BS ISO 21324:2016

BSI Standards Publication

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

Documents
Document Sharing Hub

Full document details: BS ISO 21324:2016

National foreword

This British Standard is the UK implementation of ISO 21324:2016.

The UK participation in its preparation was entrusted to Technical Committee ACE/68, Space systems and operations.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2016.
Published by BSI Standards Limited 2016

ISBN 978 0 580 93027 0

ICS 49.140

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2016.

Amendments/corrigendum issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO 21324:2016

INTERNATIONAL STANDARD

ISO 21324

First edition
2016-11-15

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

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

Reference number
ISO 21324:2016(E)

Documents
Document Sharing Hub

© ISO 2016

Full document details: BS ISO 21324:2016

COPYRIGHT PROTECTED DOCUMENT

© ISO 2016

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Published in Switzerland

© ISO 2016 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO 21324:2016

Foreword

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

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

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

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

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

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

© ISO 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21324:2016

STATEMENT OF INTENT

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

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

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

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

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

Documents
Document Sharing Hub
© ISO 2016 – All rights reserved
Full document details: BS ISO 21324:2016

FOREWORD

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CCSDS has processes for identifying patent issues and for securing from the patent holder agreement that all licensing policies are reasonable and non-discriminatory. However, CCSDS does not have a patent law staff, and CCSDS shall not be held responsible for identifying any or all such patent rights.

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

http://www.ccsds.org/

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

Documents
Document Sharing Hub
© ISO 2016 – All rights reserved
Full document details: BS ISO 21324:2016

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

Member Agencies

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

Observer Agencies

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

Documents
Document Sharing Hub
© ISO 2016 – All rights reserved
Full document details: BS ISO 21324:2016

DOCUMENT CONTROL

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

© ISO 2016 – All rights reserved
Full document details: BS ISO 21324:2016

CONTENTS

Section Page

1 INTRODUCTION 1-1

1.1 PURPOSE 1-1
1.2 SCOPE 1-1
1.3 APPLICABILITY 1-1
1.4 RATIONALE 1-2
1.5 DOCUMENT STRUCTURE 1-2
1.6 DEFINITIONS 1-3
1.7 CONVENTIONS 1-3
1.8 REFERENCES 1-4

2 OVERVIEW 2-1

2.1 CONCEPT OF SECURITY PROTOCOL 2-1
2.2 FEATURES OF SECURITY PROTOCOL 2-2
2.3 SERVICE FUNCTIONS 2-6

3 SERVICE DEFINITION 3-1

3.1 OVERVIEW 3-1
3.2 FUNCTION AT THE SENDING END 3-1
3.3 FUNCTION AT THE RECEIVING END 3-4
3.4 SECURITY ASSOCIATION MANAGEMENT SERVICE 3-7

4 PROTOCOL SPECIFICATION 4-1

4.1 PROTOCOL DATA UNITS 4-1
4.2 SECURITY PROTOCOL PROCEDURES 4-3

5 USE OF THE SERVICES WITH CCSDS PROTOCOLS 5-1

5.1 TM PROTOCOL 5-1
5.2 TC PROTOCOL 5-1
5.3 AOS PROTOCOL 5-2
5.4 SUMMARY OF PROTOCOL SERVICES 5-3

6 MANAGED PARAMETERS 6-1

6.1 OVERVIEW 6-1
6.2 REQUIREMENTS 6-1

7 CONFORMANCE REQUIREMENTS 7-1

Documents
Document Sharing Hub
© ISO 2016 – All rights reserved
Full document details: BS ISO 21324:2016

CONTENTS (continued)

Section Page

ANNEX A PROTOCOL IMPLEMENTATION CONFORMANCE STATEMENT (PICS) PROFORMA (NORMATIVE) A-1
ANNEX B SECURITY, SANA, AND PATENT CONSIDERATIONS (INFORMATIVE) B-1
ANNEX C ABBREVIATIONS AND ACRONYMS (INFORMATIVE) C-1
ANNEX D INFORMATIVE REFERENCES (INFORMATIVE) D-1
ANNEX E BASELINE IMPLEMENTATION MODE (INFORMATIVE) E-1

Figure

2-1 Security Protocol within OSI Model 2-1
2-2 Security Protocol Interaction with Space Link Frames 2-2
2-3 Security Protocol Support for TM Services 2-3
2-4 Security Protocol Support for TC Services 2-4
2-5 Security Protocol Support for AOS Services 2-5
4-1 Security Header 4-1
4-2 Security Trailer 4-3
5-1 TM Transfer Frame Using the Security Protocol 5-1
5-2 TC Transfer Frame Using the Security Protocol 5-2
5-3 AOS Transfer Frame Using the Security Protocol 5-2
E-1 Security Header (TM Baseline) E-1
E-2 Security Trailer (TM Baseline) E-2
E-3 Security Header (TC Baseline) E-2
E-4 Security Trailer (TC Baseline) E-3
E-5 Security Header (AOS Baseline) E-4
E-6 Security Trailer (AOS Baseline) E-4

Table

5-1 Summary of Protocol and Services Support 5-3
6-1 Managed Parameters for Security Protocol 6-1

Documents
Document Sharing Hub
© ISO 2016 – All rights reserved
Full document details: BS ISO 21324:2016

1 INTRODUCTION

1.1 PURPOSE

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

1.2 SCOPE

This Recommended Standard defines the Security Protocol in terms of:

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

b) the procedures performed by the service provider.

It does not specify:

a) individual implementations or products;

b) the implementation of service interfaces within real systems;

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

d) the management activities required to configure and control the service.

This Recommended Standard does not mandate the use of any particular cryptographic algorithm with the Security Protocol. Reference [4] provides a listing of algorithms recommended by CCSDS; any organization should conduct a risk assessment before choosing to substitute other algorithms. Annex E (non-normative) defines baseline implementations suitable for a large range of space missions.

1.3 APPLICABILITY

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

The Recommended Standard specified in this document is to be invoked through the normal standards programs of each CCSDS Agency, and is applicable to those missions for which interoperability and cross support based on capabilities described in this Recommended Standard is anticipated. Where mandatory capabilities are clearly indicated in sections of the

Documents
Document Sharing Hub
© ISO 2016 – All rights reserved
Full document details: BS ISO 21324:2016

Recommended Standard, they must be implemented when this document is used as a basis for interoperability and cross support. Where options are allowed or implied, implementation of these options is subject to specific bilateral cross support agreements between the Agencies involved.

1.4 RATIONALE

The goals of this Recommended Standard are to:

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

b) preserve compatibility with existing CCSDS Space Data Link Protocol Transfer Frame Header and Trailer formats and frame processing implementations so that, where appropriate, legacy frame processing infrastructure may continue to be used without modification;

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

d) facilitate the development of common commercial implementations to improve interoperability across agencies.

More discussion of the Security Protocol's goals and design choices, including its interaction with other CCSDS services, may be found in reference [D3].

1.5 DOCUMENT STRUCTURE

This document is organized as follows:

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

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

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

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

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

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

Documents
Document Sharing Hub
© ISO 2016 – All rights reserved
Full document details: BS ISO 21324:2016

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

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

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

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

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

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

1.6 DEFINITIONS

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

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

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

ApplySecurity Payload: Payload to the ApplySecurity function.

ProcessSecurity Payload: Payload to the ProcessSecurity function.

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

1.7 CONVENTIONS

1.7.1 NOMENCLATURE

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

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

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

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

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

Documents
Document Sharing Hub
© ISO 2016 – All rights reserved
Full document details: BS ISO 21324:2016

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

1.7.2 INFORMATIVE TEXT

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

- Overview;
- Background;
- Rationale;
- Discussion.

1.8 REFERENCES

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

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

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

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

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

NOTE – Informative references are listed in annex D.

Documents
Document Sharing Hub
© ISO 2016 – All rights reserved
Full document details: BS ISO 21324:2016

2 OVERVIEW

2.1 CONCEPT OF SECURITY PROTOCOL

The Space Data Link Security Protocol is a data processing method for space missions that need to apply authentication and/or confidentiality to the contents of Transfer Frames used by Space Data Link Protocols over a space link. The Security Protocol is provided only at the Data Link Layer (Layer 2) of the OSI Basic Reference Model (reference [D1]), as illustrated in figure 2-1. It is an extra service of the Space Data Link Protocols defined in references [1]–[3], and therefore is to be used together with one of these references. (The Security Protocol is *not* applicable for use with the Proximity-1 Space Data Link Protocol.)

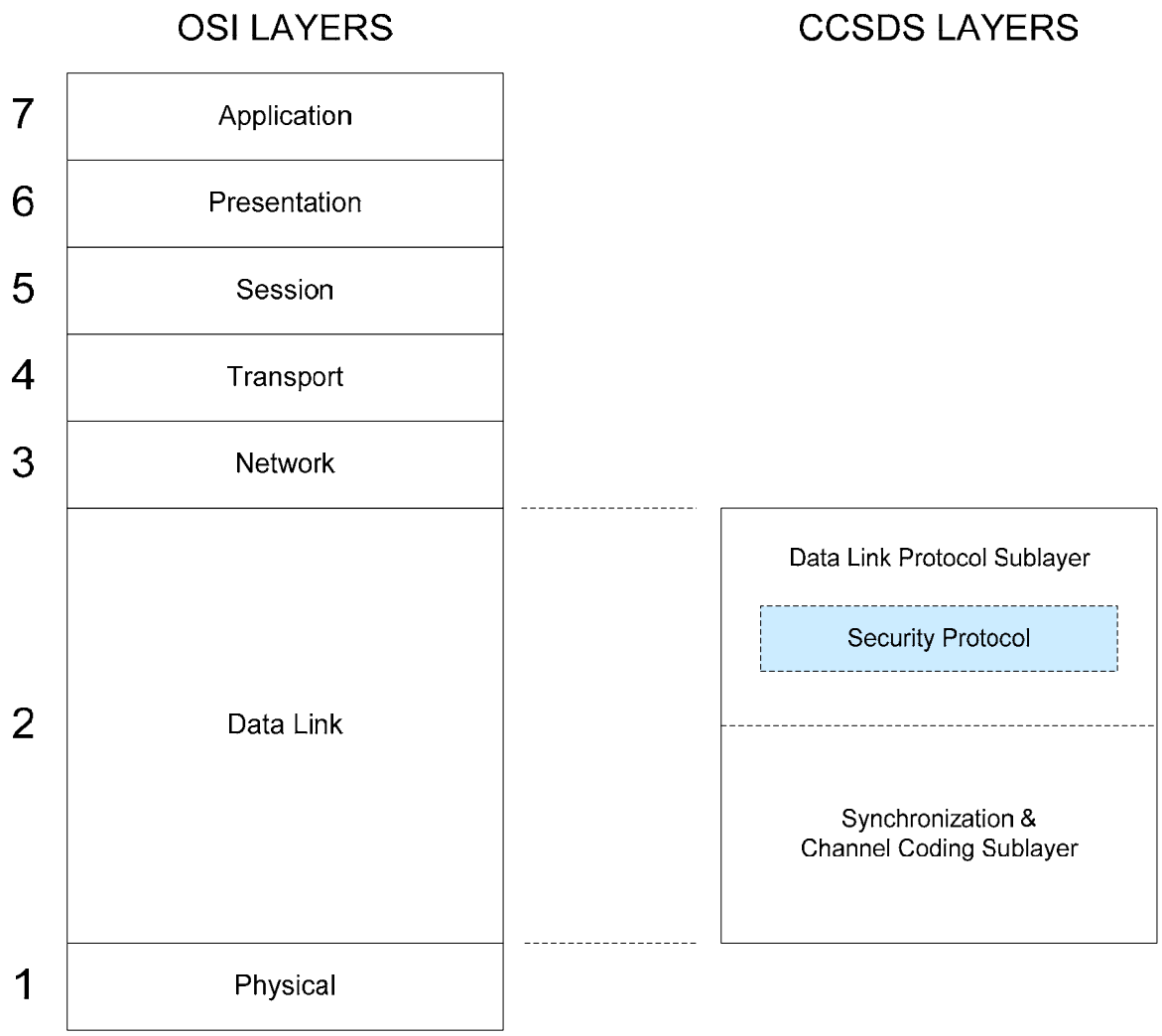

Figure 2-1: Security Protocol within OSI Model

© ISO 2016 – All rights reserved
Full document details: BS ISO 21324:2016

2.2 FEATURES OF SECURITY PROTOCOL

2.2.1 GENERAL

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

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

2.2.2 DATA LINK LAYER PROTOCOLS

Two sublayers of the Data Link Layer are defined for CCSDS space link protocols as shown in reference [D4]. Each of the three supported Space Data Link Protocols, Telemetry (TM), Telecommand (TC), and Advanced Orbiting Systems (AOS), correspond to the Data Link Protocol Sublayer. Operation of the Security Protocol is unaffected by the Synchronization and Channel Coding Sublayer.

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

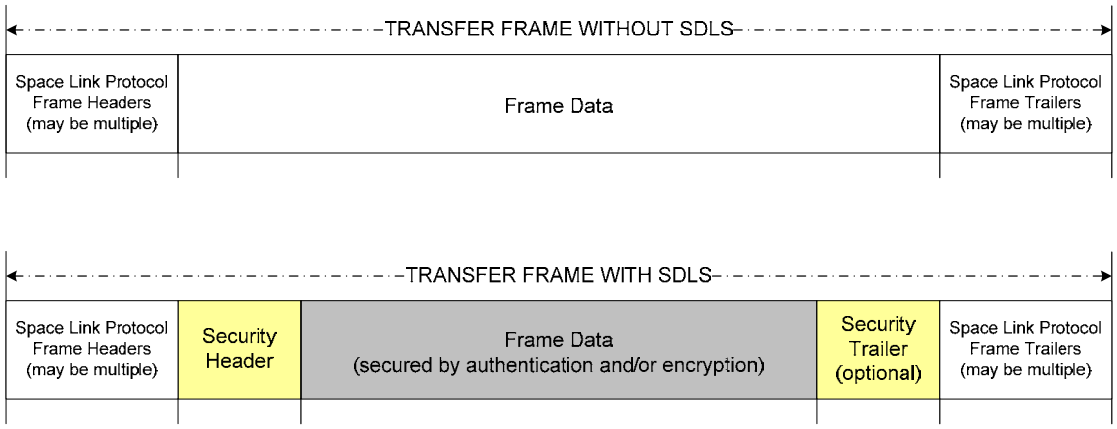

Figure 2-2: Security Protocol Interaction with Space Link Frames

Documents
Document Sharing Hub
© ISO 2016 – All rights reserved
Full document details: BS ISO 21324:2016

2.2.3 SECURITY SERVICE FOR TM

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

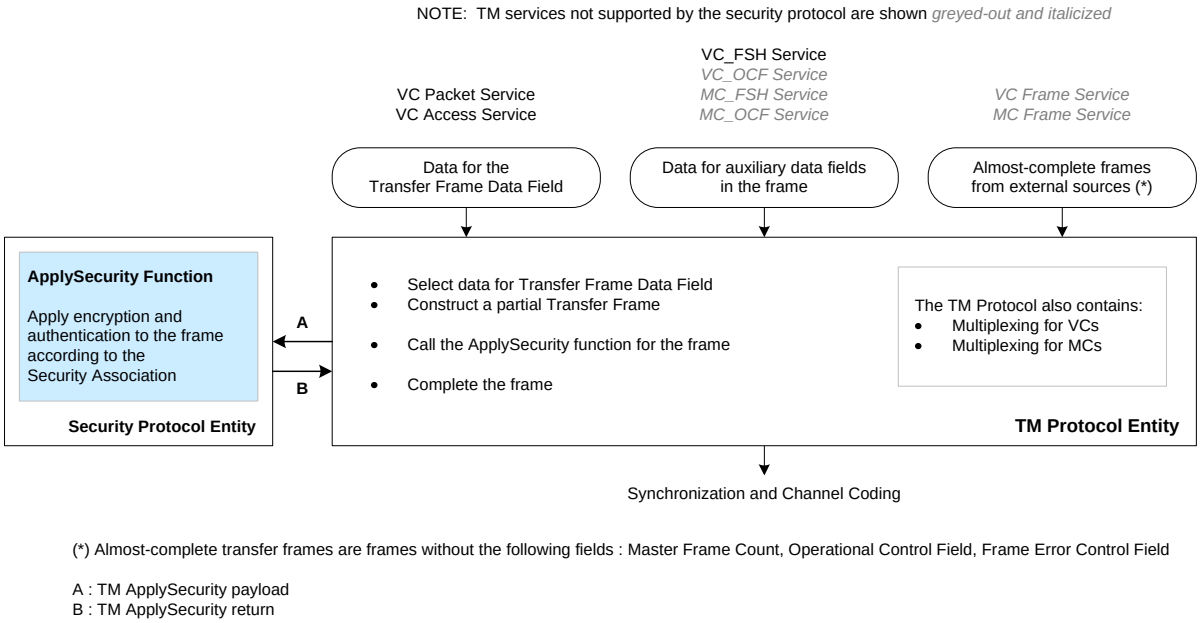

Figure 2-3: Security Protocol Support for TM Services

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

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

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

© ISO 2016 – All rights reserved
Full document details: BS ISO 21324:2016

2.2.4 SECURITY SERVICE FOR TC

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

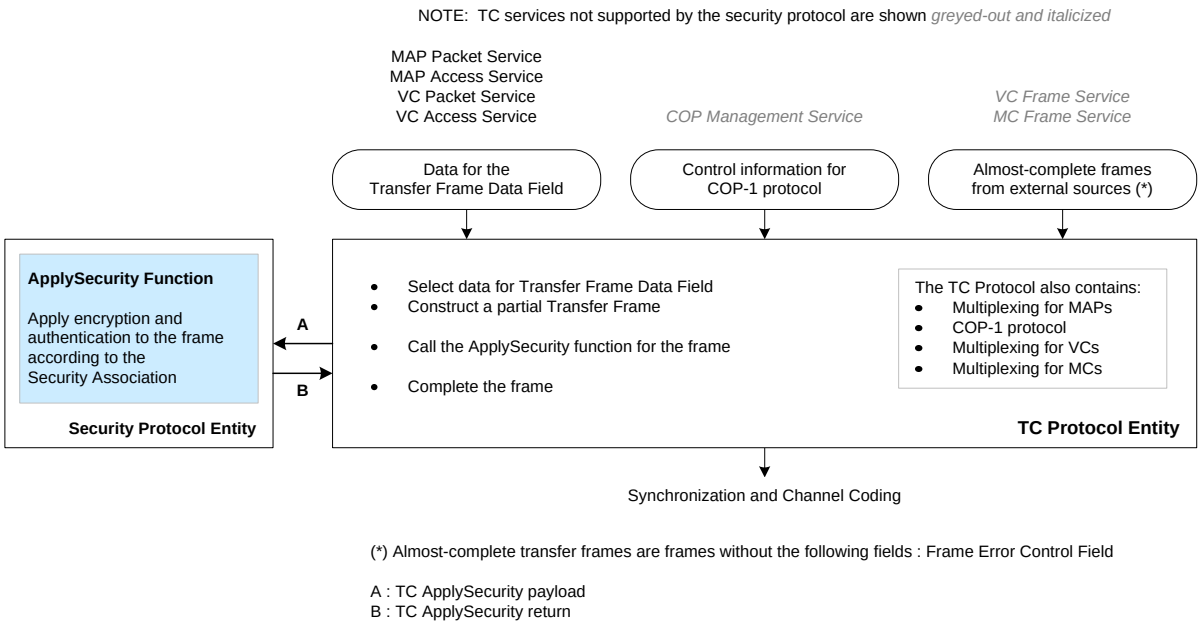

Figure 2-4: Security Protocol Support for TC Services

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

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

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

Documents
Document Sharing Hub
© ISO 2016 – All rights reserved
Full document details: BS ISO 21324:2016

2.2.5 SECURITY SERVICE FOR AOS

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

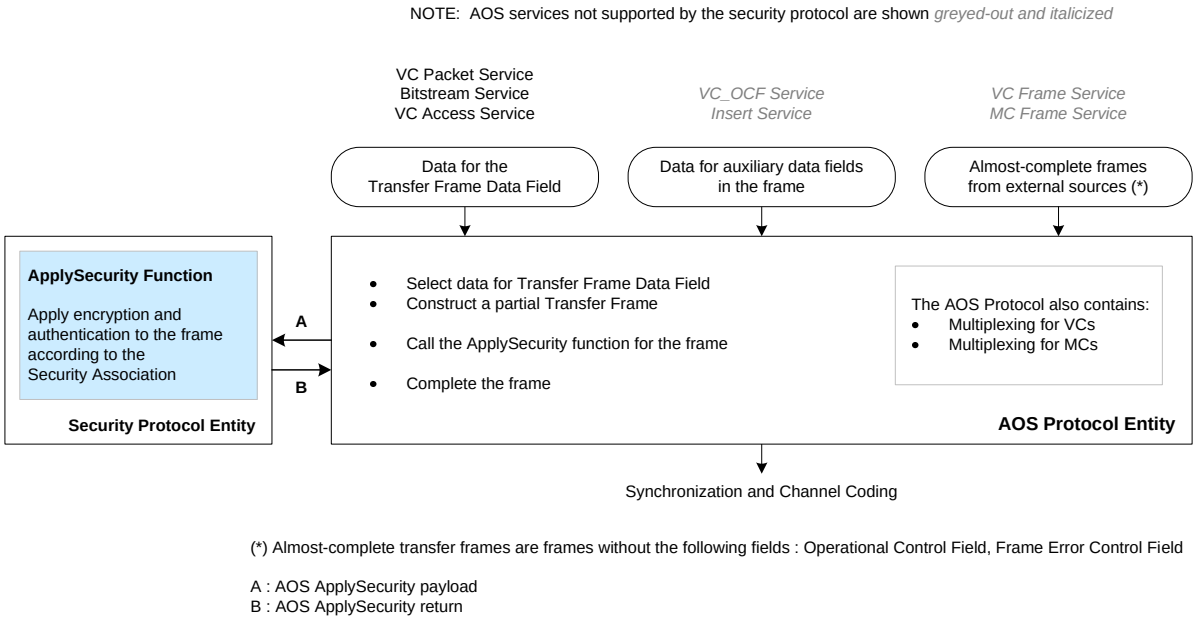

Figure 2-5: Security Protocol Support for AOS Services

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

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

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

© ISO 2016 – All rights reserved
Full document details: BS ISO 21324:2016

2.3 SERVICE FUNCTIONS

2.3.1 SECURITY ASSOCIATIONS

2.3.1.1 General

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

2.3.1.2 Security Association Context

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

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

2.3.1.3 Security Association Service Types

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

a) authentication;

b) encryption;

c) authenticated encryption.

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

2.3.1.4 Security Header and Trailer

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

Documents
Document Sharing Hub
© ISO 2016 – All rights reserved
Full document details: BS ISO 21324:2016

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

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

2.3.1.5 Security Association Management

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

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

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

2.3.2 AUTHENTICATION

2.3.2.1 General

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

2.3.2.2 Message Authentication and Integrity

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

Documents
Document Sharing Hub
© ISO 2016 – All rights reserved
Full document details: BS ISO 21324:2016

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

2.3.2.3 Replay Protection

2.3.2.3.1 General

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

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

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

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

2.3.2.3.2 Sequence Number

The sender increments its managed sequence number by one with each transmitted frame belonging to that SA. With each valid received frame belonging to that SA, the receiver will replace its stored sequence number with the received value on the condition that the received sequence number is higher than the stored sequence number. Additionally, if the received Sequence Number differs from the expected value by more than a defined positive value called the Sequence Number Window, the receiver discards the frame and neither replaces nor increments its stored sequence number.

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

2.3.2.3.3 Sequence Number Window

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

2.3.2.3.4 Sequence Number Location

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

Documents
Document Sharing Hub
© ISO 2016 – All rights reserved
Full document details: BS ISO 21324:2016