The Consultative Committee for Space Data Systems

Draft Report Concerning
Space Data System Standards

SPACE DATA LINK SECURITY PROTOCOL—SUMMARY OF CONCEPT AND RATIONALE

DRAFT INFORMATIONAL REPORT

CCSDS 350.5-G-1.1

DRAFT GREEN BOOK

October 2023

AUTHORITY

Issue:	Draft Green Book, Issue 1.1
Date:	October 2023
Location:	Not Applicable

(WHEN THIS INFORMATIONAL REPORT IS FINALIZED, IT WILL CONTAIN THE FOLLOWING STATEMENT OF AUTHORITY:)

This document has been approved for publication by the Management Council of the Consultative Committee for Space Data Systems (CCSDS) and reflects the consensus of technical working group experts from CCSDS Member Agencies. The procedure for review and authorization of CCSDS Reports is detailed in *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-4).

This document is published and maintained by:

CCSDS Secretariat
National Aeronautics and Space Administration
Washington, DC, USA
Email: secretariat@mailman.ccsds.org

FOREWORD

This document is a CCSDS Informational Report, which contains background, rationale, and a concept of operation to support the CCSDS Recommended Standard on the Space Data Link Security Protocol (reference [1]).

Through the process of normal evolution, it is expected that expansion, deletion, or modification of this document may occur. This Report 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 email 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 Science Policy Office (BELSPO)/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.
- China 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.
- Egyptian Space Agency (EgSA)/Egypt.
- 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.
- Hellenic Space Agency (HSA)/Greece.
- Indian Space Research Organization (ISRO)/India.
- Institute of Space Research (IKI)/Russian Federation.
- Korea Aerospace Research Institute (KARI)/Korea.
- Ministry of Communications (MOC)/Israel.
- Mohammed Bin Rashid Space Centre (MBRSC)/United Arab Emirates.
- National Institute of Information and Communications Technology (NICT)/Japan.
- National Oceanic and Atmospheric Administration (NOAA)/USA.
- National Space Agency of the Republic of Kazakhstan (NSARK)/Kazakhstan.
- National Space Organization (NSPO)/Chinese Taipei.
- Naval Center for Space Technology (NCST)/USA.
- Netherlands Space Office (NSO)/The Netherlands.
- Research Institute for Particle & Nuclear Physics (KFKI)/Hungary.
- Scientific and Technological Research Council of Turkey (TUBITAK)/Turkey.
- South African National Space Agency (SANSA)/Republic of South Africa.
- Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
- Swedish Space Corporation (SSC)/Sweden.
- Swiss Space Office (SSO)/Switzerland.
- United States Geological Survey (USGS)/USA.

DOCUMENT CONTROL

Document	Title	Date	Status
CCSDS 350.5-G-1	Space Data Link Security Protocol—Summary of Concept and Rationale, Informational Report, Issue 1	June 2018	Original issue
CCSDS 350.5-G-1.1	Space Data Link Security Protocol—Summary of Concept and Rationale, Draft Informational Report, Issue 1.1	October 2023	Current draft

CONTENTS

CONTENTS (continued)

Figure Page

Table

1 INTRODUCTION

1.1 PURPOSE

This Report has been developed to present the concept and rationale of the CCSDS Recommended Standard on the Space Data Link Security Protocol (reference [1]).

It has specifically been prepared to document the following:

a) architectural overview of the Space Data Link Security Protocol;

b) interaction between Space Data Link and Space Data Link Security Protocols;

c) justification of protocol services, elements, procedures, and design choices as well as the recommended profiles;

d) security analyses;

e) guidelines for the selection of Space Data Link Security Protocol parameters.

1.2 SCOPE

The information contained in this Report is not part of the CCSDS Recommended Standard on the Space Data Link Security Protocol (reference [1]). In the event of any conflict between the Recommended Standard and the material presented herein, the Recommended Standard shall prevail.

1.3 ORGANIZATION OF THIS REPORT

This document is divided into four numbered sections and five annexes:

a) section 1 presents the purpose, scope, and organization of this Report, and lists the definitions and references used throughout the Report;

b) section 2 presents an overview of the protocol; the motivation for its development, the major design goals and constraints, as well as the main requirements are discussed;

c) section 3 provides a detailed description and discussion of the key design concepts of the protocol; in particular, the selection of security services, the position of the protocol in CCSDS stacks, and its data structures, fields, and functions are given;

d) section 4 presents the operation of the protocol in detail;

e) annex A elaborates on the baseline implementations;

f) annex B provides a detailed analysis of the ISO/OSI security services;

g) annex C includes the latest version of the User Requirements Document (URD);

h) annex D illustrates the protocol interaction with data link performance;

i) annex E provides a list of acronyms and abbreviations.

1.4 CONVENTIONS AND DEFINITIONS

Generic definitions for the security terminology applicable to this and other CCSDS documents are provided in reference [2].

1.5 REFERENCES

The following publications are referenced in 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] *Space Data Link Security Protocol*. Issue 2. Recommendation for Space Data System Standards (Blue Book), CCSDS 355.0-B-2. Washington, D.C.: CCSDS, July 2022.

[2] *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.

[3] *Cross Support Reference Model—Part 1: Space Link Extension Services*. Issue 2. Recommendation for Space Data System Standards (Blue Book), CCSDS 910.4-B-2. Washington, D.C.: CCSDS, October 2005.

[4] *TM Space Data Link Protocol*. Issue 3. Recommendation for Space Data System Standards (Blue Book), CCSDS 132.0-B-3. Washington, D.C.: CCSDS, October 2021.

[5] *TC Space Data Link Protocol*. Issue 4. Recommendation for Space Data System Standards (Blue Book), CCSDS 232.0-B-4. Washington, D.C.: CCSDS, October 2021.

[6] *AOS Space Data Link Protocol*. Issue 4. Recommendation for Space Data System Standards (Blue Book), CCSDS 732.0-B-4. Washington, D.C.: CCSDS, October 2021.

[7] *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.

[8] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. Discrete Mathematics and Its Applications. Boca Raton, Florida: CRC Press, 1996.

[9] Mihir Bellare and Chanathip Namprempre. "Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm." In *Advances in Cryptology — ASIACRYPT 2000: Proceedings of the 6th International Conference on the Theory and Application of Cryptology and Information Security (December 3–7, 2000, Kyoto, Japan)*, 531–545. Edited by Tatsuaki Okamoto. Lecture Notes in Computer Science 1976. Berlin, Heidelberg: Springer, 2000.

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

[11] *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.

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

[13] *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.

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

[15] *TC Synchronization and Channel Coding*. Issue 4. Recommendation for Space Data System Standards (Blue Book), CCSDS 231.0-B-4. Washington, D.C.: CCSDS, July 2021.

[16] Morris Dworkin. *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*. National Institute of Standards and Technology Special Publication 800-38D. Gaithersburg, Maryland: NIST, November 2007.

[17] *Information Technology—Security Techniques—Message Authentication Codes (MACs)—Part 1: Mechanisms Using a Block Cipher*. 2nd ed. International Standard, ISO/IEC 9797-1:2011. Geneva: ISO, 2011.

[18] *Information Technology—Security Techniques—Modes of Operation for an n-Bit Block Cipher*. 4th ed. International Standard, ISO/IEC 10116:2017. Geneva: ISO, 2017.

[19] Morris Dworkin. *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*. NIST Special Publication 800-38B. Gaithersburg, Maryland: NIST, May 2005 (Updated 10/6/2016).

[20] *Packet Telecommand Standard*. Issue 2. ESA PSS-04-107. Paris: ESA, April 1992.

[21] *CCSDS Cryptographic Algorithms*. Issue 1. Report Concerning Space Data System Standards (Green Book), CCSDS 350.9-G-1. Washington, D.C.: CCSDS, December 2014.

[22] *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.

[23] I. Aguilar, D. Fischer, and P. Bargellini. "The Telecommand Authentication Concept for the ESA GMES Sentinels." In *Proceedings of the 5th ESA International Workshop on Tracking, Telemetry and Command Systems for Space Applications (21–23 September 2010, Noordwijk, Netherlands)*. Noordwijk, Netherlands: ESA/ESTEC, 2010.

[24] *Space Engineering—Space Data Links—Telecommand Protocols, Synchronization and Channel Coding*. ECSS-E-ST-50-04C. Noordwijk, The Netherlands: ECSS Secretariat, 31 July 2008.

[25] Marcio Juliato, Catherine Gebotys, and Ignacio Aguilar Sanchez. *Cryptographic Key Infrastructure for Security Services Protecting TT&C and Payload Links of Space Missions*. ESA Contract Report, ESTEC Contract No. 4000103681. Noordwijk, Netherlands: ESA/ESTEC, 2015. https://cwe.ccsds.org/sec/docs/Referenced/ESA-NPI_Report.pdf

[26] Nigel Smart, ed. *ECRYPT II Yearly Report on Algorithms and Keysizes (2011-2012)*. Revision 1.0. ICT-2007-216676. Luxembourg: CORDIS, 30 September 2012.

[27] Markku-Juhani O. Saarinen. *Cycling Attacks on GCM, GHASH and Other Polynomial MACs and Hashes*. Cryptology ePrint Archive: Report 2011/202. Reno, Nevada: IACR, 2011.

[28] *TC Synchronization and Channel Coding—Summary of Concept and Rationale*. Issue 3. Report Concerning Space Data System Standards (Green Book), CCSDS 230.1-G-3. Washington, D.C.: CCSDS, October 2021.

[29] *TM Synchronization and Channel Coding—Summary of Concept and Rationale*. Issue 3. Report Concerning Space Data System Standards (Green Book), CCSDS 130.1-G-3. Washington, D.C.: CCSDS, June 2020.

[30] *TM Synchronization and Channel Coding*. Issue 5. Recommendation for Space Data System Standards (Blue Book), CCSDS 131.0-B-5. Washington, D.C.: CCSDS, September 2023.

[31] *Unified Space Data Link Protocol (USLP)*. Issue 2. Recommendation for Space Data System Standards (Blue Book), CCSDS 732.1-B-2. Washington, D.C.: CCSDS, October 2021.

[32] *Space Data Link Security Protocol—Extended Procedures—Summary of Concept of Rationale*. Report Concerning Space Data System Standards (Green Book). Under development.

[33] *Space Communications Cross Support—Architecture Description Document*. Issue 1. Report Concerning Space Data System Standards (Green Book), CCSDS 901.0-G-1. Washington, D.C.: CCSDS, November 2013.

[34] *Space Communications Cross Support—Architecture Requirements Document*. Issue 1. Recommendation for Space Data System Practices (Magenta Book), CCSDS 901.1-M-1. Washington, D.C.: CCSDS, May 2015.

2 OVERVIEW

2.1 SDLS PROTOCOL

The Space Data Link Security protocol (reference [1]) is a security protocol that implements user-selected Security Services to the data transported by the Space Data Link (SDL) protocols used by space missions over a space link. The SDLS protects the service data units transported by the SDL protocol and, in addition, selected SDL protocol data structures, taking into account compatibility constraints with SDL and Space Link Extension services.

2.2 MOTIVATION

The CCSDS is working to provide security standards for space missions as well as security guidance to other areas of CCSDS standardization. The CCSDS Security Working Group has developed a space security architecture, a space mission threat document, and security protocol guidance, and has standardized cryptographic algorithms for data confidentiality and authentication.

However, while other link and network standards have been developed, no security standards for the bulk of CCSDS missions in which there is a single spacecraft in contact with its control center through a ground station had been available until now. As a result, if uplink command authentication and/or downlink payload data confidentiality requirements were specified for a space mission that is otherwise CCSDS compliant, up to this point each mission has had to invent its own security solutions. CCSDS realized that a standardized concept to integrate security on space missions with a simple end-to-end topology could be proposed at the Data Link Layer. This would avoid the above-mentioned problem of individual developments and would deliver the benefits of standardization also in the area of secure space link communication.

The CCSDS Space Link Extension (SLE) transfer services (reference [3]) extend the delivery of the SDL protocols (references [4], [5], [6] and [31]) from the ground station, typically on a remote location with limited or no personnel, to the mission control center, where mission operations are conducted and manned 24 hours/7 days a week. SLE has security provisions to guarantee identification, authentication, and confidentiality between the two exchanging parties, which for the case of SLE are the ground control center and the ground station(s). Protection on ground networks is thus ensured. But the space link itself, which is not protected by SLE, requires additional protection.

To develop this protection, CCSDS formed a joint working group made up of members from both the Space Link and the System Engineering (Security) areas. The goal was to develop a CCSDS standard for Data Link Layer security services for use with existing CCSDS telemetry (TM) (reference [4]), telecommand (TC) (reference [5]), Advanced Orbiting Systems (AOS) (reference [6]), and *Unified Space Data Link Protocol (USLP)* (reference [31]) standards without having to modify those standards. Rather the aim was to allow security services to be used with TC, TM, AOS, and USLP and not force a reengineering of those standards, which are in wide use by many missions and planned for use in many new missions.

In summary, the SDLS protocol implements an additional security function tightly integrated within the corresponding Data Link Layer of the International Standards Organization Open Systems Interconnection (ISO/OSI) model (see figure 2-1).

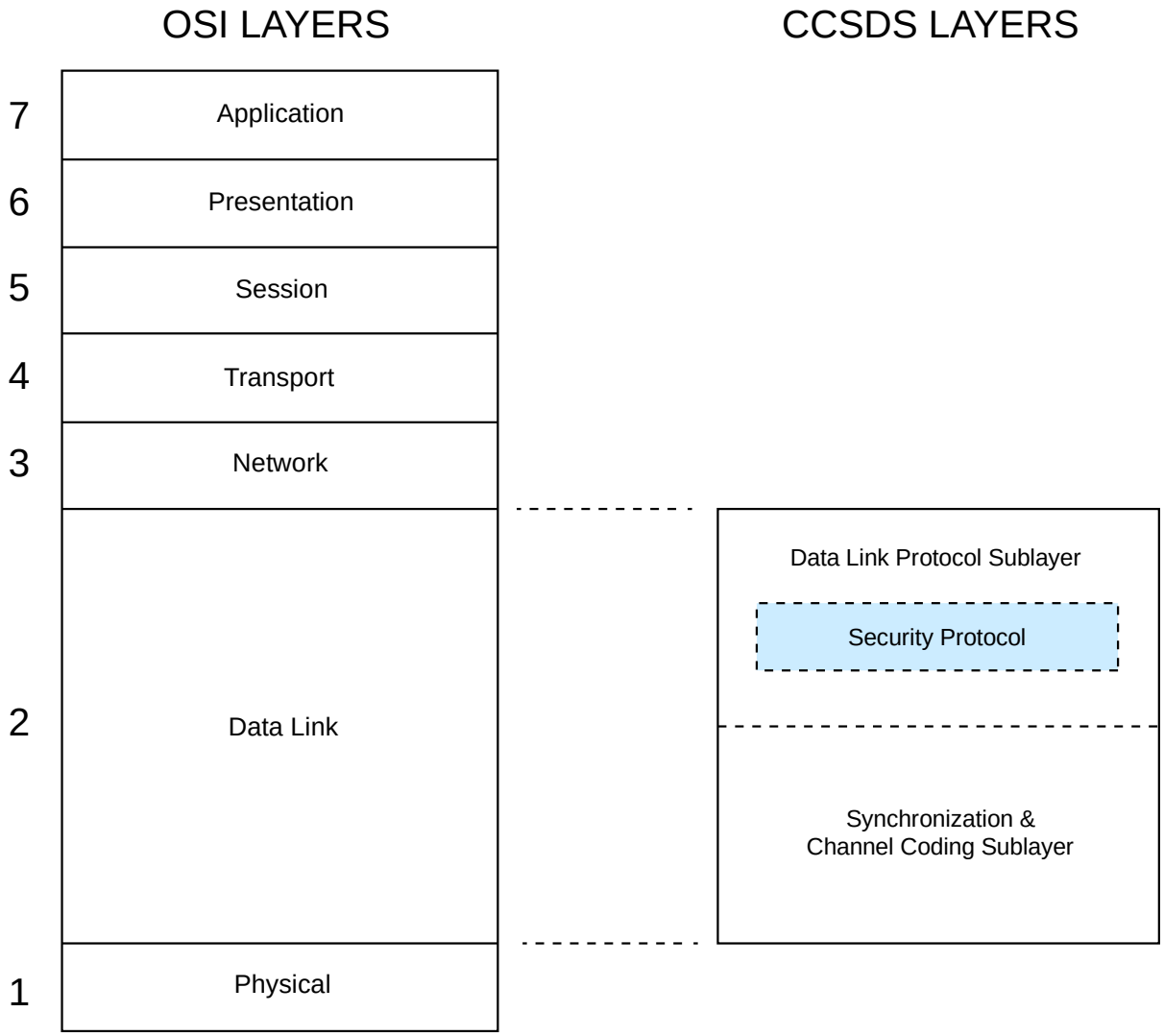


Figure 2-1: Placement of SDLS with Respect to OSI and CCSDS Layers

2.3 MAJOR DESIGN GOALS AND CONSTRAINTS

2.3.1 MISSION NETWORK TOPOLOGIES

The target space missions for the SDLS protocol are those in which, basically, a mission control center communicates with a satellite with a single ground station (see figure 2-2). The ground network between the Ground Station (GS) and the Mission Control Center (MCC) implements SLE services. The SLE services extend the ground side of the SDL protocol, formerly placed at the ground station site, up to the mission control center. The SLE services are based on ground network and transport protocols. The reader is referred to reference [3] for a detailed overview of SLE and to references [33] and [34] for detailed discussions and diagrams showing end-to-end deployments using SDLS.

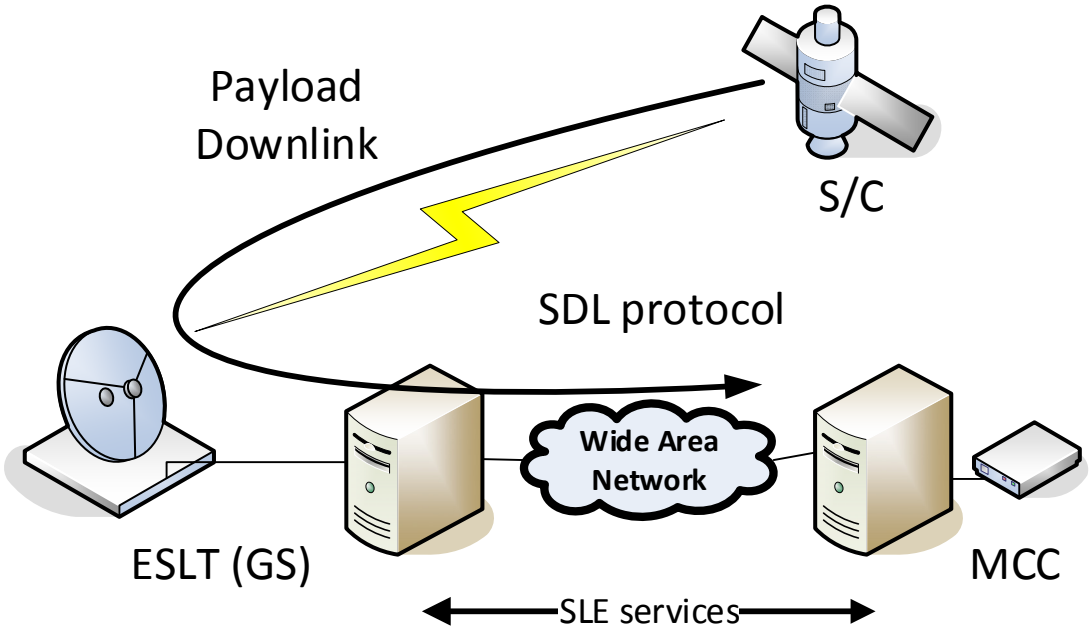


Figure 2-2: Mission Network Topology A

In this simple topology, payload and housekeeping telemetry are multiplexed on the same space link. In many missions, those telemetry data flows are segregated, thus employing two space downlinks (see figure 2-3).

Securing end-to-end communications between the mission control center and the spacecraft is divided into two tasks. The first task is protecting the SLE services and ground network interconnecting the mission control center and ground station(s).

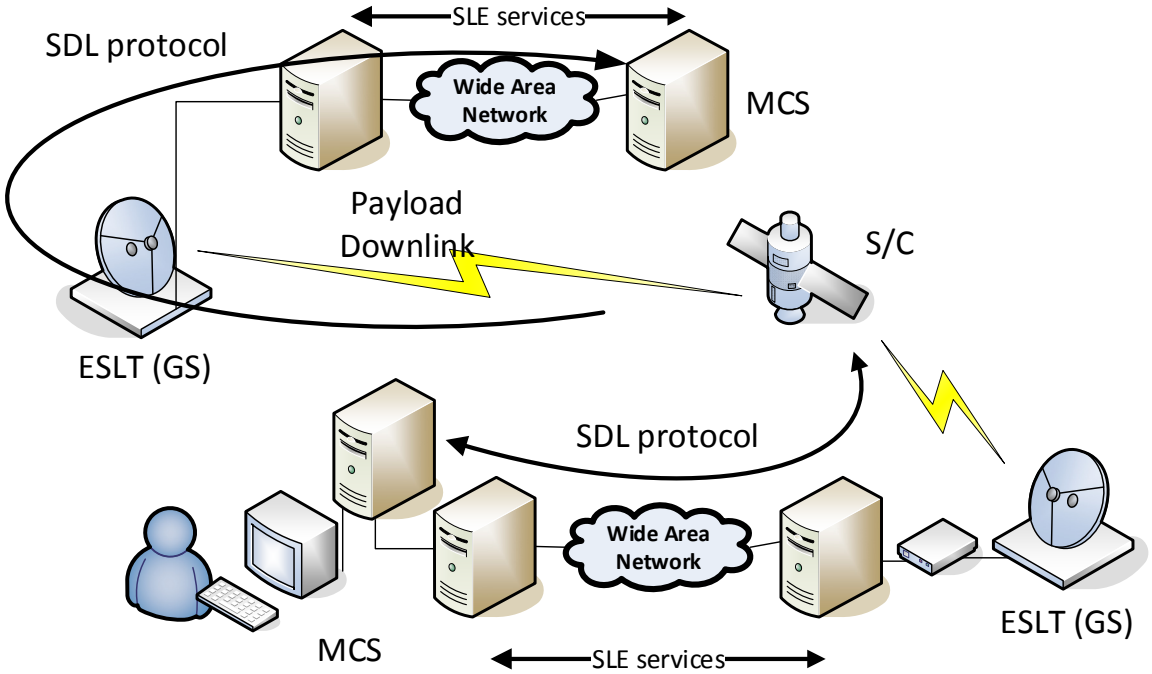


Figure 2-3: Mission Network Topology B

The second task, the subject of the SDLS protocol, involves protecting the end-to-end SDL protocols now closed between the spacecraft and the Mission Control System (MCS) on the ground side.

This communications and data systems architecture provides interoperability between space agencies with SLE services and end-to-end security between a space agency MCS and its spacecraft. A service level agreement is required to ensure secure cross support with SLE services between the agency or operator owning the mission control center and the agency owning or operating the ground station. If needed, protection against denial of service on the TC space link can be achieved by using TRANSEC techniques in the Physical Layer (e.g., spread spectrum), which are perfectly compatible with SDLS protocol.

SLE data links between ground stations and mission control centers can be protected by SLE authentication and suitable network encryption protocols.

These simple network topologies are found on many Earth observation and science missions. Those topologies can also be applicable to geostationary telecommunication missions, which rely on a single Telemetry, Command, and Ranging (TCR) link. Some advanced telecommunication payloads have segregated direct Payload Control and Configuration (PCC) links that could benefit from the second topology with the addition of an uplink.

A third mission network topology that can be considered is space-to-space links (e.g., within a constellation of satellites). SDLS protocol and its associated Extended Procedures are designed to operate in a master-slave configuration. For nominal ground-to-space and space-to-ground

links, the master is the mission operations center. It is also possible to use the SDLS protocol and its Extended Procedures for securing and managing space-to-space links. In all cases, there is no negotiation between endpoints: all directives are issued from a predetermined master (referred to as Initiator in reference [32]) toward a predetermined slave (referred to as Recipient in reference [32]). Therefore, in the case of space-to-space links, a hierarchy needs to be established among the communicating satellites so that for each connection a master (Initiator) and a slave (Recipient) is unambiguously defined. This hierarchy usually does not exist for space-to-space links and within constellation.

Moreover, a key management scheme needs to be implemented across the constellation. Possible examples are:

– a dedicated set of keys managed for each possible connection, which might become impractical when the number of communicating satellites pairs increases;

– a common set of keys shared throughout the constellation, while still ensuring that the cryptographic algorithm and mode of operation requirements are met (e.g., key-Initialization Vector [IV] uniqueness for Advanced Encryption Standard [AES]-Galois Counter Mode [GCM]).

As shown above, SDLS protocol and its Extended Procedures can be used to secure intersatellite links. In that scenario, the terms ‘telecommand link’ and ‘telemetry link’ used throughout this document should be replaced by ‘forward link’ (from Initiator satellite to Recipient satellite) and ‘return link’ (from Recipient satellite to Initiator satellite). However, for larger constellations, other approaches should be considered, such as security at a higher layer (e.g., Network or Application Layer).

2.3.2 SECURITY OBJECTIVES AND CORRESPONDING USER SERVICES

The CCSDS SDL protocols provide a number of user services to different Service Data Units (SDUs) (reference [7]). The SDUs are the data that are delivered to the receiving user. Table 2-1 shows the services selected for protection with the SDLS protocol.

The word ‘Mandatory’ implies that a fully compliant implementation of the SDLS protocol supports the protection of all of those mentioned services. The user is free to use them or not.

The word ‘Optional’ implies that, for a given implementation of the SDLS protocol, the protection for the listed services may or may not be present.

Table 2-1: User Services

User Services		***Type of SDU***	***Protection by SDLS protocol***
TC Services	MULTIPLE ACCESS POINT (MAP) PACKET	PACKETS WITH AUTHORIZED PACKET VERSION NUMBER (PVN)	MANDATORY
	MAP ACCESS	VARIABLE-LENGTH PRIVATE DATA	MANDATORY
	VIRTUAL CHANNEL (VC) PACKET	PACKETS WITH AUTHORIZED PVN	OPTIONAL
	VC ACCESS (VCA)	VARIABLE-LENGTH PRIVATE DATA	OPTIONAL
TM Services	VC PACKET	PACKETS WITH AUTHORIZED PVN	MANDATORY
	VCA	VARIABLE-LENGTH PRIVATE DATA	MANDATORY
AOS Services	VC PACKET	PACKETS WITH AUTHORIZED PVN	MANDATORY
	VCA	VARIABLE-LENGTH PRIVATE DATA	MANDATORY
	BITSTREAM	BISTREAM	OPTIONAL
	INSERT	SHORT FIXED-LENGTH DATA	NOT SUPPORTED
USLP Services	MAP Packet	Packets with authorized PVN	Mandatory
	MAP Access	Variable-length private data	Mandatory
	MAP Octet stream	Octet stream	Mandatory
	Insert	Short fixed-length data	Not supported
	MC_OCF	Fixed-length data	Not supported
	VC Frame	Transfer frame	Not supported
	MC Frame	Transfer frame	Not supported

Security objectives have been analyzed and determined for both uplink and downlink space-to-ground links. The following security objectives have been established for uplink (TC, AOS, USLP):

- command authentication, which ensures that the spacecraft can validate that the command is originating from the genuine source (i.e., the authorized mission control center);
- command integrity, which ensures that random or malicious command manipulation will be detected;
- command confidentiality, which ensures only those authorized entities will be able to read the command (i.e., the right spacecraft);
- command anti-replay protection, which ensures previously recorded commands will not be used to attack the system.

For downlink (TM, AOS, USLP) the established security objectives are:

- TM data authentication, which ensures that the mission control center can validate that the telemetry is originating from the genuine source (i.e., the authorized spacecraft);
- TM data Integrity, which ensures that random or malicious telemetry manipulation will be detected;
- TM data confidentiality, which ensures only those authorized entities will be able to read the telemetry (i.e., the right mission control center);
- TM data anti-replay protection, which avoids the re-use of previously recorded telemetries to attack the system.

The Security Services that allow fulfilling above selected security objectives are the following:

- authentication, which provides authentication, integrity, and the anti-replay function, to be used on a space link when the data confidentiality is not required;
- encryption, which provides data confidentiality but no authentication or integrity;
- authenticated encryption, which is a combination of encryption and authentication, thus providing data confidentiality, data integrity, authentication, and anti-replay function.

2.3.3 COMPATIBILITY WITH SDL SERVICES

2.3.3.1 General

The SDLS standard has been developed for use with existing CCSDS TC, TM, AOS, and USLP SDL standards. Avoiding reengineering of those widely used SDL standards has been an overriding priority.

There are two key aspects that drive SDL compatibility:

- the extent to which SDL frame protocol data structures other than the SDU to be protected are impacted by SDLS and the consequences of such impact in SDL protocol processing;
- the distinction between frames that transport SDUs and those that do not—this case is only relevant for TC SDL.

2.3.3.2 Supported Services

Services that transport typical Application Layer SDUs like packets or variable-length private data (e.g., segments) can be protected with SDLS. The user can select among authentication, encryption, and authenticated encryption. A compromise was achieved with VC Frame Secondary Header service: only authentication is provided.

2.3.3.3 Excluded Services

Services that transport Transfer Frames or other auxiliary data (e.g., audio samples on AOS or USLP Insert, Master Channel Frame Secondary Header data on TM) produced elsewhere but multiplexed on the space link are not secured. Their security may be handled at their data source by applying standard Application Layer authentication or encryption methods (see references [10], [21], [33], and [34]).

Given the impact on current implementations or compatibility with SLE as well as the acceptable residual risk, a few specific services are not protected. This is the case for TM, AOS, and USLP services concerned with the Operational Control Field (OCF), which is actually a Protocol Data Unit (PDU).

Communications Operations Procedure (COP) Management is a particular case. Although it does not transport SDUs, its role is essential for sequence-controlled telecommand transmission. The residual risk remaining when not protecting the directives of this service (BC frames) is acceptable. In addition, provision of security would basically imply incompatibility with TC protocol and its implementations.

2.3.3.4 Summary

Table 2-2 contains a complete and exhaustive list of TM, TC, AOS, and USLP SDL services and their available protection.

Table 2-2: Summary of SDLS Services

SDL Protocol	Service	Service Data Unit	Authentication	Encryption	Authenticated Encryption
TM	VC Packet	Packets with authorized PVN	Protected	Protected	Protected
	VC Access	Variable-length private data	Protected	Protected	Protected
	VC_FSH	Fixed-length data	Protected	Not protected	Authentication only
	VC_OCF	Fixed-length data	Not protected	Not protected	Not protected
	VC Frame	Transfer Frame	Not protected	Not protected	Not protected
	MC_FSH	Fixed-length data	Not protected	Not protected	Not protected
	MC_OCF	Fixed-length data	Not protected	Not protected	Not protected
	MC Frame	Transfer Frame	Not protected	Not protected	Not protected
TC	MAP Packet	Packets with authorized PVN	Protected	Protected	Protected
	MAP Access	Variable-length private data	Protected	Protected	Protected
	VC Packet	Packets with authorized PVN	Protected	Protected	Protected
	VC Access	Variable-length private data	Protected	Protected	Protected
	COP Management	N/A[1]	Not protected[1]	Not protected[1]	Not protected[1]
	VC Frame	Transfer Frame	Not protected	Not protected	Not protected
	MC Frame	Transfer Frame	Not protected	Not protected	Not protected
AOS	VC Packet	Packet with authorized PVN	Protected	Protected	Protected
	Bitstream	Bit stream	Protected	Protected	Protected
	VC Access	Variable-length private data	Protected	Protected	Protected
	VC_OCF	Fixed-length data	Not protected	Not protected	Not protected
	VC Frame	Transfer Frame	Not protected	Not protected	Not protected
	MC Frame	Transfer Frame	Not protected	Not protected	Not protected
	Insert	Short fixed-length data	Not protected	Not protected	Not protected
USLP	MAP Packet	Packet with authorized PVN	Protected	Protected	Protected
	MAP Octet stream	Octet stream	Protected	Protected	Protected
	MAP Access	Variable-length private data	Protected	Protected	Protected
	MC_OCF	Fixed-length data	Not protected	Not protected	Not protected
	VC Frame	Transfer frame	Not protected	Not protected	Not protected
	MC Frame	Transfer frame	Not protected	Not protected	Not protected
	Insert	Short fixed-length data	Not protected	Not protected	Not protected

[1] COP-1 Control directives are transmitted as type-BC frames without any security protection.

2.3.4 COMPATIBILITY WITH SLE SERVICES

2.3.4.1 General

The currently defined and specified SLE services rely on their ability to identify and process SDL frames or parts of frames for further processing and transfer between the SLE end points.

The application of security services (e.g., confidentiality) at the SDL protocol with the new SDLS may impact the SLE services' ability to 'read' and process the SDL frames, and in turn, the SLE services' compatibility with SDLS.

The goal is to apply space data link security with SDLS only at the end points of the space end-to-end data link. In this way, mission-specific cryptographic functions needed to implement SDLS security services will be located at the spacecraft and the mission control center. Hence, SDLS should be transparent for SLE service processing.

In practice this approach requires keeping certain protocol data structures of SDL frames visible and unaltered by the security processing. Those SLE services for which the required SDL frame data is not visible due to alteration by SDLS will not be supported.

Some decisions like routing may be taken by the ground station SLE processing equipment without validating the integrity of the SDL frame protocol data structure. However, the risk brought by such an approach is acceptable, as discussed in 3.1.

2.3.4.2 Supported Services

The following service compatibility requirements were established:

- for TC Services, Forward Command Link Transmission Unit (F-CLTU) Service and Forward Telecommand Frames (F-TCF) Service need to be compatible;
- for TM/AOS/USLP Services, Return All Frames (RAF), Return Channel Frames (RCF), and Return OCF need to be compatible.

These service compatibility goals can only be achieved if the full SDL frame header remains unaltered by the SDLS protocol.

2.3.5 CRYPTOGRAPHIC ALGORITHM SUPPORT

2.3.5.1 General

SDLS protocol is designed to be cryptographic-algorithms agnostic. Because cryptographic algorithms are subject to ongoing mathematical analysis to discover potential weaknesses (e.g., cryptanalysis) and are increasingly susceptible to exhaustive '*brute-force*' key attacks as computational resources multiply, it is desirable that the SDLS specification not require redefinition even if future discoveries of cryptographic weaknesses necessitate that CCSDS modify its baseline recommendations for authentication and encryption algorithms, as described in annex E of the SDLS Blue Book (reference [1]).

2.3.5.2 Authentication

Authentication primitives produce a Message Authentication Code (MAC) out of the input data as a result of a cryptographic operation with the selected cryptographic algorithm and a secret key. The SDU and additional SLP protocol data units or fields are the input data subject to authentication. Thus the MAC is generated and attached to the authenticated data as an additional protocol overhead.

In addition, to guarantee the 'freshness' of the authentication process (see *transaction authentication* in reference [8], chapter 9, definition 9.78), a critical requirement for space communications applications, the input data is jointly authenticated with a time-dependent data unit. It can be typically a counter or a time-stamp. The insertion of such time-dependent data elements as part of the message authentication is designated as *anti-replay*. In SDLS the preference is for a counter value labelled as the Sequence Counter.

Certain authentication algorithms require as well an IV as an input. Strictly speaking, its transmission would not be required but there are substantial implementation, operational, and robustness advantages if it is fully or partly transmitted.

Certain cipher-based authentication algorithms may require input data in multiples of a specified block length (e.g., Galois Message Authentication Code [GMAC]). If the input data is not a multiple, additional data is added to complete the last input block, i.e., the padding. The receiving end needs to identify the presence of padding and its length. Therefore SDLS includes the provision of protocol data unit fields for the transport of the MAC and the Sequence Counter as well as the optional IV and padding.

2.3.5.3 Encryption

Encryption primitives transform a block of plaintext data into ciphertext data. As explained elsewhere in this document, for reasons of compatibility with SLE and SDL services, only the SDU of the SDL protocol is subject to encryption.

While there are encryption algorithms that operate without an IV, e.g., Electronic Code Book (ECB), most secure encryption algorithms require an IV as input. Strictly speaking, its transmission would not be required, but there are substantial implementation, operational, and robustness advantages if it is fully or partly transmitted. Therefore SDLS includes the provision of a protocol data unit field for the transport of the optional IV.

It is important to note that the selection of encryption-only for a particular use case does not protect against malicious manipulation of data. Encryption used without authentication can provide a false sense of security, depending upon the specific implementation.

More specifically, 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. Selection of encryption-only should be done carefully after considering a mission-specific threat and risk analysis.

2.3.5.4 Authenticated Encryption

Authenticated encryption algorithms combine authentication and encryption algorithms with a single cryptographic key and algorithm. There are three generic compositions of authentication and encryption (reference [9]):

- Encrypt-then-MAC;
- MAC-then-Encrypt;
- MAC-and-Encrypt.

The SDLS is specified assuming the *Encrypt-then-MAC*, that is, at the source the SDU is first ciphered. Afterwards, the ciphered SDU together with certain SLP PDU fields is authenticated. In the receiving end the opposite order of operations takes place. The interested reader is referred to reference [9] for a thorough discussion of the security aspects of those compositions and in particular on the preference for the *Encrypt-then-MAC* composition.

Authenticated encryption algorithms represent an efficient alternative to the separate application of authentication and encryption algorithms. For this reason, they are extremely popular.

Furthermore, these algorithms offer the possibility to authenticate metadata accompanying the plaintext that is not encrypted (Additional Authenticated Data [AAD]). This is particularly useful to protect readable protocol data units against forgery.

Authenticated encryption is the CCSDS-recommended solution to provide authentication and confidentiality services to SLP SDUs and selected PDU fields.

Support for authenticated encryption algorithms may imply for SDLS the provision of protocol data unit fields for the transport of MAC, Sequence Counter, IV, and padding. However, certain authenticated encryption algorithms like AES-GCM (see baseline modes) work with a subset of those.

2.3.5.5 Authentication and Encryption

For missions that have specific security requirements, SDLS may accommodate separate authentication and encryption algorithms within certain constraints. Each algorithm would require its own cryptographic key as well as possibly its own parameters like IV, Sequence Counter, and padding.

It should be noted, however, that SDLS limits its provision to a single IV, single Sequence Counter, and single Padding field.

Furthermore, the Security Parameter Index (SPI) may constrain key management for each algorithm. Although a change of SPI could be used as a way to signal a key change, the SPI field is limited in length. Furthermore, cryptoperiods for the authentication and encryption key may differ, requiring additional SPI values.

The adequate selection of authentication and encryption algorithms that can be operated together (paired) requires knowledge of cryptography, which is beyond the scope of CCSDS (no such pairing recommendations are provided in reference [10] and, therefore, in this report or its related Blue Book, reference [1]). It is recommended that the user interested in such particular use of SDLS obtain adequate cryptographic expertise to pair authentication and encryption algorithms.

2.3.6 DECOUPLING OF SDL AND SDLS DATA INTEGRITY PERFORMANCE

When the authentication service is applied, the SDLS protocol protects against malicious attempts to manipulate the data or spoof the data source. The SDL protocol protects to a certain extent the data transactions against communications channel transmission errors.

For Failure Detection, Isolation, and Recovery (FDIR) and operational reliability, it is advisable that the integration of the SDLS and the SDL protocols is such that it allows an easy distinction and identification of the nature of errors (communications or security) when they manifest themselves. This is of particular concern for telecommand applications.

Theoretically, the efficiency of an authentication mechanism in detecting integrity errors on a message is much higher than classical communications integrity error detection mechanisms like the Cyclic Redundancy Check (CRC). The typically much greater length of the MAC compared to the CRC is the main reason for this.

The analysis provided in annex D shows that the undetected error performance of telecommand transfer using TC or USLP SDL protocol is sufficient as currently specified to allow for a discrimination of communications and security data integrity events.

For what concerns telemetry transfer using TM, AOS, or USLP, it is important to note that undetected error performance is dependent on the selected channel coding. In contrast to telecommand, there are more channel coding options available to implementers. Channel codes like Reed-Solomon (E=16) and Low Density Parity Check (LDPC) codes provide superb undetected error performance, thus ensuring excellent decoupling of transmission and security data integrity events. Further details can be found in annex D covering as well other channel codes.

2.4 REQUIREMENTS

The SDLS protocol has been specified to fulfil a set of well-identified requirements. The following is a selection of some key requirements. The complete set of requirements is found in annex C.

The Secure Space Data Link Protocol needs to support two operational modes for each logical communication channel managed over TC, TM, AOS, or USLP links:

- Clear Mode (or transparent mode) where the SDU is left unchanged but the SDLS protocol data fields are present;
- Secure Mode providing authentication, encryption, or authenticated encryption services.

The protocol needs to provide the capability to support independent secure channels. Thus clear and secure channels can coexist in a physical channel.

The detailed specification of a cryptographic key management supporting the SDLS security services is part of the extended services of the protocol (CCSDS SDLS Extended Procedures, reference [22]). The SDLS protocol is specified to accommodate the required level of flexibility. The SDLS protocol needs to be compatible with the following schemes for key management:

- Scheme 1: all session keys are preloaded on satellite before launch and cover the whole mission lifetime;
- Scheme 2: a subset of keys (master keys/Key Encryption Keys [KEKs] and session/traffic protection keys) are preloaded on satellite before launch; session keys are uploaded encrypted during satellite operation (Over The Air Rekeying [OTAR]);
- Scheme 3: a subset of keys (master keys/KEKs and session keys) are preloaded on satellite before launch; session keys are generated on board from master keys and an uploaded non-secret seed.

CCSDS has produced general documentation on key management (reference [11]). In addition, a key management service has been specified in SDLS Extended Procedures (see references [22] and [32]).

Concerning command and monitoring, the SDLS protocol needs to support a set of on-board Security Function control directives managed either as in-band commands (i.e., interpreted and executed internally by the security device immediately after the authentication/decryption process) or out-of-band commands (executed at application level).

The data overhead is limited to 32 octets per Transfer Frame for the complete protocol.

No interference between frame verification by SDLS and validation by SDL protocol can occur.

3 DESIGN CONCEPTS

3.1 SECURITY SERVICES SELECTION

3.1.1 GENERAL

This section presents the rationale for the selection of the agreed security services (authentication, confidentiality, integrity, and combinations thereof). The selected security services are taken out of the ISO OSI Security Architecture (reference [12]). Two elements need to be taken into account for the selection: the performance of the selected services and the residual risks for not implementing a security service.

Among the link layers protected by SDLS, TC and USLP are the protocols that include an optional retransmission mechanism (COP-1 or COP-P). The mechanism relies on state machines at both ends of the link and a corresponding set of directives. Some of these directives are transmitted from ground to space in order to allow for the remote control of the flight segment state machine. These directives are formatted in TC and USLP frames and are labelled BC frames. These directives do not transport SDUs.

Maintaining a separation between transmission control and security is considered essential as the security layer needs to work on an error-free frame. Therefore the directives to ensure a reliable transmission cannot be secured.

Furthermore, because the VC_OCF is an SDU inserted in TM, AOS, and USLP frames to support link layer operations like the COP, its protection cannot be taken into account by SDLS.

More specifically, the reasons why the COP Management Service (TC, USLP) and the OCF Service (TM, AOS, USLP) are not protected by SDLS, are the following:

– SDLS function has to be applied to the Transfer Frame before the COP function at the sending end, and after the COP at the receiving end (see figure 3-3). The reasons for that ordering are the following:

  • COP-1, being a go-back-*N* retransmission protocol, will eventually replay TC frames. SDLS is a function providing anti-replay protection, integrity, and confidentiality. Therefore if FOP is applied before SDLS at the sending end, and SDLS before FARM at the receiving end, SDLS at the receiving end will discard all replayed frames by COP-1, thus defeating the COP (and eventually blocking the link).

  • SDLS at the receiving end checks integrity of TC frames by checking the MAC. The MAC is a very powerful error detecting code (in fact much more powerful than the Bose-Chaudhuri-Hocquenhem [BCH] or short LDPC codes). Therefore, SDLS at the receiving end will discard all TC frames impacted by transmission errors, if the FARM is applied after SDLS. This has two impacts:

    - Accountability of transmission errors vs. security-related events cannot be achieved: some transmission errors are detected by SDLS and therefore classified as security events. Moreover, the Command Link Control Word (CLCW) is not updated, and therefore the COP at the sending end (FOP) is not informed of the reason why the frames are rejected.
    - COP-1 will replay those SDLS rejected frames, because the FARM will never see them.

- Given the mandatory order of processing at the sending end (SDLS before COP) and at the receiving end (COP before SDLS), COP commands cannot be protected, since they are generated and extracted respectively after and before SDLS is applied at both ends of the link. The same is true for the Frame Sequence Count field of the Frame Primary Header, since it is set by the COP at the sending end. It therefore cannot be authenticated.
- For the OCF Service, again the order of processing at the sending end makes it unpractical to protect the OCF: the interface to the SDLS function is either with the VC generation function or with the VC multiplexing function, in both cases before the MC_OCF is appended to the frame by the Master Channel Generation function.

Not protecting the COP commands and the OCF (i.e., CLCW and Frame Status Report [FSR]) has indeed implications as stated in annex subsection B1 (Security Considerations) of the SDLS Blue Book (reference [1]):

> 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.

Nevertheless, this residual risk was evaluated as acceptable operationally since the legitimate operator can always reinitialize the COP. Denial of service is only temporary and not so easy to implement in the first place.

The order of processing specified (‘SDLS then COP’ at the sending end and ‘COP then SDLS’ at the receiving end) (see figure 3-3) can prevent in specific scenarios correct operation of the COP when used with TC SDL protocol or USLP. It corresponds to operational scenarios where a sequence of AD frames (i.e., sequence controlled by the COP) is followed by BD-frames (Bypass, i.e., not sequence controlled). If one of the AD-frames is rejected by the COP due to undetected transmission error, and is followed by a BD-frame (which bypasses the COP), SDLS will accept the BD frame (provided its Anti-Replay Sequence Number (ARSN) window is sufficiently large) but reject all the AD frames retransmitted by the COP (because of an invalid ARSN: only up-counting ARSNs are allowed). Whenever Type-AD and Type-BD frames are mixed on the same VC, then the SDLS *ProcessSecurity* Anti-Replay function will reject retransmitted frames older that the last accepted Type-BD frame. This is due to their lower anti-replay sequence count in comparison to the Type-BD anti-replay sequence count. As a result, they are falsely

labelled as SDLS security failures. Therefore mixing Type-AD and Type-BD frames on the same VC secured by SDLS is generally not advised while acceptance of Type-AD frames is pending.

In AOS and USLP, the Insert Zone is added to the Transfer Frame shortly before transmission when the frame has already been constructed. Thus there is no opportunity to secure this portion of the frame. If the Insert Zone needs to be protected, it has to be done at the source by the user.

The SDLS protocol works only on Virtual Channels. Therefore Master Channel services, such as MC_FSH and the MC_OCF, cannot be secured.

VCs that carry Only Idle Data (OID) Frames are not protected for the following reasons:

- The functional/physical location where OID frames are generated and inserted on the sending side and identified and extracted on the receiving side may not be the same as where security is processed.
- Repetitive patterns in cleartext messages can potentially ease cryptanalysis and, therefore, introduce a vulnerability.
- Exposure of OID Frames only leaks traffic and activity patterns in the spacecraft operation and communication; risks of such exposure are considered acceptable for the scope of this SDLS protocol.

Security services can be applied individually or combined (i.e., authenticated encryption) as discussed in 2.3.5.5.

3.1.2 THREAT ANALYSIS

3.1.2.1 Trust between CCSDS Agencies

Trust between participating CCSDS Agencies is a fundamental pillar for interoperability and is taken for granted when CCSDS Agencies exchange data. While certain SDLS security services like authentication can provide protection against threats like malicious data manipulation along the end-to-end data path, it is not the goal of the SDLS protocol to protect against a CCSDS agency that intends to apply malicious action to the communications services provided to another CCSDS agency. Thus malicious denial-of-service attacks or data manipulation by an Agency are not threats considered in this analysis.

3.1.2.2 Threats

In general, protecting SDUs carried by the SDL protocols in a space link will imply ensuring the confidentiality, integrity, and availability of these SDUs as required by the user.

Threats to confidentiality and integrity are within the scope of the attacks that the SDLS needs to protect. The SDLS constitutes the countermeasure against those threats. The effectiveness to which the SDLS protects against those attacks will depend on various factors, such as the selected cryptographic algorithm, the choice of cryptographic key, and protocol parameters and their implementation.

Threats to the availability of the space link, however, are excluded. Protection against availability threats, like radio-frequency jamming, signal reception blocking, or denial-of-service attacks at the data level by engaging the SDL protocol processors with unwanted data-modulated signals, is not within the scope of the SDLS protocol. Protection against those threats requires counter-measures, such as cryptographic spread-spectrum modulation, which are applied at the Physical Layer of the CCSDS protocol stack and are therefore beyond the scope of SDLS.

3.1.2.3 Relationship with ISO Security Architecture

The ISO Security Architecture (reference [12]) establishes the optional security services, and some of the security mechanisms to implement them, that can be provided optionally within the framework of the OSI reference model.

It is interesting to note that the ISO Security Architecture postulates that the only security services that can be provided at the Data Link Layer of the OSI reference model are connection confidentiality and connectionless confidentiality. In contrast, SDLS implements additional security services like authentication that, according to the OSI security architecture, should only be implemented at the Network Layer and above.

The analysis of the OSI security services applicable to SDL protocol and its data services is provided in annex B. Out of this analysis, the security services shown in table 3-1 have been adopted.

Table 3-1: OSI Security Services vs. SDLS

OSI Security Services		SDLS	Remarks
Authentication			
	Peer entity authentication	Not adopted	Too complex
	Data origin authentication	Adopted	TC, TM, AOS, and USLP
Access Control		Not adopted	Relevant for TC, residual risk mitigated
Data Confidentiality			
	Connection confidentiality	Adopted	TC only
	Connectionless confidentiality	Adopted	TC, TM, AOS, and USLP
	Selective field confidentiality	Not adopted	
	Traffic flow confidentiality	Not adopted	
Data integrity			
	Connection integrity with recovery	Adopted	TC only
	Connection integrity without recovery	Adopted	TC, TM, AOS, and USLP
	Selective field connection integrity	Not adopted	
	Connectionless integrity	Adopted	TC, TM, AOS, and USLP
	Selective field connectionless integrity	Not adopted	
Non-repudiation			
	Non-repudiation with proof of origin	Not adopted	
	Non-repudiation with proof of delivery	Not adopted	

3.1.2.4 Residual Risks

The decision not to protect TC control frames (BC) implies that an attacker could access and disrupt the operation of the COP leading to a denial of service. However, these are the only types of frames that can be transmitted by an attacker and successfully received on board. The service can be recovered once the legal operator has the opportunity to reset the COP. Resetting the COP mitigates this residual risk.

Protection against Traffic Analysis would imply the encryption of all SDL protocol data structures. Given its negative implications on compatibility with both SLE services and SDL protocols, because of the inability of the corresponding SLE service and SDL protocol processors to ‘read’ and process the affected protocol data structures, protection against Traffic Analysis has not been considered a security objective to be covered by SDLS. This

decision brings a residual security risk, which was considered acceptable for the intended clientele of the CCSDS SDLS protocol. Missions that require protection (encryption) of all protocol data structures need to consider the application of bulk-encryption techniques (see reference [13]).

Demultiplexing is carried out at the ground station based on protocol fields like the VCID that have not yet been authenticated at that location. The risk of malicious manipulation of any of the relevant fields cannot be excluded before demultiplexing. However, for a VC that has implemented SDLS, the end processor, located at the mission control, will detect this manipulation and will reject the attack.

3.1.3 BASELINE SECURITY SERVICES

The security services shown in table 3-2 have been adopted for SDLS.

Table 3-2: Baseline SDLS Security Services

SDLS Security Services		Remarks
Authentication		
	Data origin authentication	TC, TM, AOS, and USLP
Data Confidentiality		
	Connection confidentiality	TC only
	Connectionless confidentiality	TC, TM, AOS, and USLP
Data integrity		
	Connection integrity with recovery	TC only
	Connection integrity without recovery	TC, TM, AOS, and USLP
	Connectionless integrity	TC, TM, AOS, and USLP

3.2 SECURITY ASSOCIATION

3.2.1 CONCEPT

The concept of Security Association (SA), borrowed from IPSec (reference [14]) but somewhat adapted to space communications, is crucial to the SDLS protocol. The following paragraphs, excerpts from reference [1], provide a detailed description.

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. An SA defines a simplex (one-way), stateful cryptographic session for providing authentication, data integrity, replay protection, and/or data confidentiality.

3.2.2 OPERATION

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 Security Association to another is part of the Extended Procedures (reference [22]).

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 Multiple Access Points (MAPs, for TC and USLP only) assigned to an SA at the time of its creation.

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 physical channel share a single SA. A maximum of 2^{16} simultaneous SAs may be defined across an entire physical channel.

When an SA is created, one of the following cryptographic functions are selected to be carried out 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.

3.2.3 RATIONALE

The notion of SA parameter negotiation before establishing a secure channel, a common practice in terrestrial networks, is considered to be too complex. On many occasions this is not feasible given the available time to establish communications between mission control center and spacecraft (e.g., short contact times, latency due to distance).

In addition, space links are by nature very asymmetrical:

- the ground control center wants to retain full authority (master) over the on-board system (slave) when needed;
- the on-board data system is limited in terms of processing power and anomaly handling.

Some of those parameters, like the choice of cryptographic algorithms, are simply excluded from negotiation (preselected and coded before mission operations start).

Similarly, the notion of an SA database as understood in IPSec is an unaffordable or unneeded luxury for most space communications applications. Therefore a simpler concept than the IPSec-like SA database, called Security Association Context (SAC), has been defined in the CCSDS SDLS protocol development.

3.2.4 SECURITY ASSOCIATION CONTEXT

The SAC pre-exists on board and in the control center. This managed parameter establishes the set of Global Virtual Channel IDs (GVCIDs) and/or Global MAP IDs associated with a given SA. No negotiation is needed before use of a given SA/SAC.

3.2.5 AUTHENTICATION BIT MASK

The authentication bit mask is a mechanism to enforce the inclusion or exclusion of fields during the authentication process. It provides some flexibility to extend and adjust selectively the protection provided by an authentication algorithm beyond the Transfer Frame Data Field, the SDLS Security Header, and the Frame Header fields that uniquely identify a virtual channel. However, such flexibility needs to respect certain constraints imposed by the SDL protocol.

An SA providing authentication 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 Master Channel Frame Count (TM only), optional Insert Zone (AOS and USLP only), optional 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 and the Segment Header (TC and USLP only), since those fields uniquely identify, respectively, the virtual channel and the MAP (TC and USLP only), the Security Header (except for the Initialization Vector), and the Transfer Frame Data Field.

A default configuration of the authentication bit mask is provided by the standard considering the protection of the complete identification of the VCs to which the SA applies as well as the SDLS Security Header and the Transfer Frame Data Field. The Spacecraft ID is not part of this default authentication bit mask because it is already checked by the frame validation process before SDLS is applied at the receiving end.

Additional fields can be protected. For instance, a mission may want to protect its VC_FSH if it carries sensitive data.

3.3 PROTOCOL POSITION IN CCSDS

3.3.1 GENERAL

The objective of the SDLS protocol development is to add a security function at the Data Link Layer of space links using one of the CCSDS SDL protocols, namely: TM (reference [4]), TC (reference [5]), AOS (reference [6]), or USLP (reference [31]). The relationships between CCSDS protocol layers and those of the OSI model (reference [12]), together with the position of the SDLS security functions, are depicted in figure 3-1.

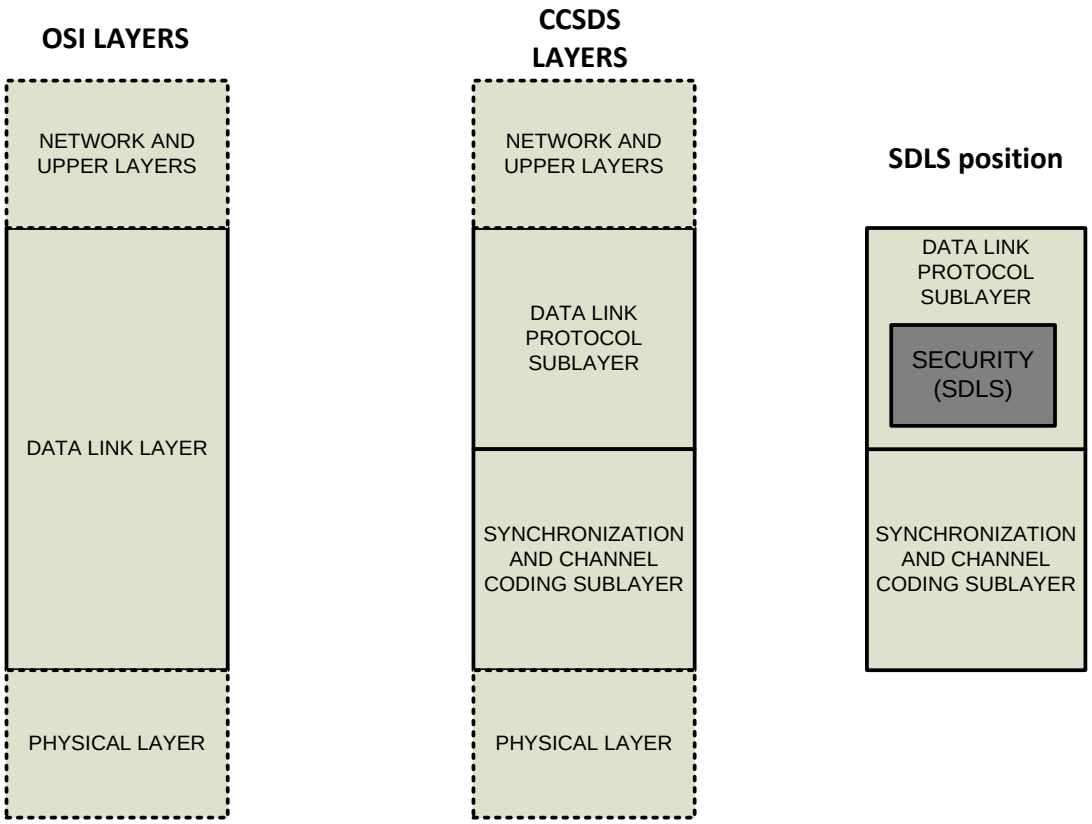


Figure 3-1: OSI vs. CCSDS Layers and SDLS Security Functions Position

Two sublayers of the Data Link Layer are defined for CCSDS SDL protocols: a data link protocol sublayer, and a synchronization and channel coding sublayer. The SDLS protocol and functions are part of the CCSDS data link protocol sublayer and are fully integrated in the TC, TM, AOS, and USLP SDL protocols. The SDLS functions insert themselves inside the stack of functions of CCSDS SDL protocols. The *ApplySecurity* Function is defined for the sending end of a physical channel and the *ProcessSecurity* Function is defined for the receiving end. These generic security functions include authentication and/or encryption functions as required by the specified security services. The SDLS protocol is not as such a distinct sublayer but rather a set of additional security features for existing SDL protocols. Each of those SDL protocols provides a set of communication services. SDLS protects only part of those services, as shown in table 2-2.

3.3.2 TELECOMMAND

The conceptual order of processing of SDLS functions with respect to other functions of the TC protocol is shown in figure 3-2. Depending on the services actually used, not all the functions may be present in a real system. The services not supported by SDLS protocol are greyed out in figure 3-2. The *ApplySecurity* function includes authentication and/or encryption according to the SA.

The Encryption function, when implemented and selected in a given SA, processes the full data field of the TC frame, providing confidentiality to its content, i.e., TC packets and/or TC segments. TC Transfer Frame Header, COP management commands, and Frame Error Control Field (FECF) are not encrypted, to maintain compatibility with existing infrastructure and protocols (e.g., some SLE protocols services (reference [3]) that require a cleartext header for ground routing of TC frames).

The Authentication function, when implemented and selected in a given SA, processes the full TC Transfer Frame apart from the optional FECF and user selected subfields of the Transfer Frame Header. It therefore provides integrity and authenticity verification on selected subfields of the Transfer Frame Header as well as the data field. FECF and TC channel coding (BCH code) are used to detect transmission errors, while authentication is used to detect security (intentional) errors.

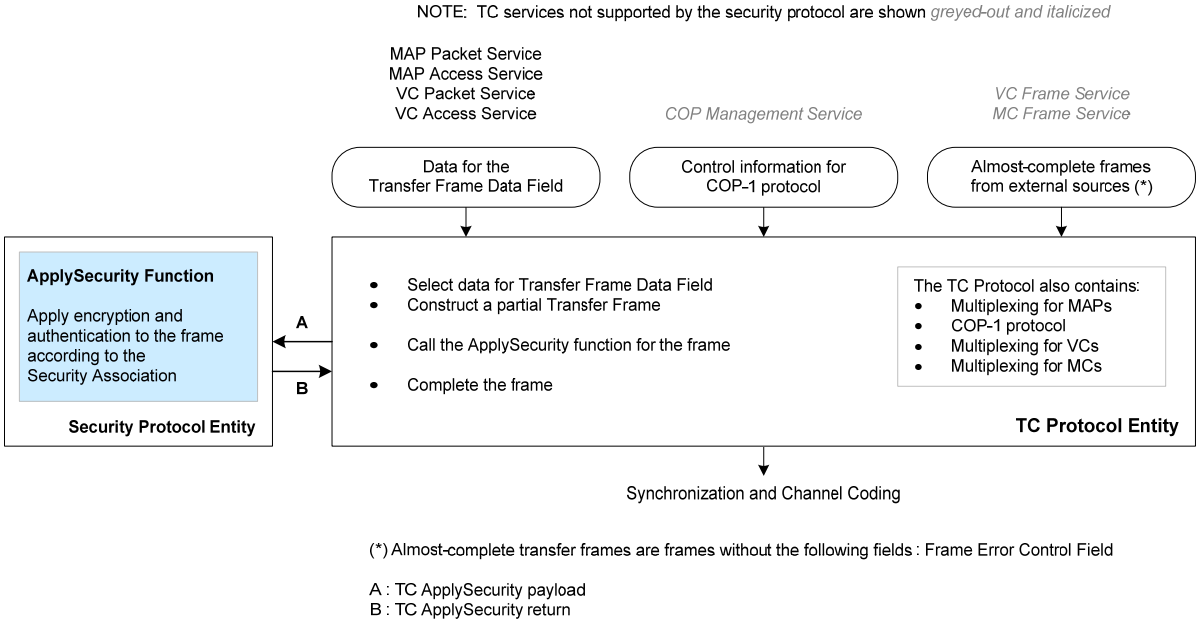


Figure 3-2: Functional Interface within TC Protocol

The definition of the SDLS functional interface point for TC is particularly involved. The TC protocol can provide a guarantee of delivery. The Command Operations Procedure-1 (COP-1), with corresponding state machines Frame Operations Procedure-1 (FOP-1) (on ground) and Frame Acceptance and Reporting Mechanism-1 (FARM-1) (on spacecraft), implements a retransmission loop in case of a failed transmission (reference [15]). In order to maintain the decoupling between transmission control and security services control, fundamental for reliable operations, it is necessary to place the interface point at the VC generation function.

The placement for the interface and the order of processing between TC SDL and SDLS functions are shown in figure 3-3 and detailed step by step in table 3-3. As implied by the figure, before security can be applied on the sending end, certain procedures of the VC generation function need to be executed. Once those have been performed, the telecommand payload can be delivered to the SDLS *ApplySecurity* function. The function returns the corresponding security header, trailer (if authentication is required), and partially ciphered Transfer Frame Data Field (if encryption is required). The security header is part of the Transfer Frame Data Field but is not ciphered.

At this point the VC generation function completes the frame generation for the particular VC where SDLS is being implemented, including the COP-1 FOP. The FOP sets the Frame Count field of the Frame Primary Header. Therefore this Frame Count field cannot be authenticated by SDLS. Further downstream processing includes the multiplexing with other VCs, eventually with other Master Channels (MCs), and the computation of the FECF as well as the construction of the Command Link Transmission Unit (CLTU).

At the receiving end the operations are inverted. Following CLTU decoding and frame verification and FARM of the COP-1, the relevant elements of the frame are delivered by the Virtual Channel Reception (VCR) function to the SDLS *ProcessSecurity* function for execution of the security services. The function returns a Verification Status Code as well as the corresponding SDU.

NOTE – Whenever Type-AD and Type-BD frames are mixed on the same VC, then the SDLS *ProcessSecurity* Anti-Replay function will reject retransmitted frames older that the last accepted Type-BD frame. This is due to their lower anti-replay sequence count in comparison to the Type-BD anti-replay sequence count. As a result, they are falsely labelled as SDLS security failures. Therefore, mixing Type-AD and Type-BD frames on the same VC secured by SDLS is generally not advised while acceptance of Type-AD frames are pending.

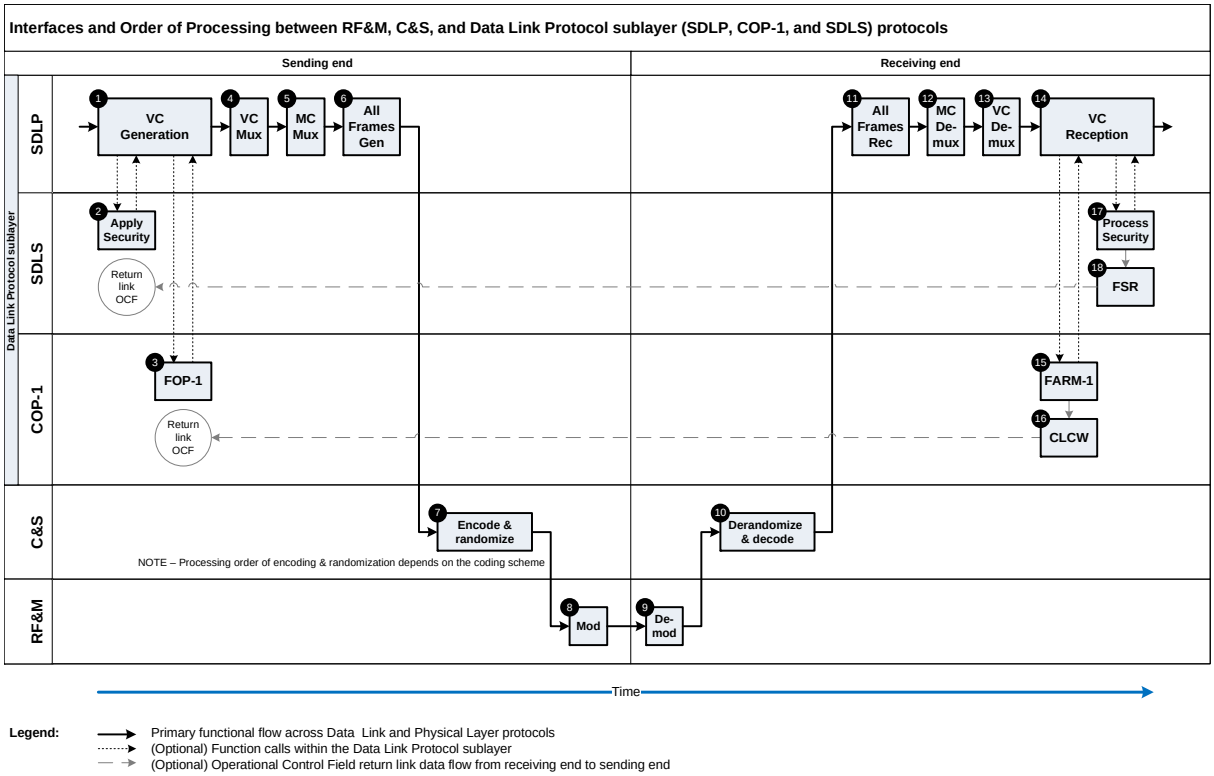


Figure 3-3: Order of Processing between TC SDL and SDLS Functions

Table 3-3: Detailed Order of Processing between TC SDL and SDLS Functions

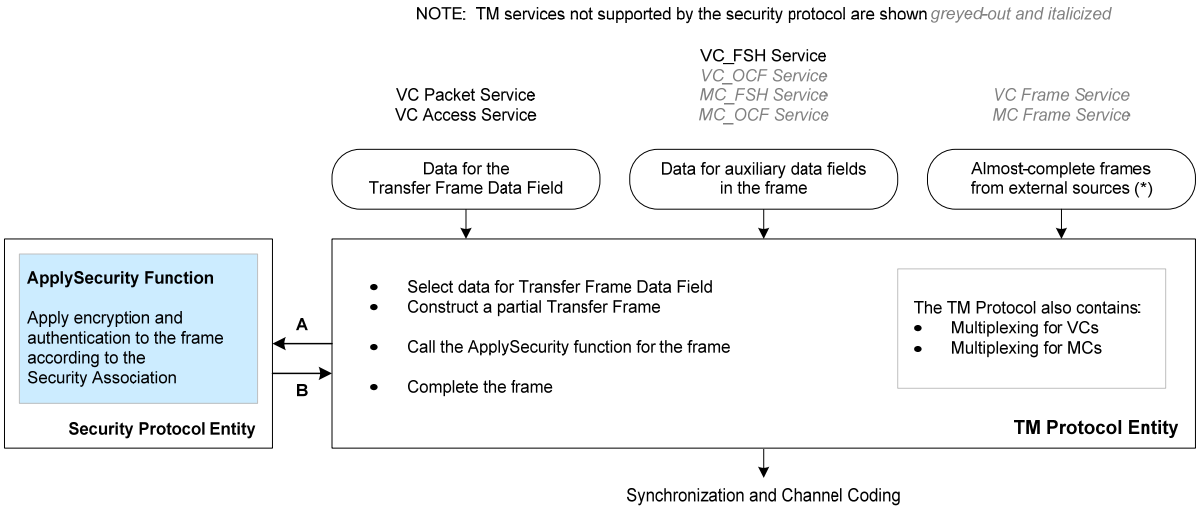
On the Ground: (sending end)		
Numbered Step in figure 3-3	CCSDS Document Number	Section Referenced
1. Virtual Channel Generation Function with SDLS	232.0-B-3	6.4.2.1
Frame Initialization Procedure: The Frame Initialization Procedure generates a (partial) TC Transfer Frame for the Frame Data Unit. The (partial) frame includes the Transfer Frame Primary Header, provision for the Security Header, Transfer Frame Data Field, and, optionally, the Security Trailer.	Future 232.0-B-3	6.4.2.1
2. SDLS *ApplySecurity* Function	232.0-B-3	6.4.2.1 (b)
Encrypt only the Transfer Frame Data Field	355.0-B-1	4.2.3.3
Populate the Security Header and the optional Security Trailer with the computed MAC (Authentication only) (note)	355.0-B-1	4.2.3.4
3. FOP-1	232.0-B-3	4.3.5.3
Frame Finalization Procedure (within VC Generation Function)	232.0-B-3	4.3.5.4
4. Virtual Channel Multiplexing Function	232.0-B-3	4.3.6
5. Master Channel Multiplexing Function	232.0-B-3	4.3.7
6. All Frames Generation Function	232.0-B-3	4.3.8
Compute and add CRC to FECF	232.0-B-3	4.3.8.2
7. Encode & Randomize the Transfer Frame (when BCH encoding, randomization is done first; the opposite for LDPC)	231.0-B-3	3 (BCH) or 4 (LDPC); 6
8. Modulate onto Subcarrier/Carrier and transmit	401.0-B-31	2.2
NOTE – MAC (authentication) is computed over masked Transfer Frame Header, complete Security Header, and complete Frame Data Field.		
Space Link *On the Spacecraft: (receiving end)*		
9. Receive and Demodulate	401.0-B-31	2.2
10. Decode & Derandomize the Transfer Frame (the order is dependent upon the coding scheme)	231.0-B-3	6.3,3.5 or 4.5
11. All Frames Reception Function with SDLS	232.0-B-3	6.5.2.1 (c)
Frame Delimiting and Fill Removal Procedure (invalid code blocks reported by C&S sublayer + fill removal)	232.0-B-3	4.4.8.2
Frame Validation Check Procedure (includes optional CRC)	232.0-B-3	4.4.8.3
12. Master Channel Demultiplexing Function	232.0-B-3	4.4.7
13. Virtual Channel Demultiplexing Function	232.0-B-3	4.4.6
14. Virtual Channel Reception Function	232.0-B-3	4.4.5
15. FARM-1 (subprocedure of the COP-1)	232.0-B-3	4.4.5.2
16. CLCW appears within either TM, AOS, or USLP OCF Field	232.0-B-3	4.4.5.2
17. SDLS *ProcessSecurity* Function	232.0-B-3	6.5.2.1 (b)
Optional: Validate the MAC; if invalid, report security error in Frame Status Report into the OCF in telemetry frame	355.0-B-1	4.2.4.4
Decrypt the Transfer Frame Data Field	355.0-B-1	4.2.4.5
18. SDLS FSR appears within either TM, AOS, or USLP OCF Field	132.0-B-3 732.0-B-3 732.1-B-2	4.1.5.5 4.1.5.5 4.1.5.2.2
Thereafter, Frame Data Units provided to on-board processing (i.e., perform VC Packet Extraction function or MAP Demultiplexing function or VCA Service User)		

3.3.3 TELEMETRY

The conceptual order of processing of SDLS functions with respect to other functions of the TM protocol is shown in figure 3-4. Depending on the services actually used, not all the functions may be present in a real system. In this figure, the services not supported by SDLS protocol are greyed out.

The Encryption function, when implemented and selected in a given SA, processes the full data field of the TM Transfer Frame apart from the OCF, Frame Secondary Header (FSH), and FECF. It provides confidentiality to its content: i.e., TM packets. The TM Transfer Frame Primary Header and Secondary Header together with OCF are not encrypted, to maintain compatibility with existing infrastructure and protocols (e.g., TC protocol, reference [5], which requires a cleartext OCF for operating the TC retransmission protocol, COP-1).

The Authentication function, when implemented and selected in a given SA, processes the full TM Transfer Frame apart from the optional FECF, the optional OCF, and user selected subfields of the Transfer Frame Header. It therefore provides integrity and authenticity verification on selected subfields of the Transfer Frame Header as well as the data field. FECF and TM channel coding (e.g., Reed-Solomon code) are used to detect transmission errors, while authentication is used to detect security (intentional) errors. The OCF was excluded from the authenticated fields since, in most implementations, the TC retransmission protocol (COP-1) has to extract and use it before authentication can be performed on the ground.



(*) Almost-complete transfer frames are frames without the following fields : Master Frame Count, Operational Control Field, Frame Error Control Field

A : TM ApplySecurity payload
B : TM ApplySecurity return

Figure 3-4: Functional Interface within the TM Protocol

The SDLS *ApplySecurity* Function may interface with the TM SDL protocol at either the Virtual Channel Generation Function or the Virtual Channel Multiplexing Function. The choice of where to apply security within the TM Data Link Layer depends upon several factors, such as the number of SAs, their type (one VC or more than one VC per SA) and the corresponding source and termination of the security function(s), key management, and the use of the anti-replay feature.

There can be security configurations in which, for example, one or several SAs covering just one VC each are present. The physical location of the security processing may not be the same for all VCs, at the sending end or at the receiving end. This case can be supported by placing the SDLS interface in the Virtual Channel Generation Function where the greatest flexibility in managing the security function occurs.

Conversely, with the SDLS interface in the Virtual Channel Multiplexing Function, the security configuration can include multiple Virtual Channels (not necessarily all) sharing an SDLS SA. The call to the SDLS *ApplySecurity* function follows the VC multiplexing, so that the SDLS processing is applied to the multiplexed stream of frames.

3.3.4 ADVANCED ORBITING SYSTEMS

AOS protocol can be used with SDLS both on the uplink and the downlink. The conceptual order of processing of SDLS functions with respect to other functions of the AOS protocol is shown in figure 3-5. Depending on the services actually used, not all the functions may be present in a real system. In this figure, the services not supported by SDLS protocol are greyed out.

The Encryption function, when implemented and selected in a given SA, processes the full data field of the AOS Transfer Frame apart from OCF and FECF. It provides confidentiality to its content, i.e., Application Layer data (Transfer Frame Data Field). The AOS Transfer Frame Primary Header together with OCF and FECF are not encrypted, to maintain compatibility with existing infrastructure and protocols (e.g., TC protocol, reference [5], which requires a cleartext OCF for operating the TC retransmission protocol, COP-1).

The Authentication function, when implemented and selected in a given SA, processes the full AOS Transfer Frame apart from the optional FECF, the optional OCF, the Insert Zone, and user selected subfields of the Transfer Frame Primary Header. It therefore provides integrity and authenticity verification on selected subfields of the Transfer Frame Primary Header as well as the Transfer Frame Data Field. FECF and TM channel coding (e.g., LDPC or Reed-Solomon codes) are used to detect transmission errors, while authentication is used to detect security (intentional) errors. The OCF was excluded from the authenticated fields since, in most implementations, the TC retransmission protocol (COP-1) has to extract and use it before authentication can be performed on the ground.

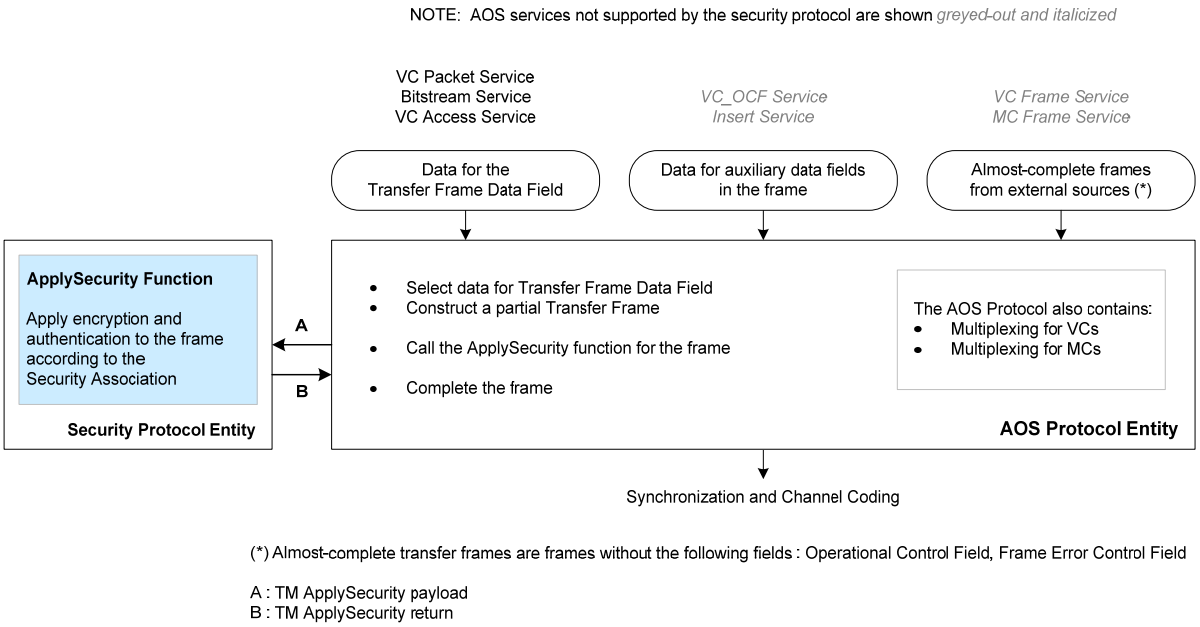


Figure 3-5: Functional Interface within the AOS Protocol

The Insert Zone is not authenticated because this field is physically inserted on the fly when the frame is shifted to the modulator to preserve synchronicity of data transmitted in the Insert Zone. It is therefore impractical to authenticate this field. The application behind the Insert Zone service needs to incorporate its specific security, if required.

The SDLS *ApplySecurity* Function may interface with the AOS SDL protocol at either the Virtual Channel Generation Function or the Virtual Channel Multiplexing Function. The choice of where to apply security within the AOS Data Link Layer depends upon several factors, such as the number of SAs, their type (one VC or more than one VC per SA), and the corresponding source and termination of the security function(s), key management, and the use of the anti-replay feature.

There can be security configurations in which, for example, one or several SAs covering just one VC each are present. The physical location of the security processing may not be the same for all Virtual Channels, at the sending end or at the receiving end. This case can be supported by placing the SDLS interface in the Virtual Channel Generation Function where the greatest flexibility in managing the security function occurs.

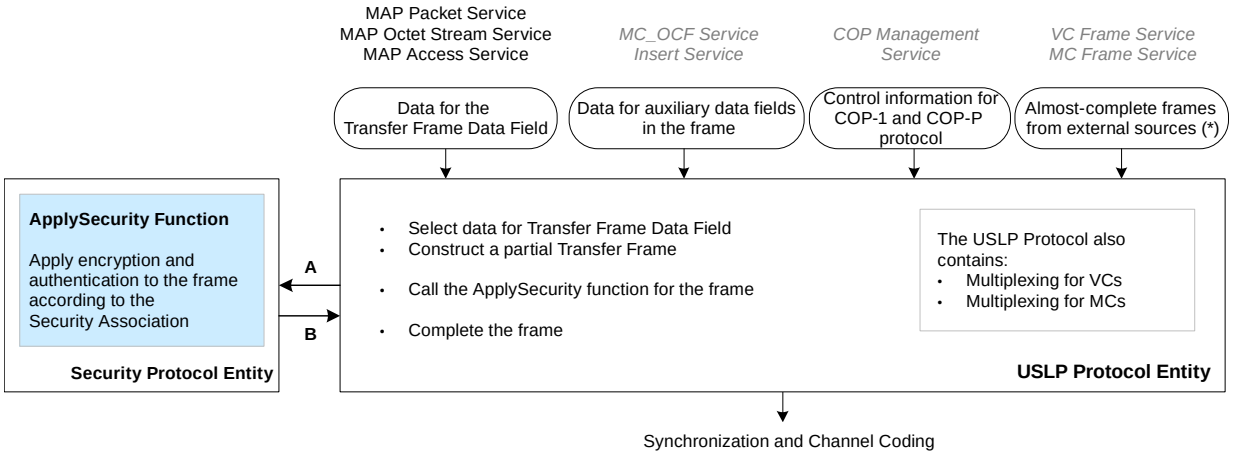
Conversely, with the SDLS interface in the Virtual Channel Multiplexing Function, the security configuration can include multiple Virtual Channels (not necessarily all) sharing an SDLS SA. The call to the SDLS *ApplySecurity* function follows the Virtual Channel multiplexing, so that the SDLS processing is applied to the multiplexed stream of frames.

3.3.5 UNIFIED SPACE LINK PROTOCOL (USLP)

USLP can be used with SDLS both on the uplink and the downlink. The conceptual order of processing of SDLS functions with respect to other functions of USLP (reference [31]) is shown in figure 3-6. Depending on the services actually used, not all the functions may be present in a real system. In the figure, the services not supported by SDLS protocol are greyed out.

The Encryption function, when implemented and selected in a given SA, processes the full data field of the USLP Transfer Frame apart from OCF and FECF. It provides confidentiality to its content, that is, Application Layer data (Transfer Frame Data Field). The USLP Transfer Frame Primary Header together with OCF and FECF are not encrypted to maintain compatibility with existing infrastructure and protocols (e.g., TC protocol, reference [5], which requires a clear text OCF for operating the TC retransmission protocol [COP]).

The Authentication function, when implemented and selected in a given SA, processes the full USLP Transfer Frame apart from the optional FECF, the optional OCF, the Insert Zone, and user-selected subfields of the Transfer Frame Primary Header. It therefore provides integrity and authenticity verification on selected subfields of the Frame Primary Header as well as the Frame Data Field. FECF and TM channel coding (e.g., LDPC or Reed-Solomon codes) are used to detect transmission errors, while authentication is used to detect security (intentional) errors. OCF was excluded from the authenticated fields since, in most implementations, the TC retransmission protocol (COP) has to extract and use it before authentication can be performed on the ground.



(*) Almost-complete transfer frames are frames without the following fields: Operational Control Field, Frame Error Control Field

A: USLP ApplySecurity payload
B: USLP ApplySecurity return

NOTE – USLP services not supported by the security protocol are shown *greyed-out and italicized*.

Figure 3-6: Functional Interface within the USLP Protocol

The Insert Zone is not authenticated as well because this field is physically inserted on the fly when the frame is shifted to the modulator to preserve synchronicity of data transmitted in the Insert Zone. It is therefore impractical to authenticate this field. The application behind the Insert Zone service will have to incorporate its specific security, if required.

The SDLS *ApplySecurity* Function may interface with USLP at either the Virtual Channel Generation Function or the Virtual Channel Multiplexing Function. The choice of where to apply security within the USLP Data Link Layer depends upon several factors such as the number of SAs, their type (one VC or more than one VC per SA), and the corresponding source and termination of the security function(s), key management, and the use of the anti-replay feature.

There can be security configurations in which, for example, one or several SAs covering just one VC each are present. The physical location of the security processing may not be the same for all Virtual Channels, at the sending end or at the receiving end. This case can be supported by placing the SDLS interface in the Virtual Channel Generation Function where the greatest flexibility in managing the security function occurs.

Conversely, with the SDLS interface in the Virtual Channel Multiplexing Function, the security configuration can include multiple Virtual Channels (not necessarily all) sharing an SDLS Security Association. The call to the SDLS *ApplySecurity* function follows the Virtual Channel multiplexing, so that the SDLS processing is applied to the multiplexed stream of frames.

NOTE – When USLP Space Data Link Protocol uses the COP-1 or COP-P retransmission protocol, the order of processing between SDLS function and USLP functions needs to be the same as the one specified for the TC Space Data Link Protocol (see 3.3.2).

3.4 PROTOCOL DATA STRUCTURES, FIELDS, AND FUNCTIONS

3.4.1 GENERAL

The SDLS encapsulates processed Application Layer data (Transfer Frame Data Field) carried in SDL protocol Transfer Frames between two protocol data structures: a Security Header and Trailer. While in theory such a protocol can be designed with just one additional protocol data structure (a header or a trailer), the provision of two protocol data structures allows optimization of implementations, particularly for very high data rate application.

The Security Header and Trailer contain the contextual information necessary to perform decryption and/or integrity verification at the receiving end. This contextual information does impose some additional transmission overhead; the sender must ensure that the overall length of the Transfer Frame does not exceed the maximum allowed by the underlying SDL protocol. The amount of overhead depends upon the options chosen for each SA.

3.4.2 SECURITY HEADER

3.4.2.1 General

The structural components of the Security Header are shown in figure 3-7. The actual specification of the Security Header is defined in reference [1].

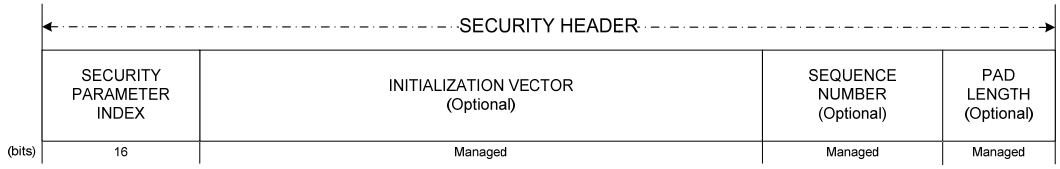


Figure 3-7: Security Header

The Security Header contains a mandatory two-octet SPI identifying the Security Association context.

For SAs that employ encryption (cipher) or certain authentication (e.g., GMAC) algorithms, the Security Header includes optional fields for initialization vector and pad length. These fields may or may not be needed depending upon the specific algorithm and mode of operation implemented. Fields that are not needed for a Security Association may be omitted, but if present must remain present in all frames using that Security Association.

For SAs that employ authentication algorithms, the Security Header includes an optional field for an anti-replay sequence number. Since replay protection is easily defeated unless the sequence number is protected, this field is used only where authentication is used.

3.4.2.2 Security Parameter Index

The SPI is a two-octet mandatory and critical data field of the Security Header. There can be up to 65534 SAs per Master Channel; two values are reserved for future use (0, 65535). The receiver uses the SPI to reference the corresponding SA, and therefore to determine the presence and lengths of optional fields in the Security Header and Trailer.

3.4.2.3 Initialization Vector

The IV is an optional data field in the security header, specified in the SDLS protocol to provide flexibility with respect to the choice of cryptographic algorithms. Thus, some recommended cryptographic algorithms require an initial block of input before processing the user data. This initial block of data is the IV. It serves to preload the cryptographic process and enhance its security by adding variability.

Those cryptographic algorithms that require IVs usually specify particular requirements to their IVs. Some have to be unique, that is, not used more than once for all the invocations of the algorithm with a given cryptographic key. Some have to be random, that is, it is not possible to predict which will be the next value taken by the IV for the next invocation of the

cryptographic algorithm. The reader is referred to reference [16] for further guidance concerning the particular requirements of IVs.

In general, the length of the IV is driven by the block size of the cryptographic algorithm to be used. Thus with currently recommended algorithms with a 128-bit block size, a maximum value of 128 bits can be specified for an IV. However, in the usual quest for efficiency (lower protocol overhead) particular constructs allow for shorter IVs even when the underlying algorithm block size is 128 bits.

Those constructs are unique to each cryptographic algorithm. They may combine the transmission of a part of the IV with the synchronized regeneration by the user receiver processor of the non-transmitted part. While constructs like this may improve protocol efficiency, they do it at the expense of operational robustness and an additional synchronization process.

In some particular cases, a single block of data can fulfill the role not only of IV but also Sequence Number, as illustrated in the next subsection.

It is important to warn users that improper management of the IV, that is, not respecting their particular construct and management requirements, can result in critical degradation of the security service provided to the point of rendering it useless. Thus, extreme care needs to be exercised in conceiving and implementing an IV concept for a particular SDLS implementation.

3.4.2.4 Sequence Number

The Sequence Number field is used if authentication or authenticated encryption is selected for an SA. This field may be a portion of a longer managed anti-replay sequence number. The Sequence Number field length is managed and is fixed for the duration of the SA.

Including the sequence number as part of the transmitted data, while not strictly needed, has clear design and operational advantages. The validity of a received message is broken down in two separate tests: MAC and sequence count value.

The receiver can verify first the validity of a MAC without needing to recreate the sequence counter. The received value is used for the computation. Without such transmission, and assuming the receiver manages a range of acceptable sequence count values (window), the receiver would need to test the received message with every possible MAC in accordance with every possible sequence count value. While this would be technically possible, it would add substantial complexity to the receiver in exchange of a minimum protocol efficiency gain.

Afterwards, in a second validity check, the receiver can compare the received value against the range of expected values.

Only if both tests are successful is the message accepted.

For systems that implement authenticated encryption algorithms that use a simple incrementing counter as an initialization vector (i.e., as in Galois/Counter-Mode algorithms), the Initialization Vector field of the Security Header may serve also as the transmitted portion of the Sequence Number. In this case, the separate Sequence Number field is unnecessary and is omitted from the Security Header.

3.4.2.5 Pad Length

The optional Pad Length field specifies the number of fill bits used to pad the input data message for its cryptographic processing.

The cryptographic algorithms recommended by CCSDS do not require external padding. The SDLS baseline modes adopt those recommended algorithms. Thus introducing a pad length field in SDLS could appear to be superfluous. However, in order to support the protocol flexibility and its independence of cryptographic algorithms, padding needs to be considered.

Certain cryptographic algorithm implementation modes (i.e., cipher block modes) require that their input data be an exact multiple of a data block size. Whenever the input data is not an exact multiple, the SDLS protocol has to fill in the last remaining input data block with additional data: the padding.

The amount of padding (pad length) and its position has to be established with a proper convention. The receiver processor needs to be able to determine if padding is present and where in order to process the data and deliver the initial SDU to the user application.

The padding may not need to be transmitted with the data. In this case its proper regeneration by the receiver processor is sufficient.

If padding is present, the Security Header includes 1 octet, placed at the end of the security header, to indicate the number of padding bits (0-127).

An example of an efficient padding concept is the *Padding Method 2* specified by ISO for the Message Authentication Code based on Cipher Block Chaining (CBC-MAC) (reference [17], section 6.3.3). The same method is specified for the Cipher Block Chaining encryption algorithm (reference [18], section B.2.3).

The method consists of appending a ‘1’ followed by $n-1$ ‘0’ after the last input data block smaller than the size of the cipher block for which n padding bits are required to complete the cipher block. The padding is granular at bit level. Thus the padding can be as follows:

> 1, 10, 100, 1000, 10000,…, 1000…000 with $n-2$ number of ‘0’ for the extreme case of just one input bit as part of the last cipher data block.

The *Padding Method 2* does not require the transmission of the padding data.

Concerning the security aspects, the suitability of the presented padding concept has been studied for CBC and CBC-MAC (see relevant references in reference [18], Bibliography). A

careful assessment is required for other authentication or encryption algorithms. Attacks are known to exploit padding weakness. Therefore, it is a critical user responsibility to make informed decisions on how to implement padding for particular cryptographic algorithms other than the two presented above.

However, in recognition of the fact that other encryption algorithms that can be used with SDLS do not require padding (e.g., stream modes like the Counter mode), the field is omitted when those are used.

3.4.3 SECURITY TRAILER

3.4.3.1 Message Authentication Code

The Security Trailer is present whenever authentication or authenticated encryption is applied by the SDLS. The contents of the Security Trailer is exclusively a Message Authentication Code or MAC, which is the result of applying the authentication or authenticated encryption algorithm to the following input data:

- the SDU;
- a flexible selection of fields of the Frame Header;
- additional fields present between the Frame Header and the Security Header; and
- the Security Header itself.

Flexibility is provided for the selection of fields within the Frame Header to be protected with authentication. The identification data of the virtual channel(s) in which SDLS is applicable could be subject to manipulation, whereby data addressed to one virtual channel could be intercepted, manipulated, and attempted to be replied to on another virtual channel. The protection of the virtual channel identification is, therefore, crucial for the proper operation of SDLS.

The global virtual channel identification is defined for TC, TM, AOS, and USLP protocols according to their respective standards. A common element to the global virtual channel identification is the Spacecraft Identifier (SCID), which appears on the Frame Header. Fortunately, the verification of a valid SCID field is an integral element of the frame verification process included in TC, TM, AOS, and USLP SDL protocols. Thus the SCID is assumed to be correct before SDLS is called for at the receive side.

However, the other components of the identification, like the VCID or the MAP (exclusive for TC and USLP but actually part of the Segment Header), are not verified by the SDL protocol. Therefore, in order to protect the identification completely these fields require mandatory protection against undetected malicious manipulation by SDLS. As a minimum, the Virtual Channel Identifier (VCID) is the field selected from the Frame Header to be protected with SDLS.

Users can flexibly decide which additional Frame Header fields as well as additional protocol data units between the Frame Header and the Security Header (always authenticated!) can be protected with authentication. The concept of the authentication bit mask is introduced to ease the implementation of this flexibility. The mask could be set to provide protection to the complete Frame Header, if desired by the user. For example, in a scenario of a satellite constellation sharing SAs, it would be prudent to include the SCID as part of the authentication bit mask.

In cross-support scenarios the authentication bit mask has to be provided to the supporting agency so that the proper protocol data unit fields are included (or not) on authentication or authenticated encryption (decryption) operations. The Authentication bit mask is part of the managed parameters that have to be exchanged out of band between the communicating agencies.

MAC computation is the latest cryptographic data processing operation for authentication or authenticated encryption services. Thus the position of the MAC after the data required for its computation favors implementations for very high data rate application.

3.4.3.2 Message Authentication Code Length and Security

The MAC length is a critical design parameter of an authentication or authenticated encryption algorithm since it is directly related to its security strength. In establishing the acceptable range of values for the MAC length, consideration needs to be given to the attainable security strength, the cryptographic algorithm to be used, and the length of its cryptographic key. In general, given a certain cryptographic key length l, in order to achieve the full potential security strength provided by such a key for attacks like the birthday attack, the MAC needs to have a length $2 \times l$.

Since currently recommended cryptographic algorithms employ keys that range from 128 to 256 bits, it follows that the MAC could range between 256 and 512 bits. The latter has been selected as the maximum value for the MAC length provided by SDLS. Longer MAC lengths with currently recommended cryptographic algorithms would result in inefficient design (no security gain, additional useless overhead).

For the minimum value of the MAC length, consideration is given as well to the possibility of changing keys more frequently, thus allowing for shorter MACs and the potential benefit this could provide for applications where the 256 bits is considered onerous (e.g., Telecommand). It should be noted that the recommended authenticated encryption algorithm (AES GMAC, see reference [16]) mandates a 128-bit MAC length, but shorter lengths are possible provided certain precautions are taken with the length of the authenticated data block and the lifetime of the key (see Appendix B of reference [16]).

Similar efficiency considerations are reflected in recommended standards for authentication (see reference [19]), which allow for MACs as short as 64 bits or even smaller if the controlling protocol limits the number of attempts that can return an INVALID result with a given key. However, this is not considered a reasonable approach for space application where

continued resistance to illegal attempts, by using a sufficiently long MAC, is preferable to a state machine that could block the legitimate access after a limited number of failed attempts later on.

Finally, it needs to be noted that the maximum MAC length for the recommended authenticated encryption algorithm (AES-GCM) is limited to 128 bits. This limitation applies as well if the algorithm is used for authentication only.

3.4.3.3 Trailer Position

MAC computation is the latest cryptographic data processing operation for authentication or authenticated encryption services. Thus the position of the MAC after the data required for its computation (no further data is processed by SDLS after the SDU) favors very high data rate implementations.

3.5 PROTOCOL MANAGEMENT

3.5.1 SECURITY ASSOCIATION

3.5.1.1 Clear Mode Management

Experience has shown that the inclusion of a Clear Mode (bypass of security functions) on an otherwise protected SA is often requested by spaceflight projects. From the security standpoint, such Clear Mode is not recommended given the security risk it poses. Nevertheless, such a request may be justified for civilian missions in which the risk of losing a spacecraft because of a safety issue (e.g., critical telecommand link outage) prevails over a security issue (e.g., telecommand spoofing). For these missions, the Clear Mode may be activated in flight by an on-board FDIR mechanism as well as by a ground-transmitted telecommand.

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. This SA may be activated with a hardwired-based solution (e.g., strap) and inhibited before flight.

In order to avoid a data throughput change when the mode transition occurs, the presence of the security header and trailer may be maintained, even though there is no security processing whatsoever.

Transitions from secure to clear and the opposite when commanded by ground control should preferably and systematically proceed through a separate authenticated SDLS SA.

3.5.1.2 Recovery SA in TC SDL

An SA can only cover a single VC on TC SDL. However, SDLS does not exclude the duplication of SAs over a given TC SDL VC. Experience acquired with previous ad-hoc implementations of security functions for the protection of TC SDL (reference [20]) has shown that the existence of a redundant SA, only to be called as a last resource, could be very beneficial. When the 'nominal' SA has failed and possibly left the spacecraft telecommanding unavailable, this 'redundant' SA allows restoration of telecommanding without jeopardizing security. This special SA is labelled *Recovery SA*.

Special care should be taken to store and segregate the context of this SA at both ends of the space link. This Recovery SA should not be used for regular operations. In order to maximize operational safety, the on-board keys associated with this Recovery SA should not be erasable, reloadable, or revocable.

3.5.2 MANAGED PARAMETERS

In order to conserve bandwidth on the space link and in line with CCSDS practice for protocol management, certain parameters associated with the Security Protocol are handled by management rather than by the 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.

Since the SDLS is an optional add-on to the SDL protocols, all managed parameters of the corresponding SDL protocol service provider that implements SDLS are applicable (e.g., Spacecraft ID).

Furthermore, SDLS has its unique managed parameters. 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.

SDLS defines the managed parameters classified and defined in table 3-4 below. These parameters are defined in an abstract sense, and are not intended to imply any particular implementation of a management system.

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

Table 3-4: Managed Parameters

Managed Parameter	Description
Managed Parameters from the SDL protocol used on the physical channel:	
All Managed Parameters of the SDL protocol used on the physical channel need to be treated as also applicable to the Security Protocol	The reader is referred to the Blue Books of the SDL protocols (references [4], [5], [6], and [31]).
Managed Parameters held static for a given mission:	
Presence of Space Data Link Security Header (per Virtual Channel or per MAP)	The presence or absence of a Security Header on a Virtual Channel or MAP needs to remain constant throughout a Mission. Thus this parameter indicates whether the corresponding Virtual Channel or MAP is part of an SDLS Security Association and, therefore, secured.
Presence of Space Data Link Security Trailer (per Virtual Channel or per MAP)	The presence or absence of a Security Trailer on a Virtual Channel or MAP needs to remain constant throughout a Mission. Thus this parameter indicates whether the corresponding Virtual Channel or MAP is part of an SDLS Security Association implementing authentication or authenticated encryption. As already mentioned, a trailer is not present for encryption-only security association.
Length of Security Header in Transfer Frame (per Virtual Channel or per MAP)	This parameter indicates the octet length of the security header. It can reach up to 42 octets.
Length of Security Trailer in Transfer Frame (per Virtual Channel or per MAP)	This parameter indicates the octet length of the security trailer. It can reach up to 64 octets, which is considered sufficient to accommodate authentication algorithms up to 256-bit strength.

Managed Parameter	Description
Security Association Data Base Parameters held static for the duration of the applicable SA:	
Security Parameter Index	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 physical channel share a single SA. The SPI can be considered as a table index key to an SA database that stores all of the managed information required by each of the SAs on a physical channel.
Security Association Service Type	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. Thus, this managed parameter identifies the selected cryptographic function.
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 and USLP only) assigned to an SA at the time of its creation. This parameter identifies the GVCIDs or Global MAP IDs with which an SA is used. It should be noted that for bidirectional space links using AOS or USLP, GVCIDs may not be unique identifiers (see 3.5.8).
Transmitted length of Initialization Vector (if used)	This managed parameter needs to indicate the length of the Initialization Vector field in the Security Header. The reader is referred to 3.4.2.3 for further information. This parameter is optional.

Managed Parameter	Description
Transmitted length of Sequence Number (if used)	This managed parameter indicates the length of the Sequence Number field in the Security Header. The reader is referred to 3.4.2.4 for further information. This parameter is optional.
Transmitted length of Pad Length (if used)	This parameter indicates the length of the Pad Length field in the Security Header. This parameter is optional.
Transmitted length of MAC (if used)	This managed parameter indicates the length of the MAC field in the Security Trailer. This parameter is optional.
Authentication algorithm	The Authentication algorithm parameter indicates the applicable authentication algorithm and mode of operation. (See Cryptographic Algorithms Blue Book, reference [10], and Green Book, reference [21], for further guidance.)
Authentication mask	The authentication mask indicates the value of a provided bit mask that is applied against the Transfer Frame in a bitwise-AND operation to generate an Authentication Payload.
Sequence number window	The sequence number window indicates the amount of deviation the receiving end will accept between the expected anti-replay sequence number and the sequence number in the received frame.
Encryption algorithm	This parameter indicates the applicable encryption algorithm and mode of operation. (See Cryptographic Algorithm Blue Book, reference [10], and Green Book, reference [21] for further guidance.)
Security Association Data Base Parameters held static while the applicable SA is active on the channel:	
Authentication key	This parameter indicates the value of a provided authentication key, or of an index that refers to the actual key.
Encryption key	This parameter indicates the value of a provided encryption key, or of an index that refers to the actual key.

Managed Parameter	Description
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)	This parameter indicates the present value of a managed anti-replay sequence number. The synchronization of the sequence number is discussed in 4.3.4.
Encryption initialization vector (sender's current value)	This parameter indicates the present value of a managed initialization vector. The synchronization of the initialization vector is discussed in 4.3.3.

3.5.3 SIGNALING, MONITORING, AND CONTROL

Certain information elements essential for the reliable operation of the SDLS protocol are transmitted (in-band signaling) together with the SDU to which the corresponding security services apply. They are included in the Security Header and, when authentication or authenticated encryption applies, on the Security Trailer of the corresponding frames.

But others, like the managed parameters presented in the preceding subsection, are not. Typical examples are the cryptographic algorithm applicable to the corresponding SA and the cryptographic key used by the algorithm. In particular for symmetric algorithms, the latter has to remain secret to external parties during the cryptographic key lifetime.

For the control and monitoring of the managed parameters, a separate logical communications channel (out-of-band signaling) is used. As figure 3-8 below shows, there are at least two general concepts to set up this logical communications channel in the spacecraft avionics.

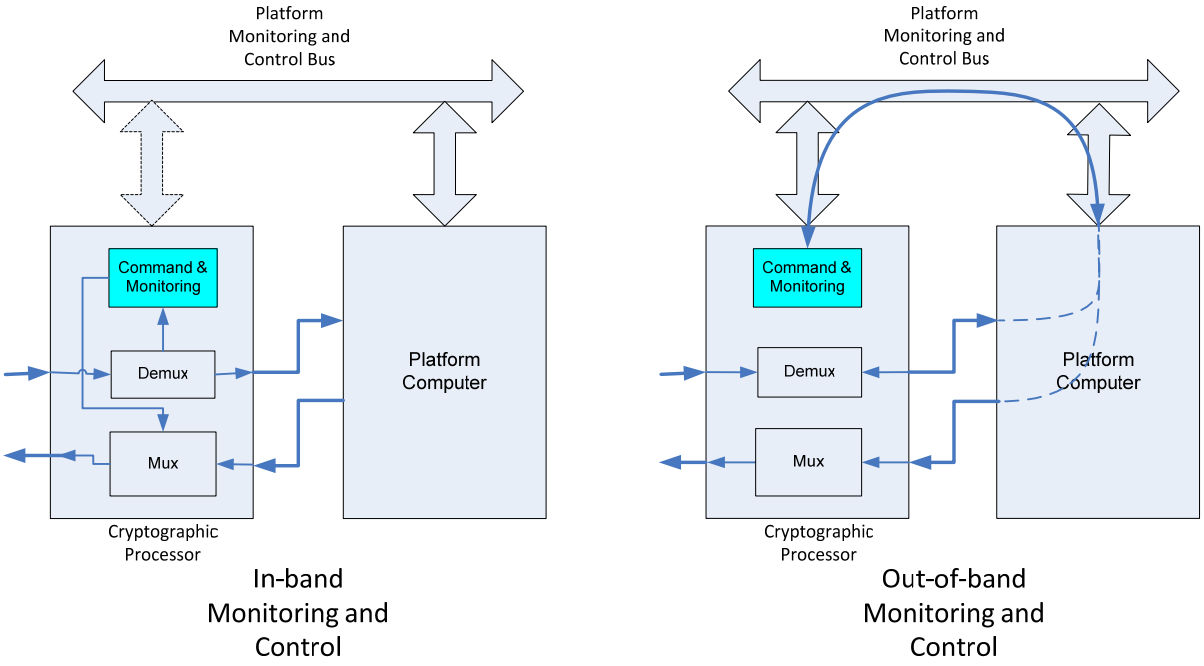


Figure 3-8: Monitoring and Control Options

In the first option, the control and monitoring messages are multiplexed and demultiplexed at the device implementing the SDLS security functions (cryptographic processor in figure 3-8 above). In the second option, these messages are routed to the platform computer and from there are rerouted to the security function by means of the spacecraft avionics bus (platform monitoring and control bus in figure 3-8 above).

The proposed concepts are assumed to be mainly applicable for the SDLS protocol when used for Telecommand, but they can apply as well to the control of the Telemetry security function. It may be noted as well that the reporting of security function telemetries to ground requires a specific telemetry channel, which is discussed after the telecommand channel.

In deciding which option is more advisable, one needs to realize that the control of Telecommand/Telemetry authentication and decryption (security functions) can be considered a vital function, that is, essential to mission success, and *permanent mission degradation* can result if the security functions are not executed when they should be, or are wrongly executed, or are executed in the wrong context.

Given the logical and physical placement of the telecommand (and telemetry) security function, it might be desirable to be able to control the security function regardless of the availability of the spacecraft On-Board Computer (OBC).

In practice, such control requires the identification of a logical destination of control telecommands. Two typical CCSDS mechanisms to multiplex/route telecommands are the VC at the Data Link Layer and the MAP at the Segment Layer.

On certain missions, the VC is used to route commands to the primary or secondary telecommand decoder. The MAP is used to route High Priority Commands (HPCs) towards Command Pulse generators or to route SW Commands towards the OBC.

In theory, a VC mechanism could be used to route on-board Security Function control commands towards the Security processor. However, the implementation of a FARM-1 state machine and COP-1 for these additional VCs would be required, increasing the complexity of the telecommand security processor, the On-Board Data Handling (OBDH), the CLCW reporting, and the ground operations.

The MAP mechanism avoids this additional complexity but requires the insertion of the Security protocol at the Segment layer, where a simpler routing decision can be made, as well as the reservation of MAP addresses for the control of the security function. The latter is not a problem given the large number of MAP addresses available. As a consequence, MAP IDs should be reserved for this function.

In the second option, which is an alternative concept used in some missions, the in-band command and monitoring of the Telecommand security processor is replaced by an out-of-band concept. The security processor, which is resident on a device interfaced with the spacecraft avionics bus, exchanges commands and telemetries formatted as CCSDS packets with the platform computer as any other avionics equipment.

The security processor may be able to accept both HPCs and SW Commands via the OBDH bus. In this way a minimum commanding capability is retained even when the OBC is not available.

Concerning the specific telemetry channel for security function monitoring, it may be recalled that the monitoring of telecommand/telemetry security functions is also considered a vital function. The implication is that the spacecraft always needs to provide indication of the telecommand/telemetry security function status regardless of the status of the spacecraft OBC.

Some missions use an Application Layer solution. High-Priority Telemetry (HPTM) packets can be generated without the OBC's being present and are guaranteed to be inserted cyclically in Telemetry. The definition of this HPTM takes into account a number of parameters required to monitor the proper operation of the security function.

As part of the SDLS Extended Procedures [22] (see 3.5.9), a new OCF at the Data Link Layer, similar to the CLCW but applicable only to SDLS reporting, is specified to be generated and inserted at the security function processor. This security function report is designated as the Frame Security Report (FSR).

3.5.4 REDUNDANCY

Spacecraft communications systems and processors at both ends of the space link implement redundancy for reliability purpose. Some agencies and corresponding implementations exploit certain features of the data communications protocol to manage redundancy. For

instance, different virtual channels of an implementation following the SDL protocol may be assigned to the primary and secondary receiver communications protocol processor. Thus the capability to address a particular logical (virtual) channel is used to select which of the receiver processors will handle the incoming data.

SDLS has been designed to be agnostic with respect to the redundancy management concept. Thus it is compatible with implementations that want to exploit the addressing capability of SDL protocol and with implementations that do not. For the latter case, the SDLS receiver protocol processor behaves like a radio unit. Two identical physical and logical SDLS processors simultaneously handle the incoming data flows. The user application selects one of the two in accordance with criteria and solution, which is beyond the scope of this document. This concept requires a full synchronization of all the relevant SDLS managed parameters so that the behavior of the processors will always be identical. Failure in one of the processors may trigger different behavior.

3.5.5 CRYPTOGRAPHIC KEYS

A cryptographic key is an attribute of an SA. Cryptographic keys of SAs need to be changed after a certain period of time, which may be driven by operational and security considerations.

By selecting different SPIs, switching from one cryptographic key to another can be performed on a frame basis. It is assumed that the new key has been activated previously.[2]

3.5.6 TELECOMMAND

One of the important restrictions that apply to use of the Security Protocol with TC is the following: each SA needs to be associated with one VC and one VC only.

The decision to place SDLS before the FOP-1 process on the sending end and after the FARM-1 process on the receiving end (see 3.3.2) has implications on the scope of SAs: they cannot span two or more VCs. This means there cannot be a single SA covering all TC data flow (i.e., master channel security). However, it is possible to have within a single VC one or more SAs at the MAP level, each one covering one or more MAP channels.

Interestingly, it is possible to have more than one SA covering a VC (see 3.5.1.2 and 4.5.6 for the Recovery SA).

[2] Further details concerning cryptographic key management are the subject of the SDLS Extended Procedures (see references [22] and [32]). The SDLS Extended Procedures Green Book (reference [32]) provides comprehensive discussion of key management using the Extended Procedures.

3.5.7 TELEMETRY

In contrast to TC restriction discussed on 3.5.6, an SA can span over more than one VC. Thus it is possible to protect a number of VCs with the same SA.

However, it is worth noting that SAs cannot be created for use with VCs reserved for carrying only ‘fill’ or ‘idle’ data (i.e., OID Transfer Frames as defined in reference [4]) for the reasons explained in 3.1.

If a secured VC is used for carrying both packets and OID Transfer Frames, then the idle pattern of the OID Transfer Frames should be carefully selected by the user to avoid degrading system security (e.g., known plaintext attacks).

3.5.8 ADVANCED ORBITING SYSTEMS OR UNIFIED SPACE LINK PROTOCOL

In contrast to TC restriction discussed on 3.5.6, an SA can span over more than one VC. Thus it is possible to protect a number of VCs with the same SA.

However, it is worth noting that SAs cannot be created for use with VCs reserved for carrying only ‘fill’ or ‘idle’ data (i.e., OID Transfer Frames as defined in reference [6]) for the reasons explained in 3.1.

In addition, GVCID may not be a unique identifier. In missions using AOS or USLP for both uplink and downlink there is no way to uniquely identify the direction based solely on GVCID. Therefore a different SPI should be selected for uplink and downlink GVCID.

3.5.9 EXTENDED PROCEDURES

CCSDS has developed an extension of the SDLS protocol: the Extended Procedures (see references [22] and [32]). These procedures cover in detail the specification of the following management functions:

- SA Management;
- Cryptographic Key Management; and
- Security Unit Monitoring and Control.

– These procedures are discussed in details in reference [32].

4 CONCEPT OF OPERATION

4.1 SECURITY ASSOCIATION

The mechanism for switching from one active Security Association to another is an Application Layer function. In order to change a cryptographic key dynamically from one Transfer Frame to the next, a user can change the key by changing the SPI. The corresponding SAs are assumed to be active.

The SA Management Procedures are specified in SDLS Extended Procedures (reference [22]).

4.2 GENERIC OPERATION

Figure 4-1 illustrates the generic operation of the SDLS protocol at the sending end, which is described in the following paragraphs. Afterwards, the generic operation at the receiving end as depicted in figure 4-2 is explained.

The Security Association database contains the selected Managed Parameters for all the SAs in place for the user(s). There can be more than one SA, but the description of the generic operation is valid for all of them. Thus the operation of only one SA is presented.

The SA may implement the following cryptographic algorithms: encryption, authentication, or the combination of both with authenticated encryption. In order to provide a complete description, and because authentication and encryption algorithms apply to different sets of data, both operations are presented in detail. It is important to note that the sequence of operations implies encryption and afterwards authentication at the sender end, with the opposite order at the receiving end.

The boxes highlighted in yellow identify the key elements of SDLS. Not all of these elements may be necessary. Their presence depends on the selected security services as well as the corresponding cryptographic algorithms.

The data processing starts with the higher-layer data. The user supplies the SDUs in the form of Transfer Frame Data Field (Frame Data block in the picture). Based on the settings of the SA and the identified virtual channel with corresponding settings for the space data link, the service provider determines the required size for the Frame Data block.

The encryption payload, which is identified as the user-supplied data (Frame Data box containing the frame data block) is input to the encryption algorithm (encryption processing ‘factory’). The encryption algorithm requires as a minimum an encryption key. Furthermore, depending on the selected algorithm, an Initialization Vector may be needed. It is important to note that the Initialization Vector may have specific constraints (e.g., uniqueness).

Furthermore, for some algorithms the Initialization Vector is actually a counter. In this case, the Initialization Vector can play the role of Sequence Number.

In addition, padding may be added in accordance with the selected padding method. As already mentioned, some encryption algorithms do not require padding.

After application of the encryption algorithm (encryption processing 'factory') to the input Frame Data block with the corresponding IV, optional padding, and specified encryption key, the data output block is delivered to the next SDLS data processing step: authentication.

In parallel and in tight coordination, the Security Header, a mandatory PDU of the SDLS, is created based on the specific SA parameters applying to the Virtual Channel Frame where the Frame Data (encrypted in this example) will be inserted. The Security Header includes both static and dynamic fields, the latter being related to the specific instance of the encryption algorithm application.

The SDL service provider delivers the Primary Header and possibly other optional fields like the Secondary Header or the Insert Zone, depending on the selected SDL protocol and the user-selected settings (SDL managed parameters). The output of the encryption algorithm is appended after the Security Header.

In order to select the specific fields to be protected with authentication, the authentication mask is applied, substituting zeros in place of the masked-out bits in accordance with the specified mask for that SA. The result of this operation is the authentication payload, which is the selected data block input for the authentication algorithm (authentication 'factory').

It should be noted that the authentication algorithm is processing the Security Header among other fields; since the Security Header provides a sequence number changing with every instance of the SDLS application on a given SA, authentication protects against replay attacks. Nevertheless, depending on the selected authentication algorithm, an Initialization Vector may be required.

The authentication algorithm uses the selected authentication key and produces as output a MAC, which is appended to the Transfer Frame Data Field to further continue the generation of a complete and now secure frame. Depending on the applicable SDL, an OCF and a FECF may be appended.

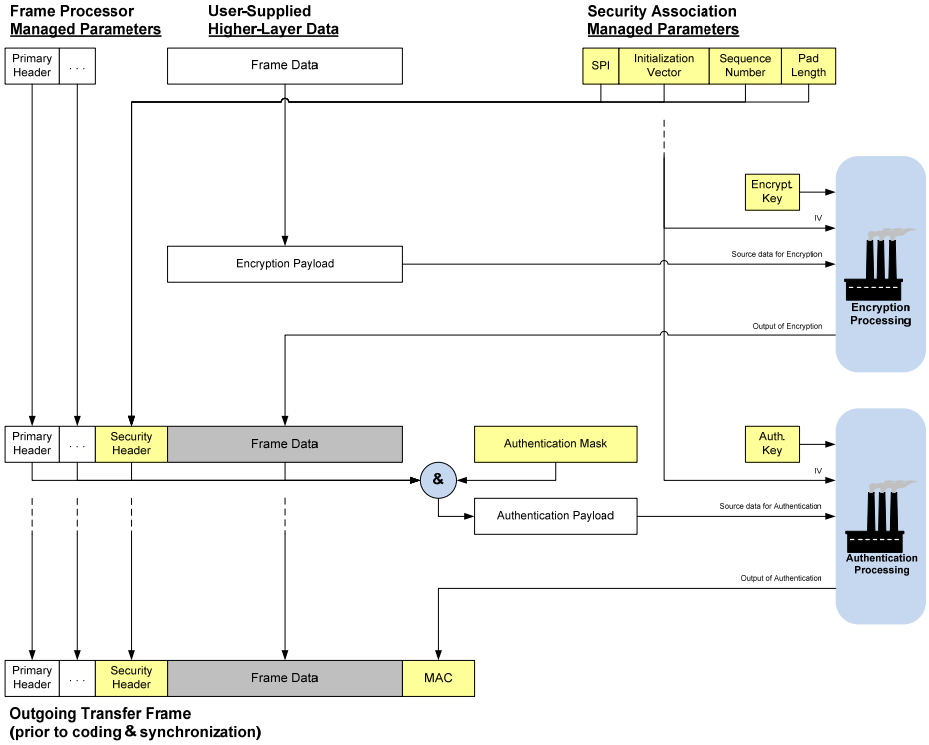


Figure 4-1: Generic SDLS Operation—Sending End

On the receiving end, as shown by figure 4-2, operations are inverted.

The SDL protocol entity validates first the incoming Transfer Frame before any security data processing operation can take place. This validation basically implies an application of the transmission integrity error detection mechanisms like the frame CRC (if present), as well as a general format checking of the candidate received frame.

Once this frame validation has been passed, the security operations are initiated. The received Security Header will provide the receiving end with an identification of the proper SPI, IV (if present), Sequence Number (if present) and Pad Length (if present). A format check (SPI match) of the received Security Header vs. the expected Security Header according to the SPI programmed in the receiver database will take place. If there is an SPI mismatch, an error indication will be produced.

Assuming a successful SPI match, the next operation will consist of a verification of the authentication (if present). This verification requires a generation of a local replica MAC (see ‘authentication processing factory’) based on selected incoming Frame fields and the use of an authentication key and an authentication bit mask, as dictated by the particular SPI, for comparison with the received MAC as well as a check of the incoming Sequence Number. These two steps of the authentication verification can be performed in any order.

The MAC comparison verification will result in one of two possible results:

– Positive MAC verification. The received MAC and the local replica MAC match. Security operations will continue.

– Negative MAC verification. The received MAC and the local replica MAC do not match. Security operations will conclude and a corresponding report will be produced.

The Sequence Number check will result in one of two possible results:

– Positive Sequence Number check. The received Sequence Number is within the acceptance window. Security operations will continue.

– Negative Sequence Number check. The received Sequence Number is outside the acceptance window. Security operations will conclude and a corresponding report will be produced.

Assuming both MAC verification and Sequence Number check provide positive results, security operations will continue with the processing of the received Frame Data (encrypted in this example). The decryption process will rely on the encryption key identified by the SPI and will transform the incoming Encryption Payload into an output Frame Data.

Finally, the receiving SDL protocol processor will resume SDL operations based on the received and processed Primary Header and Frame Data.

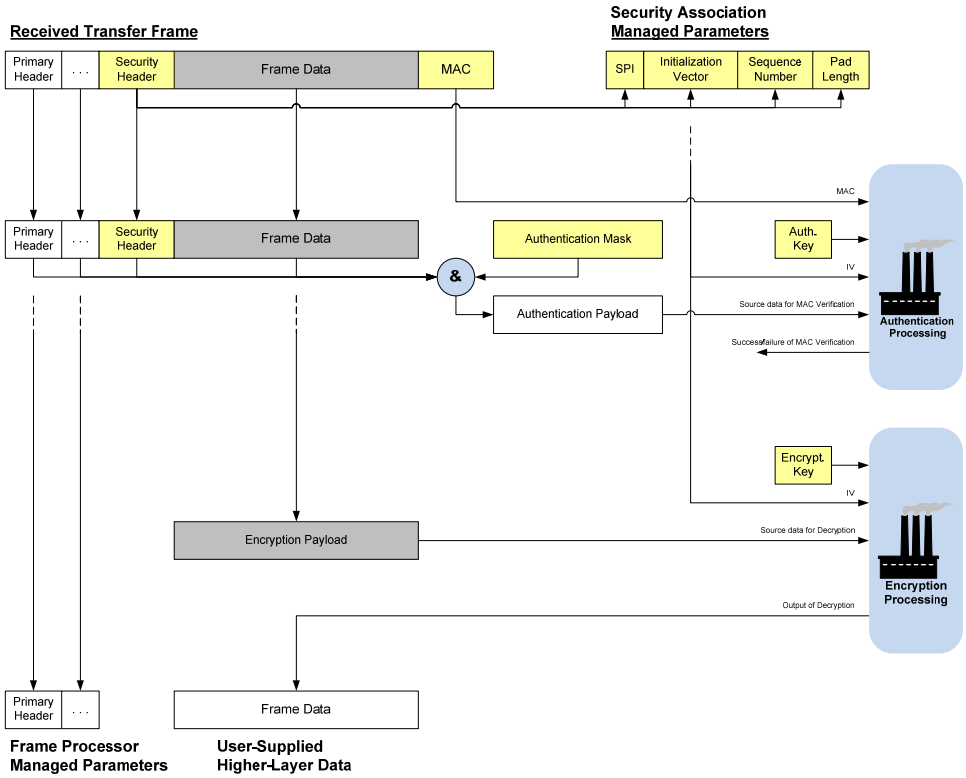


Figure 4-2: Generic SDLS Operation—Receiving End

4.3 SYNCHRONIZATION

4.3.1 OVERVIEW

For an effective operation of the implemented SDLS protocol, the following cryptographic and protocol parameters require synchronization and management:

- Cryptographic Key;
- Initialization Vector;
- Sequence Count.

The following subsections address each of them.

4.3.2 CRYPTOGRAPHIC KEY SYNCHRONIZATION

Essential for effective operation of the SDLS protocol is the synchronization of cryptographic keys employed at both ends of the communications link by the corresponding transmit and receive cryptographic algorithms. Failure to maintain key synchronization will result in meaningless SDUs for the receiving user application and, therefore, service failure.

As discussed in 3.5.3, in-band or out-of-band directives can be incorporated to ensure cryptographic key synchronization. A typical example of in-band synchronization consists of transmitting an index to point to a position in a logical table (key memory) where the key to be used is stored. Obviously, this approach requires the proper management on ground and on board of mirrored tables that always store identical sets of keys.

Detailed procedures for key management are specified in the CCSDS SDLS Extended Procedures (reference [22]).

This cryptographic key synchronization is a necessary condition for the effective operation of the protocol. However, with security services that employ authentication, an additional synchronization process is required: sequence count.

4.3.3 INITIALIZATION VECTOR SYNCHRONIZATION

Certain cryptographic algorithms like the recommended AES-GCM require an IV for their operation. Always maintaining the association between the IV and the corresponding cryptographic key as well as the ciphered message is critical for the correct authentication and decryption of the message.

Although in theory the IV does not need to be transmitted, for operational robustness, a practical solution is to transmit the IV with the corresponding ciphered and authenticated message.

4.3.4 SEQUENCE COUNT SYNCHRONIZATION

Authentication requires the verification of the proper sequence of the received frame to be able to reject replay attacks. The mechanism used in SDLS is based on sequence counters for every Security Association. These counters are managed at both sending and receiving ends.

In order to maintain a reliable data flow, it is essential that counters at the sending and receiving end be sufficiently synchronized. Ideally, if all the frames were received in sequence at the receiving end, the counters would be naturally synchronized.

Such synchronization could be forced for an SDL protocol like TC with the request of a sequence-controlled service. However, this is not possible for TM and AOS, and even for TC when expedited service is used. For this reason, provision needs to be made to allow missing frames (gaps) without blocking the flow of frames at the receiving end.

The provision of a sequence counter 'window' allows for a certain extent of desynchronization, due to time of flight and/or lost frames, between the counters at both ends. The verification and acceptance of a subsequent frame will recover the counter synchronization. Furthermore, the SDLS Extended Procedures (reference [22]) allow monitor and control of the on-board counter synchronization.

4.4 SDL PROTOCOL BASELINE IMPLEMENTATIONS

4.4.1 TELECOMMAND

Figure 4-3 depicts the operation of the SDLS protocol in the so-called Baseline Implementation mode for TC (see annex subsection E2 of reference [1]). This mode specifies the following selections:

- security services: authentication;
- cryptographic algorithm: AES Cipher-based Message Authentication Code (CMAC);
- authentication bit mask: VC ID and Frame Data protection;
- anti-replay sequence number: 32 bits, transmitted in-line;
- authentication key length: 256 bits;
- MAC length: 128 bits.

Authentication is considered to be the most valuable security service for TC. Hence, it is expected to be applicable to missions where a simple yet effective secure spacecraft control is desired.

Since the AES-CMAC algorithm requires neither an IV nor padding, the corresponding fields in the Security Header are not used. The authentication bit mask is set to the default value (selectable mask bits set to 'all zeros' meaning VC ID protected in addition to Frame Data).

Thus the database for SA Management Parameters is simplified and the impact on on-board implementations limited.

Furthermore, limiting the security services to authentication removes encryption-related operations from the generic SDLS operation previously presented in 4.2.

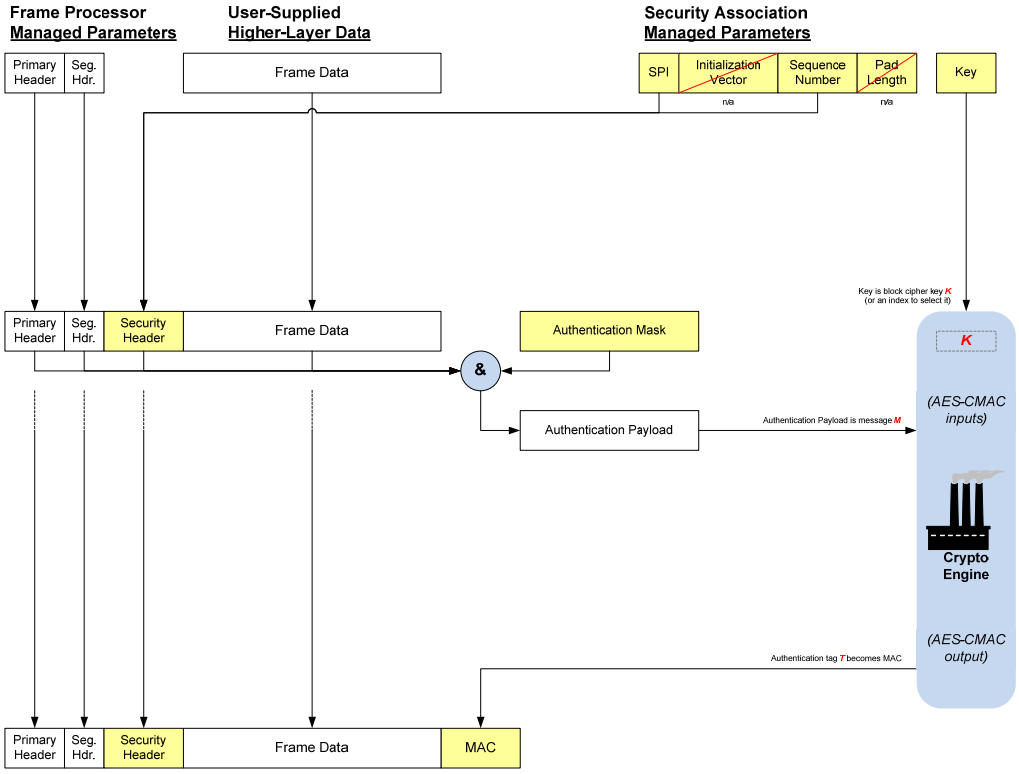


Figure 4-3: TC Authentication (Baseline Implementation)

4.4.2 TELEMETRY

Figure 4-4 depicts the operation of the SDLS protocol in the so-called Baseline Implementation mode for TM (see annex subsection E1 of reference [1]). This mode specifies the following selections:

- security services: authenticated encryption;
- cryptographic algorithm: GCM;
- authentication bit mask: VC ID and Frame Data protection;
- anti-replay sequence number: 32 bits, transmitted in-line;
- authentication key length: 256 bits;
- MAC length: 128 bits;
- IV length: 96 bits.

Authenticated encryption is considered the most valuable security service for TM. Hence it is expected to be applicable to missions where a simple yet effective secure spacecraft monitoring or instrument data delivery is desired.

Since the AES-GCM algorithm does not require padding, the corresponding field in the Security Header is not used. Since the IV can be implemented with an incrementing counter, the Sequence Number field is not required. The authentication bit mask is set to the default value (selectable mask bits set to 'all zeros' meaning VC ID protected in addition to Frame Data). Thus the database for SA Management Parameters is simplified.

Furthermore, the implementation of the authenticated encryption with AES-GCM algorithm removes the need for separate cryptographic keys for authentication and encryption. A single key is used by a joint 'authenticated encryption factory', shown as a somewhat simplified version of the generic SDLS operation previously presented in 4.2.

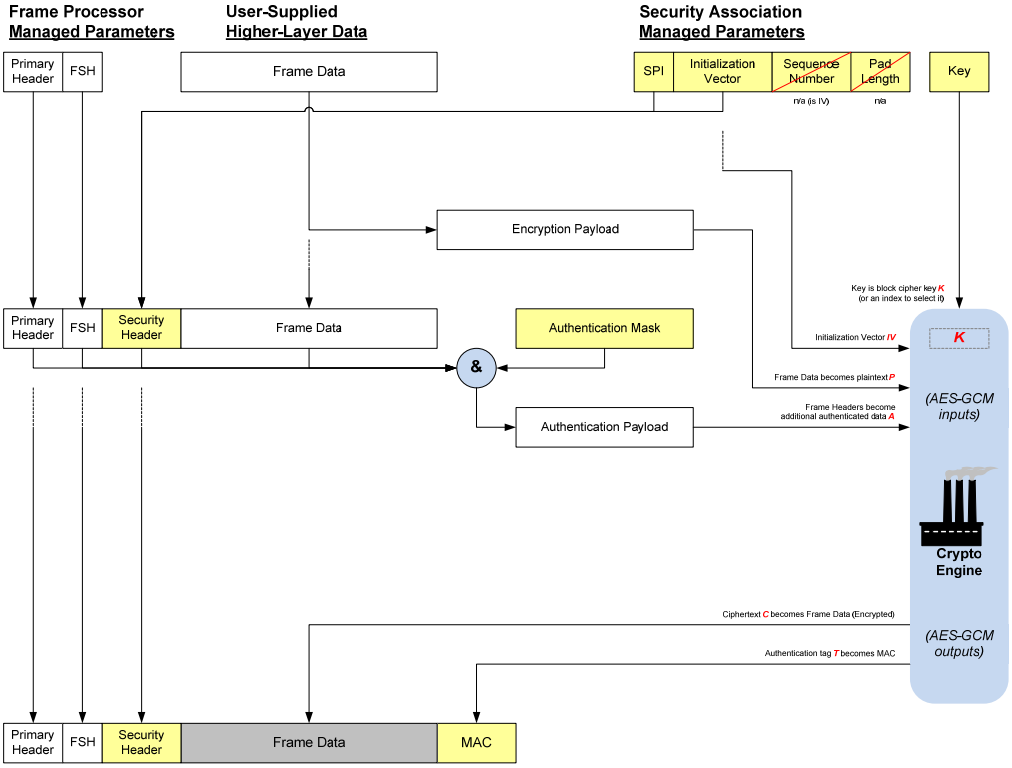


Figure 4-4: TM Authenticated Encryption (Baseline Implementation)

4.4.3 ADVANCED ORBITING SYSTEMS AND UNIFIED SPACE LINK PROTOCOL

Figure 4-5 depicts the operation of the SDLS protocol in the so-called Baseline Implementation mode for AOS and USLP (see annex subsection E3 and E4 in reference [1]). This mode specifies the following selections:

– security services: authenticated encryption;

- cryptographic algorithm: AES-GCM;
- authentication bit mask: VC ID and Frame Data protection and Insert Zone exclusion;
- anti-replay sequence number: 32 bits, transmitted in-line;
- authentication key length: 256 bits;
- MAC length: 128 bits;
- IV length: 96 bits.

Authenticated encryption is considered the most valuable security service for AOS and USLP. Hence it is expected to be applicable to missions where a simple yet effective secure spacecraft monitoring or instrument data delivery is desired.

Since the AES-GCM algorithm does not require padding, the corresponding field in the Security Header is not used. Since the IV can be implemented with an incrementing counter, the Sequence Number field is not required. The authentication bit mask is set to the default value (selectable mask bits set to ‘all zeros’ meaning VC ID protected in addition to Frame Data but exclusion of the Insert Zone). Thus the database for SA Management Parameters is simplified.

Furthermore, the implementation of the authenticated encryption with AES-GCM algorithm removes the need for separate cryptographic keys for authentication and encryption. A single key is used by a joint ‘authenticated encryption factory’, shown as a somewhat simplified version of the generic SDLS operation previously presented in 4.2.

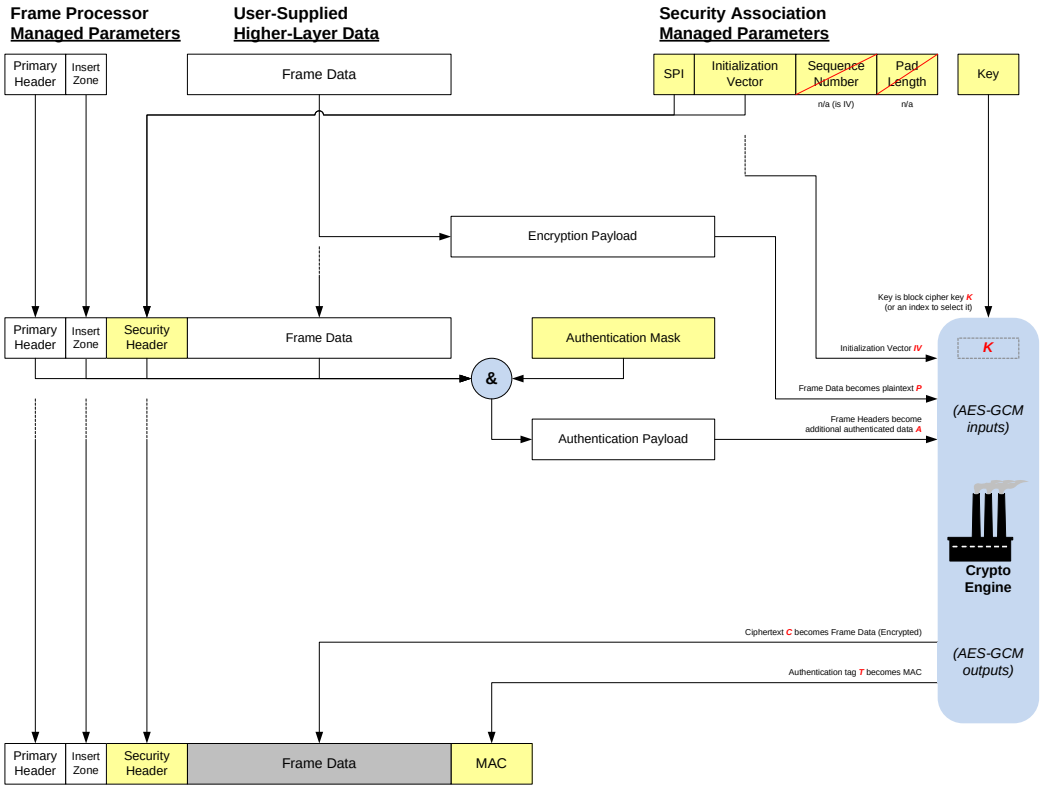


Figure 4-5: AOS and USLP Authenticated Encryption (Baseline Implementation)

4.5 SCENARIOS

4.5.1 OVERVIEW

This subsection provides examples that illustrate the implications of some of the Cryptographic Service design options on mission planning and overall system infrastructure.

4.5.2 BASIC SCENARIO

Perhaps the simplest operational scenario, depicted below in figures 4-6 and 4-7, is one in which a ground operations center sends spacecraft telecommand data over a forward link. Following information security conventional usage, red is used to denote the condition in which data requires protection, and black is used to denote the condition in which data is secured.

In this conceptual processing flow (not intended to imply any specific physical implementation), the element marked 'Authentication/Encryption Processing' carries out the actual cryptographic operations defined in each Security Association upon each applicable Transfer Frame, for instance, TC Authentication as specified in Baseline Mode (see annex A). In a real system, some of these functions could be combined in a single hardware or software processing unit, as shown in figure 4-7.

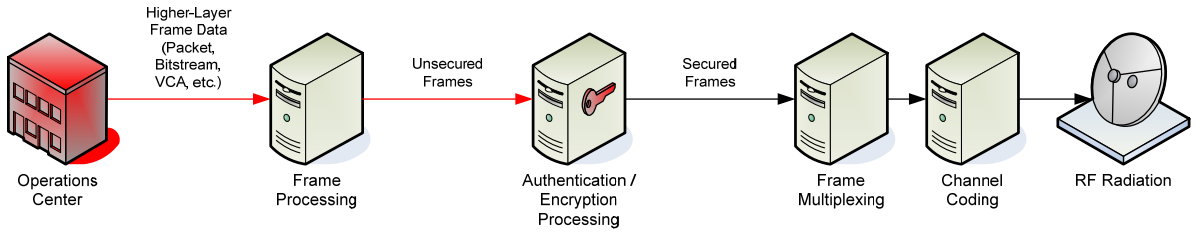


Figure 4-6: Simple Forward Link Scenario (Ground)

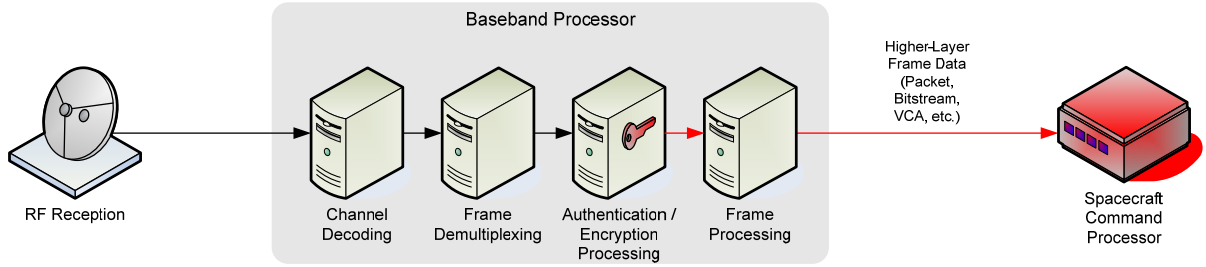


Figure 4-7: Simple Forward Link Scenario (Onboard)

4.5.3 COMPLEX SCENARIO

A more complex operational scenario, involving a spacecraft with multiple onboard elements providing return link data to multiple ground support elements, is depicted in figures 4-8 and 4-9 below. Three data flows are illustrated. Two of these (shown in red and orange) require protection, while the third (shown in black) needs no protection. The separate red and orange data flows represent the use of separate Security Associations and cryptographic keys by each data flow.

4.5.4 ONBOARD PROCESSING

In figure 4-8, each of three onboard processing elements provides its own individual portion of a return link channel as a higher-layer service (e.g., Packet, Bitstream, or Virtual Channel Access). Link-layer security processing and cryptographic key management is shown as provided in common by a trusted baseband processor unit.

Because the Cryptographic Service does not obscure the Transfer Frame Primary Header information, it is possible that multiple data flows may each have a separate Security Association (with its own context, algorithms, and keys). In practice, this is likely to be limited by the capabilities of available cryptographic processing hardware and software.

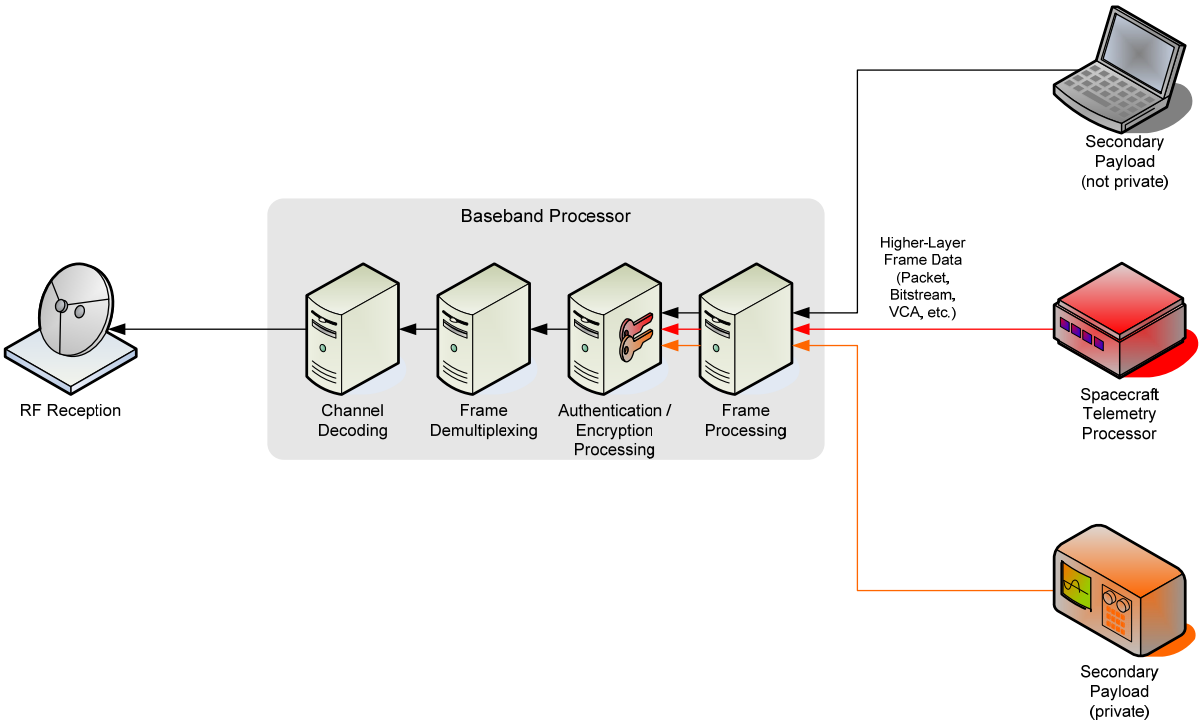


Figure 4-8: Complex Return Link Scenario (Onboard)

4.5.5 GROUND PROCESSING

Figure 4-9 depicts the same three return data flows. Two of them separately implement link-layer security; the third simply receives channel frames without any link-layer protection. Each of several ground processing elements receives its own individual portion of a return link channel as a VC Frame or MC Frame service and performs its own link-layer security processing and frame data extraction. Each ground processing element that performs link-layer security processing manages its own cryptographic keys. Because the Cryptographic Service does not obscure the Transfer Frame Primary Header information, CCSDS SLE return services may be used where applicable.

The ground operations scenario of figure 4-9 represents how cross-support at the link layer might be accomplished between multiple entities sharing a space link physical channel but with each entity separately providing security for its own data. This scenario could represent the sharing of a physical RF channel by multiple missions (each conducting operations separately), or it could represent the sharing of a single mission's physical channel by multiple operations groups (e.g., spacecraft housekeeping and payload operations).

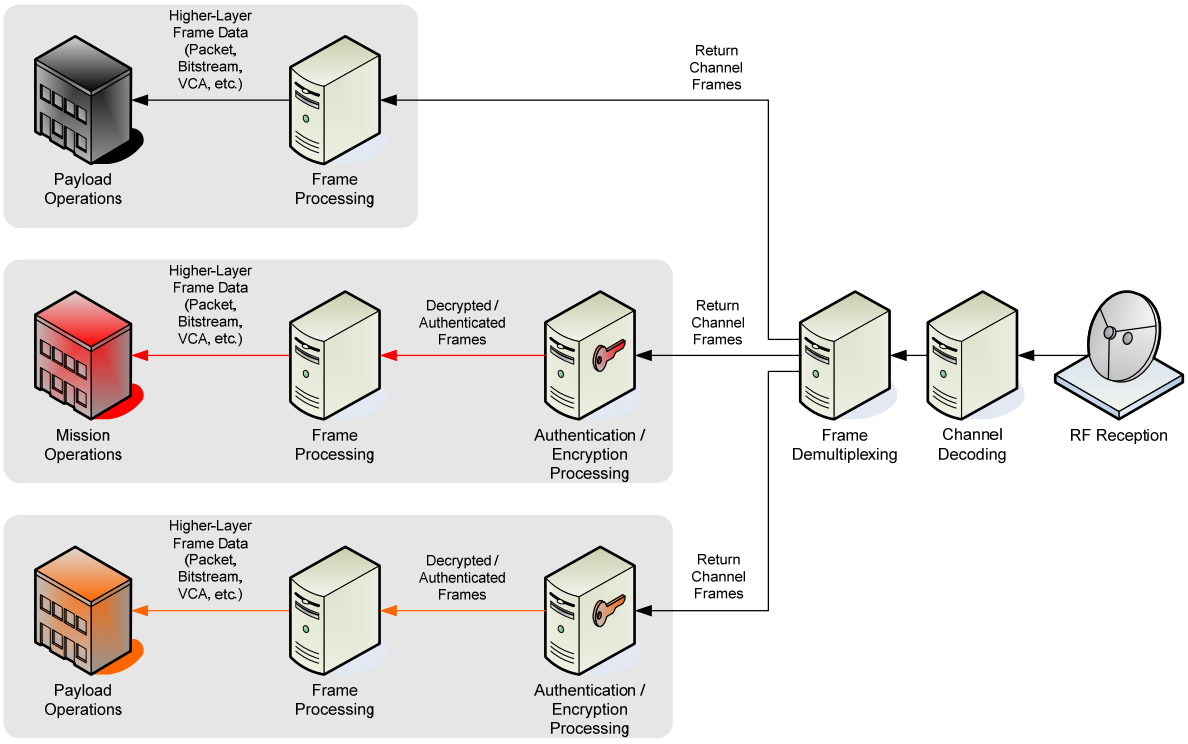


Figure 4-9: Complex Return Link Scenario (Ground)

4.5.6 RECOVERY SA SCENARIO

This subsection elaborates on the need for so-called recovery SA(s) in order to cope with emergency situations where the use of operational SAs is no longer possible.

Some emergency situations that can impact SDLS operation and are likely to be encountered include but are not limited to the following:

- Spacecraft is tumbling or TM subsystem on board has failed, resulting in interruption of the TM downlink. This forces the use of blind commanding, meaning no reporting from the on-board SDLS function is available. In that configuration, it is impossible to guarantee that secured TC frames, sent with operational SA, will be accepted on board by the SDLS function. Moreover, a mismatch in anti-replay counter between the ground sending end and the on-board receiving end is likely. Telecommands need to be sent to the spacecraft in a secure manner to restore the TM link (e.g., by switching to the redundant TM transmitter) or the attitude control of the spacecraft.
- Content of the programmable keys storage has been corrupted by the environment or a malfunction (i.e., programmable keys are not known anymore). New values for operational keys need to be uploaded in a secure manner by telecommand.
- Synchronization on the anti-replay counter of operational SA in use has been lost between SDLS ground sending end and on-board receiving end. Re-initialization of anti-replay counter (i.e., re-initialization of the SA context) on board is needed.

In all those emergency situations, there is a need to reestablish a secure TC channel. The usual way to achieve that is to define so-called Recovery SA(s), to be called only as a last resort. When the ‘nominal’ SA has failed and possibly left the spacecraft telecommanding unavailable, this Recovery SA will allow restoration of telecommanding without jeopardizing security. Special care should be taken to store and segregate the context of this SA at both ends of the space link. This Recovery SA *should never be used for regular operations*. The context of this (these) Recovery SA(s), including the on-board keys associated with it (them), *should be kept in non-erasable, non-volatile memory* so as to survive on-board transient power loss and operational errors.

ANNEX A

BASELINE MODES

A1 INTRODUCTION

This annex provides the rationale for the baseline implementations specified in annex E of the SDLS Blue Book, reference [1].

A2 TELECOMMAND

A2.1 SELECTION OF SECURITY SERVICES

Authentication as defined in reference [1] is the key security service for the protection of space asset control. Telecommands will be processed only by the spacecraft computer and/or hardware decoders once their legitimate origin and their integrity, including their freshness, has been verified on board.

A2.2 SELECTION OF CRYPTOGRAPHIC ALGORITHM

The cryptographic algorithm is selected from the CCSDS Standard on Cryptographic Algorithms (reference [10]), in particular from the recommended algorithms for Authentication. The Cipher-based Message Authentication Code (CMAC) presents the following attractive properties:

- Standard algorithm, originally coming from the United States National Institute of Standards and Technology (NIST).
- ISO Standard (reference [17]) since 2011.
- Does not require an IV. IVs are delicate and critical cryptographic parameters. Their proper management during operations is vital to maintain security. Cryptographic algorithms that do not require IVs are, therefore, favored whenever their use is viable for the required security services.
- Does not require padding. Improper padding could open the door to attacks. Cryptographic algorithms that do not require padding are, therefore, favored whenever their use is viable for the required security services.
- Being cipher-based offers both versatility and efficiency for implementations; CMAC implementation can reuse cipher for Authentication Key Management (Authentication Key Encryption, Authentication Key Decryption), which is a key support function of the authentication algorithm.

In summary, not only does AES-CMAC fulfil adequately the required security services (authentication), but also results in a streamlined security protocol overhead (no IV, no padding).

A2.3 DESIGN OF CRYPTOGRAPHIC ALGORITHM PARAMETERS

The essential cryptographic parameters for AES-CMAC are the Cryptographic Key, the MAC, and the Anti-replay Counter span. They are all addressed in reference [19].

AES-CMAC length is discussed in detail on Appendix A of reference [19]. A first consideration is the protection against guessing attacks. The longer the MAC, the more unlikely a random guess will result in a successful MAC verification. In order to limit the scope of such an attack, a control of the number of failed verification attempts by means of a 'system' protection is proposed by NIST. While this approach may be viable for a ground application (e.g., automatic teller machine), it is not considered appropriate for a space mission, given the possibility to lock out the TC function. For this reason, no controlling system or protocol is taken into account.

Instead, the protection is achieved with a sufficiently long MAC. Rather than choosing the NIST suggested minimum 64 bits with a controlling protocol or system, a minimum of 128 bits is proposed.

The AES-CMAC key length can take three possible lengths: 128, 192, and 256. The longer the key, the more randomness.

In addition, the longer the key, the larger the key storage (memory) requirements will be for a given number of keys. But this needs to be moderated by the fact that crypto-periods could be longer.

The following security analysis provides a justification for both MAC and Key length values.

To determine adequate lengths for both MAC and authentication key, the following attacks to MACs are considered (references [8] and [23]):

- guessing attack on the MAC key space, which is a brute-force guess of the key;
- guessing attack on the bit-size of the MAC, which is a brute-force guess of the MAC or the input;
- birthday attacks, which exploit the birthday paradox (i.e., collisions between text and MAC pairs).

An attack on the underlying block cipher and/or hash function has already been considered for the selection of the MAC algorithm and is therefore not discussed.

Furthermore, the following operational worst-case scenario, necessary for calculations concerning attacks requiring access to the spacecraft, is assumed: the attacker is able to uplink malicious telecommands continuously to the spacecraft between two legal contacts.

Since there is no limit considered on the number of repeated failed attempts to telecommand the spacecraft, the security of the concept relies simply on ensuring that the probability of randomly guessing the proper MAC for a chosen command is extremely low between two contacts.

The value of this probability could be chosen somewhat arbitrarily. However, it is considered that such a probability needs to be consistent with, and comparable to, the probability of accepting a telecommand with an undetected communications channel error. Higher probabilities would undermine the engineering effort that has been put into designing and standardizing a robust telecommand communications protocol.

For consistency of the analysis, the same probability of success is considered for the brute force key recovery.

For the calculation of the MAC and the key length, the following formula is used:

$$t >= ld(MaxInvalids / Risk)$$

where

MaxInvalids: maximum tries for the attacker

Risk: maximum acceptable probability of successful MAC forgery / key recovery

ld: logarithmus dualis

For the risk, the probability of undetected errors in frames as presented in Appendix D of reference [24] is taken. The presence of 130 codeblocks (128 is the maximum for a TC) is assumed. Medium, Low, and Lowest risk categories are defined in accordance with various channel Bit Error Rates (BERs) values (10^{-4}, 10^{-5}, and 10^{-6}).

The calculation of the MAC length is based on the number of tries the attacker has to test whether he successfully forged a MAC. For this, a commanding rate of 64 TC/s is assumed. This calculates to 11,059,200 TC in 48 hours. Forty-eight hours is the maximum time a key is assumed to be valid.

For the key length, the situation is different, as the attacker can actually perform his cryptanalysis on a local machine and is not dependent on the telecommand rate. One precondition is, however, that he or she can eavesdrop on at least one TC, meaning he or she has at least one text/MAC pair. The more pairs he or she has, however, the less verification of potential key candidates he or she requires.

If the attacker's goal is to compute a key from a number of text/MAC pairs, the following calculation can be made for the key length: a basic speed of 60 GIPS = 60,000,000,000 instructions/second = 10,368,000,000,000,000 instructions/48h is assumed. This assumption is based on extrapolating to the year 2018 with Moore's law, the computational feasibility limit considered by cryptographic experts in 1997 (references [8] and [23]).

The results for both MAC and key length calculations are shown on table A-1 below. For practical implementation reasons and additional margin, a 128-bit value for both is chosen.

Table A-1: MAC and Key Lengths

	MAC length	Key length
Medium risk	78	107
Low risk	98	127
Lowest risk	118	147
Conclusion	128	128

Targeted research conducted more recently on cryptographic key infrastructure for space missions with refined attack models for the typical security services has proven, among other things, that the 128-bit value proposed both for MAC and key length will hold well beyond 2032 (reference [25]). Since the first publication of this report, the quantum computing threat to cryptographic algorithms has become more credible. In the case of symmetric algorithms, the well-known Grover algorithm divides by 2 the exponent of the number of trials for brute force attack. The proposed mitigation is to simply multiply by 2 the key length. Therefore, the key length for baseline mode of SDLS was doubled to 256-bit.

The Anti-replay counter span has to be consistent with the number of times the authentication algorithm can be invoked with a given key. For practical implementation reasons, it is preferable that the counter span can be expressed with an integer number of hexadecimal words. Hence, 2 words (32 bits) are proposed, which will allow up to about 4 billion invocations before the counter rolls over.

A2.4 DIMENSIONING PROTOCOL DATA FIELDS

SDLS Authentication requires both a header and a trailer. The presence or absence of certain protocol data fields in the header is driven by the selected cryptographic algorithm for authentication. The length of the trailer is driven by the length of a key parameter of the algorithm: the MAC length.

The Security Header is depicted in figure A-1. Since neither IV nor padding is needed, the Security Header length is set by the union of the SPI (16 bits) and the Sequence Number (32 bits).

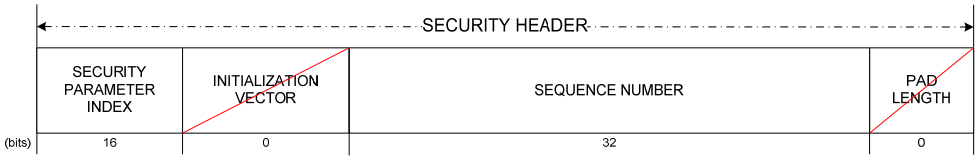


Figure A-1: Security Header (TC Baseline)

The Security Trailer is depicted in figure A-2. Its length is 16 octets (128 bits).

Figure A-2: Security Trailer (TC Baseline)

A3 TELEMETRY

A3.1 SELECTION OF SECURITY SERVICES

Authenticated Encryption as defined in reference [1] is the key security service for the protection of mission products, i.e., instrument and housekeeping telemetry data. Encryption alone provides confidentiality but does not provide protection against integrity attacks (e.g., forgery, impersonation). Higher security is achieved if the data is protected with Authentication as well. Thus the CCSDS recommendation is to couple Encryption with Authentication. The preferred CCSDS approach is by means of the Authenticated Encryption Service.

A3.2 SELECTION OF CRYPTOGRAPHIC ALGORITHM

A3.2.1 General

The cryptographic algorithm is selected from the CCSDS standard on Cryptographic Algorithms (reference [10]), in particular from the recommended algorithms for Authenticated Encryption. Therefore the AES-GCM is the recommended algorithm for the TM Baseline mode.

Recent cryptographic research on AES-GCM has identified a weakness concerning certain keys (references [26] and [27]). The user is invited to carefully consider the key generation and selection process in order to avoid the use of ‘weak’ keys.

A3.2.2 Design of Cryptographic Algorithm Parameters: MAC and Key Lengths

With the selection of AES-GCM, the selection of MAC and key length is as follows:

- The MAC length is set to 128 bits. This value is considered sufficiently secure for civilian missions, as justified by the security analysis in A2.3.
- The key length is limited to three possible values: 128, 192, and 256 bits. A value of 256 bits is considered sufficient for civilian missions, as justified by the security analysis in A2.3.

A3.3 INITIALIZATION VECTOR CONSTRUCTION

AES-GCM requires an IV. There are two specified approaches to construct an IV for AES-GCM (see section 8.2 of reference [16]). The recommended construction is the following: deterministic with 96 bits in total length.

To maintain security, it is essential to avoid a repetition of the IV with the same cryptographic key. Failure to meet this requirement will imply a security leakage. Further details can be found in reference [16].

A3.4 DIMENSIONING PROTOCOL DATA FIELDS

SDLS Authenticated Encryption requires both a header and a trailer. The presence or absence of certain protocol data fields in the header is driven by the selected cryptographic algorithm for authenticated encryption. The length of the trailer is driven by the length of a key parameter of the algorithm: the MAC length.

The Security Header is depicted in figure A-3. AES-GCM normally uses a simple incrementing counter as its initialization vector. A separate anti-replay Sequence Number is unnecessary. Since neither a Sequence Number nor padding is needed, the Security Header length is set by the union of the SPI (16 bits) and the IV (96 bits).

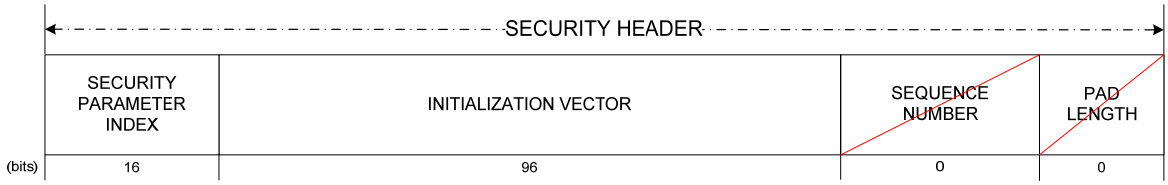


Figure A-3: Security Header (TM Baseline)

The Security Trailer is depicted in figure A-4. Its length is 16 octets (128 bits).

Figure A-4: Security Trailer (TM Baseline)

A4 ADVANCED ORBITING SYSTEMS

A4.1 SELECTION OF SECURITY SERVICES

Authenticated Encryption, as defined in reference [1], is the key security service for the protection of mission products, i.e., instrument and housekeeping telemetry data. Encryption alone provides confidentiality but does not provide protection against integrity attacks (e.g., forgery, impersonation). Higher security is achieved if the data is protected with Authentication as well. Thus the CCSDS recommendation is to couple Encryption with Authentication. The preferred CCSDS approach is by means of the Authenticated Encryption Service.

A4.2 SELECTION OF CRYPTOGRAPHIC ALGORITHM

A4.2.1 General

The cryptographic algorithm is selected from the CCSDS Standard on Cryptographic Algorithms (reference [10]), in particular from the recommended algorithms for Authenticated Encryption. Therefore the AES-GCM is the recommended algorithm for the AOS Baseline mode.

Recent cryptographic research on AES-GCM has identified a weakness concerning certain keys (references [26] and [27]). The user is invited to carefully consider the key generation and selection process in order to avoid the use of ‘weak’ keys.

A4.2.2 Design of Cryptographic Algorithm Parameters: MAC and Key Lengths

With the selection of AES-GCM, the selection of MAC and key length is as follows:

- The MAC length is set to 128 bits. This value is considered sufficiently secure for civilian missions, as justified by the security analysis on A2.3.
- The key length is limited to three possible values: 128, 192, and 256 bits. A value of 256 bits is considered sufficient for civilian missions, as justified by the security analysis on A2.3.

A4.3 INITIALIZATION VECTOR CONSTRUCTION

AES-GCM requires an IV. There are two specified approaches to construct an IV for AES-GCM (see section 8.2 of reference [16]). The recommended construction is the following: deterministic with 96 bits in total length.

To maintain security, it is essential to avoid a repetition of the IV with the same cryptographic key. Failure to meet this requirement will imply a security leakage. Further details can be found in reference [16].

A4.4 DIMENSIONING PROTOCOL DATA FIELDS

SDLS Authenticated Encryption requires both a header and a trailer. The presence or absence of certain protocol data fields in the header is driven by the selected cryptographic algorithm for authenticated encryption. The length of the trailer is driven by the length of a key parameter of the algorithm: the MAC length.

The Security Header is depicted in figure A-5. AES-GCM normally uses a simple incrementing counter as its initialization vector. A separate anti-replay Sequence Number is unnecessary. Since neither a Sequence Number nor padding is needed, the Security Header length is set by the union of the SPI (16 bits) and the IV (96 bits).

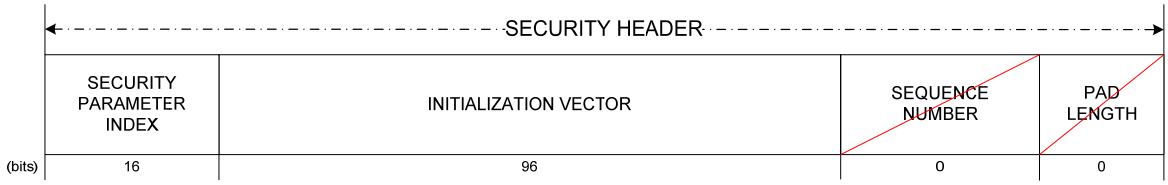


Figure A-5: Security Header (AOS Baseline)

The Security Trailer is depicted in figure A-6. Its length is 16 octets (128 bits).

Figure A-6: Security Trailer (AOS Baseline)

A5 UNIFIED SPACE DATA LINK PROTOCOL

A5.1 SELECTION OF SECURITY SERVICES

Authenticated Encryption, as defined in reference [1], is the key security service for the protection of mission products, that is, instrument and housekeeping telemetry data. Encryption alone provides confidentiality but does not provide protection against integrity attacks (e.g., forgery, impersonation). Higher security is achieved if the data is protected with Authentication as well. Thus the CCSDS recommendation is to couple Encryption with Authentication. The preferred CCSDS approach is by means of the Authenticated Encryption Service.

A5.2 SELECTION OF CRYPTOGRAPHIC ALGORITHM

A5.2.1 General

The cryptographic algorithm is selected from the CCSDS Standard on Cryptographic Algorithms (reference [10]), in particular from the recommended algorithms for Authenticated Encryption. Therefore the AES-GCM is the recommended algorithm for the USLP Baseline mode.

Recent cryptographic research on AES-GCM has identified a weakness concerning certain keys (references [26] and [27]). The user is invited to carefully consider the key generation and selection process in order to avoid the use of ‘weak’ keys.

A5.2.2 Design of Cryptographic Algorithm Parameters: MAC and Key Lengths

With the selection of AES-GCM, the selection of MAC and key length is as follows:

- The MAC length is set to 128 bits. This value is considered sufficiently secure for civilian missions, as justified by the security analysis on A2.3.
- The key length is limited to three possible values: 128, 192, and 256 bits. A value of 256 bits is considered sufficient for civilian missions, as justified by the security analysis on A2.3.

A5.3 INITIALIZATION VECTOR CONSTRUCTION

AES-GCM requires an IV. There are two specified approaches to construct an IV for AES-GCM (see section 8.2 of reference [16]). The recommended construction is the following: deterministic with 96 bits in total length.

To maintain security, it is essential to avoid a repetition of the IV with the same cryptographic key. Failure to meet this requirement will imply a security leakage. Further details can be found in reference [16].

A5.4 DIMENSIONING PROTOCOL DATA FIELDS

SDLS Authenticated Encryption requires both a header and a trailer. The presence or absence of certain protocol data fields in the header is driven by the selected cryptographic algorithm for authenticated encryption. The length of the trailer is driven by the length of a key parameter of the algorithm: the MAC length.

The Security Header is depicted in figure A-7. AES-GCM normally uses a simple incrementing counter as its initialization vector. A separate anti-replay Sequence Number is unnecessary. Since neither a Sequence Number nor padding is needed, the Security Header length is set by the union of the SPI (16 bits) and the IV (96 bits).

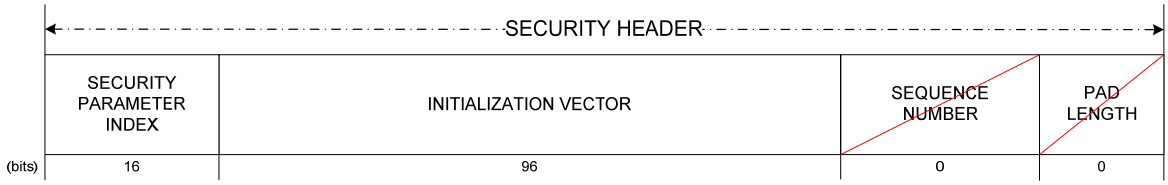


Figure A-7: Security Header (USLP Baseline)

The Security Trailer is depicted in figure A-8. Its length is 16 octets (128 bits).

Figure A-8: Security Trailer (USLP Baseline)

ANNEX B

ISO/OSI SECURITY SERVICES VS. SDL PROTOCOLS

B1 INTRODUCTION

This annex provides a justified selection of the Security Services found in the ISO OSI Security Architecture to be implemented by the Space Data Link Security Protocol.

B2 SELECTION METHODOLOGY

The security services defined in ISO OSI Security Architecture are listed. For each service, the following is provided:

- its definition;
- the threats the security service is mitigating;
- the impact if the security service is not implemented;
- the priority for selection, inclusion, and implementation as part of SDLS Security Services;
- the applicability as an objective to be covered by SDLS;
- the residual risks following its adoption;
- additional remarks.

Table B-1: Telecommand Selection

Security Service	Telecommand SDL Protocol Analysis						Remarks
	Definition	Threats	Impact	Priority	Applicability	Residual Risk	
Authentication							
Peer entity authentication	The corroboration that a peer entity in association is the one claimed. This service, when provided by the (N)-layer, provides corroboration to the (N+l)-entity that the peer entity is the claimed (N+l)-entity.	Impersonation, spoofing.		Low.	Telecommand implements a master-slave relationship rather than peer-to-peer. Considered too costly and complex for space missions where precious time could be lost and where network effects are not applicable.	Minor if Data origin authentication is implemented. However, session keys may not be fresh. Longer session keys may be required.	Used extensively in ground networks, in which, typically, peer entity authentication precedes the establishment of secured communications sessions. Difficult to conceive this service without Data origin authentication as well.
Data origin authentication	The corroboration that the source of data received is as claimed. This service, when provided by the (N)-layer, provides corroboration to an (N+l)-entity that the source of the data is the claimed peer (N+1)-entity.	Impersonation, spoofing.	Mission loss.	High.	Considered a very critical objective of SDLS protocol.	Minor if implementation of countermeasure is adequate and well managed.	Dependent on cryptographic strength (MAC length, key length, algorithm) and key management policy.

Table B-1: Telecommand Selection (Continued)

Security Service	Telecommand SDL Protocol Analysis						Remarks
	Definition	Threats	Impact	Priority	Applicability	Residual Risk	
Access Control	The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.	- Unauthorized access to TC receiver; - Denial of access to TC receiver (e.g., jamming); - Unauthorized access to COP-1 protocol state machine (FARM); - Denial of access to COP-1 protocol state machine; - Unauthorized access to security processor; - Denial of access to security processor.	Command availability hampered.	N/A	Denial of service is not an objective for SDLS protocol.	Unavailability due to jamming or blockage by unauthorized uplink. Alteration of FARM counters that can be recovered with Control frame from legal operator.	Spacecraft autonomy, ground station diversity, spread spectrum modulations, and null-steering antennas can counteract this threat. It is important to note that those are countermeasures beyond the scope of SDLS.

Table B-1: Telecommand Selection (Continued)

Security Service	Telecommand SDL Protocol Analysis						Remarks
	Definition	Threats	Impact	Priority	Applicability	Residual Risk	
Data Confidentiality							
Connection confidentiality	This service provides for the confidentiality of all (N)-user-data on an (N)-connection.	Information is disclosed to an unauthorized party.	Confidentiality compromised. Impact in accordance with information value and the possibility to elaborate more sophisticated attacks to user assets.	High.	Confidentiality in connection mode is an objective of the SDLS protocol.	Minor if implementation of countermeasure is adequate and well managed.	Dependent on cryptographic strength (key length, algorithm) and key management policy.
Connection less confidentiality	This service provides for the confidentiality of all (N)-user-data in a single connectionless (N)-SDU.	Information is disclosed to an unauthorized party.	Confidentiality compromised. Impact in accordance with information value and the possibility to elaborate more sophisticated attacks to user assets.	High.	Confidentiality in connectionless is an objective of the SDLS protocol.	Minor if implementation of countermeasure is adequate and well managed.	Dependent on cryptographic strength (key length, algorithm) and key management policy.
Selective field confidentiality	This service provides for the confidentiality of selected fields within the (N)-user-data on an (N)-connection or in a single connectionless (N)-SDU.			N/A.			The SDLS protocol will protect the SDUs identified and defined in the TC SDL protocol. There is no need identified to protect part of an SDU.

Table B-1: Telecommand Selection (Continued)

Security Service	Telecommand SDL Protocol Analysis						Remarks
	Definition	Threats	Impact	Priority	Applicability	Residual Risk	
Traffic flow confidentiality	This service provides for the protection of the information that might be derived from observation of traffic flows.	Observation of traffic flows indicate spacecraft operation activity.	Understanding by hostile entity about spacecraft operations.	Medium.	Traffic flow protection may be required by high-security missions.	Exploitation of certain information may support other attacks, such as denial of service. However, the latter is not an objective of SDLS.	Traffic flow protection should be considered as a candidate for future SDLS protocol update/extension.
Data Integrity							
Connection integrity with recovery	This service provides for the integrity of all (N)-user-data on an (N)-connection and detects any modification, insertion, deletion, or replay of any data within an entire SDU sequence (with recovery attempted).	Malicious message modification.	Up to loss of mission.	High.	Considered a very critical objective of SDLS protocol. Recovery to be addressed with SDLS Extended Procedures.	Minor if implementation of countermeasure is adequate and well managed.	Recovery requires manual intervention with supporting information (e.g., protocol reports, diagnosis). Dependent on cryptographic strength (MAC length, key length, algorithm) and key management policy.
Connection integrity without recovery	This service provides for the integrity of all (N)-user-data on an (N)-connection and detects any modification, insertion, deletion, or replay of any data within an entire SDU sequence (with no recovery attempted).	Malicious message modification.	Up to loss of mission.	High.	Considered a very critical objective of SDLS protocol.	Minor if implementation of countermeasure is adequate and well managed.	Dependent on cryptographic strength (MAC length, key length, algorithm) and key management policy.

Table B-1: Telecommand Selection (Continued)

Security Service	Telecommand SDL Protocol Analysis						Remarks
	Definition	Threats	Impact	Priority	Applicability	Residual Risk	
Selective field connection integrity	This service provides for the integrity of selected fields within the (N)-user- data of an (N)-SDU transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.				N/A.		The SDLS protocol will protect the SDUs identified and defined in the TC SDL protocol. There is no need identified to protect part of an SDU.
Connection less integrity	This service, when provided by the (N)-layer, provides integrity assurance to the requesting (N+l)-entity. This service provides for the integrity of a single connectionless SDU and may take the form of determination of whether a received SDU has been modified. Additionally, a limited form of detection of replay may be provided.	Malicious message modification.	Up to loss of mission.	High.	Considered a very critical objective of SDLS protocol.	Minor if implementation of countermeasure is adequate and well managed.	Dependent on cryptographic strength (MAC length, key length, algorithm) and key management policy. Replay detection is an integral part of SDLS.

Table B-1: Telecommand Selection (Continued)

Security Service	Telecommand SDL Protocol Analysis						Remarks
	Definition	Threats	Impact	Priority	Applicability	Residual Risk	
Selective field connection less integrity	This service provides for the integrity of selected fields within a single connectionless SDU and takes the form of determination of whether the selected fields have been modified.				N/A.		The SDLS protocol will protect the SDUs identified and defined in the TC SDL protocol. There is no need identified to protect part of an SDU.
Non-repudiation							
Non-repudiation with proof of origin	The recipient of data is provided with proof of the origin of data. This will protect against any attempt by the sender to falsely deny sending the data or its contents.				Not relevant for space data links.		The TC application is not concerned with denial of telecommand sending.
Non-repudiation with proof of delivery	The sender of data is provided with proof of delivery of data. This will protect against any subsequent attempt by the recipient to falsely deny receiving the data or its contents.				Not relevant for space data links.		The TC application is not concerned with denial of telecommand reception.

Table B-2: Telemetry Selection

Security Service	Telemetry SDL Protocol Analysis						Remarks
	Definition	Threats	Impact	Priority	Applicability	Residual Risk	
Authentication							
Peer entity authentication	The corroboration that a peer entity in association is the one claimed. This service, when provided by the (N)-layer, provides corroboration to the (N+l)-entity that the peer entity is the claimed (N+l)-entity.	Impersonation, spoofing.		Low.	Telemetry reflects a master-slave relationship rather than peer-to-peer. Considered too costly and complex for space missions in which precious time could be lost and in which network effects are not applicable.	Minor if Data origin authentication is implemented. However, session keys may not be fresh. Longer session keys may be required.	Used extensively in ground networks, in which, typically, peer entity authentication precedes the establishment of secured communications sessions. Difficult to conceive this service without Data origin authentication as well.
Data origin authentication	The corroboration that the source of data received is as claimed. This service, when provided by the (N)-layer, provides corroboration to an (N+l)-entity that the source of the data is the claimed peer (N+1)-entity.	Impersonation, spoofing.	Up to mission loss if operator commands spacecraft based on faulty housekeeping telemetry. TBD for instrument telemetry.	High.	Considered a very critical objective of SDLS protocol.	Minor if implementation of countermeasure is adequate and well managed.	Dependent on cryptographic strength (MAC length, key length, algorithm) and key management policy.

Table B-2: Telemetry Selection (Continued)

Security Service	Telemetry SDL Protocol Analysis						Remarks
	Definition	Threats	Impact	Priority	Applicability	Residual Risk	
Access Control	The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.	- Unauthorized access to TM receiver; - Denial of access to TM receiver (e.g., jamming); - Unauthorized access to COP-1 protocol state machine (FOP); - Denial of access to COP-1 protocol state machine (FOP).	Telemetry availability hampered. Telecommand availability hampered by wrong COP-1 parameters.	N/A.	Denial of service is not an objective for SDLS protocol	Unavailability due to jamming or blockage by unauthorized downlink.	Ground station diversity, spread spectrum modulations, and null-steering antennas can counteract this threat. It is important to note that those are countermeasures beyond the scope of SDLS.
Data Confidentiality							
Connection confidentiality	This service provides for the confidentiality of all (N)-user-data on an (N)-connection.				N/A.		Telemetry does not have connection mode.
Connection less confidentiality	This service provides for the confidentiality of all (N)-user-data in a single connectionless (N)-SDU.	Information is disclosed to an unauthorized party.	Confidentiality compromised. Impact in accordance with information value and the possibility to elaborate more sophisticated attacks to user assets.	High.	Confidentiality in connectionless is an objective of the SDLS protocol.	Minor if implementation of countermeasure is adequate and well managed.	Dependent on cryptographic strength (key length, algorithm) and key management policy.

Table B-2: Telemetry Selection (Continued)

Security Service	Telemetry SDL Protocol Analysis						Remarks
	Definition	Threats	Impact	Priority	Applicability	Residual Risk	
Selective field confidentiality	This service provides for the confidentiality of selected fields within the (N)-user-data on an (N)-connection or in a single connectionless (N)-SDU.			N/A.			The SDLS protocol will protect the SDUs identified and defined in the TM SDL protocol. There is no need identified to protect part of an SDU.
Traffic flow confidentiality	This service provides for the protection of the information that might be derived from observation of traffic flows.	Observation of traffic flows indicate spacecraft operation activity.	Understanding by hostile entity about spacecraft operations.	Medium.	Traffic flow protection may be required by high-security missions.	Exploitation of certain information may support other attacks, such as denial of service. However, the latter is not an objective of SDLS.	Traffic flow protection could be considered as a candidate for future SDLS protocol update/extension.
Data Integrity							
Connection integrity with recovery	This service provides for the integrity of all (N)-user-data on an (N)-connection and detects any modification, insertion, deletion, or replay of any data within an entire SDU sequence (with recovery attempted).				N/A.		Telemetry does not have connection mode.

Table B-2: Telemetry Selection (Continued)

Security Service	Telemetry SDL Protocol Analysis						Remarks
	Definition	Threats	Impact	Priority	Applicability	Residual Risk	
Connection integrity without recovery	This service provides for the integrity of all (N)-user-data on an (N)-connection and detects any modification, insertion, deletion, or replay of any data within an entire SDU sequence (with no recovery attempted).				N/A.		Telemetry does not have connection mode.
Selective field connection integrity	This service provides for the integrity of selected fields within the (N)-user- data of an (N)-SDU transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.				N/A.		Telemetry does not have connection mode.
Connection less integrity	This service, when provided by the (N)-layer, provides integrity assurance to the requesting (N+l)-entity. This service provides for the integrity of a single connectionless SDU and may take the form of determination of whether a received SDU has been modified. Additionally, a limited form of detection of replay may be provided.	Malicious message modification.	Up to mission loss if operator commands spacecraft based on faulty housekeeping telemetry. TBD for instrument telemetry.	High.	Considered a very critical objective of SDLS protocol.	Minor if implementation of countermeasure is adequate and well managed.	Dependent on cryptographic strength (MAC length, key length, algorithm) and key management policy. Replay detection is an integral part of SDLS.

Table B-2: Telemetry Selection (Continued)

Security Service	Telemetry SDL Protocol Analysis						Remarks
	Definition	Threats	Impact	Priority	Applicability	Residual Risk	
Selective field connection less integrity	This service provides for the integrity of selected fields within a single connectionless SDU and takes the form of determination of whether the selected fields have been modified.				N/A.		The SDLS protocol will protect the SDUs identified and defined in the TC SDL protocol. There is no need identified to protect part of an SDU.
Non-repudiation							
Non-repudiation with proof of origin	The recipient of data is provided with proof of the origin of data. This will protect against any attempt by the sender to falsely deny sending the data or its contents.				Not relevant for space data links.		The TM application is not concerned with denial of telemetry sending.
Non-repudiation with proof of delivery	The sender of data is provided with proof of delivery of data. This will protect against any subsequent attempt by the recipient to falsely deny receiving the data or its contents.				Not relevant for space data links.		The TM application is not concerned with denial of telemetry reception.

Table B-3: Advanced Orbiting Systems Selection

Security Service	Advanced Orbiting Systems SDL Protocol Analysis						
	Definition	Threats	Impact	Priority	Applicability	Residual Risk	Remarks
Authentication							
Peer entity authentication	The corroboration that a peer entity in association is the one claimed. This service, when provided by the (N)-layer, provides corroboration to the (N+l)-entity that the peer entity is the claimed (N+l)-entity.	Impersonation, spoofing.		Low.	Both Telecommand and Telemetry implement a master-slave relationship rather than peer-to-peer. Considered too costly and complex for space missions where precious time could be lost and where network effects are not applicable.	Minor if Data origin authentication is implemented. However, session keys may not be fresh. Longer session keys may be required.	Used extensively in ground networks, in which, typically, peer entity authentication precedes the establishment of secured communications sessions. Difficult to conceive this service without Data origin authentication as well.
Data origin authentication	The corroboration that the source of data received is as claimed. This service, when provided by the (N)-layer, provides corroboration to an (N+l)-entity that the source of the data is the claimed peer (N+1)-entity.	Impersonation, spoofing.	Mission loss (mainly for TC).	High.	Considered a very critical objective of SDLS protocol.	Minor if implementation of countermeasure is adequate and well managed.	Dependent on cryptographic strength (MAC length, key length, algorithm) and key management policy.
Access Control	The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.	- Unauthorized access to TC or TM receiver; - Denial of access to TC or TM receiver (e.g., jamming).	Command availability hampered	N/A.	Denial of service is not an objective for SDLS protocol	Unavailability due to jamming or blockage by unauthorized uplink.	Spacecraft autonomy, ground station diversity, spread spectrum modulations and null-steering antennas can counteract this threat. It is important to note that those are countermeasures beyond the scope of SDLS.

Table B-3: Advanced Orbiting Systems Selection (Continued)

Security Service	Advanced Orbiting Systems SDL Protocol Analysis						Remarks
	Definition	Threats	Impact	Priority	Applicability	Residual Risk	
Data Confidentiality							
Connection confidentiality	This service provides for the confidentiality of all (N)-user-data on an (N)-connection.				N/A.		AOS does not provide a connection mode.
Connection less confidentiality	This service provides for the confidentiality of all (N)-user-data in a single connectionless (N)-SDU.	Information is disclosed to an unauthorized party.	Confidentiality compromised. Impact in accordance with information value and the possibility to elaborate more sophisticated attacks to user assets.	High.	Confidentiality in connectionless is an objective of the SDLS protocol.	Minor if implementation of countermeasure is adequate and well managed.	Dependent on cryptographic strength (key length, algorithm) and key management policy.
Selective field confidentiality	This service provides for the confidentiality of selected fields within the (N)-user-data on an (N)-connection or in a single connectionless (N)-SDU.			N/A.			The SDLS protocol will protect the SDUs identified and defined in the AOS SDL protocol. There is no identified need to protect part of an SDU.
Traffic flow confidentiality	This service provides for the protection of the information which might be derived from observation of traffic flows.	Observation of traffic flows indicates spacecraft operation activity.	Understanding by hostile entity about spacecraft operations.	Medium.	Traffic flow protection may be required by high-security missions.	Exploitation of certain information may support other attacks like denial of service. However, the latter is not an objective of SDLS.	Traffic flow protection could be considered as a candidate for future SDLS protocol update/extension.

Table B-3: Advanced Orbiting Systems Selection (Continued)

Security Service	Advanced Orbiting Systems SDL Protocol Analysis						Remarks
	Definition	Threats	Impact	Priority	Applicability	Residual Risk	
Data Integrity							
Connection integrity with recovery	This service provides for the integrity of all (N)-user-data on an (N)-connection and detects any modification, insertion, deletion or replay of any data within an entire SDU sequence (with recovery attempted).				N/A.		Telecommand or Telemetry do not have connection mode under AOS. Telecommand may have recovery at application layer, which is beyond SDLS scope.
Connection integrity without recovery	This service provides for the integrity of all (N)-user-data on an (N)-connection and detects any modification, insertion, deletion, or replay of any data within an entire SDU sequence (with no recovery attempted).	Malicious message modification.	Up to loss of mission.	High.	Considered a very critical objective of SDLS protocol.	Minor if implementation of countermeasure is adequate and well managed.	Dependent on cryptographic strength (MAC length, key length, algorithm) and key management policy.
Selective field connection integrity	This service provides for the integrity of selected fields within the (N)-user-data of an (N)-SDU transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted or replayed.				N/A.		The SDLS protocol will protect the SDUs identified and defined in the TC SDL protocol. There is no identified need to protect part of an SDU.

Table B-3: Advanced Orbiting Systems Selection (Continued)

Security Service	Advanced Orbiting Systems SDL Protocol Analysis						Remarks
	Definition	Threats	Impact	Priority	Applicability	Residual Risk	
Connection less integrity	This service, when provided by the (N)-layer, provides integrity assurance to the requesting (N+l)-entity. This service provides for the integrity of a single connectionless SDU and may take the form of determination of whether a received SDU has been modified. Additionally, a limited form of detection of replay may be provided.	Malicious message modification.	Up to loss of mission.	High.	Considered a very critical objective of SDLS protocol.	Minor if implementation of countermeasure is adequate and well managed.	Dependent on cryptographic strength (MAC length, key length, algorithm) and key management policy. Replay detection is an integral part of SDLS.
Selective field connection less integrity	This service provides for the integrity of selected fields within a single connectionless SDU and takes the form of determination of whether the selected fields have been modified.				N/A.		The SDLS protocol will protect the SDUs identified and defined in the TC SDL protocol. There is no need identified to protect part of an SDU.

Table B-3: Advanced Orbiting Systems Selection (Continued)

Security Service	Advanced Orbiting Systems SDL Protocol Analysis						Remarks
	Definition	Threats	Impact	Priority	Applicability	Residual Risk	
Non-repudiation							
Non-repudiation with proof of origin	The recipient of data is provided with proof of the origin of data. This will protect against any attempt by the sender to falsely deny sending the data or its contents.				Not relevant for space data links.		The TC application is not concerned with denial of telecommand sending.
Non-repudiation with proof of delivery	The sender of data is provided with proof of delivery of data. This will protect against any subsequent attempt by the recipient to falsely deny receiving the data or its contents.				Not relevant for space data links.		The TC application is not concerned with denial of telecommand reception.

ANNEX C

CCSDS SPACE DATA LINK SECURITY PROTOCOL

USER'S REQUIREMENTS DOCUMENT

VERSION 3 – 10/10/2012

Table of contents

C1 INTRODUCTION

This version is the final version, resulting from various discussions and a conclusion at the October 2012 meeting of the WG. This URD was the agreed basis for the protocol development to be undertaken.

C2 PURPOSE AND SCOPE

C2.1 PURPOSE

The purpose of the document is to list all the functional, operational, performance and non-functional requirements applicable to a future CCSDS interoperable Data Link Layer security protocol. In this document, we want to avoid specifying any solution or pieces of it.

C2.2 SCOPE

This URD focuses on the security protocol to be integrated with the Data Link Layer of CCSDS space links. Choice and definition of algorithms (authentication and/or encryption) are not part of this specification, only constraints (if any) applicable to algorithms are listed.

C3 REFERENCE DOCUMENTS

[RD 1] : *Overview of Space Communications Protocols*. Issue 4. Report Concerning Space Data System Standards (Green Book), CCSDS 130.0-G-4. Washington, D.C.: CCSDS, April 2023.

[RD 2] : CCSDS handbook, “Space data link protocols – Summary of concept and rationale”, CCSDS 130.2-G-1

[RD 3] : ECSS standard, “Space data links – Telecommand protocols, synchronization and channel coding”, ECSS-E50-04A

[RD 4] : ECSS standard, « Space data links – Telemetry transfer frame protocol”, ECSS-E50-03A

[RD 5] : Agence Spatiale Européenne, « Telecommand Decoder Specification », ESA PSS-04-151 Issue 1, September 1993

C4 APPLICABLE DOCUMENTS

[AD 1] : CCSDS recommendation, “TM space data link protocol”, CCSDS 132.0-B-1

[AD 2] : CCSDS recommendation, “TC space data link protocol”, CCSDS 232.0-B-1

[AD 3] : CCSDS recommendation, “Proximity-1 Space data link protocol – Data Link Layer”, CCSDS 211.0-B-4

[AD 4] : CCSDS recommendation, “AOS space data link protocol”, CCSDS 732.0-B-1

[AD 5] : CCSDS draft recommended practice, “CCSDS recommended practice for symmetric encryption”, CCSDS 353.0-R-1

[AD 6] : CCSDS draft recommended practice, “CCSDS recommended practice for authentication”, CCSDS 352.0-R-0

[AD 7] : CCSDS recommendation, “Communications Operations Procedure -1 (COP-1)”, CCSDS 232.1-B-1

C5 REQUIREMENTS

C5.1 OVERVIEW

The security protocol operates at the data link layer. It protects the data field of transfer frames, not the header. The frame headers and OCF are left in clear so that the security protocol is transparent for frame synchronisation, acquisition and validation. Security protocol may contribute to frame validation.

Security protocol is based on symmetric cryptographic system. The keys are kept secret between sending entity and receiving entity.

The security protocol shall be compatible with the three CCSDS data link protocols (TM, TC, AOS) [AD1, 2, 4].

C5.2 CONVENTIONS

The following conventions apply throughout this Recommendation:

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.

C5.3 COMPATIBILITY WITH CCSDS STANDARDS

C5.3.1 TM space data Link

N£ SECTMTC_URD_1010 £N

T£ The Secure Space Data Link Protocol shall be compatible with the CCSDS TM Space Data Link Protocol, as defined in [AD 1]. It shall not interfere with frame synchronization, acquisition and validation (also it can contribute to frame validation when active) . Presently defined fields of primary header of transfer frames should be unaltered by the security protocol. £T

[COMPLIANT]

C5.3.2 TC space data link

N£ SECTMTC_URD_1020 £N

T£ The Secure Space Data Link Protocol shall be compatible with the CCSDS TC Space Data Link Protocol, as defined in [AD 2]. It shall not interfere with frame synchronization ,

acquisition and validation (also it can contribute to frame validation when active). Presently defined fields of primary header of transfer frames should be unaltered by the security protocol. £T

[COMPLIANT]

C5.3.3 AOS space data link protocol

N£ SECTMTC_URD_1030 £N

T£ The Secure Space Data Link Protocol shall be compatible with the CCSDS AOS Space Data Link Protocol, as defined in [AD 4], both for uplink and downlink. It shall not interfere with frame synchronization , acquisition and validation (also it can contribute to frame validation when active).. Presently defined fields of primary header of transfer frames should be unaltered by the security protocol. £T

[COMPLIANT]

C5.3.4 COP-1

N£ SECTMTC_URD_1040 £N

T£ The Secure Space Data Link Protocol shall be compatible with the Communications Operations Procedure-1 (COP-1), as described in [AD 7] when used in conjunction with the TC space data link protocol or with the AOS space data link protocol (both uplink and downlink). £T

[COMPLIANT]

C5.4 USER SERVICES REQUIREMENTS

N£ SECTMTC_URD_2010 £N

T£ For the TC space data link, the Secure Space Data Link Protocol shall protect the following user services :

- MAPP, MAPA : mandatory
- VCP, VCA, VCF, MCF : optional. £T

[COMPLIANT]

N£ SECTMTC_URD_2020 £N

T£ For the TM space data link, the Secure Space Data Link Protocol shall protect the following user services :

- PACKET, VCA : mandatory
- VC_FSH, MC_FSH, VCF, MCF : optional. £T

[COMPLIANT]

N£ SECTMTC_URD_2030 £N

T£ For the AOS space data link, the Secure Space Data Link Protocol shall protect the following user services :

- PACKET, VCA : mandatory
- BITSTREAM, INSERT, VCF, MCF : optional. £T

[COMPLIANT]

C5.5 SECURE CHANNELS AND PROTOCOL SELECTIVITY

N£ SECTMTC_URD_3010 £N

T£ For the TC link, the Secure Space Data Link Protocol shall provide establishment and management of end to end logical secure channels between a ground system and a spacecraft, these logical secure channels being based on a combination of :

- MAPID
- VCID
- MCID i.e. on SCID (support of multi-satellites configuration). £T

[PARTIALLY COMPLIANT]

[The current version of the SDLS is compatible with this requirement. However, no establishment or management procedure is defined in the standard.]

N£ SECTMTC_URD_3020 £N

T£ For the TC link, the Secure Space Data Link Protocol shall provide establishment and management of end to end logical secure channels between a ground system and a spacecraft, these logical secure channels being based on a combination of :

- VCID
- MCID i.e. on SCID . £T

[PARTIALLY COMPLIANT]

[The current version of the SDLS is compatible with this requirement. However, no establishment or management procedure is defined in the standard.]

N£ SECTMTC_URD_3030 £N

T£ The Secure Space Data Link Protocol shall allow establishment of several concurrent secure channels (i.e. simultaneously active) over a physical channel. £T

[COMPLIANT]

N£ SECTMTC_URD_3040 £N

T£ The Secure Space Data Link Protocol shall allow establishment of new secure channels while other secure channels are already established and active. £T

[COMPLIANT]

N£ SECTMTC_URD_3050 £N

T£ The Secure Space Data Link Protocol shall insure independent management of each secure channel, this covering at least (non exhaustive list):

- Security service selection and configuration (cryptographic algorithm, mode of operation,…)
- Key management
- Anti-replay counter management,
- … £T

[PARTIALLY COMPLIANT]

[The current version of the SDLS is compatible with this requirement. However, no management procedure is defined in the standard.]

N£ SECTMTC_URD_3060 £N

T£ The Secure Space Data Link Protocol shall be compatible with the multiplexing of both clear and secure channels over a physical channel. £T

[COMPLIANT]

C5.6 SECURITY REQUIREMENTS

C5.6.1 Security objectives

The Secure Space Data Link Protocol shall implement four security functions based on cryptographic mechanisms : Confidentiality, integrity, authentication, anti-replay. The non-

repudiation function is not seen as necessary for space data links and therefore not part of the Secure Space Data Link Protocol .

N£ SECTMTC_URD_4010 £N

T£ The Secure Space Data Link Protocol shall fulfil the following security objectives for all secure channels established over a TC / Forward link :

- Command Authenticity
- Command Integrity
- Command Confidentiality
- Command Anti-replay protection
- Denial of Service Protection for Sequenced Control Service (COP-1 procedure) (TBC)
- Protection against TC link Traffic Analysis applicable at least at APID level. £T

[PARTIALLY COMPLIANT]

[The current version of the SDLS does not allow Denial of Service protection of the Sequenced Control Service (COP-1 procedure).]

[The current version of the SDLS does not allow TC link Traffic Analysis protection at APID level (MAPID always transmitted in cleartext).]

N£ SECTMTC_URD_4020 £N

T£ The Secure Space Data Link Protocol shall fulfil the following security objectives for all secure channels established over a TM / AOS Return link :

- TM data Authenticity
- TM data Integrity
- TM data Confidentiality
- TM Frame Anti-replay protection (optional)
- Protection against TM link Traffic Analysis applicable at least at APID level. £T

[PARTIALLY COMPLIANT]

[The current version of the SDLS does not allow TM link Traffic Analysis protection at APID level.]

N£ SECTMTC_URD_4030 £N

T£ Anti-replay protection shall be an optional facility for TM/AOS links, i.e. it shall be possible to select it or not for a given mission. £T

[COMPLIANT]

C5.6.2 Security services

Considering the following :

- Encryption only (without data integrity) is not recommended for a space link, even for the TM link, as it can lead to security breaches,
- The Data Integrity function also provides Authentication,

Then two security services can be defined :

- Authentication service, which provides authentication, integrity, and anti-replay functions, to be used on a space link when the data confidentiality function is not required,
- Encryption + Authentication, called Authenticated Encryption, which provides data confidentiality, data integrity, authentication, and anti-replay functions.

[The current version of the SDLS defines a third service, “Encryption Only”, to be used only on the TM link. Although theoretically not secure, it provides confidentiality, and can be secure if the authentication service is achieved by another channel. It has been judged useful for some missions (ex. Video channel)]

N£ SECTMTC_URD_5010 £N

T£ The Secure Space Data Link Protocol shall provide two independent security services applicable to the secure channels established over a TC link :

- Authentication service, which provides command authenticity, integrity, and anti-replay protection,
- Authenticated Encryption service, which provides command confidentiality, integrity, authenticity, and anti-replay protection. £T

[COMPLIANT]

N£ SECTMTC_URD_5020 £N

T£ The Secure Space Data Link Protocol shall provide two independent security services applicable to the secure channels established over a TM / AOS link :

- Authentication service, which provides TM data authenticity, integrity, and (optional) anti-replay protection,

- Authenticated Encryption service, which provides TM data confidentiality, integrity, authenticity, and (optional) anti-replay protection. £T

[COMPLIANT]

[The current version of the SDLS also defines a third service, “Encryption Only”, to be used only on the TM link. Although theoretically not secure, it provides confidentiality and can be secure if the authentication service is achieved by another channel. It has been judged useful for some missions (ex. Video channel)]

N£ SECTMTC_URD_5030 £N

T£ For a TC / Forward link, the Secure Space Data Link Protocol shall allow the selection between Authentication service or Authenticated Encryption service for any secure channel. £T

[COMPLIANT]

N£ SECTMTC_URD_5040 £N

T£ For a TM / Return link, the Secure Space Data Link Protocol shall allow the selection between Authentication service or Authenticated Encryption service for any secure channel. £T

[COMPLIANT]

N£ SECTMTC_URD_5050 £N

T£ The Secure Space Data Link Protocol shall insure full independence of security services selection between the TC / Forward link and the TM/ Return link. £T

[COMPLIANT]

N£ SECTMTC_URD_5060 £N

T£ For anti-replay protection over a given secure channel, the Secure Space Data Link Protocol shall use a dedicated counter which is part of the authenticated data and which size shall not be less than 32 bits (TBC). £T

[PARTIALLY COMPLIANT]

[The current version of the SDLS allows a transmitted counter size down to 16 bits.]

N£ SECTMTC_URD_5070 £N

T£ For the anti-replay counter management, the Secure Space Data Link Protocol shall allow a jump / forward mechanism within a sliding window. £T

[COMPLIANT]

C5.7 SECURITY SERVICES DESCRIPTION

C5.7.1 Authentication

N£ SECTMTC_URD_6010 £N

T£ The Secure Space Data Link Protocol shall implement a security function allowing authentication of the sender. This security function shall be based on a cryptographic algorithm and a mode of operation as specified in [AD 6] for symmetric keys systems. Authentication without confidentiality should be implemented using a "clear text with appended Message Authentication Code (MAC)" system. £T

Also full flexibility of choice is left to the user for the cryptographic algorithm to be used with this Data Link Security protocol (cf. requirement C5.6.1), a baseline algorithm for authentication is selected to enable interoperability testing. This baseline algorithm for authentication with symmetric keys is : HMAC with SHA256 (cf. [AD6]).

[COMPLIANT]

C5.7.2 Authenticated encryption

N£ SECTMTC_URD_6020 £N

T£ The Secure Space Data Link Protocol shall implement a security function allowing authentication of the sender and integrity/confidentiality of the frame data field. This security function shall be based on a cryptographic algorithm and a mode of operation as specified in [AD5] for symmetric keys systems and authentication encryption mode. £T

Also full flexibility of choice is left to the user for the cryptographic algorithm to be used with this Data Link Security protocol (cf. requirement C5.6.1), a baseline algorithm for authenticated encryption is selected to enable interoperability testing. This baseline algorithm for authenticated encryption with symmetric keys is : Galois Counter Mode (GCM) of AES block cipher algorithm (cf. [AD5]).

[COMPLIANT]

C5.8 SECURITY FUNCTIONS POSITION

N£ SECTMTC_URD_7010 £N

T£ The Secure Space Data Link Protocol shall operate within the data link protocol sub-layer of the CCSDS data link layer. £T

[COMPLIANT]

N£ SECTMTC_URD_7020 £N

T£ The full TC security function covering both Authentication and Authenticated Encryption security services shall be located in a unique position within the TC data link protocol sub-layer. £T

[COMPLIANT]

N£ SECTMTC_URD_7030 £N

T£ The full TM / AOS security function covering both Authentication and Authenticated Encryption security services shall be located in a unique position within TM or AOS data link protocol sub-layer. £T

[COMPLIANT]

C5.9 PROTECTED FIELDS

N£ SECTMTC_URD_8010 £N

T£ The Secure Space Data Link Protocol shall operate on the TC transfer frame data field. £T

[COMPLIANT]

N£ SECTMTC_URD_8020 £N

T£ The Secure Space Data Link Protocol shall let both TC transfer frame header and FEC trailer in clear form (i.e. unencrypted) whatever the selected security service for a secure channel is. £T

[COMPLIANT]

N£ SECTMTC_URD_8030 £N

T£ The Secure Space Data Link Protocol shall operate on the TM/AOS transfer frame data field. £T

[COMPLIANT]

N£ SECTMTC_URD_8040 £N

T£ The Secure Space Data Link Protocol shall let both TM/AOS transfer frame header and OCF/FEC trailer in clear form (i.e. unencrypted) whatever the selected security service for a secure channel is. £T

[COMPLIANT]

N£ SECTMTC_URD_8050 £N

T£ The Secure Protocol Data Unit (SPDU) shall consist of :

- a security header,
- a secure data field
- a security trailer (optional). £T

[COMPLIANT]

N£ SECTMTC_URD_8060 £N

T£ The security header shall include all required security context information from the sending side about the concerned secure channel to allow the receiving side to perform authentication / encryption or decryption on the received SPDU. £T

[COMPLIANT]

N£ SECTMTC_URD_8070 £N

T£ The secure data field shall contain the result of the clear data field authentication / encryption operation performed by the sending side. £T

[COMPLIANT]

N£ SECTMTC_URD_8080 £N

T£ The (optional) security trailer may contain the Integrity Check Value (ICF) computed by the authentication process. £T

[COMPLIANT]

N£ SECTMTC_URD_8090 £N

T£ The authentication process shall apply at least to the full frame data field including the security header (if any) inserted by the Secure Space Data Link Protocol. £T

[COMPLIANT]

N£ SECTMTC_URD_8100 £N

T£ The encryption process shall apply to the frame data field. £T

[COMPLIANT]

C5.10 CRYPTOGRAPHIC ALGORITHMS AND PROTOCOL DEPENDANCY

N£ SECTMTC_URD_9000 £N

T£ The Secure Space Data Link Protocol shall not be dependant on a particular cryptographic algorithm. It shall be able to work with a family of algorithms, as described in [AD 5] and [AD 6]. This family is part of the symmetric-key algorithms family.

The Secure Space Data Link Protocol shall be independent from the three following data link protocols : TC, TM, AOS, and should be able to operate with the same data formats with all three protocols. £T

[COMPLIANT]

C5.11 OPERATION MODES

C5.11.1 Secure / Clear modes

N£ SECTMTC_URD_ 10000 £N

T£ The Secure Space Data Link Protocol shall support two operational modes for each logical communication channel managed over TC and TM / AOS links :

- Clear Mode, or transparent mode, where data is left unchanged
- Secure Mode covering either Authentication or Authenticated Encryption services. £T

[COMPLIANT]

N£ SECTMTC_URD_ 10010 £N

T£ The Secure Space Data Link Protocol shall support the following configurations for TC and TM / AOS Clear Mode :

- Clear Mode is limited to ground activities only
- Clear Mode is limited to ground activities and on-board contingency situations
- Clear Mode can be selected on-board at any time from ground segment. £T

[COMPLIANT]

N£ SECTMTC_URD_ 10020 £N

T£ The on-board TC or TM / AOS Clear Mode selection from ground shall only be possible via a secure command. £T

[PARTIALLY COMPLIANT]

[The current version of the SDLS is compatible with this requirement. However, it does not define any clear mode / secure mode selection command]

N£ SECTMTC_URD_10030 £N

T£ For a TC link it shall be possible to either authorise on-board automatic switch to Clear Mode following a set of predefined on-board events (emergency situation, safe mode, TC timer expiration,…) or to forbid on-board automatic switch to Clear Mode. £T

[PARTIALLY COMPLIANT]

[The current version of the SDLS is compatible with this requirement. However, it does not define any management for switching between clear mode / secure mode]

N£ SECTMTC_URD_ 10040 £N

T£ For a TC link, it shall be possible in case on-board automatic switch in Clear Mode is forbidden, to authorise on-board automatic switch in a Reduced Secure Mode following a set of predefined on-board events (Emergency situation ,safe mode, TC timer expiration,...). £T

[PARTIALLY COMPLIANT]

[The current version of the SDLS is compatible with this requirement. However, it does not define any management for switching between clear mode / secure mode]

N£ SECTMTC_URD_ 10050 £N

T£ The TC Reduced Secure Mode shall include at least :

- Deactivation of TC encryption function (i.e. Authentication only)
- Deactivation of anti-replay protection or acceptation of TC which are out of sequence (ARC sliding window). £T

[PARTIALLY COMPLIANT]

[The current version of the SDLS is compatible with this requirement. However, it does not define any Reduced Secure Mode]

N£ SECTMTC_URD_10060 £N

T£ The TC Reduced Secure Mode may allow (TBC) a subset of telecommands to be transmitted in clear form (only low priority commands which can endanger neither satellite safety nor the mission). £T

[PARTIALLY COMPLIANT]

[The current version of the SDLS is compatible with this requirement. However, it does not define any Reduced Secure Mode]

N£ SECTMTC_URD_10070 £N

T£ The Secure Space Data Link Protocol shall be compatible with a constant TM / AOS frame length (fixed value for a given mission) whatever TM / AOS Clear Mode or Secure Mode is selected on the logical communication channel. £T

[COMPLIANT]

N£ SECTMTC_URD_10080 £N

T£ The Secure Space Data Link Protocol shall insure a constant TM / AOS frame data field useful length available to TM / AOS users. £T

[COMPLIANT]

N£ SECTMTC_URD_10090 £N

T£ For the secure TM / AOS protocol and for a given secure channel, the current Clear / Secure mode shall be explicitly indicated within the dedicated security protocol data unit (security header or trailer). £T

[NOT COMPLIANT]

[The current version of the SDLS does not define any flag explicitly indicating clear or secure mode]

C5.11.2 Key Management

N£ SECTMTC_URD_11010 £N

T£ The Secure Space Data Link Protocol shall support the use of shared keys between ground and on-board security functions. £T

[COMPLIANT]

N£ SECTMTC_URD_11020 £N

T£ The Secure Space Data Link Protocol shall be compatible with the following schemes for key management :

- Scheme 1 : all session keys are pre-loaded on satellite before launch and cover the whole mission lifetime,
- Scheme 2 : a subset of keys (master keys / KeK and session keys) are pre-loaded on satellite before launch; session keys are uploaded encrypted during satellite operation (On The Air Rekeying, OTAR),
- Scheme 3 : a subset of keys (master keys / KeK and session keys) are pre-loaded on satellite before launch; session keys are generated on-board from master keys and an input uploaded non secret seed. £T

[COMPLIANT]

N£ SECTMTC_URD_11030 £N

T£ The Secure Space Data Link Protocol shall provide an efficient reporting mechanism, detailing key status (last key used, integrity of master keys and sessions keys stored on-board,…) as well as the status of key reception / generation / validation / storage process of the OTAR facility. £T

[PARTIALLY COMPLIANT]

[The current version of the SDLS is compatible with this requirement. However, it does not define any reporting mechanism]

N£ SECTMTC_URD_11040 £N

T£ The Secure Space Data Link Protocol shall support explicit key selection for all TC or TM channels (key number / identifier present in TC / TM security header). £T

[COMPLIANT]

N£ SECTMTC_URD_11050 £N

T£ The Secure Space Data Link Protocol shall provide the following facilities via security control directives :

- Key selection (for TM link),
- Key upload (OTAR) or on-board key renewal,
- Key status request covering from one key up to the complete key set,
- Key disabling (i.e. deactivation). £T

[PARTIALLY COMPLIANT]

[The current version of the SDLS is compatible with this requirement. However, it does not define any key management procedure]

C5.11.3 On-board TM/TC control and monitoring

N£ SECTMTC_URD_12010 £N

T£ The Secure Space Data Link Protocol shall support a set of on-board TC Security control directives managed as in-band commands, i.e. interpreted and executed internally by the security device immediately after the security process (Authentication / Decryption). £T

[PARTIALLY COMPLIANT]

[The current version of the SDLS is compatible with this requirement. However, it does not define any security control directive]

N£ SECTMTC_URD_12020 £N

T£ For a given secure channel, the TC Security control directives shall cover :

- ARC value setting
- ARC window value setting

- On-board security function test request
- On-board keys status request
- Key upload (OTAR facility) or on-board key renewal
- Dummy command (Requiring no action. Used for test purposes)
- (Others commands to be defined). £T

[PARTIALLY COMPLIANT]

[The current version of the SDLS is compatible with this requirement. However, it does not define any security control directive]

N£ SECTMTC_URD_12030 £N

T£ The TC Security control directives shall be protected at least at the same level as the one currently applied to the TC link and carried through a dedicated secure TC channel. £T

[PARTIALLY COMPLIANT]

[The current version of the SDLS is compatible with this requirement. However, it does not define any security control directive]

N£ SECTMTC_URD_12040 £N

T£ The Secure Space Data Link Protocol shall support a set of on-board TC Security monitoring data covering at least :

- Acknowledgement / response to on-board security control directives
- Status of on-board current security session (identifier of last key used, current ARC value, current ARC window value,…)
- Events / Alarms associated with on-board security function
- (Others to be defined). £T

[PARTIALLY COMPLIANT]

[The current version of the SDLS is compatible with this requirement. However, it does not define any TC security monitoring data]

N£ SECTMTC_URD_12050 £N

T£ The TC Security monitoring data management shall be compatible with ground secure TC protocol operation and synchronisation constraints (ex : ground automation for ARC synchronisation from TM). £T

[PARTIALLY COMPLIANT]

[The current version of the SDLS is compatible with this requirement. However, it does not define any TC security monitoring data]

N£ SECTMTC_URD_12060 £N

T£ The TC Security monitoring data shall be carried by a dedicated TM channel, secure if necessary. £T

[PARTIALLY COMPLIANT]

[The current version of the SDLS is compatible with this requirement. However, it neither defines any TC security monitoring data nor the way to transmit them to ground]

N£ SECTMTC_URD_12070 £N

T£ The Secure Space Data Link Protocol shall support a set of on-board TM/AOS security control directives covering at least :

- Key selection
- On-board security function test request
- On-board key status request
- Key upload (OTAR facility) or on-board key renewal
- (Others to be defined). £T

[PARTIALLY COMPLIANT]

[The current version of the SDLS is compatible with this requirement. However, it does not define any TM/AOS security control directives]

N£ SECTMTC_URD_12080 £N

T£ The TM/AOS security control directives shall be protected at least as the same level as the one currently applied to the TC link and carried through a dedicated TC secure channel. £T

[PARTIALLY COMPLIANT]

[The current version of the SDLS is compatible with this requirement. However, it does not define any TM/AOS security control directives]

N£ SECTMTC_URD_12090 £N

T£ The Secure Space Data Link Protocol shall support a set of on-board TM/AOS monitoring data covering at least :

- Acknowledgement / response to on-board security control commands
- Status of on-board current TM security session
- Events / Alarms associated with on-board TM/AOS security function
- (Others to be defined). £T

[PARTIALLY COMPLIANT]

[The current version of the SDLS is compatible with this requirement. However, it does not define any TM/AOS security monitoring data]

N£ SECTMTC_URD_12100 £N

T£ The TM/AOS Security monitoring data shall be carried by a dedicated TM/AOS channel, secure if necessary. £T

[PARTIALLY COMPLIANT]

[The current version of the SDLS is compatible with this requirement. However, it does not define any TM/AOS security monitoring data]

N£ SECTMTC_URD_12110 £N

T£ The Secure Space Data Link Protocol shall provide efficient reporting of on-board TC / TM security functions status, allowing adequate diagnostic of failure cases. £T

[PARTIALLY COMPLIANT]

[The current version of the SDLS is compatible with this requirement. However, it does not define any on-board TC/TM security functions status]

C5.12 DESIGN CONSTRAINTS

C5.12.1 Performances

N£ SECTMTC_URD_ 13010 £N

T£ The Secure Space Data Link Protocol shall not introduce more than 50% overhead on shortest CLTU (for TC), depending on security associations settings, so that emergency operations (e.g. : tumbling spacecraft) could be potentially be conducted in secure mode. £T

[PARTIALLY COMPLIANT]

[The current version of the SDLS may introduce more than 50% overhead on short CLTU]

N£ SECTMTC_URD_13020 £N

T£ The Secure Space Data Link Protocol shall support the management of at least 256 (TBC) secure channels over a physical channel. £T

[COMPLIANT]

N£ SECTMTC_URD_13030 £N

T£ The Secure Space Data Link Protocol shall insure via adequate secure channel configuration (selection of authentication or authenticated encryption algorithms) a probability of non detection and rejection of an invalid TC less than 10^{-20} (TBC). £T

[PARTIALLY COMPLIANT]

[The current version of the SDLS is compatible with this requirement. However, the minimum length allowed for the transmitted MAC is 8 octets, leading to a probability of non detection and rejection of an invalid TC of 5.42 10^{-20}]

N£ SECTMTC_URD_13040 £N

T£ The Secure Space Data Link Protocol shall not introduce more than 5% overhead on TM/AOS link. £T

[COMPLIANT]

N£ SECTMTC_URD_13050 £N

T£ The Secure Space Data Link Protocol shall not impact availability and reliability of so-called High Priority Commands supporting critical commands (ON/OFF, nominal/redundant equipment selection,…) used during satellite bus configuration / reconfiguration operations. £T

Note : in the current ESA TC decoder, this apply to direct commands using MAP0 address which are routed to the CPDU interface of the TC decoder.

[NOT APPLICABLE]

[Implementation dependant]

N£ SECTMTC_URD_13060 £N

T£ The Secure Space Data Link Protocol shall allow the generated security monitoring data to be managed as high priority TM and by-pass the on-board computer if required. £T

[PARTIALLY COMPLIANT]

[The current version of the SDLS is compatible with this requirement. However, it does not define any security monitoring data]

N£ SECTMTC_URD_13070 £N

T£ The Secure Space Data Link Protocol shall allow adequate secure channel configuration (selection of efficient cryptographic algorithm and modes of operation) to insure there is no error propagation for a given space link. £T

[COMPLIANT]

N£ SECTMTC_URD_13080 £N

T£ The Secure Space Data Link Protocol shall not allow any loss of a frame for a secure channel following a change of key. £T

[COMPLIANT]

N£ SECTMTC_URD_13090 £N

T£ The Secure Space Data Link Protocol shall not allow any loss of frame for a secure channel following the switch from Clear Mode to Secure Mode or from Secure Mode to Clear Mode. £T

[COMPLIANT]

C5.12.2 Operational constraints

N£ SECTMTC_URD_14010 £N

T£ The Secure Space Data Link Protocol shall insure a clear separation between the telecommunication function and the security function within the data link layer. £T

[COMPLIANT]

N£ SECTMTC_URD_14020 £N

T£ The Secure Space Data Link Protocol shall not interfere with standard SDLP TC or TM/AOS frame verification and validation procedures. £T

[COMPLIANT]

N£ SECTMTC_URD_14030 £N

T£ The Secure Space Data Link Protocol shall provide efficient recovery and reporting from contingency situations linked to on-board security unit (ARC or session key corruption, on-board authentication failure, power loss, …). £T

[PARTIALLY COMPLIANT]

[The current version of the SDLS is compatible with this requirement. However, it does not define any reporting or recovery policy]

N£ SECTMTC_URD_14040 £N

T£ The Secure Space Data Link Protocol shall provide efficient recovery and reporting from contingency situations at satellite level (ex : TM loss, on-board reconfiguration). £T

[PARTIALLY COMPLIANT]

[The current version of the SDLS is compatible with this requirement. However, it does not define any reporting or recovery policy]

C5.12.3 Compatibility with on board configurations

N£ SECTMTC_URD_15010 £N

T£ The Secure Space Data Link Protocol shall allow establishment of end to end secure channels between a ground system and a spacecraft accessed via an on-board space network, without implying implementation of TC or TM/AOS security functions in intermediate space relay nodes (ex : relay satellites). £T

[COMPLIANT]

N£ SECTMTC_URD_15020 £N

T£ The Secure Space Data Link Protocol shall be compatible with both :

- On-board centralised security architecture (i.e. it shall not cause unexpected spreading of on-board security functions)
- On-board distributed security architecture. £T

[COMPLIANT]

N£ SECTMTC_URD_15030 £N

T£ The Secure Space Data Link Protocol shall not impact on-board TC chain and TM chain redundancy. £T

[COMPLIANT]

C5.12.4 Compatibility with ground configurations

N£ SECTMTC_URD_16010 £N

T£ The Secure Space Data Link Protocol shall allow establishment of end to end secure channels between a spacecraft and either a ground station or an operation control or data processing center, without implying implementation of TC or TM/AOS security functions in any intermediate ground nodes. £T

[COMPLIANT]

N£ SECTMTC_URD_16020 £N

T£ The Secure Space Data Link Protocol shall be compatible with the following CCSDS SLE services for ground segment :

- For TC : F-CLTU, F-TCF
- For TM / AOS : R-AF, R-CF, R-OCF (TBC). £T

[COMPLIANT]

N£ SECTMTC_URD_16030 £N

T£ The Secure Space Data Link Protocol shall not impact ground segment TC chain and TM chain redundancy. £T

[COMPLIANT]

N£ SECTMTC_URD_16040 £N

T£ The Secure Space Data Link Protocol shall be compatible with both :

- Ground segment centralised security architecture (i.e. it shall not cause unexpected spreading of ground security functions)
- Ground segment distributed security architecture. £T

[COMPLIANT]

C5.12.5 Security constraints

N£ SECTMTC_URD_17010 £N

T£ The Secure Space Data Link Protocol shall be compatible with secure on-board or ground configurations where the security unit is physically in-line. £T

[COMPLIANT]

N£ SECTMTC_URD_17020 £N

T£ The Secure Space Data Link Protocol shall be compatible with security evaluation of corresponding on-board and ground security functions implementations based on Common Criteria requirements. £T

[COMPLIANT]

N£ SECTMTC_URD_17030 £N

T£ The Secure Space Data Link Protocol shall be compatible with security validation of corresponding on-board and ground security functions implementations based on NIST FIPS-140-2. £T

[COMPLIANT]

ANNEX D

INTERACTION WITH DATA LINK PERFORMANCE

D1 PURPOSE

This analysis illustrates the compatibility of TC, TM, AOS, and USLP SLPs with SDLS protocol with respect to data integrity performance.

D2 INTRODUCTION

When the authentication service is applied, the SDLS protocol protects against malicious attempts to manipulate the data or spoof the data source. The SDL protocol protects, to a certain extent, the data transactions against communications channel transmission errors. Thus, although for different objectives, both protocols incorporate integrity error detection mechanisms.

For FDIR and operational reliability, it would be advisable that the integration of the SDLS and the SDL protocols is such that it allows an easy distinction and identification of the nature of integrity errors (communications or security) when they manifest themselves. This is of particular concern for TC application.

Theoretically, the efficiency of an authentication mechanism in detecting integrity errors on a message is much higher than classical communications integrity error detection mechanisms like the CRC. The typically much longer length of the MAC, ranging from 64 to 512 bits in SDLS, compared to the CRC (16-bits), is the main reason for this.

If the data received before security processing is not sufficiently protected against undetected data bit transmission errors, there could be a risk that such errors will be detected by the security mechanism (MAC) but not by the channel error detection (and correction) mechanism. Such an event could lead to confusion and unreliable error detection and recovery during mission operations.

D3 TELECOMMAND

In order to prevent that mission operations event and anticipating a deficit in TC SDL performance, the following two options to reinforce the separation between SDL and SDLS were identified, considered, and investigated:

- recommend the mandatory use of a CRC on the TC SDL protocol (now optional) when implementing as well the SDLS protocol;
- introduce an additional CRC mechanism on the SDLS protocol for the sole purpose of ensuring a ‘cleaner’ message before security processing.

The first option appeared to introduce a reasonable penalty in data throughput with a clear operational benefit. Nevertheless, the performance advantage in using a CRC on undetected error detection had to be evaluated. The second option would duplicate functions typical of SDL into the SDLS and would, therefore, not be advisable.

Actions were taken to determine numerical requirements for the separation between security and transmission error detections; to evaluate the performance advantage in using a CRC on undetected error detection, considering all channel coding options supported by TC SLP; and to conclude on a broader recommendation for the need (or not) of CRCs.

D4 TELECOMMAND ANALYSIS

Reference [28] provides detailed rationale for the TC channel coding and, in particular, presents tables reporting the undetected error performance data and the relationship of that performance data to BER, with respect to the coding mode and the presence or absence of CRC.

The TC channel coding provides two modes of BCH channel coding: Triple Error Detection (TED) and Single Error Correction (SEC).

The decision to incorporate a CRC is left to the discretion of the user. However, the choices made by the user need to be consistent with meeting the required SDL integrity performance.

The requirement for TC Transfer Frame undetected error rate is provided in reference [28], subsection 9.2.3. Quoting from the document: “A maximum of one TC Transfer Frame for every 10^9 frames transmitted is erroneously accepted (that is, contains one or more undetected bit errors).”

The examination of the previously mentioned tables on undetected error performance indicates that such a requirement is met with the following conditions:

Evaluation without CRC:

- BER< 10^{-4} when in TED mode, regardless of the number of codeblocks;
- BER<10^{-5} when in SEC mode, regardless of the number of codeblocks.

Evaluation with CRC:

- BER<10^{-4} when in TED mode, regardless of the number of codeblocks;
- BER<10^{-4} when in SEC mode, regardless of the number of codeblocks.

Some points are worth recalling:

- TED mode offers a better performance than SEC mode for undetected error. SEC mode cannot meet the requirement when 10^{-5}<BER<10^{-4}.
- The presence of CRC substantially reduces the probabilities.

Is it important that the SDL integrity performance requirement (10^{-9}) remain or become more stringent when security is applied? The requirement implies that, on average, one in a billion frames could contain an undetected error.

To have an indication of what this means in practice, with an 8-kbit/s TC uplink (~1 frame/s with 1000 octet frame), it would take approximately 500 million seconds (~ 16 years) of continuous transmission to face an undetected error.

As an example, ESA has adopted the SEC mode and the mandatory presence of CRC in its TC Standard (reference [24]). With BER<10^{-4}, the achievable undetected frame error rate is below 10^{-15}. This is 6 orders of magnitude better than the requirement.

D5 TELECOMMAND CONCLUSION

A modification of the performance requirement for undetected error (10^{-9}) does not appear to be required.

As long as the BER conditions to fulfill this performance are met for the particular missions (i.e., BER<10^{-5}), undetected error is expected to be present typically once in 10 years of operation.

Given this frequency of undetected error, it does not seem worthwhile to impose a mandatory CRC for frames, when security is applied, in order to reduce even more the likelihood that an undetected error is only detected by security (MAC). This conclusion is also valid for the newly introduced short LDPC codes in reference [28], which demonstrate even lower undetected error rates than TC BCH code.

This conclusion is also valid for USLP (reference [31]) when used on the uplink with Variable Length Frames or Fixed Length Frames.

D6 TM, AOS, AND USLP

In contrast to TC, there is no specified undetected error performance for TM, AOS, or USLP, when used on the downlink (transmission of telemetry to ground). However, this does not mean that data integrity is not important or not considered by those standards. Data integrity during transmission and data handling may be protected by TM, AOS, and USLP at their two sublayers: data link and synchronization & channel coding.

For TM, AOS, and USLP data links, the FECF is an optional structural component of the TM Transfer Frame. The purpose of this field is to provide a capability for detecting errors that may have been introduced into the Transfer Frame during the transmission and data handling process. The FECF is a CRC protecting the full Transfer Frame. Whether this field should be used on a particular Physical Channel is determined based on the mission requirements for data quality and the selected options for the underlying channel coding sublayer. This field may be mandatory depending on the selected options for the channel coding sublayer.

Both TM, AOS, and USLP include several synchronization and channel coding options with their particular undetected error performance.

Table D-1 presents the available channel coding options and whether the FECF is optional or mandatory for each one of them.

NOTE – Table D-1 was compiled when LDPC with slicing was not yet available.

Table D-1: Channel Coding Options and CRC Requirement

Channel Coding	CRC	Remarks
No code	Mandatory	
Convolutional	Mandatory	
Reed-Solomon	Optional	With E=16 undetected error performance outperforms a CRC. With E=8 undetected error performance is of the same order of magnitude as the CRC.
Concatenated (Convolutional and Reed-Solomon)	Optional	(See above remarks for Reed-Solomon.)
Turbo	Mandatory	
LDPC	Optional	LDPC undetected error performance outperforms a CRC.

D7 TM, AOS, AND USLP ANALYSIS

USLP, AOS, and TM data link sublayers specify a CRC to enhance data integrity: the 16-bit CCITT CRC. The typical performance of this mechanism is discussed in detail in reference [29], subsection 9.4. USLP provides also an option with a 32-bit CRC.

In particular, it is worth recalling the CRC usage circumstances (reference [29], subsection 9.4.4) reproduced to some extent hereafter and complemented with a consideration of the security aspects.

The 16-bit CRC code can reliably detect incorrect frames with an undetected error rate of around $2^{-15} \approx 3 \cdot 10^{-5}$. This code achieves approximately the same undetected error rate for any of the recommended telemetry channel codes.

As discussed in D2 above, MAC will outperform a CRC in detecting data integrity errors if the CRC is the only mechanism employed by the space link protocol to protect data integrity against transmission and data handling errors.

A much lower undetected error rate than that provided by the 16-bit CRC alone is achieved when the RS code with $E = 16$ is used, either by itself or concatenated with an inner convolutional code. In this case, the undetected error rate of the RS decoder is on the order of $1/E! \approx 5 \cdot 10^{-14}$, which is many orders of magnitude better than the validation offered by the CRC code and even than the requirement established for TC (Undetected Frame Error Rate of 10^{-9}). Thus the error detection capability of the CRC code is superfluous when the RS code with $E = 16$ is used.

The RS code with $E = 8$ offers much lower error detection capability, on the same order as that provided by the 16-bit CRC code. Therefore when RS E=8 is used CRC is optional.

For Turbo codes, a decoder equipped with a smart stopping rule that notes whether the decoder's iterations converge to a valid codeword can achieve some degree of error detectability and somewhat alleviate the need for the 16-bit CRC code. However, in these borderline cases the CRC code is still required.

The CRC is also required for uncoded data or convolutionally coded data, which offer absolutely no capability for error detection on their own.

Concerning the LDPC codes and as specified by the TM synchronization & channel coding Blue Book (reference [30]), subsection 7.2.3.2), the FECF is optional. The undetected frame and bit error rates of these LDPC codes lie several orders of magnitude below the corresponding detected error rates for any given operating signal-to-noise ratio.

If a lower undetected error rate is desired than that offered by the recommended 16-bit CRC code, and RS coding is not used, then one option is to use a 32-bit (option available with USLP) or 48-bit CRC code (not in the CCSDS Recommended Standards).

D8 TELEMETRY AND ADVANCED ORBITING SYSTEMS CONCLUSION

The previous subsection has outlined the existing TM, AOS, and USLP mechanisms to provide data integrity against transmission and data handling errors. Although some coding options, such as Convolutional or Turbo, already mandate the use of a CRC, the use of a CRC is recommended whenever SDLS is applied, except when R-S (E=16) or LDPC codes are employed as channel coding.

If a mission desires an even higher data integrity protection against transmission and data handling errors, the option to use a longer (but non-standard) CRC should be considered. For USLP (reference [31]), a 32-bit CRC is also specified to provide higher data integrity protection against transmission and data handling errors.

ANNEX E

ACRONYMS AND ABBREVIATIONS

This annex lists the acronyms and abbreviations used in this Report.

AAD	additional authenticated data
AES	Advanced Encryption Standard
AOS	Advanced Orbiting Systems
APID	application process identifier
ARSN	anti-replay sequence number
BC	bypass of acceptance check and control
BCH	Bose-Chaudhuri-Hocquenhem
BER	bit error rate
CBC	cipher block chaining
CCSDS	Consultative Committee for Space Data Systems
CLCW	communications link control word
CLTU	command link transmission unit
CMAC	Cipher-based Message Authentication Code
COP	Communications Operation Procedure
COP-1	Communications Operation Procedure-1
CRC	cyclic redundancy check
E	error correcting capability of Reed-Solomon code
ECB	electronic code book
ECF	error control field
ECSS	European Cooperation for Space Standardization
F-CLTU	Forward Command Link Transmission Unit
FDIR	failure detection, isolation, and recovery
FECF	frame error control field
FSH	frame secondary header
FSP	Forward Space Packet
FSR	frame security report

F-TCF	forward telecommand frame
GCM	Galois Counter Mode
GMAC	Galois Message Authentication Code
GVCID	global virtual channel ID
HMAC	Hash-based Message Authentication Code
HPC	high priority command
HPTM	high-priority telemetry
IEC	International Electrotechnical Commission
IP	Internet Protocol
IPSec	Internet Protocol Security
ISO	International Standards Organization
IV	initialization vector
KEK	key encryption key
MAC	Message Authentication Code
MAP	multiplexer access point
MC	master channel
MC_FSH	Master Channel Frame Secondary Header
MC_OCF	Master Channel Operational Control Field
MCID	master channel identifier
MCS	mission control system
N/A	not applicable
NIST	National Institute of Standards and Technology
OBC	on-board computer
OBDH	on-board data handling
OCF	operational control field
OID	only idle data
OSI	Open Systems Interconnection
OTAR	over-the-air rekeying
PCC	payload control and configuration

PDU	protocol data unit
PVN	packet version number
RAF	Return All Frames
RCF	Return Channel Frames
RFSH	return frame secondary header
RS	Reed-Solomon
RSP	Return Space Packet
SA	Security Association
SCID	spacecraft identifier
SDL	space data link
SDLS	Space Data Link Security Protocol
SDU	service data unit
SEC	single error correction
SLE	Space Link Extension
SLP	space link protocol
SPI	security parameter index
TC	telecommand
TCR	telemetry, command, and ranging
TED	triple error detection
TM	telemetry
TRANSEC	transmission security
TTC	telemetry, tracking, and command
URD	user requirements document
USLP	Unified Space Link Protocol
VC	virtual channel
VC_FSH	Virtual Channel Frame Secondary Header
VC_OCF	Virtual Channel Operational Control Field
VCA	virtual channel access
VCID	virtual channel identifier