The Consultative Committee for Space Data Systems

Draft Recommendation for
Space Data System Standards

SPACE DATA LINK SECURITY PROTOCOL

PROPOSED DRAFT RECOMMENDED STANDARD

CCSDS 355.0-P-1.0

PROPOSED PINK SHEETS

April 2021

PREFACE

This document is a draft CCSDS Recommended Standard. Its 'Pink Sheet' 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-B-1	Space Data Link Security Protocol, Recommended Standard, Issue 1	September 2015	Original issue
CCSDS 355.0-P-1.0	Space Data Link Security Protocol, Proposed Draft Recommended Standard, Issue 1.0	April 2021	Current draft update: – adds specifications for Unified Space Data Link Protocol support; – adds normative reference to *Space Data Link Security Protocol—Extended Procedures*.

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])~~, and Unified Space Data Link Protocols (references [1], [2], [3], and [5]) 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.

To manage the Security Protocol over a space link, a set of procedures has been specified: the Space Data Link Security (SDLS) Protocol Extended Procedures (EP) (reference [6]).

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.

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].~~

1.6.1 DEFINITIONS FROM INFORMATION SECURITY GLOSSARY OF TERMS

This Recommended Standard makes use of a number of terms defined in reference [7].

1.6.2 TERMS DEFINED IN THIS RECOMMENDED STANDARD

For the purposes of this Recommended Standard, the following definitions also apply.

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.

1.8 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.~~

[4] *CCSDS Cryptographic Algorithms*. Issue 2. Recommendation for Space Data System Standards (Blue Book), CCSDS 352.0-B-2. Washington, D.C.: CCSDS, August 2019.

[5] *Unified Space Data Link Protocol*. Issue 1. Recommendation for Space Data System Standards (Blue Book), CCSDS 732.1-B-1. Washington, D.C.: CCSDS, October 2018.

[6] *Space Data Link Security Protocol—Extended Procedures*. Issue 1. Recommendation for Space Data System Standards (Blue Book), CCSDS 355.1-B-1. Washington, D.C.: CCSDS, February 2020.

[7] *Information Security Glossary of Terms*. Issue 2. Recommendation for Space Data System Practices (Magenta Book), CCSDS 350.8-M-2. Washington, D.C.: CCSDS, February 2020.

NOTE – Informative references are listed in annex D.

2 OVERVIEW

2.1 CONCEPT OF SECURITY PROTOCOL

The ~~Space Data Link Security~~SDLS 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]~~–~~, [2], [3], and [5], 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.)

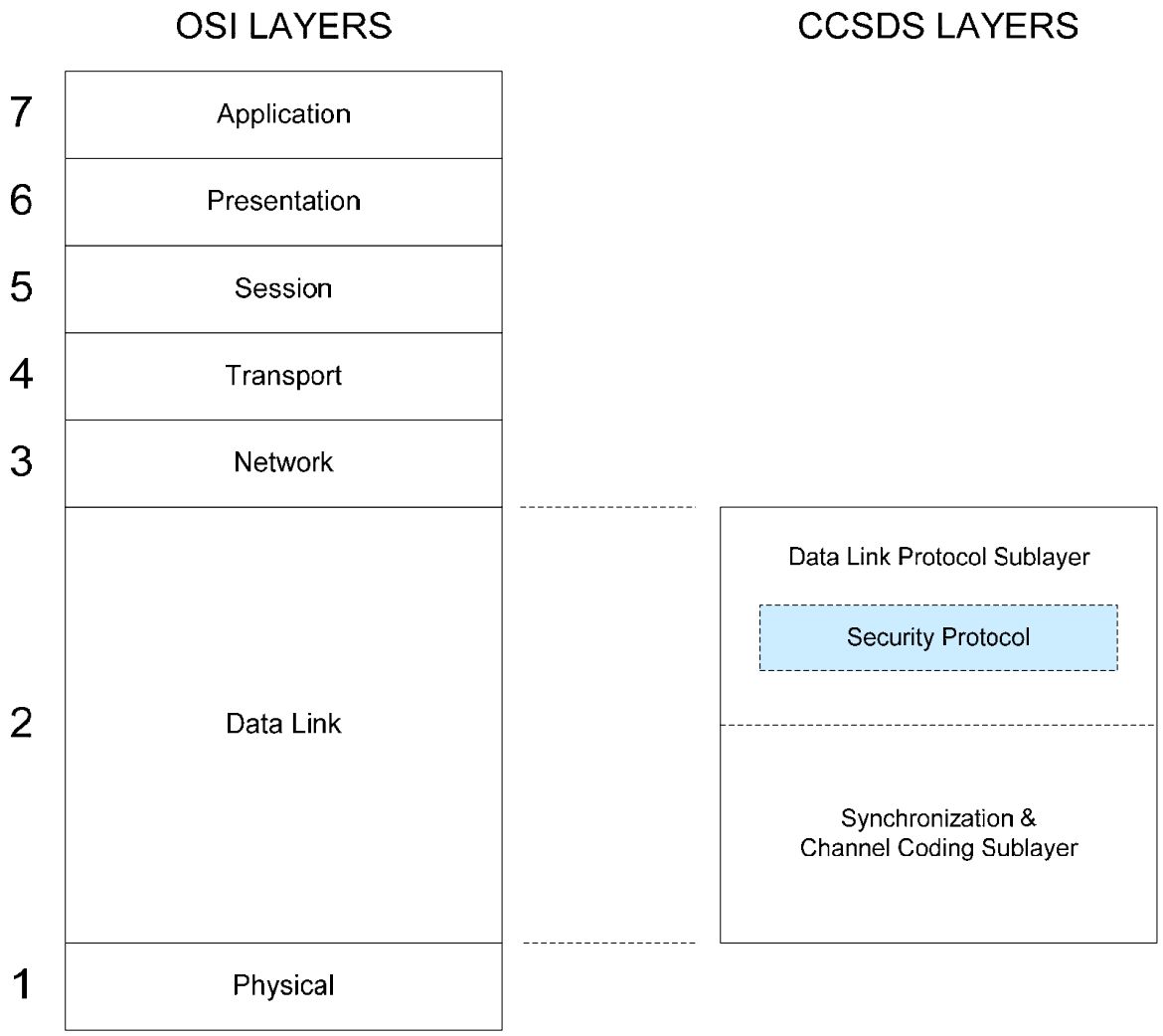

Figure 2-1: Security Protocol within OSI Model

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.

To operate the Security Protocol over a space link, a set of procedures is specified in *Space Data Link Security Protocol—Extended Procedures* (reference [6]). Those extended procedures define:

- key management, security association management, and SDLS monitoring and control services;
- procedures and associated protocol data units for those three services;
- interfaces with the SDLS and Space Data Link (SDL) protocols.

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~~four supported Space Data Link Protocols, Telemetry (TM), Telecommand (TC), ~~and~~ Advanced Orbiting Systems (AOS), and USLP, 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, and USLP Transfer Frames with the Security Protocol is given in references [1], [2], ~~and~~ [3], and [5], respectively, and repeated below in figures 5-1, 5-2, ~~and~~ 5-3, and 5-4 for reference.

2.2.6 SECURITY SERVICE FOR USLP

The relationship of the Security Protocol's functions to USLP is shown in figure 2-6. The figure shows the sending end of a physical channel.

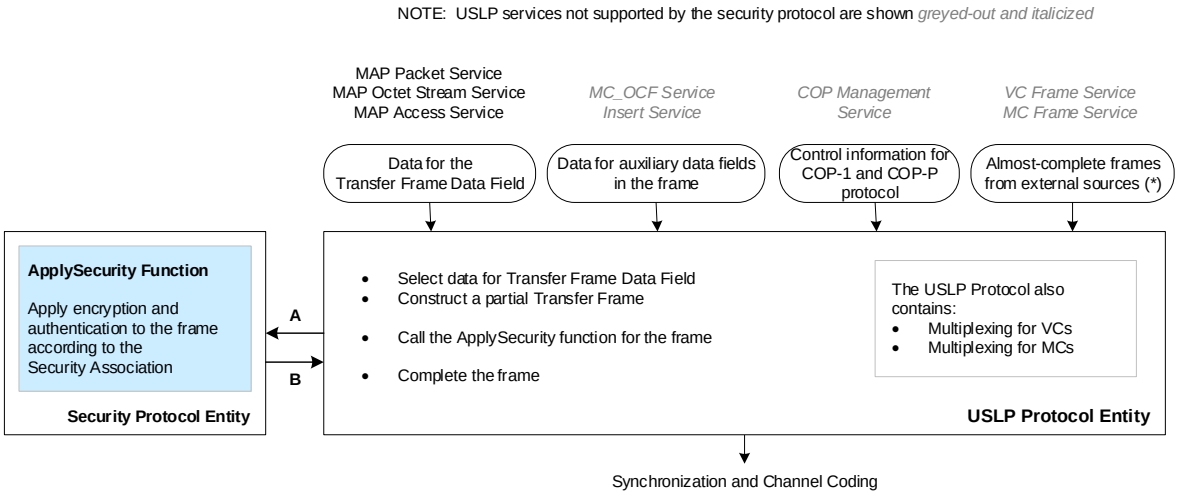

Figure 2-6: Security Protocol Support for USLP Services

The Security Protocol provides all its functions (authentication, encryption, and authenticated encryption) for the data in the Transfer Frame Data Field of a USLP Transfer Frame. It therefore provides full protection for the service data of the following USLP Services: the Multiplexer Access Point Packet (MAPP) Service, the Multiplexer Access Point Octet Stream (MAP Octet Stream) Service, and the Multiplexer Access Point Access (MAPA) Service.

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

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

The Security Protocol provides no protection for the control frames generated for the COPs Management Service.

The detailed structure of the TM, TC, ~~and~~ AOS, and USLP Transfer Frames with the Security Protocol is given in references [1], [2], ~~and~~ [3], and [5], respectively, and repeated below in figures 5-1, 5-2, ~~and~~ 5-3, and 5-4 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 and USLP 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, and USLP, 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:

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, or USLP) 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 and USLP 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.

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 USLP ApplySecurity Payload

The USLP ApplySecurity Payload shall consist of the portion of the USLP Transfer Frame (see reference [5]) from the first octet of the Transfer Frame Primary Header to the last octet of the Transfer Frame Data Field.

NOTES

1 The USLP Transfer Frame is the fixed-length or variable-length protocol data unit of USLP. The length of a fixed-length USLP Transfer Frame transferred on a physical channel is established by management.

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

3 For fixed-length USLP Transfer Frames, the size of the Transfer Frame Data Field is reduced by the size of the Security Header and Trailer. For variable-length USLP Transfer Frames, the size of the Transfer Frame Data Field is not impacted by the insertion of the Security Header and Trailer.

3.2.2.6 GLOBAL VIRTUAL CHANNEL (GVCID) ID

The GVCID parameter shall contain the ID of the Global Virtual Channel (see references [1], [2], [3], and [5]) 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.

3.2.2.7 GLOBAL MULTIPLEXER ACCESS POINT (GMAP) ID

The GMAP_ID parameter shall contain the ID of the Global Multiplexer Access Point (see references [2] and [5]) of the partially formatted TC or USLP Transfer Frame contained in the TC or USLP ApplySecurity Payload.

NOTES

1 The GMAP_ID consists of a GVCID and a TC or USLP 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 or USLP ApplySecurity Payload and the Virtual Channel specified by the GVCID is using Segment Headers (applicable only to TC).

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 and USLP 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.

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 [D5]). The length of any Transfer Frame transferred on a physical channel is constant, and is established by management.

3.3.2.5 USLP ProcessSecurity Payload

The USLP ProcessSecurity Payload shall consist of the portion of the USLP Transfer Frame (see reference [5]) 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 USLP Transfer Frame is the variable- or fixed-length protocol data unit of USLP.

3.3.2.6 GVCID

The GVCID parameter shall contain the ID of the Global Virtual Channel (see references [1]–, [2], [3], and [5]) of the partial Transfer Frame contained in the ProcessSecurity Payload.

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

3.3.2.7 GMAP ID

The GMAP_ID parameter shall contain the ID of the Global Multiplexer Access Point (see references [2] and [5]) of the partial TC or USLP Transfer Frame contained in the TC or USLP ProcessSecurity Payload.

NOTES

1 The GMAP_ID consists of a GVCID and a TC or USLP 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 or USLP ProcessSecurity Payload and the Virtual Channel specified by the GVCID is using Segment Headers (applicable only to TC).

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

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 [6]). ~~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]~~–~~, [2], [3], and [5]) applicable to the SA.

NOTES

1 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)).

2 If USLP and a COP are used on the physical channel, a single Global Virtual Channel is applicable to the SA (see requirement 5.4 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 references [2] and [5]) applicable to the SA.

NOTE – The GMAP_ID consists of a GVCID and a TC or USLP 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 or USLP is used on the physical channel and Segment Headers are used on the TC Virtual Channel. In all other cases it is not applicable.

3.4.3 ~~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]~~[6], which may be used to provide key management, SA management, SDLS monitoring and control services, procedures and associated protocol data units for those services, and interfaces needed for operation of SDLS over a space link. ~~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 Security Header is 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, the field lengths are kept constant, including Security Header, frame data field, and Security Trailer, across all supported operational configurations. The content of the Security Header is undefined when a VC is operating in clear mode.

3 The format of the Security Header is shown in figure 4-1.

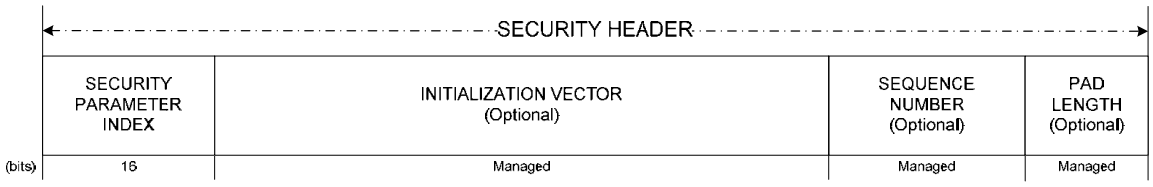

Figure 4-1: Security Header

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~~is 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 are kept constant, including Security Header, frame data field and Security Trailer, across all supported operational configurations. The content of the Security Trailer is undefined when a VC is operating in clear mode.

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

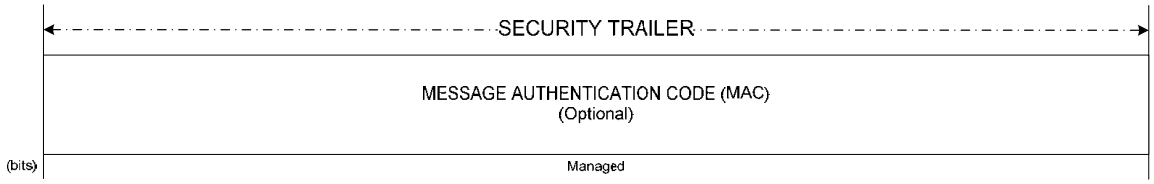

Figure 4-2: Security Trailer

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 and USLP 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 USLP is used on the physical channel, or 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], and [5]).

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 or USLP 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) (USLP only) the mask bits corresponding to the MAP ID field of the Transfer Frame Primary Header shall contain ‘all ones’;

d) (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);

e) (AOS only) the mask bits corresponding to the optional Frame Header Error Control field shall contain ‘all zeros’ (i.e., the field shall be excluded from the authenticated data);

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

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

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

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

5.4 USLP

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

a) The MAP Packet, MAP Octet Stream, and MAP Access Services may be used on a Global Multiplexer Access Point (GMAP) with the Authentication, Encryption, or Authenticated-Encryption Services, and are protected by each of these services.

b) The COPs Management Service, MC_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.

c) Each SA shall be associated to one VC and one VC only if COPs are used.

NOTE – The format of the USLP Transfer Frame is defined in reference [5]. The format of a USLP Transfer Frame using the Security Protocol is shown in figure 5-4.

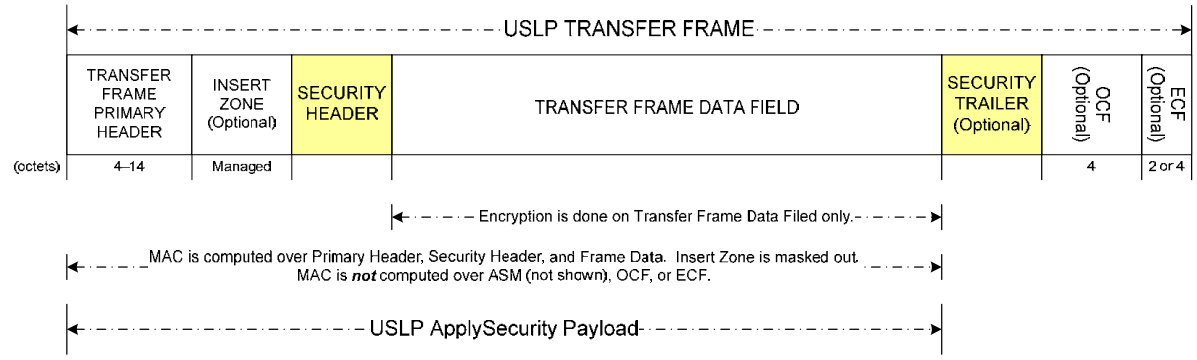

Figure 5-4: USLP Transfer Frame Using the Security Protocol

5.5 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
USLP	MAP Packet	Protected	Protected	Protected
	MAP Access	Protected	Protected	Protected
	MAP Octet Stream	Protected	Protected	Protected
	USLP_MC_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
	COPs Management	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~~. A set of procedures to manage Security Associations and Keys is specified in reference [6].

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], and [5]) 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	

Managed Parameter	Allowed Values	Defined In Reference
Security Association Context (identifies the GVCIDs or Global MAP IDs with which an SA is used)	GVCID Global MAP ID	[1], [2], [3], [5] [2], [5]
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)	[4]
Encryption key	Length (in bits): ~~128, 192, 256~~ Algorithm-specific Value (Binary)	[4]
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	

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	
4	Unified Space Data Link Protocol	Reference [5]	O.1	
	O.1: Support for at least one of [A4/1 | A4/2 | A4/3 | A4/4] 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			

A7 SERVICE PRIMITIVES

Item	Protocol Feature	Reference	Sender		Receiver	
			Status	Support	Status	Support
1	ApplySecurity	3.2.1	M		n/a	
2	ProcessSecurity	3.3.1	n/a		M	

A7.1 SECURITY FUNCTIONS

A7.1.1 ApplySecurity (Sending)

Item	Protocol Feature	Reference	Status	Support
1	TM ApplySecurity Payload	3.2.2.2	C.5	
2	TC ApplySecurity Payload	3.2.2.3	C.1	
3	AOS ApplySecurity Payload	3.2.2.4	C.6	
4	USLP ApplySecurity Payload	3.2.2.5	C.7	
5	GVCID	3.2.2.5	M	
6	GMAP_ID	3.2.2.7	C.1	
7	AEAD algorithms' plaintext	4.2.3.2.2.3 a) 1)	C.~~7~~8	
8	AEAD algorithms' AAD	4.2.3.2.2.3 a) 2)	C.~~7~~8	
9	Encrypt frame data	4.2.3.3 a)	C.3	
10	Put length of pad in header	4.2.3.3 b)	O	
11	Increment SN	4.2.3.4 a)	C.2	
12	Put SN in header	4.2.3.4 b)	C.2	
13	Get Authentication Payload data	4.2.3.4 c)	C.2	
14	Apply mask	4.2.3.4 d)	C.2	
15	Compute MAC	4.2.3.4 e)	C.2	
16	Truncate MAC	4.2.3.4 f)	O	
17	Put MAC in trailer	4.2.3.4 g)	C.2	
18	Return status to caller	3.2.3	M	

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.5: if [A4/1] is supported then M, else n/a
C.6: if [A4/3] is supported then M, else n/a
C.7: if [A4/4] is supported then M, else n/a
C.~~7~~8: if [A5/3] is supported then M, else n/a

A7.1.2 ProcessSecurity (Receiving)

Item	Protocol Feature	Reference	Status	Support
1	TM ProcessSecurity Payload	3.3.2.2	C.5	
2	TC ProcessSecurity Payload	3.3.2.3	C.1	
3	AOS ProcessSecurity Payload	3.3.2.4	C.6	
4	USLP ProcessSecurity Payload	3.3.2.5	C.7	
5	GVCID	3.3.2.5	M	
6	GMAP_ID	3.3.2.7	C.1	
7	Discard frames with wrong SA and report exceptions	4.2.4.3	M	
8	AEAD algorithms' plaintext	4.2.4.2.3.2 a) 1)	C.~~7~~8	
9	AEAD algorithms' AAD	4.2.4.2.3.2 a) 2)	C.~~7~~8	
10	Get Authentication Payload data	4.2.4.4 a)	C.2	
11	Apply mask	4.2.4.4 a)	C.2	
12	Compute MAC	4.2.4.4 b)	C.2	
13	Truncate computed MAC	4.2.4.4 c)	O	
14	Compare to received MAC	4.2.4.4 d)	C.2	
15	Report MAC exceptions	4.2.4.4 e)	C.2	
16	Discard frames with bad MAC	4.2.4.4 e)	C.2	
17	Archive rejected-MAC frames	4.2.4.4 e)	O	
18	Read received SN	4.2.4.4 f)	C.2	
19	Compare to managed SN	4.2.4.4 g)	C.2	
20	Report SN exceptions	4.2.4.4 i)	C.2	
21	Discard frames with bad SN	4.2.4.4 i) 4.2.4.4 i)	C.2	
22	Archive rejected-SN frames	4.2.4.4 i) 4.2.4.4 i)	O	
23	Update managed SN	4.2.4.4 j)	C.2	
24	Remove trailer	4.2.4.4	C.2	
25	Decrypt frame data	4.2.4.5 a)	C.3	
26	Remove header	4.2.4.5 b)	M	
27	Return status to caller	–	M	

	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.5: if [A4/1] is supported then M, else n/a C.6: if [A4/3] is supported then M, else n/a C.7: if [A4/4] is supported then M, else n/a C.~~7~~8: if [A5/3] is supported then M, else n/a

A8 PROTOCOL DATA UNITS

A8.1 SECURITY HEADER

Item	Protocol Feature	Reference	Status	Support
1	SPI	4.1.1.1.3 a) 4.1.1.2	M	
2	IV	4.1.1.1.3 b) 4.1.1.3	C.4	
3	SN	4.1.1.1.3 c) 4.1.1.4	C.2	
4	PL	4.1.1.1.3 d) 4.1.1.5	C.3	
5	Max length	4.1.1.1.4	M	
	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			

A8.2 SECURITY TRAILER

Item	Protocol Feature	Reference	Status	Support
1	MAC	4.1.2.1	C.~~8~~9	
	C.~~8~~9: if [A5/2 | A5/3] is supported then M, else O			

The Security Protocol provides no cryptographic key management protocol. Specifying the successful implementation of cryptographic key management or operational key change criteria is beyond the scope of this document. (See references [D3] and [D8] for more information.)

The Security Protocol provides no protection to TC or USLP COP control commands nor to COP-1 CLCW or COP-P PLCW 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 [D2].

B1.4 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.

B2 SANA CONSIDERATIONS

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

B3 PATENT CONSIDERATIONS

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

ANNEX C

ABBREVIATIONS AND ACRONYMS

(INFORMATIVE)

AAD	Additional Authenticated Data
AEAD	Authenticated Encryption with Associated Data
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
EP	(SDLS) Extended Procedures
FSH	Frame Secondary Header
GCM	Galois/Counter Mode
GMAP_ID	Global Multiplexer Access Point ID
GVCID	Global Virtual Channel ID
IV	Initialization Vector
M_PDU	Multiplexing Protocol Data Unit
MAC	Message Authentication Code
MAP	Multiplexer Access Point
MC	Master Channel
OCF	Operational Control Field
PLCW	Proximity Link Control Word

RF	Radio Frequency
SA	Security Association
SANA	Space Assigned Numbers Authority
SDLS	Space Data Link Security
SLE	Space Link Extension
SPI	Security Parameter Index
TC	Telecommand
TM	Telemetry
USLP	Unified Space Data Link Protocol
VC	Virtual Channel
VCA	Virtual Channel Access
VCA_SDU	Virtual Channel Access Service Data Unit

ANNEX D

INFORMATIVE REFERENCES

(INFORMATIVE)

[D1] *Information Technology—Open Systems Interconnection—Basic Reference Model: The Basic Model*. 2nd ed. International Standard, ISO/IEC 7498-1:1994. Geneva: ISO, 1994.

[D2] *Information Processing Systems—Open Systems Interconnection—Basic Reference Model—Part 2: Security Architecture*. International Standard, ISO 7498-2:1989. Geneva: ISO, 1989.

~~[D3] *Space Data Link Security Concept of Operation*. Report Concerning Space Data System Standards, CCSDS 350.5-G. Washington, D.C.: CCSDS, forthcoming.~~

[D3] *Space Data Link Security Protocol—Summary of Concept and Rationale*. Issue 1. Report Concerning Space Data System Standards (Green Book), CCSDS 350.5-G-1. Washington, D.C.: CCSDS, June 2018.

[D4] *Overview of Space Communications Protocols*. Issue 3. Report Concerning Space Data System Standards (Green Book), CCSDS 130.0-G-3. Washington, D.C.: CCSDS, July 2014.

~~[D5] *Information Security Glossary of Terms*. Issue 1. Report Concerning Space Data System Standards (Green Book), CCSDS 350.8-G-1. Washington, D.C.: CCSDS, November 2012.~~

~~[D6] *TM Synchronization and Channel Coding*. Issue 2. Recommendation for Space Data System Standards (Blue Book), CCSDS 131.0-B-2. Washington, D.C.: CCSDS, August 2011.~~

~~[D7] *The Application of CCSDS Protocols to Secure Systems*. Issue 2. Report Concerning Space Data System Standards (Green Book), CCSDS 350.0-G-2. Washington, D.C.: CCSDS, January 2006.~~

[D5] *TM Synchronization and Channel Coding*. Issue 3. Recommendation for Space Data System Standards (Blue Book), CCSDS 131.0-B-3. Washington, D.C.: CCSDS, September 2017.

[D6] *The Application of Security to CCSDS Protocols*. Issue 3. Report Concerning Space Data System Standards (Green Book), CCSDS 350.0-G-3. Washington, D.C.: CCSDS, March 2019.

[D7] *Security Architecture for Space Data Systems*. Issue 1. Recommendation for Space Data System Practices (Magenta Book), CCSDS 351.0-M-1. Washington, D.C.: CCSDS, November 2012.

[D8] *Space Missions Key Management Concept*. Issue 1. Report Concerning Space Data System Standards (Green Book), CCSDS 350.6-G-1. Washington, D.C.: CCSDS, November 2011.

[D9] *National Information Assurance (IA) Glossary*. Revised. CNSSI No. 4009. Fort Meade, Maryland: CNSS, April 6, 2015.

[D10] *Glossary of Key Information Security Terms*. Rev. 2. Edited by Richard Kissel. NIST IR 7298. Gaithersburg, Maryland: NIST, May 2013.

[D11] Elaine Barker, et al. *Recommendation for Key Management—Part 1: General*. Rev. 3. National Institute of Standards and Technology Special Publication 800-57. Gaithersburg, Maryland: NIST, July 2012.

[D12] *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.

~~[D14] *Space Data Link Security Protocol—Extended Procedures*. Recommendation for Space Data System Standards, CCSDS 355.1-B. Washington, D.C.: CCSDS, forthcoming.~~

NOTE – Normative references are listed in 1.8.

ANNEX E

BASELINE IMPLEMENTATION MODE

(INFORMATIVE)

E1 BASELINE MODE FOR USE WITH TM

E1.1 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 [4]. In addition:

a) the key is ~~128~~256 bits in total length;

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

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

E1.2 SECURITY HEADER

The baseline implementation uses a Security Header of 14 octets in length. The format of the Security Header is shown in figure E-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 E-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 E-1 is zero octets.

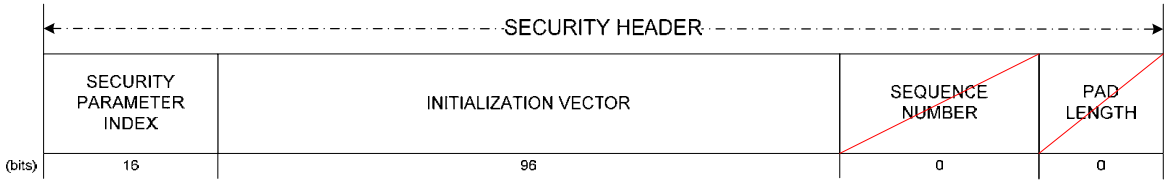

Figure E-1: Security Header (TM Baseline)

E1.3 SECURITY TRAILER

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

Figure E-2: Security Trailer (TM Baseline)

E1.4 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 4.2.2.6.2 contain zeros.

E2 BASELINE MODE FOR USE WITH TC

E2.1 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 [4]. In addition:

a) the key is ~~128~~256 bits in total length;

b) 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;

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

E2.2 SECURITY HEADER

The baseline implementation uses a Security Header of 6 octets in length. The format of the Security Header is shown in figure E-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 E-3 are zero octets each.

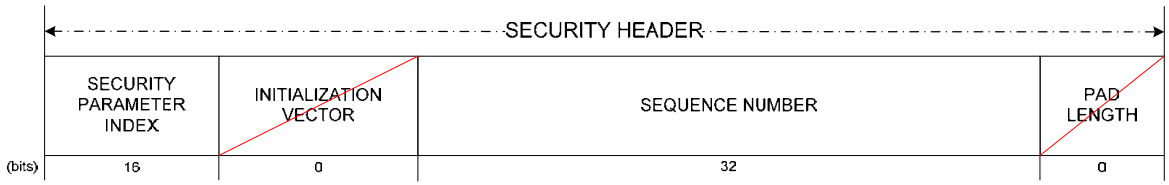

Figure E-3: Security Header (TC Baseline)

E2.3 SECURITY TRAILER

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

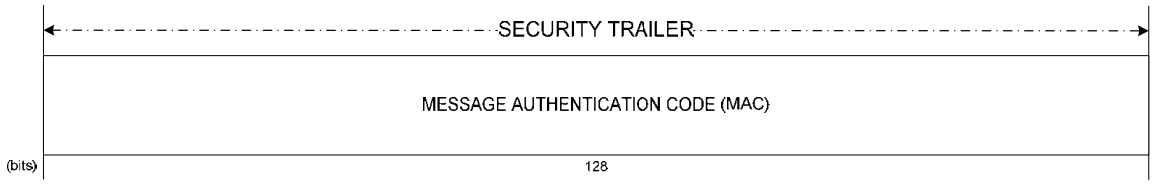

Figure E-4: Security Trailer (TC Baseline)

E2.4 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 4.2.2.6.2 contain zeros.

E3 BASELINE MODE FOR USE WITH AOS

E3.1 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 [4]. In addition:

a) the key is ~~128~~256 bits in total length;

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

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

E3.2 SECURITY HEADER

The baseline implementation uses a Security Header of 14 octets in length. The format of the Security Header is shown in figure E-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 E-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 E-5 is zero octets.

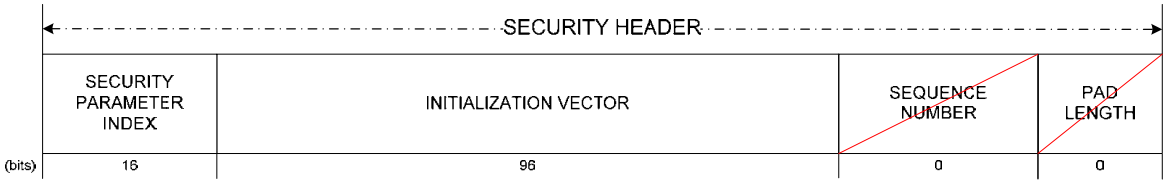

Figure E-5: Security Header (AOS Baseline)

E3.3 SECURITY TRAILER

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

Figure E-6: Security Trailer (AOS Baseline)

E3.4 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 4.2.2.6.2 contain zeros.

E4 BASELINE MODE FOR USE WITH USLP

E4.1 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 [4]. In addition:

d) the key is 256 bits in total length;

e) 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;

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

E4.2 SECURITY HEADER

The baseline implementation uses a Security Header of 14 octets in length. The format of the Security Header is shown in figure E-7.

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 E-7 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 E-7 is zero octets.

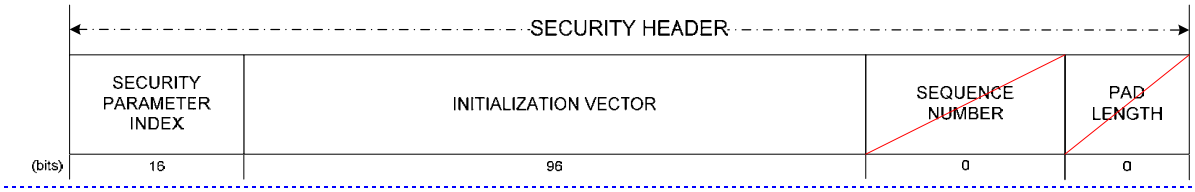

Figure E-7: Security Header (USLP Baseline)

E4.3 SECURITY TRAILER

The baseline implementation uses a Security Trailer of 16 octets in length. The format of the Security Trailer is shown in figure E-8.

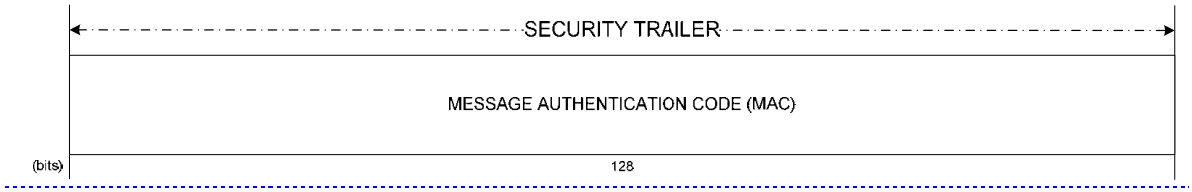

Figure E-8: Security Trailer (USLP Baseline)

E4.4 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 4.2.2.6.2 contain zeros.