOL PROCEDURES

4.2.1 GENERAL

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

4.2.1.2 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.

4.2.1.3 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.

4.2.2 SECURITY ASSOCIATION MANAGEMENT PROCEDURES

4.2.2.1 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:

a) create the SA;

b) associate it with cryptographic key(s); and

c) 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.

4.2.2.2 Security Association Context

4.2.2.2.1 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 physical channel and Segment Headers are used on the TC Virtual Channel. In all other cases it is invalid.

4.2.2.2.2 SA Uniqueness on Virtual Channels and MAPs

At the sending end, only one SA at a time shall be used (i.e., ‘active’) for transferring frames over a particular Global Virtual Channel or Global MAP ID.

4.2.2.2.3 Idle Transfer Frame Virtual Channels

SAs shall not be created for use with Virtual Channels carrying Only Idle Data (OID) Transfer Frames as defined in references [1] and [3]).

4.2.2.3 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.

4.2.2.4 Security Association Service Type

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

a) authentication;

b) encryption;

c) 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. In this scenario, the Security Header and Trailer field lengths are kept constant across all supported configurations. For security reasons, the use of such an SA is not recommended in normal operation.

4.2.2.5 Parameters Common to All SAs

Every SA shall specify the following:

a) SPI;

b) length of Initialization Vector field in Security Header;

c) length of Sequence Number field in Security Header;

d) length of Pad Length field in Security Header;

e) length of MAC field in Security Trailer.

4.2.2.6 Parameters for Authentication SAs

4.2.2.6.1 General

Every SA providing authentication shall specify the following:

a) authentication algorithm and mode of operation;

b) authentication bit mask;

c) managed anti-replay sequence number;

d) managed sequence number window.

4.2.2.6.2 Authentication Bit Mask

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

a) the mask to be applied shall be greater or 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;

NOTE – For variable length TC Transfer Frames, accounting for the largest expected frame data field will result in a mask suitable for all Transfer Frames.

b) the mask bits corresponding to the Virtual Channel ID field of the Transfer Frame Primary Header shall contain ‘all ones’;

c) (TM only) the mask bits corresponding to the Master Channel Frame Count field of the Transfer Frame Primary Header shall contain ‘all zeros’ (i.e., the field shall be ***excluded*** from the authenticated data);

d) (TC only) the mask bits corresponding to the Segment Header shall contain ‘all ones’;

e) (AOS only) the mask bits corresponding to the Insert Zone shall contain ‘all zeros’ (i.e., the field shall be ***excluded*** from the authenticated data);

f) the mask bits corresponding to the Security Header, except for the mask bits corresponding to the Initialization Vector field, shall contain ‘all ones’;

g) the mask bits corresponding to the Frame Data Field shall contain ‘all ones’;

h) the mask bits corresponding to all other Transfer Frame header fields should contain ‘all zeros’, unless otherwise specified according to mission requirements.

NOTE

1 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 h) above. Possible security concerns affecting the selection of an authentication mask are discussed in reference [D3].

2 If the Master (not Virtual) Channel Frame Secondary Header Service (TM only) is used, the TM Frame Secondary Header is excluded from the authenticated data.

4.2.2.7 Parameters for Encryption SAs

Every SA providing encryption shall specify the following:

a) encryption algorithm and mode of operation;

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

b) managed initialization vector.

4.2.2.8 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.

4.2.3 SENDING PROCEDURES

4.2.3.1 Overview

This subsection describes procedures at the sending end when a Space Data Link Protocol entity calls the ApplySecurity function for a frame as shown in figures 2-3, 2-4, and 2-5. (See 3.2 for the definition of the interface for the ApplySecurity function.)

4.2.3.2 General

4.2.3.2.1 When the ApplySecurity function is called, the function shall use the GVCID parameter, and the GMAP ID parameter if applicable, to determine the Security Association that applies to the frame.

4.2.3.2.2 The actions of the ApplySecurity function shall depend on the Security Type of the Security Association as follows:

4.2.3.2.2.1 When the Security Type is encryption:

a) the encryption operations specified in 4.2.3.3 shall be applied to the partial frame contained in the ApplySecurity Payload parameter;

b) the Security Header shall be completed;

c) the Security Header and the encrypted Transfer Frame Data Field shall be returned in the ApplySecurity Return parameter.

4.2.3.2.2.2 When the Security Type is authentication:

a) the authentication operations specified in 4.2.3.4 shall be applied to the partial frame contained in the ApplySecurity Payload parameter;

b) the Security Header, the unencrypted Transfer Frame Data Field, and the Security Trailer shall be returned in the ApplySecurity Return parameter.

4.2.3.2.2.3 When the Security Type is authenticated encryption:

a) If the cryptographic algorithm requires both plaintext and Additional Authenticated Data (AAD) as separate inputs, then:

   1) the plaintext shall be the Transfer Frame Data Field, and

   2) the AAD shall be the portion from the first octet of the Authentication Payload to the octet immediately preceding the Transfer Frame Data Field;

   NOTE – This definitional distinction is common to a class of cryptographic algorithms known as 'Authenticated Encryption with Associated Data' (AEAD) algorithms.

b) the encryption operations specified in 4.2.3.3 shall be applied to the partial frame contained in the ApplySecurity Payload parameter;

c) the authentication operations specified in 4.2.3.4 shall be applied to the partial frame resulting from the encryption operations;

d) the Security Header, the encrypted Transfer Frame Data Field, and the Security Trailer shall be returned in the ApplySecurity Return parameter.

4.2.3.3 Encryption Operations

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

a) encrypt the Transfer Frame Data Field;

b) if the algorithm and mode selected for the SA require the use of fill padding, place the number of fill bytes used into the Pad Length field of the Security Header.

4.2.3.4 Authentication Operations

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

a) increment the SA's managed sequence number by one;

b) place the managed sequence number in the Sequence Number field of the Security Header, unless that SA specifies use of the Initialization Vector field of the Security Header instead;

NOTE – The interpretation of a sequence number rollover (to zero) is mission-specific. Possible interpretations and problems linked with this rollover are discussed in reference [D3].

c) complete the Security Header as specified in 4.1.1;

d) apply the SA's authentication bit mask in a bitwise-AND operation against the partial frame, thus resulting in the Authentication Payload;

NOTE – The partial frame supplied in the ApplySecurity Payload consists of the portion from the start of the Transfer Frame Primary Header to the end of the Transfer Frame Data Field. The result is used for the masking operation.

e) compute a MAC over the Authentication Payload;

f) (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;

g) place the computed MAC in the Security Trailer;

h) if the algorithm and mode selected for the SA require the use of fill padding, place the number of fill bytes used into the Pad Length field of the Security Header.

4.2.4 RECEIVING PROCEDURES

4.2.4.1 Overview

This subsection describes procedures at the receiving end when a Space Data Link Protocol entity calls the ProcessSecurity function for a frame. (See 3.3 for the definition of the interface for the ProcessSecurity function.)

The parameters containing partial frames described in this subsection are defined in an abstract sense and are not intended to imply any particular implementation approach for the handling of frames or for the transfer of frame data between the Space Data Link Protocol entity and the Security Protocol entity.

4.2.4.2 General

4.2.4.2.1 When the ProcessSecurity function is called, the function shall verify the Security Association that applies to the frame as specified in 4.2.4.3.

4.2.4.2.2 If the verification of the Security Association fails, the ProcessSecurity function shall exit, giving an indication of the failure in the Verification Status and Verification Status Code return parameters.

4.2.4.2.3 If the verification of the Security Association succeeds, the actions of the ProcessSecurity function shall depend on the Security Type of the Security Association as follows:

4.2.4.2.3.1 When the Security Type is authentication:

a) the authentication operations specified in 4.2.4.4 shall be applied to the partial frame contained in the ProcessSecurity Payload parameter;

b) the Verification Status and Verification Status Code parameters shall be set, and the ProcessSecurity function shall exit if an authentication failure is detected;

c) the Transfer Frame Data Field in the ProcessSecurity Return parameter and a success indication in the Verification Status shall be returned, and the ProcessSecurity function shall exit if no authentication failure is detected.

4.2.4.2.3.2 When the Security Type is authenticated encryption:

a) If the cryptographic algorithm requires both plaintext and AAD as separate inputs, then:

   1) the plaintext shall be the Transfer Frame Data Field, and

   2) the AAD shall be the portion from the first octet of the Authentication Payload to the octet immediately preceding the Transfer Frame Data Field;

   NOTE – This definitional distinction is common to a class of cryptographic algorithms known as Authenticated Encryption with Associated Data (AEAD) algorithms.

b) the authentication operations specified in 4.2.4.4 shall be applied to the partial frame contained in the ProcessSecurity Payload parameter;

c) the Verification Status and Verification Status Code parameters shall be set, and the ProcessSecurity function shall exit if an authentication failure was detected;

d) the encryption operations specified in 4.2.4.5 shall be applied to the partial frame contained in the ProcessSecurity Payload parameter;

e) the decrypted Transfer Frame Data Field in the ProcessSecurity Return parameter and a success indication in the Verification Status shall be returned, and the ProcessSecurity function shall exit.

4.2.4.2.3.3 When the Security Type is encryption:

a) the encryption operations specified in 4.2.4.5 shall be applied to the partial frame contained in the ProcessSecurity Payload parameter;

b) the decrypted Transfer Frame Data Field in the ProcessSecurity Return parameter and a success indication in the Verification Status shall be returned, and the ProcessSecurity function shall exit.

4.2.4.3 Security Association Verification

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

a) 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;

b) 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.

4.2.4.4 Authentication Operations

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

a) apply the SA's authentication bit mask in a bitwise-AND operation against the portion of the partial Transfer Frame in the ProcessSecurity Payload parameter, 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, thus resulting in the Authentication Payload;

b) compute a MAC over the Authentication Payload;

c) (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;

d) verify that the computed MAC matches the MAC received in the Security Trailer;

e) 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.

f) 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;

g) compare the received sequence number to the managed sequence number;

h) report an exception to the service user for frames in which the received sequence number is lower or equal to the managed sequence number (i.e., the value stored in the receiver), and discard those frames;

i) report an exception to the service user for frames in which the received sequence number is larger than the managed sequence number by a value greater than the window defined for that SA, and discard those frames;

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

j) only upon receipt of frames that pass the verification operations a)–i) above, replace the managed sequence number with the received sequence number;

NOTE – The interpretation of a sequence number rollover (to zero) is mission-specific. Possible interpretations and problems linked with this rollover are discussed in reference [D3].

k) (optionally) if specified for that SA, extract the count of fill bytes used from the Pad Length field of the Security Header and remove those fill bytes from the Frame Data Field to be returned.

4.2.4.5 Encryption Operations

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

a) decrypt the Transfer Frame Data Field;

b) (optionally) if specified for that SA, extract the count of fill bytes used from the Pad Length field of the Security Header, and remove those fill bytes from the Frame Data Field to be returned.

5 USE OF THE SERVICES WITH CCSDS PROTOCOLS

5.1 TM PROTOCOL

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

a) 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;

b) the VC_FSH Service may be used on a Global Virtual Channel with the Authentication, Encryption, or Authenticated-Encryption Service, and may be protected by authentication but is **not** protected by encryption;

c) the VC_OCF, VC Frame, MC_FSH, 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.

NOTE – The format of the TM Transfer Frame is defined in reference [1]. The format of a TM Transfer Frame using the Security Protocol is shown in figure 5-1.

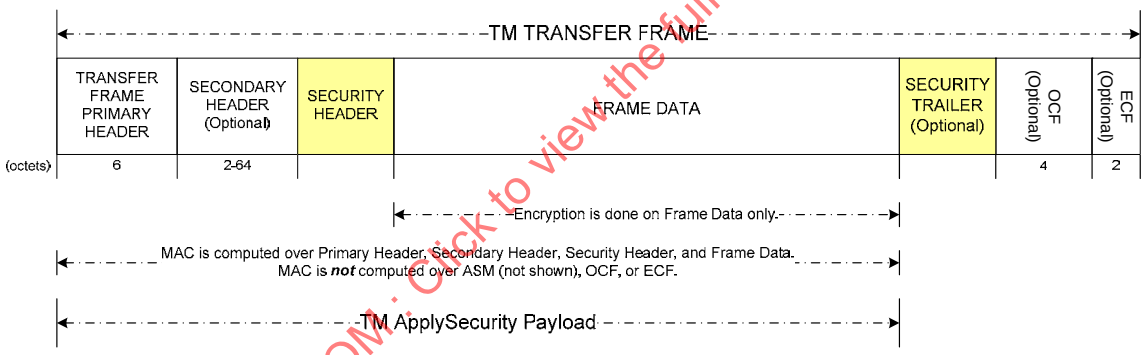

Figure 5-1: TM Transfer Frame Using the Security Protocol

5.2 TC PROTOCOL

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

a) 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;

b) 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;

c) each SA shall be associated to one VC and one VC only.

NOTE – The format of the TC Transfer Frame is defined in reference [2]. The format of a TC Transfer Frame using the Security Protocol is shown in figure 5-2.

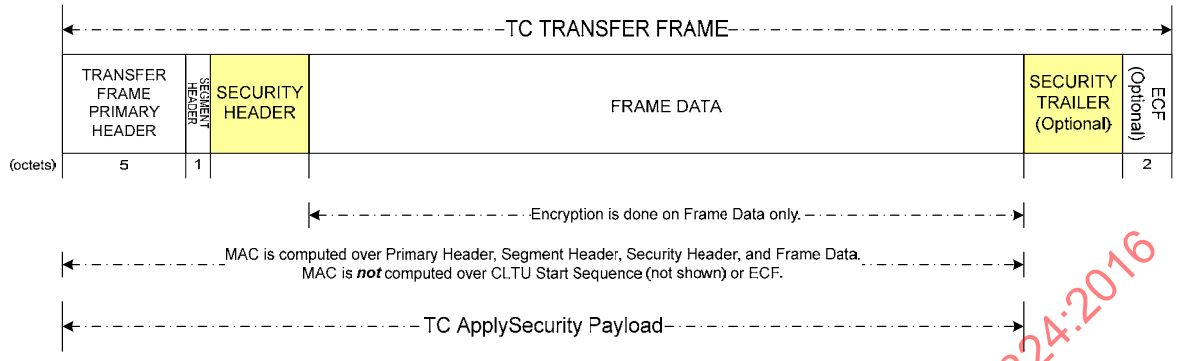

Figure 5-2: TC Transfer Frame Using the Security Protocol

5.3 AOS PROTOCOL

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

a) 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;

b) 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.

NOTE – The format of the AOS Transfer Frame is defined in reference [3]. The format of an AOS Transfer Frame using the Security Protocol is shown in figure 5-3.

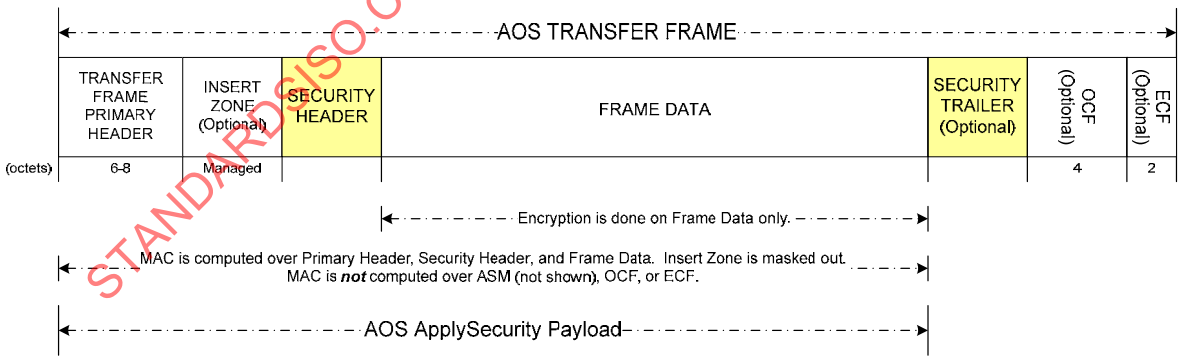

Figure 5-3: AOS Transfer Frame Using the Security Protocol

5.4 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	Not protected	Not protected	Not protected
	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

6 MANAGED PARAMETERS

6.1 OVERVIEW

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. These managed parameters are intended to be included in any service-provider system that manages Security Associations, but no specification for such a management system is provided or implied.

6.2 REQUIREMENTS

6.2.1 The managed parameters used for the Security Protocol shall be those listed in table 6-1.

NOTES

1 These parameters are defined in an abstract sense, and are not intended to imply any particular implementation of a management system.

2 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.

6.2.2 All managed parameters of the Space Data Link Protocol (see references [1], [2], and [3]) used on the physical channel shall be treated as also applicable to the Security Protocol.

Table 6-1: Managed Parameters for Security Protocol

Managed Parameter	Allowed Values	Defined In Reference
Security Association Data Base Parameters held static for 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)	Authentication Encryption Authenticated Encryption	
Security Association Context (identifies the GVCIDs or Global MAP IDs with which an SA is used)	GVCID Global MAP ID	[1], [2], [3] [2]

Managed Parameter	Allowed Values	Defined In Reference
Transmitted length of Initialization Vector (if used) (SA_length_IV)	1-32 octets	
Transmitted length of Sequence Number (if used) (SA_length_SN)	2-8 octets	
Transmitted length of Pad Length (if used) (SA_length_PL)	1-2 octets	
Transmitted length of MAC (if used) (SA_length_MAC)	8-64 octets	
Authentication algorithm	HMAC, CMAC, GMAC, DSS, RSA, GCM , Agency-specific	[4]
Authentication mask	Bit mask	
Sequence number window	Integer greater than zero (> 0)	
Encryption algorithm	AES/Counter Mode, GCM, Agency-specific	[4]
Security Association Data Base Parameters held static while the applicable SA is active on the channel:		
Authentication key	Length (in bits): Algorithm-specific Value (Binary)	
Encryption key	Length (in bits): 128, 192, 256 Value (Binary)	
Security Association Data Base Parameters that vary dynamically while the applicable SA is active on the channel:		
Sequence number (sender's next frame value, receiver's expected value).	Integer	
Encryption initialization vector (sender's current value)	Algorithm-specific	

NOTE – This table has been built taking the authentication and encryption algorithms allowed by the current version of reference [4]. As such, the allowed values for the Authentication/Encryption Algorithms and for Key Length refer to those in the current version of reference [4] and users of this document are encouraged to investigate the possibility of applying the most recent editions of that publication.

Moreover, as the protocol defined in this book is quite independent from the applied algorithms, users would still be able—if needed—to apply this protocol with other algorithms defined via bilateral agreement (out of CCSDS scope) among agencies. This is shown by the ‘Agency-Specific’ value.

7 CONFORMANCE REQUIREMENTS

An implementer of the Security Protocol shall verify conformance with this Recommended Standard by completing a Protocol Implementation Conformance Statement (PICS) based on a CCSDS-defined PICS proforma for the protocol.

NOTE – A compliant PICS proforma is provided in annex A of this document.

ANNEX A

PROTOCOL IMPLEMENTATION CONFORMANCE STATEMENT (PICS) PROFORMA

(NORMATIVE)

A1 INTRODUCTION

A1.1 OVERVIEW

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.

A1.2 CONFORMANCE TO THIS PICS PROFORMA

If it is claimed to conform to this Recommended Standard, 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 Recommended Standard shall be a conforming PICS proforma completed in accordance with the instructions for completion given in A2.

A1.3 COPYRIGHT

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

A2 INSTRUCTIONS FOR COMPLETING THE PICS PROFORMA

A2.1 OVERVIEW

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.

A2.2 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.

A2.3 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.

A2.4 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:

a) a reference to the smallest subsection enclosing the relevant item;

b) a solidus character, '/';

c) the reference number of the row in which the response appears;

d) if, and only if, more than one response occurs in the row identified by the reference number, then each possible entry is implicitly labeled 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.

A2.5 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.

A3 GENERAL INFORMATION

A3.1 REFERENCED BASE STANDARDS

The Space Data Link Security (SDLS) Protocol (this Recommended Standard) 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.

A3.2 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 [D13]). It contains a declaration of the layers of the Reference Model covered by the implementation to be tested.

A3.3 IDENTIFICATION OF THE SYSTEM SUPPLIER AND/OR TEST LABORATORY CLIENT

Organization name	
Contact name	
Address	
Telephone	
E-mail	
Other information	

A3.4 IDENTIFICATION OF THE IMPLEMENTATION UNDER TEST

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

A3.5 IDENTIFICATION OF THE PROTOCOL

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

A3.6 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)	

A4 SUPPORTED SPACE DATA LINK PROTOCOLS

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

A5 SUPPORTED SECURITY SERVICES

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

A6 SECURITY ASSOCIATION MANAGEMENT DATA

Item	Protocol Feature	Reference	Status	Support
1	GVCID	3.4.2.2.1 4.2.2.2.1	M	
2	GMAP_ID	3.4.2.2.2 4.2.2.2.1	C.1	
3	SPI	3.4.2.2.3 4.2.2.3	M	
4	SA_service_type	3.4.2.2.4 4.2.2.4	M	
5	SA_length_SN	3.4.2.2.5 4.2.2.5 c)	M	
6	SA_length_IV	3.4.2.2.6 4.2.2.5 b)	M	
7	SA_length_PL	3.4.2.2.7 4.2.2.5 d)	M	
8	SA_length_MAC	3.4.2.2.8 4.2.2.5 e)	M	
9	SA_authentication_algorithm	3.4.2.3.1 4.2.2.6.1 a)	C.2	
10	SA_authentication_key	3.4.2.3.2	C.2	
11	SA_authentication_mask	3.4.2.3.3 4.2.2.6.1 b) 4.2.2.6.2	C.2	
12	SA_sequence_number	3.4.2.3.4 4.2.2.6.1 c)	C.2	
13	SA_sequence_window	3.4.2.3.5 4.2.2.6.1 d)	C.2	
14	SA_encryption_algorithm	3.4.2.4 4.2.2.7 a)	C.3	
15	SA_encryption_key	3.4.2.4.2	C.3	
16	SA_initialization_vector	3.4.2.4.3 4.2.2.7 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/a
C.3: if [A5/1 | A5/3] is supported then M, else n/a
C.4: if [A5/1 | A5/3] is supported then M, else O