The Consultative Committee for Space Data Systems

Report Concerning Space Data System Standards

THE APPLICATION OF SECURITY TO CCSDS PROTOCOLS

INFORMATIONAL REPORT

CCSDS 350.0-G-3

GREEN BOOK

March 2019

The Consultative Committee for Space Data Systems

Report Concerning Space Data System Standards

THE APPLICATION OF SECURITY TO CCSDS PROTOCOLS

INFORMATIONAL REPORT

CCSDS 350.0-G-3

GREEN BOOK

March 2019

AUTHORITY

Issue:	Informational Report, Issue 3
Date:	March 2019
Location:	Washington, DC, USA

This document has been approved for publication by the Management Council of the Consultative Committee for Space Data Systems (CCSDS) and reflects the consensus of technical panel 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
E-mail: secretariat@mailman.ccsds.org

FOREWORD

This document is a CCSDS Informational Report that contains background and explanatory material to supplement the CCSDS Recommended Standards for conventional telecommand and telemetry, Advanced Orbiting Systems (AOS), Space Communications Protocol Specification (SCPS), and Proximity links.

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 e-mail address indicated on page i.

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

Member Agencies

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

Observer Agencies

- Austrian Space Agency (ASA)/Austria.
- Belgian Federal Science Policy Office (BFSPO)/Belgium.
- Central Research Institute of Machine Building (TsNIIMash)/Russian Federation.
- China Satellite Launch and Tracking Control General, Beijing Institute of Tracking and Telecommunications Technology (CLTC/BITTT)/China.
- Chinese Academy of Sciences (CAS)/China.
- 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.
- 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.
- 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 350.0-G-1	The Application of CCSDS Protocols to Secure Systems, Issue 1	March 1999	Original issue, superseded
CCSDS 350.0-G-2	The Application of CCSDS Protocols to Secure Systems, Informational Report, Issue 2	January 2006	Issue 2, superseded
CCSDS 350.0-G-3	The Application of Security to CCSDS Protocols, Informational Report, Issue 3	March 2019	Current issue

CONTENTS

CONTENTS (continued)

1 INTRODUCTION

1.1 PURPOSE

This Informational Report is intended to provide guidance to mission planners who wish to use the CCSDS Recommended Standards for spacecraft control and data handling, but also need to protect mission communication. The report provides background information on security, details various options for security implementation in space missions, and outlines the impact of security on defined CCSDS services.

1.2 SCOPE

The information contained in this report is not part of any CCSDS Recommended Standard. In the event of conflict between any CCSDS Recommended Standard and the material presented herein, the CCSDS Recommended Standard is to be regarded as authoritative.

This report is intended as an implementation guide to aid space missions requiring secure CCSDS space mission data systems. It primarily addresses security of the space-ground ground-space data link. Ground systems are addressed by the use of off-the-shelf security solutions such as IPSec. Detailed information on security analysis and risk assessment methodologies are beyond the scope of this report.

1.3 RATIONALE

In the past, civil space missions relied on their uniqueness to deter unauthorized access to the space- and ground-mission data systems, whereas military missions have implemented mission-specific security measures to protect the spacecraft command and telemetry data. This situation has changed with the advent of open systems for mission control and data distribution, increased Internet connectivity, and cross support activities. Civil space mission and ground system developers must consider security as part of their system architecture and design process.

Space missions require a level of data-system security to protect the spacecraft and ground systems from unauthorized access. This is particularly evident as space mission control activities make more use of public networks, such as the Internet, for ground network connectivity. Some missions will require increasingly higher levels of security for a variety of operational and commercial reasons.

The work performed by CCSDS has provided a sound basis for the spacecraft control and mission data systems for all types of space missions. The CCSDS Recommended Standards for conventional telecommand (references [1] and [2]) and telemetry (references [3] and [4]), and Advanced Orbiting Systems (AOS—reference [5]) have been developed by civil space Agencies and are primarily intended to satisfy the communications requirements of civil missions. However, the CCSDS initiative has generated significant interest within the other

space communities, such as government/military and commercial, for a number of reasons, including

a) increased complexity of spacecraft and payloads for all mission types requiring more advanced control and monitoring systems, including packet-based mechanisms and on-board autonomy;

b) reduction in space mission budgets with encouragement to utilize commercial technologies and standards as appropriate;

c) availability of space- and ground-segment commercial products to reduce mission development costs;

d) initiatives to consolidate civil and military ground-station networks requiring widespread data-systems standardization; and

e) increased reliance on national and international co-operation to achieve space mission objectives.

Promoting the use of CCSDS Recommended Standards for a wider range of missions, including commercial and military, will make possible further reductions in mission-development costs for all mission types through the wider availability of commercial products. In the same way, establishing generic security concepts to satisfy the security requirements of future commercial and military missions will further extend the CCSDS user environment. Establishing generic security concepts is one of the objectives of this implementation guide.

1.4 ORGANIZATION OF THIS REPORT

This document is organized as follows:

Section 2 provides an introduction to security, defines terms that are used in this report, and identifies generic space mission security threats.

Section 3 presents a space mission security architecture based on a CCSDS reference model and establishes the security requirements of different types of space missions.

Section 4 describes the specific security mechanisms that may be utilized to achieve required security services.

Section 5 highlights the various available options for security for missions using CCSDS Recommended Standards, and describes the impact on protocol data structures.

Section 6 presents the implications of security on the space mission architecture and cross-support services. A comparison of possible security options, with guidance on option selection, is also provided.

Annex A describes some known implementation examples of CCSDS missions that have incorporated additional security features.

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] *TC Synchronization and Channel Coding*. Issue 3. Recommendation for Space Data System Standards (Blue Book), CCSDS 231.0-B-3. Washington, D.C.: CCSDS, September 2017.

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

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

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

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

[6] *Space Communications Protocol Specification (SCPS)—Transport Protocol (SCPS-TP)*. Issue 2. Recommendation for Space Data System Standards (Blue Book), CCSDS 714.0-B-2. Washington, D.C.: CCSDS, October 2006.

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

[8] *Space Packet Protocol*. Issue 1. Recommendation for Space Data System Standards (Blue Book), CCSDS 133.0-B-1. Washington, D.C.: CCSDS, September 2003.

[9] *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.

[10] *Cross Support Concept—Part 1: Space Link Extension Services*. Issue 3. Report Concerning Space Data System Standards (Green Book), CCSDS 910.3-G-3. Washington, D.C.: CCSDS, March 2006.

[11] S. Kent and R. Atkinson. *Security Architecture for the Internet Protocol*. RFC 2401. Reston, Virginia: ISOC, November 1998.

[12] *Advanced Encryption Standard (AES)*. Federal Information Processing Standards Special Publication 197. Gaithersburg, Maryland: NIST, 2001.

[13] *Proximity-1 Space Link Protocol—Data Link Layer*. Issue 5. Recommendation for Space Data System Standards (Blue Book), CCSDS 211.0-B-5. Washington, D.C.: CCSDS, December 2013.

[14] *Security Threats against Space Missions*. Issue 2. Report Concerning Space Data System Standards (Green Book), CCSDS 350.1-G-2. Washington, D.C.: CCSDS, December 2015.

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

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

[17] *Security Guide for Mission Planners*. Issue 1. Report Concerning Space Data System Standards (Green Book), CCSDS 350.7-G-1. Washington, D.C.: CCSDS, October 2011.

[18] *Information Security Glossary of Terms*. Issue 1.1. Draft Recommendation for Space Data System Practices (Pink Book), CCSDS 350.8-P-1.1. Washington, D.C.: CCSDS, August 2018.

[19] *CCSDS Guide for Secure System Interconnection*. Issue 1. Report Concerning Space Data System Standards (Green Book), CCSDS 350.4-G-1. Washington, D.C.: CCSDS, November 2007.

[20] *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.

[21] *Space Data Link Security Protocol*. Issue 1. Recommendation for Space Data System Standards (Blue Book), CCSDS 355.0-B-1. Washington, D.C.: CCSDS, September 2015.

[22] *Telemetry and Telecommand Packet Utilization*. ECSS-E-ST-70-41C. Noordwijk, The Netherlands: ECSS Secretariat, 15 April 2016.

[23] *CCSDS Streamlined Bundle Security Protocol Specification*. Issue 1. Draft Recommendation for Space Data System Standards (Red Book), CCSDS 734.5-R-1. Washington, D.C.: CCSDS, March 2018.

2 SPACE SECURITY CONCEPTS

2.1 INFORMATION SECURITY OVERVIEW

Information Security can be described as the effect or process of minimizing the vulnerabilities of assets or resources. The key elements of information security for a data-communications system are access control, authentication, availability, confidentiality, integrity, and accountability. Access control results in the limiting system access to specified individuals or groups (or processes acting on their behalf). Authentication is the assurance that the claimed identity of the source of information is not forged. *Availability* is the assurance that a system will be available for use. *Confidentiality* is protection against unauthorized disclosure of information, and *integrity* is protection against unauthorized modification of data (reference [18]).

To incorporate security into a space mission data system, the following entities may require protection:

a) information and data contained within the system (i.e., *information*);

b) communications and data processing (i.e., *services*); and

c) space mission ground equipment and spacecraft (i.e., *resources*).

Security can be achieved by implementing a number of different 'security services' at specific locations in the space mission data system. To incorporate the appropriate level of security for a particular mission, at least one security service or a combination of security services is required.

2.2 SYSTEM SECURITY POLICY

In selecting the appropriate security services for a particular mission, the first task is to assess the possible security threats to the system. This task is normally part of the development of a System Security Policy (SSP). The SSP is usually a formal document providing a description of the system, the top-level security objectives, and identification of the specific information-security and system-availability threats against the system. Other information may be included in the SSP, such as the security standards and evaluation requirements to be applied to the system, rules for access and operation of security critical systems (e.g., certificate authority), and if encryption is used, the means by which keys are distributed and managed. The CCSDS Security Guide for Mission Planners (reference [17]) discusses the development of the System Security Policy in greater detail.

As discussed in the Mission Planners Guide (reference [17]), a *threat assessment* should be performed. The threat assessment should assess the vulnerabilities of the system and then establish the likelihood, consequences, and cost of realization of each threat to the system. A threat is a problem only if a system is found to be vulnerable. Once the threat assessment process is complete, specific security services can be identified to counter each threat/vulnerability. The selection of countermeasures is likely to require a cost-benefit

analysis to justify the implementation cost of security services within the system. Any remaining vulnerabilities are deemed 'residual risk' and must be acceptable by system management before putting the system into production. Detailed information on threat assessment is beyond the scope of this report. *Security Threats against Space Missions* (reference [14]) discusses space mission threats in greater detail.

2.3 TYPES OF THREAT

A threat is defined as any circumstance or event having the potential to cause harm to a system through destruction, disclosure, or modification of data, or through denial of service. A threat can also be defined as a potential violation of security. However, a threat remains only a *potential* violation of security until it can be shown that there is a high likelihood the threat can cause harm. At that time, the threat is recategorized as a vulnerability. More information and use cases regarding threats to space systems can be found in reference [14].

Threats can be classified as accidental or intentional, and may be active or passive. The threats to a space mission data system include

a) unauthorized destruction of information and/or resources (e.g., spacecraft or ground systems);

b) unauthorized corruption or modification of information within the system;

c) theft or loss of information and/or resources;

d) disclosure of information to unauthorized entities; and

e) interruption of services.

Accidental threats have no premeditated intent and include system malfunctions and operational errors. Intentional threats range from casual examination of system information to sophisticated attacks using specific knowledge about the system.

Passive threats, if realized, would not result in modification to any information in the space data system, and the system itself would remain unaffected. Security violations falling into this category are generally associated with loss of data confidentiality, since this is the only security property that can be compromised without trace.

Realization of active threats would involve modification of information contained within the system or malicious changes to the operation or state of the system (space and/or ground segment). Active threats can compromise the information passing across a space mission data communication system by violating the integrity of the data or by degrading the availability of the system.

3 CCSDS PROTOCOL LAYER SECURITY REQUIREMENTS

3.1 SPACE DATA SYSTEM REFERENCE MODEL

The space link reference model shown in figure 3-1 highlights the various CCSDS protocols available and four security-implementation points that have been selected for a variety of reasons explained in this report. The five security implementation points considered are

– Physical Layer;

– Data Link Layer (conventional and AOS);

– Network (or packet) Layer;

– Transport Layer; and

– Application Layer.

These are illustrated in figure 3-1.

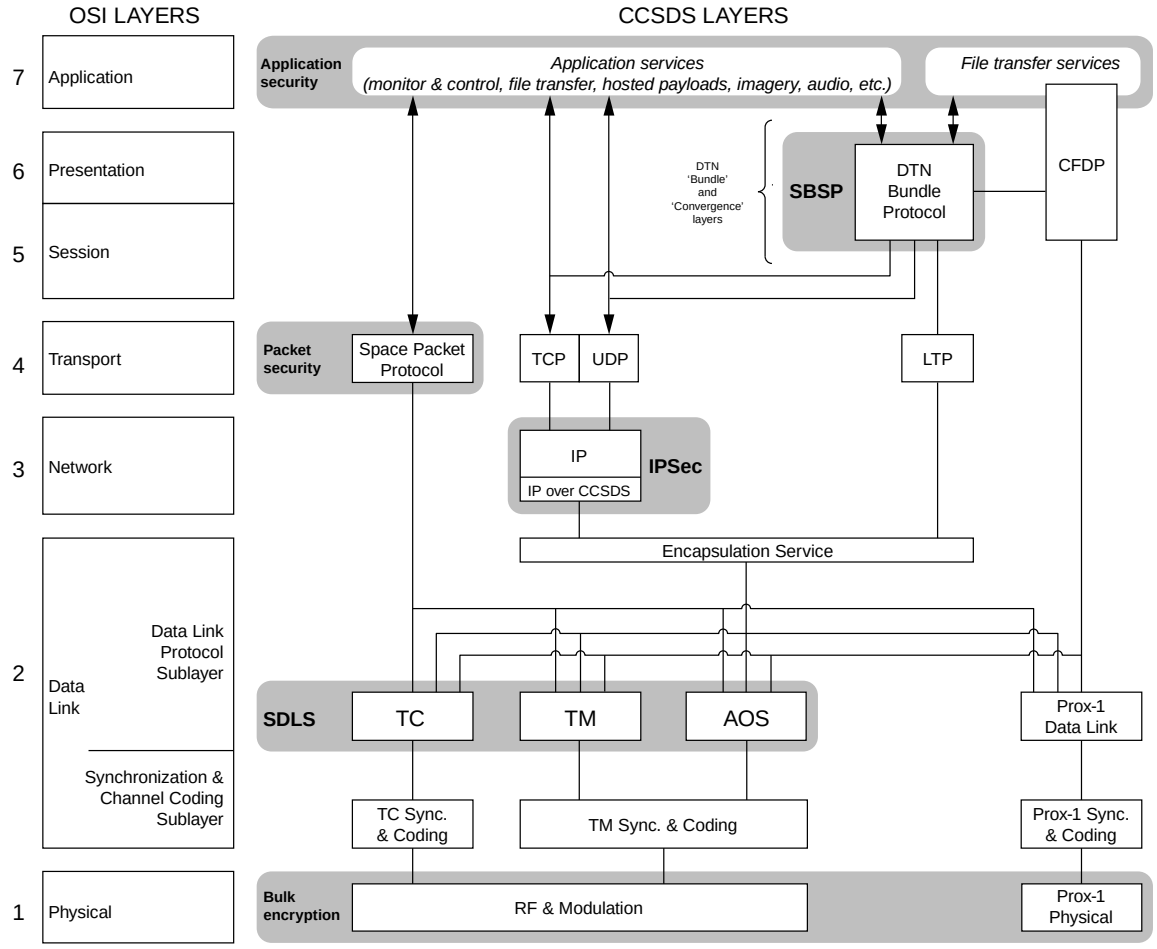

Figure 3-1: CCSDS Space Mission Protocols and Security Options

The security implementation approach selected for any particular space mission is dependent on the following factors:

a) the mission Agency's security policy;

b) the mission security requirements;

c) the mission operational requirements (to include cross support and interoperability);

d) the CCSDS Recommended Standard in use, for example, conventional telecommand (TC) (references [1] and [2]) and telemetry (TM) (references [3] and [4]), AOS [5], SCPS-TP (reference [6]), Proximity-1 (reference [13]); and

e) the capability of the on-board systems.

Different security services may be applied at different layers of the spacecraft communications system, as indicated in figure 3-1.

3.2 MISSION SECURITY REQUIREMENTS

3.2.1 GENERAL

To define sets of generic security requirements for different space mission types, missions have been classified as requiring either *high*, *moderate*, or *minimal* levels of security. This grouping is intended to act as a guide for the purposes of this report and is not meant to be restrictive. Some missions may find that they have security requirements that cannot be contained within one of these groups.

Different mission types will require the implementation of varying security services to satisfy specific mission requirements. In addition, different mission types may require different *assurance of correctness of operation* for each security service. For example, high security missions will require many security services and the highest assurance that those services are operating as intended (e.g., use of high grade, government-approved cryptographic algorithms). Moderate security missions may require the same security services as high-security missions, but with lower levels of assurance. Minimal security missions will require the fewest security services and the lowest levels of assurance.

3.2.2 HIGH SECURITY

Missions requiring high security are generally associated with the government or military sector. They may be life-critical crewed missions that would require high security in order to ensure life. Commercial telecommunications missions may also fall into this class due to the mission's high cost and the operational nature of the system once on orbit. Secure access to the spacecraft control system is required at all times during the mission and under all possible operational or environmental conditions. The mission data system must be protected from unauthorized access, and measures must be implemented to prevent detection, interception, and exploitation of the data links.

The following security requirements are *likely* for high security missions:

a) protection of all telecommand data
   - confidentiality,
   - authentication,
   - access controls,
   - data integrity (including anti-replay measures),
   - availability;

b) protection of all telemetry data
   - confidentiality,
   - data integrity,
   - possibly other security services such as authentication and access controls,
   - availability;

c) protection of all data in the ground data system
   - confidentiality,
   - authentication,
   - data integrity,
   - availability,
   - access controls.

3.2.3 MODERATE SECURITY

Missions requiring moderate security may include commercial-communications, meteorological, and remote-sensing missions. Satellite navigation systems may also be included in this class (but may fall into the high-security class depending on the nature of the system).

These missions will require spacecraft and ground system protection from unauthorized access and may need to protect payload data that is commercially or operationally sensitive or critical to safety. Protection from unauthorized access is especially important if the mission utilizes open ground networks such as the Internet to provide ground-station connectivity.

At a minimum, moderate security missions may have the following security requirements:

a) protection of telecommand data
   - authentication,

  - data integrity,
  - possible requirement for confidentiality;

b) protection of some or all telemetry data
  - confidentiality,
  - data integrity;

c) protection of some or all data in the ground data system
  - authentication,
  - data integrity,
  - possible requirement for access control,
  - possible requirement for confidentiality.

3.2.4 MINIMAL SECURITY

Missions requiring minimal security include all other space missions. These missions are likely to require security of the telecommand system to prevent unauthorized access or tampering with the data, whether intentional or unintentional. There may also be confidentiality requirements for specific telemetry information (e.g., proprietary scientific data, imagery).

Minimal security missions may have the following security requirements:

a) protection of all telecommand data
  - authentication,
  - data integrity,
  - possible requirements for confidentiality;

b) protection of some telemetry data: confidentiality, data integrity;

c) protection of some data in the ground data system: confidentiality, data integrity, access control.

4 SECURITY MECHANISMS

4.1 CONFIDENTIALITY

4.1.1 GENERAL

The security mechanism that provides a confidentiality service for communications is *encryption*. Encryption may also contribute to the achievement of other security services such as data integrity and authentication. Encryption, when used for confidentiality, transforms sensitive data to a non-sensitive form. When used for integrity or authentication, cryptographic techniques are used to generate unforgeable functions such as a digital signature as described in 4.2.

Encryption is performed on *plaintext* to produce *ciphertext*. The reverse process is known as decryption. A key is used during both encryption and decryption to direct specific transformations as part of the cryptographic process, as shown in figure 4-1. When a key is changed, different ciphertext is obtained for the same plaintext input. The security of the encryption process is dependent on the strength of the cryptographic algorithm being used, the length of the cryptographic keys, and maintaining the secrecy of the keys. Often the details of the cryptographic algorithm being used are publicly known, as is the case with the Advanced Encryption Standard (AES) (see references [12], [15], and [16]). In this case, because the details of the algorithms are known, security of the system is designed to be dependent on the secure handling of the cryptographic keys: their management, distribution, use, and destruction.

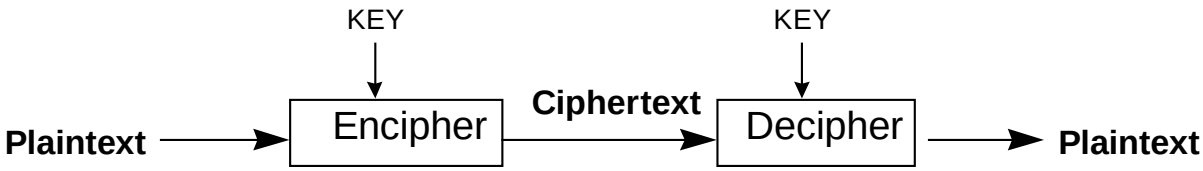

Figure 4-1: The Concept of Encryption and Decryption

Encryption may be performed on a *point-to-point*, *hop-by-hop*, or *end-to-end* basis. In the case of a point-to-point system, encryption is provided only between the two communicating end-points (see figure 4-2).

In the case of a hop-by-hop system (see figure 4-2), the data is encrypted for transmission and then decrypted by an intermediary before being re-encrypted for further transmission towards its final destination.

In an *end-to-end* system (see figure 4-2), regardless of intermediate systems, encryption is applied at the source and decryption is only applied at the final destination. The data may pass through intermediary systems; however, unlike hop-by-hop systems, these intermediaries do not decrypt nor do they have the ability to examine the data.

Encryption algorithms may be *symmetric* or *asymmetric*. In a symmetric system, both the encryption and decryption keys are the same and are kept secret. Thus a secure key distribution system must be implemented to generate, distribute, and account for all the keys that are required in the system. AES is an example of a symmetric cryptographic algorithm.

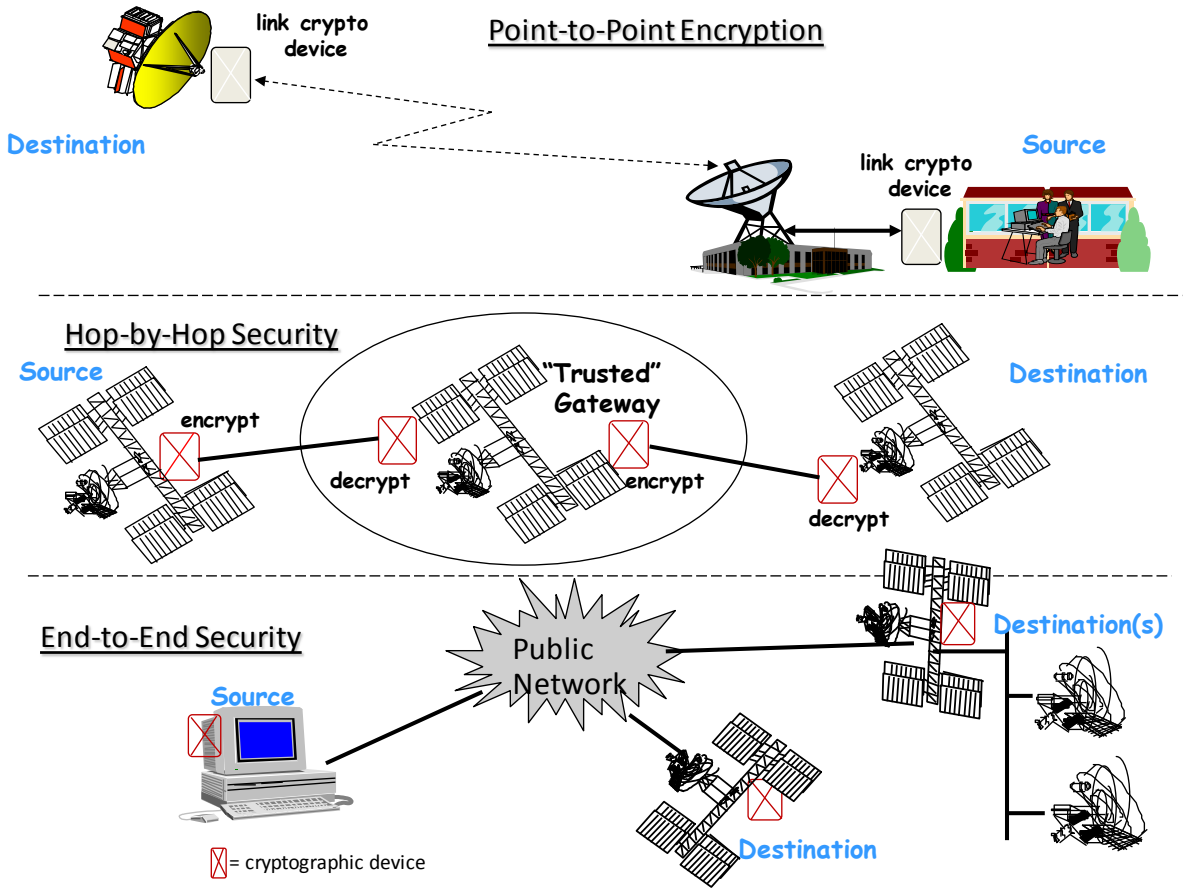

Figure 4-2: Illustration of Point-to-Point, Hop-by-Hop, and End-to-End Encryption

4.1.2 KEY MANAGEMENT

In an asymmetric (or public-key) system, each communicating end system possesses a key pair: a *public* key and a *private* key. The private key is kept secret, but the public key is made available to anyone who wants it. It may be posted to a publicly available server (e.g., a key server). An asymmetric system relies on the fact that it is practically impossible to obtain knowledge of the decryption key from knowledge of the encryption (public) key. For example, the Rivest-Shamir-Adleman (RSA) public key system, the best known and most commercialized public key system in use, is based on the difficulty of finding factors of large prime numbers. The public key does not need to remain secure, which implies that no prior secret key exchange is required, and which in-turn leads to reduced security-development and operations costs. However, in practice RSA uses a combination of asymmetric and symmetric key systems (hybrid encryption) to improve efficiency. A public key exchange is used between the communicating assets in order to agree on a shared key (the traffic or

session encryption key), which is then used with a symmetric algorithm to provide data confidentiality.

However, since public keys are openly shared, there must be a secure, high-assurance *binding* between the owner identity of the public key and the key itself, to ensure that a false or substituted public key is not used. The binding occurs when the public key is digitally signed by a trusted third party (e.g., a certificate authority) whose identity is well known, and who vouches for the true identity of the public key owner.

Before they are used, cryptographic systems must be subjected to in-depth analysis to ensure that there are no weaknesses that could be exploited by a potential attacker. During an analysis, the following worst-case assumptions are usually made:

a) an attacker has complete knowledge of the algorithm;

b) an attacker has obtained a considerable amount of ciphertext; and

c) an attacker knows the plaintext equivalent of some ciphertext.

Therefore symmetric keys must be distributed and maintained securely, as they are the primary means by which information is protected.

There are several types of symmetric cryptographic algorithms that operate in different cryptographic modes. For example, a symmetric *stream cipher* encrypts one bit of plaintext at a time (e.g., AES/GCM), whereas a *block cipher* encrypts data in blocks, which can be more convenient for octet-oriented systems. For example, the (old, weak, and no longer recommended for use) DES algorithm is a block cipher that has a 64-bit input and produces a 64-bit output under the control of a 56-bit key (56 bits + 8 parity bits). AES uses a larger block size (128-bits) and uses larger keys such as 128, 192 or 256 bits. Detailed information on cryptographic algorithms can be found elsewhere (see references [12], [15], and [16]).

4.2 AUTHENTICATION

Data authentication is achieved by appending an extra unit of information to the original message. The additional information takes the form of either a *digital signature* or a *message digest*. This is illustrated in figure 4-3.

The digital signature definitively identifies the origin of the data, and the receiver of the data is thus assured that the data is from the claimed source. The essential characteristic of the digital-signature mechanism is that the signed data unit cannot be created by an unauthorized entity.

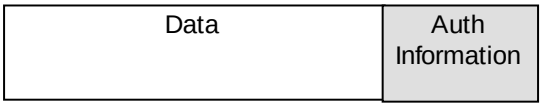

Figure 4-3: Authentication Information

Many digital-signature generation mechanisms require the use of an asymmetric cryptographic algorithm for which sender and receiver do not hold the same cryptographic keys (as described in 4.1.2). Rather, a pair of public and private keys that are mathematically related to each other are used. At the origin of the data, the cryptographic algorithm generates a digital signature using the sender's private key. The signature may be generated from the data itself and is of a specific length, depending on the algorithm used. Data-origin authentication is achieved when the digital signature is successfully verified by the receiver using the sender's public key.

A message digest, as described in detail in the section on data integrity, may also be used to provide authentication. A message digest generates a unique check value that indicates to the receiver that the data has not been changed or modified. In order to perform authentication as well, the message digest is generated over a shared secret that only the sender and receiver possess.

Encryption of the data itself can also provide implicit authentication when using a symmetric cryptographic algorithm. Authentication is achieved because the recipient must have and use the correct key to decipher the digital signature appended to the data. This assumes there is an assured key-distribution mechanism. Also, encryption provides implicit authentication when using an asymmetric (public key) system if there is assurance that the public key is bound to the originator (e.g., signed by a certificate authority). However, caution must be used because authentication may be compromised if the encrypted data is captured and later replayed without replay protection.

4.3 DATA INTEGRITY

Data integrity can be considered as having two different functions: the integrity of the individual data units and the integrity of a stream of data units. Different mechanisms are generally used to provide these different integrity functions.

Integrity of individual data units is achieved by appending an Integrity Check Value (ICV) to the data structure in a manner similar to the way a digital signature is appended. However, the ICV is always a function of the data itself. A Cyclic Redundancy Check (CRC) is a simple example of such a function. A stronger function is provided in the Secure Hash Algorithm (SHA-2). The receiver generates a corresponding check value by performing an operation on the data and compares the result to a received value to determine if the data has been modified in transit. In some applications, both authentication and individual data-unit integrity can be provided by one mechanism. Coding specifications, such as Reed-Solomon and Turbo Codes, provide data integrity by virtue of their error detection and correction capabilities.

To provide integrity of a stream of data units, a sequence number is employed to protect against replay attacks. Alternatively, time stamping of data may be used to provide limited replay protection.

To ensure that it is not modified or corrupted, the ICV is often keyed (e.g., a keyed hash), or the ICV value can be encrypted using a symmetric encryption algorithm (e.g., AES CMAC—see references [12], [15], and [16]).

4.4 ACCESS CONTROL

The basic function of access control is to ensure that data or information-technology resources are available only for authorized users or processes. As a result of ensuring data availability, access-control mechanisms may provide limited confidentiality and integrity. It should be noted, however, that access control is not a fundamental technique for providing these other two security services; it is purely a barrier in the path of a potential intruder.

Access control requires the use of a number of techniques, including the establishment of access-control information bases in which the access rights of users or processes are maintained securely. Authentication information such as identification, cryptographic credentials (e.g., X.509 certificate, Kerberos ticket), and passwords provide management and control of access to the system. Passwords should be administered effectively by establishing details such as appropriate password length and content, implementing procedures for regularly changing passwords, and ensuring that password secrecy is maintained. It should be noted that automation of password generation increases security significantly. Plaintext passwords should **never be transmitted over an unprotected medium**. If passwords must be sent over a network, an encryption function (e.g., SSH, TLS, IPSec, or another Virtual Private Network [VPN]) should be used. Audit trails are an important mechanism in security management. They are used to monitor system usage and password changes, and should contain as much information regarding the system details and previous accesses as possible.

4.5 Availability

Availability is the assurance that a system will be usable when it is required to function. Although not entirely a security matter, it is a security concern from the perspective of an attacker attempting to deny access to a system, either by denial-of-service attacks or by crashing the system.

In a space environment, there are Radio Frequency (RF) communications links. Unlike wire-line communications, RF communications can be jammed by devices emitting high power levels on the same (or nearby) frequency. When a frequency is jammed, communication over that RF link is interrupted. This impedes telemetry and telecommand to/from a spacecraft. This also impedes the collection of data from a spacecraft, potentially resulting in total, unrecoverable data loss. It can also result in the loss of the spacecraft if housekeeping data is not received on the ground and there is an emergency situation that must be dealt with immediately. Likewise, a spacecraft can be lost if telemetry is received but the telecommand uplink is jammed so that no commands can be sent. Spread spectrum and frequency hopping, discussed in 5.2, are techniques used to counter jamming.

5 CCSDS SECURITY IMPLEMENTATION OPTIONS

5.1 OVERVIEW

This implementation guide considers the incorporation of security within four specific layers of the space mission data system: the Application, Network, Data Link, and Physical Layers, as shown in figure 5-1. The various security options considered are described in this section, and the implications on the defined services of each layer are presented in section 6.

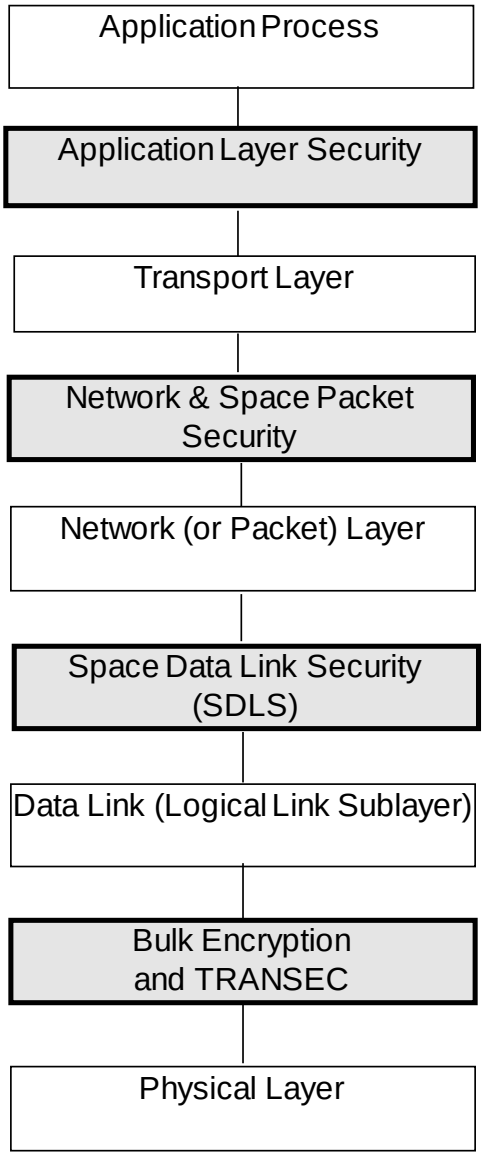

Figure 5-1: Security Implementation Options Considered in This Report

5.2 BULK ENCRYPTION

Bulk encryption provides confidentiality to the communication system data structure. It is implemented at the Physical Layer and provides the highest possible level of data confidentiality available on a point-to-point basis; often this is termed 'link encryption'. However, this is not to imply encryption at the Data Link Layer but rather over the physical link. No separate integrity, authentication, or access-control services are implied other than those implicitly provided by encryption. For example, if symmetric key encryption is used, authentication is implicitly achieved because the receiving end must have the correct key, which has been distributed by an assured key distribution system in order to decipher the data.

If applied to missions using the CCSDS Recommended Standards, bulk encryption would result in encryption of the full Physical Layer data structure. For telecommand (see reference [1]), the use of bulk encryption implies that the Command Link Transmission Unit (CLTU), as well as the acquisition and idle sequences, would be encrypted. A similar result would be obtained if bulk encryption were applied to telemetry (reference [4]) or AOS (reference [5]), in which case the entire stream of Channel Access Data Units (CADUs) (see reference [3]) would be encrypted.

Similarly, to prevent jamming of the Physical Layer, techniques such as *spread spectrum* using *direct sequence* and *frequency hopping* can be employed. This technology is known as TRANsmission SECurity (TRANSEC). When data is transmitted using spread spectrum techniques, the information is transmitted over a wide range of frequencies and then collected by a receiver onto a single frequency. In direct sequence spread spectrum, the stream of information to be transmitted is divided into small pieces, each of which is allocated to a frequency channel across the spectrum. This technique spreads the signal so that it appears to be noise rather than data and therefore is hard to intercept and jam.

Using frequency-hopping techniques, data is transmitted over a single frequency, but the frequency changes over time during the transmission. The receiver must be synchronized in order to change frequencies, as is being done by the transmitter.

The implications of bulk encryption on the various Physical Layer protocol data structures are shown in figure 5-2 and discussed in section 6.

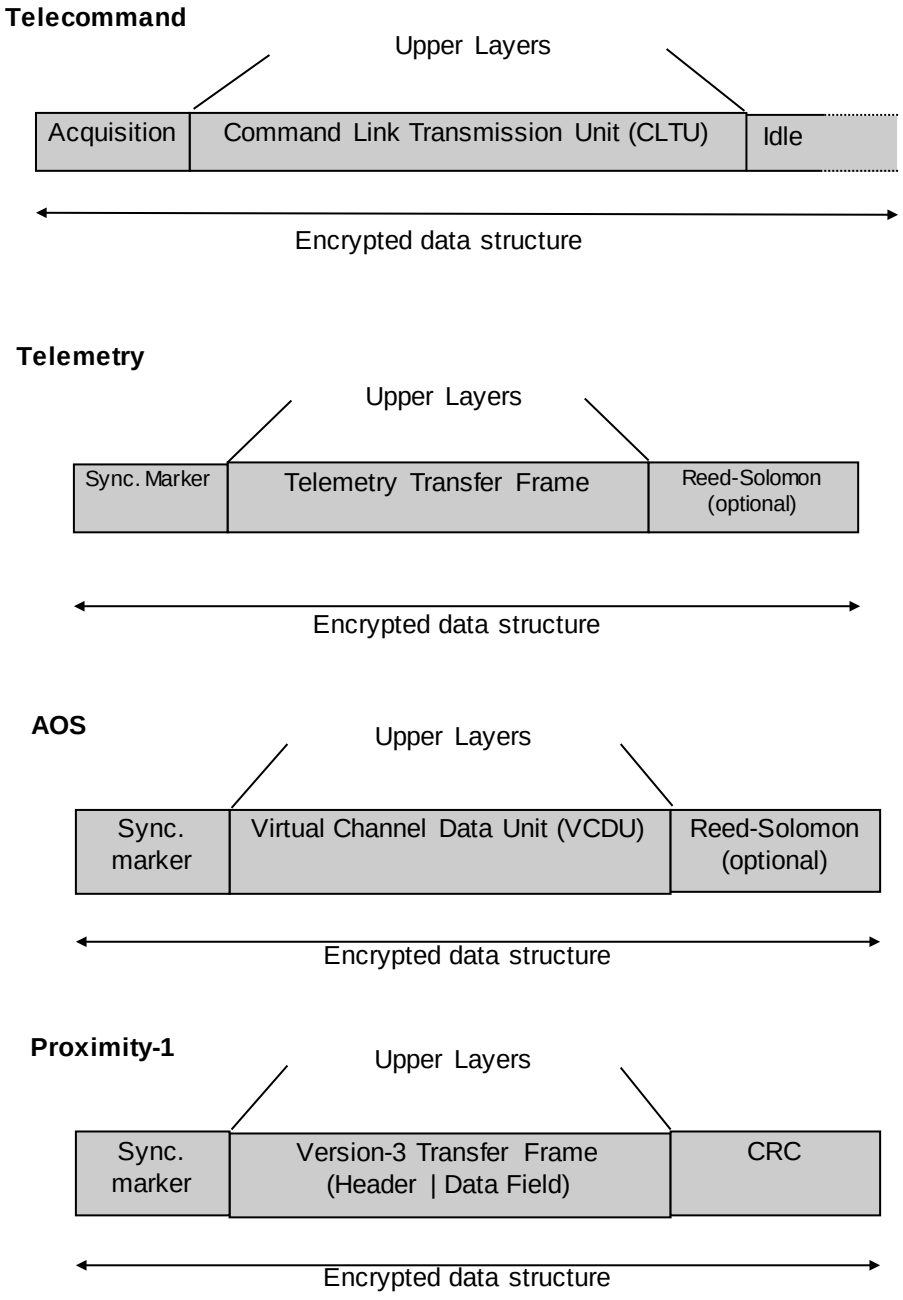

Figure 5-2: Bulk Encryption of CCSDS Protocols

5.3 DATA LINK SECURITY

5.3.1 GENERAL

Within this report, the conventional CCSDS Data Link Layers are defined to include all the protocol layers defined within the CCSDS Space Data Link and Coding Recommended Standards (references [1]–[4]). The packet layer (including the packet header and data fields) is assumed to be located at the Network Layer.

NOTE – Open Systems Interconnection (OSI) protocol layers are defined in reference [7].

The AOS Data Link Layer includes all the AOS point-to-point Space Link Subnet (SLS) services defined in the AOS Recommended Standard (see reference [5]).

The Proximity-1 Data Link Layers are defined to include all the protocol layers defined within the CCSDS Proximity-1 (reference [13]).

The CCSDS Data Link Layer provides protocol synchronization, increases the space data link performance by implementing channel-coding mechanisms, and provides low-level data-routing functions. Also, a reliable data channel is provided through the ARQ process within the telecommand and AOS data link protocols (not available within the conventional telemetry data link). The Data Link Layer operates on the space link of the data transmission path only (i.e., not end-to-end). Proximity-1 provides a bi-directional link.

A range of security services may be applied at the Data Link Layer to provide confidentiality, integrity, and authentication services. Implementation of access control at the Data Link Layer is not considered; if needed, it is assumed to be provided at the Application Layer (OSI Layer 7).

CCSDS has issued the Space Data Link Security (SDLS) Protocol (reference [21]) as a Recommended Standard for providing authentication and/or confidentiality to the contents of transfer frames used by the three Space Data Link Protocols that SDLS supports, namely TM, TC, and AOS. SDLS operates at the data link protocol sublayer of the Data Link Layer (OSI Layer 2) and is unaffected by the Synchronization and Channel Coding sublayer. SDLS is not applicable for use with the Proximity-1 Space Data Link Protocol.

SDLS provides three classes of cryptographic service for TC, TM, and AOS:

Authentication provides data integrity, source authentication, and anti-replay protection, but not confidentiality:

a) *Integrity:* SDLS provides for the use of a Message Authentication Code (MAC) appended to the transfer frame data field. The MAC is used to detect the presence of either random or deliberate alterations to the frame data.

b) *Source Authentication:* SDLS provides for the use of a keyed-hash MAC for cryptographic confirmation that the contents of the received transfer frame originated from a genuine source (i.e., the authorized mission control center).

c) *Anti-Replay Protection:* SDLS provides for the use of an incrementing sequence number for transfer frames belonging to the same security session context. The sequence number's integrity is also protected by the MAC, and provides confirmation that the frame received is not a replay of a previously transmitted and recorded frame.

Encryption provides data confidentiality but not authentication or integrity:

Confidentiality: SDLS provides for optional encryption of the transfer frame data (or TC segment). The transfer frame header and error control field are not encrypted.

Authenticated Encryption provides a combination of both encryption and authentication services, thus providing all the attributes of confidentiality, source authentication, integrity, and anti-replay protection listed above.

It should be noted that security services do not have to be applied to all data units in the space link. SDLS services can be selectively applied to different Virtual Channels (TC, TM, and AOS). However, selective Virtual Channel security may increase the difficulty of implementation because of the incorporation of different encryption/authentication algorithms within the system, and implies an increased level of key-management complexity.

SDLS inserts a Security Header and (optional) Security Trailer surrounding the transfer frame data field; these data structures carry the security session parameters and enable most other Data Link Layer procedures of the underlying Space Link Protocol to be unaffected by the presence of SDLS. Figure 5-3 shows a simplified representation of Space Data Link Protocol frames and the effect of the Security Protocol's inserting header and optional trailer fields to surround the frame data supplied by higher layers.

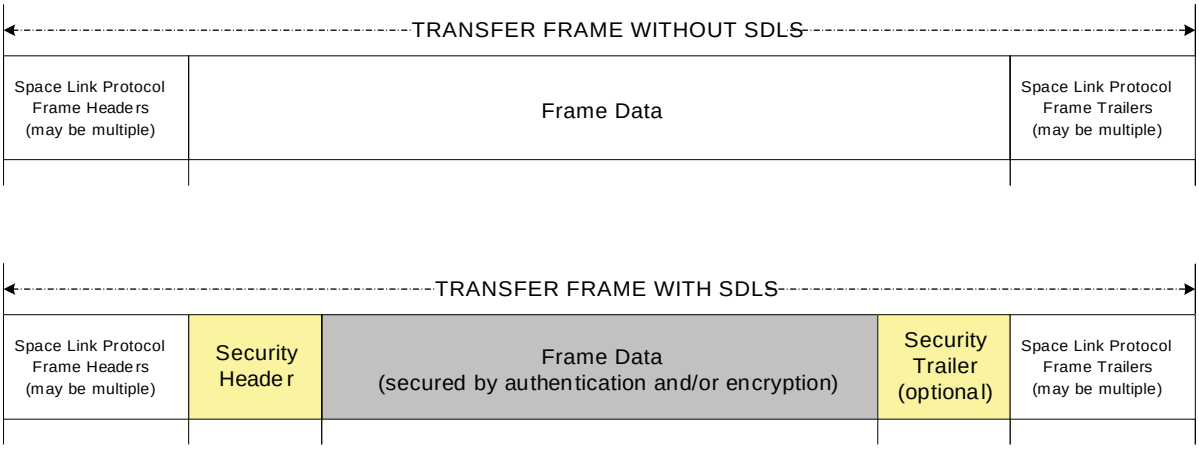

Figure 5-3: SDLS Insertion into Space Link Protocol Transfer Frames

5.3.2 TELECOMMAND DATA LINK SECURITY

SDLS provides confidentiality, authentication, and integrity services for the data in the Transfer Frame Data Field of a TC Transfer Frame. It therefore provides full protection for the Multiplexer Access Point (MAP) Packet, MAP Access, Virtual Channel Packet (VCP), and Virtual Channel Access (VCA) services of the TC Protocol.

SDLS provides authentication for some fields in the Transfer Frame Primary Header in a TC Transfer Frame, but it does not provide encryption for these fields.

SDLS provides no protection for the control frames generated for the Communications Operation Procedure (COP) Management service. SDLS also provides no protection for frames supplied to the TC Protocol by external sources using the Virtual Channel Frame or the Master Channel Frame services.

5.3.3 TELEMETRY DATA LINK SECURITY

SDLS provides confidentiality, authentication, and integrity services for the data in the Transfer Frame Data Field of a TM Transfer Frame. It therefore provides full protection for the VCP and VCA services of the TM Protocol.

SDLS provides authentication for some fields in the Transfer Frame Primary Header and for some auxiliary data fields in a TM Transfer Frame, but it does not provide encryption for these fields. SDLS can provide authentication for the Virtual Channel Frame Secondary Header service.

SDLS provides no protection for the Virtual Channel Operational Control Field, Master Channel Frame Secondary Header, and Master Channel Operational Control Field services of the TM Protocol. SDLS also provides no protection for frames supplied to the TM Protocol by external sources using the Virtual Channel Frame or the Master Channel Frame services.

5.3.4 AOS DATA LINK SECURITY

SDLS provides confidentiality, authentication, and integrity services for the data in the Transfer Frame Data Field of an AOS Transfer Frame. It therefore provides full protection for the VCP, Bitstream, and VCA services of the AOS Protocol.

SDLS provides authentication for some fields in the Transfer Frame Primary Header in an AOS Transfer Frame, but it does not provide encryption for these fields.

SDLS provides no protection for the Virtual Channel Operational Control Field or the Insert services of the AOS Protocol. SDLS also provides no protection for frames supplied to the AOS Protocol by external sources using the Virtual Channel Frame or the Master Channel Frame services.

5.3.5 PROXIMITY-1

SDLS is not applicable for use with the Proximity-1 Space Data Link Protocol.

For Proximity-1, data link security services are best implemented above the I/O sublayer as shown in figure 5-4.

The security services are applied to the User Data. All Proximity-1 protocol handling is carried out as it normally would be. This is analogous to Transport Layer Security (TLS).

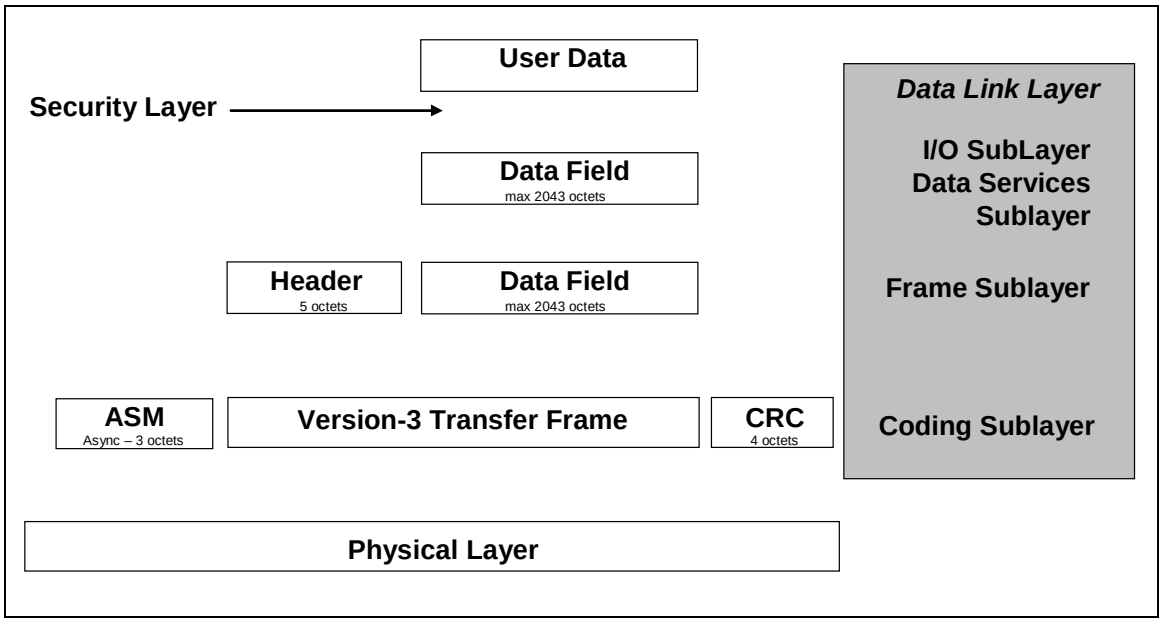

Figure 5-4: Proximity-1 Data Link Layer Security

5.4 NETWORK LAYER SECURITY—INTERNET PROTOCOL SECURITY (IPSEC)

Developed by the Internet Engineering Task Force (IETF), IPSec provides end-to-end security for internet protocol packet payloads (see reference [11]). That is, IPSec provides confidentiality and authentication for all data contained in an Internet Protocol (IP) datagram. This includes the Transmission Control Protocol (TCP) header and the information payload.

The primary benefit of IPSec is its ability to provide end-to-end security, that is, from the source of the data to its final destination. Any non-security-related intermediate systems and networks will not have access to the data unless explicitly authorized, and therefore insecure networks may be utilized to transmit sensitive data. The communication end points are implementation specific and are defined by the implementing system. IPSec does not mandate any specific security algorithm but defines the protocol framework to provide Network Layer data confidentiality, integrity, and authentication services for space communications systems. Algorithms for use with IPSec should be selected from the CCSDS Algorithms Recommended Standard (reference [15]).

The structure of IPSec is shown in figure 5-5. The protocol adds a clear header of 8 bytes, containing a Security Parameters Index (SPI) (4 bytes) and a sequence number (4 bytes), a variable-length payload containing algorithm-specific information (e.g., an initialization vector), variable-length padding (if required by the chosen algorithm), a 1-byte pad-length field to indicate the amount (if any) of padding used, a 1-byte next-header field, and an optional variable-length ICV.

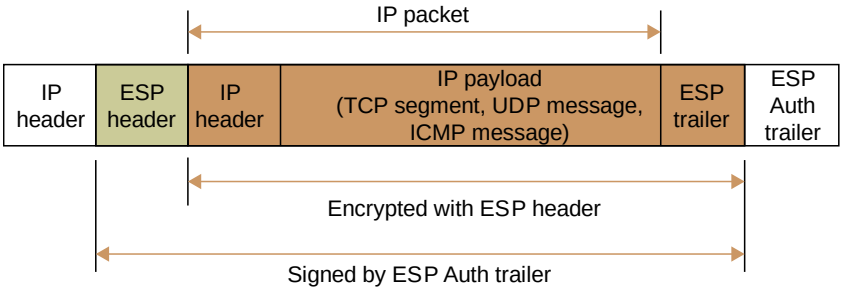

Figure 5-5: IPSec Protocol Structure

5.5 TRANSPORT LAYER SECURITY—SPACE PACKET PROTOCOL SECURITY

Security may be applied at the space packet layer (see reference [9]) to protect the telecommand and telemetry data, or to achieve spacecraft command authentication. It can be achieved by encrypting the packet data field for confidentiality and including a digital signature and/or ICV within the packet data field for authentication and data integrity, respectively. The space packet protocol headers would remain unencrypted.

The concept of space packet layer security is shown in figure 5-6. Only the application data field is encrypted. The optional secondary header may also be encrypted. All other protocol fields in the lower layers of the system remain in plaintext. However, it should be noted that without an authenticated replay counter in the primary header, the packet is open to replay attacks. Prevention of such attacks would require a protocol revision.

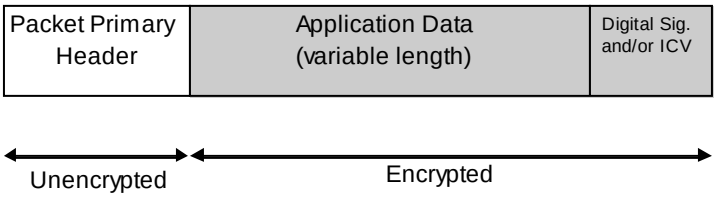

Figure 5-6: CCSDS Packet Security Concept

It should be noted that if a mission requires security of selected packets in the space link, then the Application Process Identifier (APID) in the packet header may be used to differentiate between encrypted or plaintext packets.

5.6 APPLICATION SECURITY

Security services may be applied at the Application Layer; however, in the case of a space mission using the space packet protocol, implementation of confidentiality, integrity, and authentication services is likely to be similar to the space packet security case, as outlined in 5.5.

The use of Transport Layer Security (TLS) technology at the Application Layer allows individual applications the option of implementing security services independent of the rest of the data handling system.

Likewise, missions utilizing the Delay-Tolerant Network (DTN) bundle protocol (BP) can use the Streamlined Bundle Security Protocol (SBSP) (reference [23] to provide bundle authentication, payload integrity, payload confidentiality and security for non-payload-related bundle blocks. SBSP specifies two security blocks – a block confidentiality block (BCB), and a block integrity block (BIB). The BCB provides confidentiality and the BIB provides authentication and integrity.

Notably, the use of such services at the Application Layer does not require any security investment by the lower layers. Furthermore, each application requiring security services has to independently make the investment to implement security mechanisms rather than taking advantage of lower-layer security services that benefit all applications. In this way, an application may make the decision to enforce security despite the fact that the underlying mission data handling system has decided against doing so. If it is decided to implement specific security services at the Application Layer, then it is important to ensure that consistency is maintained throughout the entire system to ensure that the security services are not compromised.

Another primary security service to be applied at the Application Layer is access control. Access control may be achieved by implementing secure access-rights database facilities at the mission-data-system access points. Access control is granted based on authenticated identity. An entity requiring access may possess a token such as an X.509 certificate containing credentials that would be authenticated before allowing access.

5.7 CCSDS SECURITY OPTION COMBINATIONS

To meet specific space mission requirements, it may be necessary to utilize a combination of the CCSDS security options defined in the previous sections. When this is the case, security services may be implemented in multiple layers of the mission data system simultaneously.

For example, some advanced high-security missions may require a combination of the Network Layer security to provide end-to-end data protection, particularly across ground networks, and lower-layer security operating over only the space link to prevent traffic analysis between the ground and space segments. This concept, with the respective security end points, is shown in figure 5-7.

In some cases, Network Layer security may not be provided by the network, and Application Layer security may be utilized instead to provide source-to-destination data protection. In this case, the data is protected at its source rather than in the network protocol stack, potentially affording even greater data protection. However, rather than using a network security service mechanism, each application would be responsible for implementing and calling the security service. The service may be found in a library and therefore not required to be implemented for each application, but nevertheless, the application must still make an overt action to use the security mechanism rather than it being automatically applied while passing through the Network Layer.

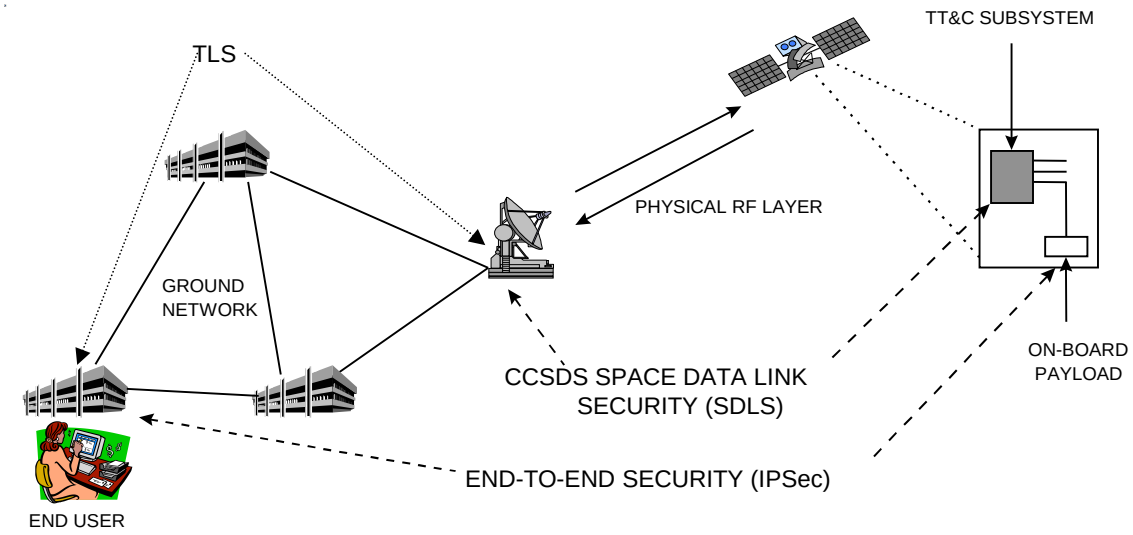

Figure 5-7: CCSDS Data Link and Network Security Combination Architecture

6 CCSDS SECURITY IMPLICATIONS

6.1 IMPACT OF ENCRYPTION

In general, confidentiality has the greatest impact on the CCSDS architecture and services, compared with authentication and data integrity services, because specific protocol information (headers and trailers) may be hidden through encryption and may therefore be unavailable for use for other network or cross-support services. In contrast, authentication and data-integrity services only require inclusion of a small number of additional fields at an appropriate point in the data structure, although these services may add a large number of additional bits.

The impact of confidentiality on the various CCSDS layer fields for the different security options is shown in table 6-1. The fields that are unencrypted are shown as 'Plain'.

Table 6-1: Impact of Confidentiality on CCSDS Data Fields

CCSDS Security Option	ASM + EDAC	Frame Header	Frame Data Field	Packet Header	Packet Data Field
Network Layer Security	Plain	Plain	Plain	Plain	Encrypted
Space Data Link Security (SDLS)	Plain	Plain	Encrypted	Encrypted	Encrypted
Physical (Bulk Encryption)	Encrypted	Encrypted	Encrypted	Encrypted	Encrypted
(**ASM** - Attached Synchronization Marker, **EDAC** - Error Detection and Correction)					

6.2 IMPACT ON EMERGENCY COMMANDING

On occasion, problems arise with spacecraft after launch or while on orbit. Upon launch, a spacecraft may end up tumbling, unable to orient its antennas correctly, and therefore not able to receive commands. Likewise, an on-orbit spacecraft may be subject to an upset due to a wide variety of occurrences (e.g., memory latching, processor upsets).

When problems arise, the operations personnel attempt to transmit emergency commands to the spacecraft. In the case of a tumbling spacecraft, this consists of a short command to allow the vehicle to reset itself and orient its antennas correctly. The emergency command is sent over and over again in the hope that it might be received during a short window when the antennas are correctly oriented. In the case of a faulty spacecraft, this consists of a short command to cause the vehicle to go into a 'safe mode' to attempt to reset the fault(s) or invoke backup equipment.

Typically, these emergency commands bypass the onboard computer and are acted upon directly by the hardware command decoder. But the question is, from a security perspective, should such emergency commands be allowed to be acted upon with or without command authentication?

If the commands are not authenticated, a security hole is opened for a potential attacker. A risk analysis must be performed to determine if this is of concern and if it should be allowed. Potentially, the sending of a reset emergency command could have no effect on a spacecraft other than the loss of availability during the subsequent restart. However, if the spacecraft has high-availability requirements, then such a reset may not be welcomed. Likewise, such an unauthorized reset is highly problematic if a spacecraft is in the midst of performing navigation maneuvers or other sensitive operations.

On the other hand, if authenticated commands are required, the size of the emergency command might increase depending on the type of command authentication employed. Because emergency commands are designed to be very short in the hope that one may be quickly and easily received and acted upon, the size increase due to authentication might negate the ability to receive emergency commands.

6.3 IMPACT ON CROSS-SUPPORT SERVICES

6.3.1 GENERAL

The CCSDS Space Link Extension (SLE) cross-support services are a set of services that provide access to the ground termination of the space link services from a remote ground-based system (see reference [10]). The SLE services can be separated into two categories:

– Return SLE services;

– Forward SLE services.

6.3.2 RETURN SLE SERVICES

The various types of cross-support services have been split into different Functional Groups (FGs) based on the CCSDS Reference Model layers. Figure 6-1 shows FGs and services included in the Return SLE architecture and the impact that each of the CCSDS security options has on the SLE services provided. The impact is defined as whether or not the cross-support service is available when using that particular security option. Physical Layer security is not considered because cross-support services are not available for this option (it is assumed that the data can be decrypted only by the end user, and that no protocol information is available to enable cross-support).

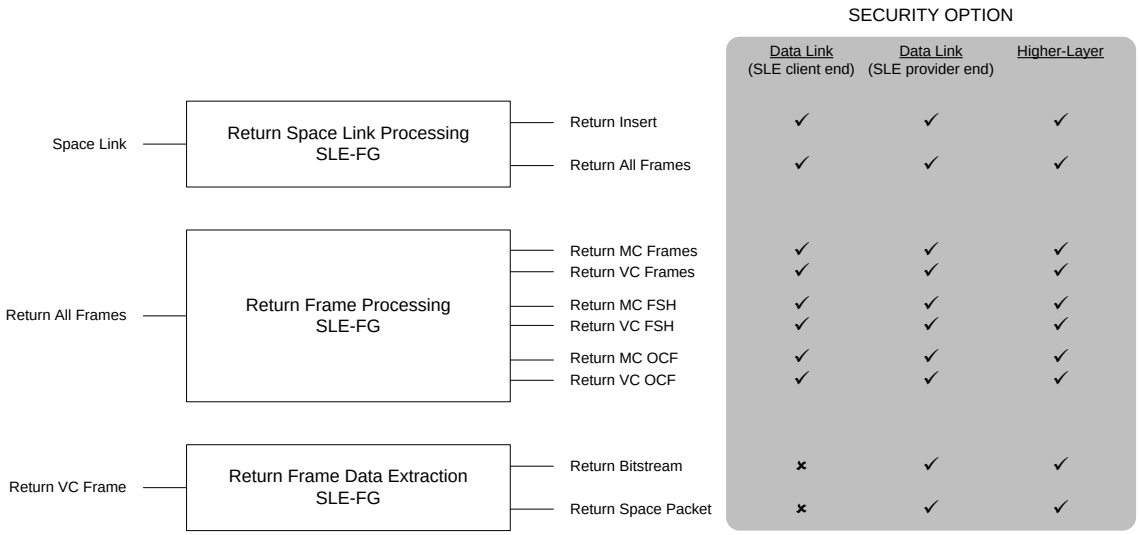

Figure 6-1: Impact of Security on Return SLE Services

6.3.3 FORWARD SLE SERVICES

Figure 6-2 shows the Forward SLE services in FGs based on the CCSDS Reference Model and the impact that each of the security options has on the services provided. Again, Physical Layer security is not considered.

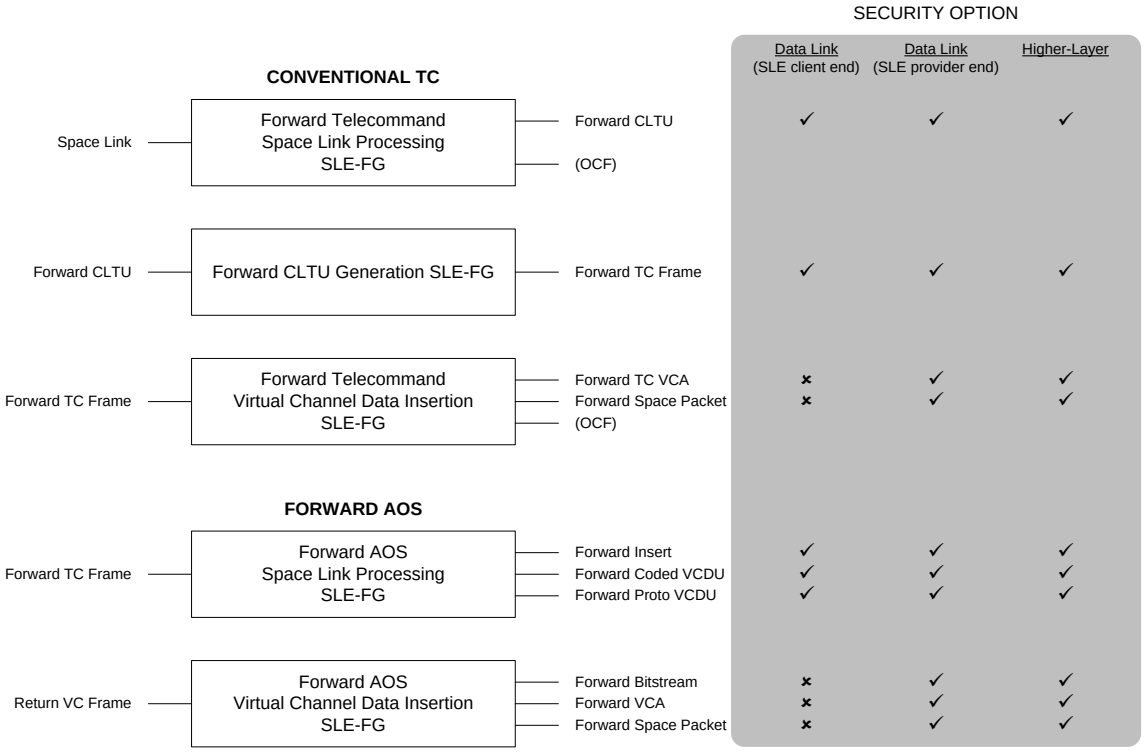

Figure 6-2: Impact of Security on Forward SLE Services

6.4 SECURITY OPTION COMPARISON

6.4.1 PHYSICAL LAYER (BULK ENCRYPTION)

Physical Layer security (bulk encryption) provides the highest possible level of data confidentiality for space mission data systems, but only on a point-to-point basis. No additional security services are implied other than those provided by the encryption mechanism used to provide data confidentiality.

The application of bulk encryption to the CCSDS conventional telecommand, telemetry, and AOS Recommended Standards will deny all cross-support services without pre-placed copies of the encryption keys at system access points or the use of public key technology used to encrypt content encryption keys. Also, bulk encryption does not allow the CCSDS link-layer synchronization services to operate, and as a result, the cryptographic devices utilized must provide data synchronization.

Bulk encryption does not allow any Error Detection and Correction (EDAC) information to be available in plaintext. Thus all CCSDS channel-coding services would be rendered meaningless, as the data must be acquired, synchronized, and decrypted before the coding sublayer information becomes available. The CCSDS EDAC information would therefore be unnecessary overhead in such a scheme. However, it should be noted that some high-grade cryptographic devices might include independent EDAC functionally.

Bulk encryption does not provide any concept of end-to-end security in the OSI sense. It is applied to the data on a point-to-point basis with a cryptographic device at each end of a link in the communications network. However, anti-jam techniques that provide link availability (e.g., spread spectrum, frequency hopping) can and should be employed at the Physical Layer to ensure non-interference over the RF link.

In summary, the security requirements of high-security missions would be satisfied by bulk encryption at the Physical Layer; however, specific operational benefits provided by the CCSDS Recommended Standards would not be available.

6.4.2 DATA LINK SECURITY

Data Link Layer security can be considered as a compromise for missions requiring a relatively high level of security but required to retain a number of CCSDS benefits. Specific CCSDS data-link benefits such as link synchronization and performance enhancement through EDAC mechanisms are retained as the EDAC information remains in plaintext over the space link.

The CCSDS data structure may be used throughout the mission data system; however, only the coding sublayer of the Data Link Layer and the Physical Layer remain in plaintext.

When SDLS is used, encryption only protects higher-layer data and not the TC, TM, or AOS Data Link Layer protocol structures. SDLS provides no protection against traffic flow

analysis at the Data Link Layer. If SDLS is used for authentication without encryption, both the higher-layer data and the TC, TM, or AOS Data Link Layer protocol structures remain in plaintext.

Data Link Layer encryption does not provide end-to-end security in the OSI sense. It is applied to the data on a hop-by-hop basis; however, some low-level cross-support services are available to extend the secure space link within the ground network.

6.4.3 NETWORK

IPSec provides security on an end-to-end basis, from the source of the transmitted data to the final destination. For example, an instrument control center could be one end point where the security services (confidentiality, integrity, and authentication) are applied to the data, and an instrument on board a spacecraft could be the other end point. All intermediate systems, such as routers, gateways, and control centers, would not have access to the user data unless explicitly authorized. All applications using the network would be able to make use of the IPSec-provided security services with no additional burden placed on the application itself.

In order to provide end-to-end security, the IPSec approach allows the headers from the layers below (e.g., network, link, and physical) to remain in plaintext to enable the intermediate routing of the IPSec protocol data units. Thus traffic analysis protection is not provided, and the encrypted data may be intercepted in the intermediate networks. However, because the data is encrypted, confidentiality is maintained.

6.4.4 APPLICATION LAYER SECURITY

The CCSDS packet protocol or Application Layer security (e.g., TLS) approaches are suitable for implementations requiring protection of only the application data itself. However, there may be requirements for a number of different application-specific security mechanisms, which could lead to duplicated effort or, more importantly, to the introduction of security flaws in the system (see 6.5.1). But for those payloads that must use security mechanisms when no such mechanisms are provided by the mission bus, or if the provided mechanisms are not adequate, Application Layer security may be the fallback without impacting the entire program.

6.5 SECURITY OPTION SELECTION

6.5.1 CHOICE OF POSITION OF ENCRYPTION

Most space missions that require confidentiality services will not require encryption at more than one layer in the data systems architecture. By limiting the implementation of encryption to one layer, the following benefits are obtained:

– a simplified system-security approach;

– minimized security-development and operating costs; and

– low overall security processing requirements on the data system.

Also, if encryption implementation is limited to the Network Layer or below, different applications will not need to implement their own encryption mechanisms. Multiple encryption mechanisms duplicate efforts and could introduce security flaws as well as increase development and operations costs. Flaws can be introduced through multiple implementations in which security services are incorrectly implemented. There is less of a chance of propagating problems if a single, verified encryption implementation is used within the space data system.

If full traffic-analysis protection is required, then encryption will need to be implemented at the Physical Layer on a point-to-point basis. Physical Layer encryption (or bulk encryption) may be combined with TRANSEC techniques such as frequency hopping or spread spectrum to enhance the level of security by reducing the probability jamming, detection, and interception of the RF link.

If a mission requires a high level of security with some traffic-flow confidentiality, and requires key benefits provided by use of CCSDS Recommended Standards, Data Link Layer security will provide the solution. It is noted that Data Link Layer security will operate almost exclusively over the space link; however, low-level SLE services (Return All Frames and Forward CLTU) may be used to extend the secure space data link within the ground network.

If a mission requires confidentiality of different virtual channels, which could correspond to confidentiality between different payloads on a shared spacecraft, then encryption should be included above the frame sublayer (conventional transfer frame or AOS VCDU) within the Data Link Layer. This approach corresponds to the CCSDS Space Data Link Security approach described in 5.3.

If a mission requires end-to-end protection of all data in the space mission data system, either Application Layer or Network Layer encryption should be chosen. Depending on the mission-data-system architecture, Network Layer encryption may be implemented via use of the IPSec confidentiality service or via encryption of the space packet protocol as described in 5.4. Alternatively, Option B as described in 5.3 would also provide end-to-end protection as long as no intermediate systems or SLE services come into play.

If a mission requires a high granularity of data protection (for example, a separate key for encryption of different application data in the system) or selective field-data protection, then encryption of the different application processes is necessary. Although more complex to implement, selective field encryption may be beneficial to protect only the sensitive fields in the application data, as most cryptographic algorithms consume large amounts of processing power.

If a mission requires high security over the RF medium, with additional end-to-end security services in the ground network or on board the spacecraft, then encryption may need to be provided at more than one layer. For example, bulk encryption or Data Link Layer security may be applied on all space-ground and ground-space links with additional encryption at the Network Layer to achieve end-to-end data protection.

6.5.2 LOCATION OF OTHER SECURITY SERVICES

The choice of implementation of authentication, data integrity, and access-control services has less impact on the data-system architecture. For example, it may be beneficial to locate the additional fields (e.g., digital signature, ICV, sequence number) that may be required for authentication and data-integrity services at the same layer as encryption to keep all security services in one ‘clean’ security layer.

Otherwise, it may be appropriate to provide authentication and data integrity between different Network Layer or Application Layer entities. The choice is very much dependent on the data-system architecture, the protocol in use, and the mission security requirements.

Access-control security services are likely to be implemented at the Application Layer. Many missions may wish to utilize the access-control mechanisms built into network operating systems (e.g., Windows UNIX/Linux). Other missions may elect to use other access-control systems such as Radius or certificate-based identity.

ANNEX A

SPECIFIC AGENCY SECURITY IMPLEMENTATIONS

A1 THE ESA COPERNICUS TELECOMMAND AUTHENTICATION SYSTEM

ESA, in cooperation with industry, has developed a telecommand authentication system that is currently being used in the Copernicus program Sentinel fleet of spacecraft. The system was one of the predecessors of the Space Data Link Layer Security (SDLS) standard and shares many features with it, such as the selected cryptographic algorithm (baseline mode for Telecommand). It also includes the functionality to upload new authentication keys to the spacecraft.

The system uses a two-key-tier hierarchy with master keys and session (authentication) keys (in line with the specifications in the CCSDS Symmetric Key Management Recommended Standard. Session keys are used for the actual telecommand authentication and can be replenished using an Over-The-Air-Rekeying (OTAR) process similar to the one in the SDLS Extended Procedures. Master keys are used for protecting the confidentiality of the session keys during the OTAR process and for other critical operations.

Telecommand authentication occurs at the segmentation layer (see figure A-1). Telecommand security associations are differentiated using MAPs identified in the segment header. The authentication trailer identifies the key that is being used, contains the current value of the Logical Authentication Counter (LAC), and the MAC. The LAC is an anti-replay counter that increments with each telecommand and prevents successful replay of intercepted commands with proper MACs (but wrong anti-replay). The MAC is calculated over the entire telecommand segment except for the space reserved for MAC insertion, taking into account the key and the LAC values. The authentication trailer is generated by the mission control system on the ground and then validated by the security unit on board the spacecraft. Should the authentication on the spacecraft fail, the command will be rejected and the operator informed about the nature of the authentication failure.

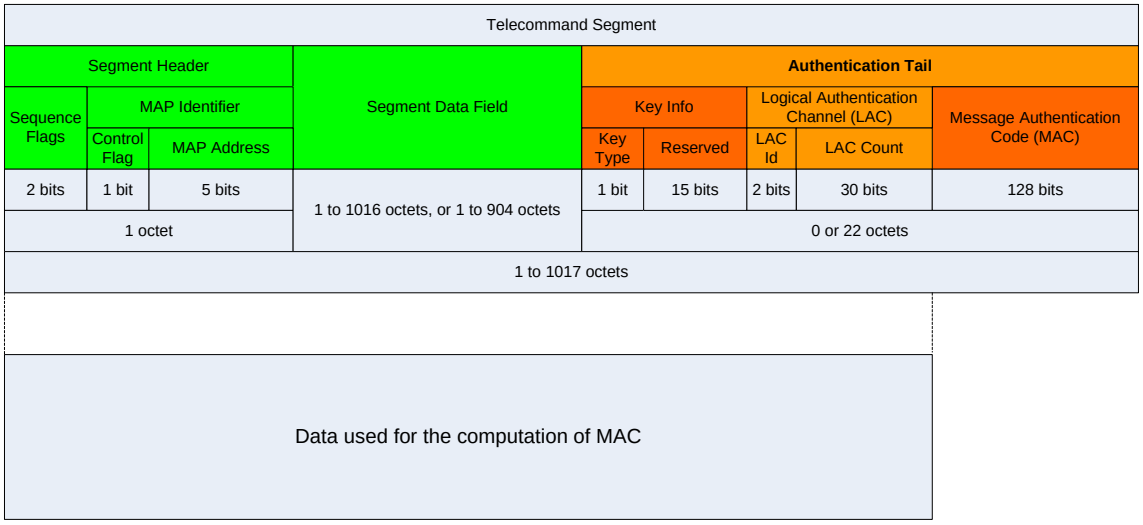

Figure A-1: ESA Copernicus Authenticated Telecommand Segment

The OTAR mechanism is implemented using a custom ESA Packet Utilization Standard (PUS) (reference [22]) service at Application Layer. All OTAR commands are addressed directly to the security unit of the spacecraft. The key generation and management on ground happens in a separated and isolated Key Management Facility (KMF). This KMF uses a state-of-the-art random-number generator for the production of new authentication keys.

A2 INTERNATIONAL SPACE STATION

The International Space Station (ISS) mission-communications system uses the AOS Recommended Standard (reference [5]) for the telecommand and telemetry links. The Multiplex Protocol Data Unit (MPDU) and Bitstream services are used to support different data types.

Encryption using the Triple Data Encryption Standard (3DES) algorithm is incorporated on the uplink at the VCA sublayer as described in 5.3 of this report. This means that the VCDU data unit zone is encrypted. The insert zone (set to 64 bits) is used to provide cryptographic synchronization.

A3 THE SPACE TECHNOLOGY RESEARCH VEHICLE 1C/D MISSIONS

The Space Technology Research Vehicle (STRV) 1c/d microsatellite missions designed and implemented conventional CCSDS Data Link Layer security on the telecommand and telemetry links. Confidentiality and authentication services were implemented as part of the security layer on the telecommand link, with confidentiality only on the telemetry link.

A4 THE ESA AUTOMATED TRANSFER VEHICLE

The Automated Transfer Vehicle (ATV), the European servicing vehicle for the International Space Station (ISS), protected its Telecommand link by applying encryption and time authentication to its Telecommand Packets.

The encryption sublayer concept illustrated in figure A-2 below follows the Triple Data Encryption Standard (3-DES) as per ANSI-X.9-52. The Segment Data field includes the following three fields:

- a 2-octet key index, pointing to the decryption key;
- an 8-octet Initialization Vector (IV), which is unique per message; and
- encrypted packet data.

Telecommand packets include a Time Authentication field. The spacecraft Telecommand Packet processor compares the packet value of this field with the spacecraft Onboard Time. If the value is higher than a threshold value, the Packet is rejected.

<table>
<tr><td rowspan="2">Segment Header</td><td colspan="3">Segment Data Field</td></tr>
<tr><td>Key Index</td><td>Init. Vector</td><td>Encrypted Packet Data</td></tr>
</table>

Figure A-2: ESA ATV Telecommand Encryption Sublayer Structure