INTERNATIONAL STANDARD

ISO 15892

First edition
2000-09-15

Space data and information transfer systems — Protocol specification for space communications — Security protocol

Systèmes de transfert des informations et données spatiales — Spécification d'un protocole pour communications spatiales — Protocole de sécurité

Reference number
ISO 15892:2000(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.ch
Web www.iso.ch

Printed in Switzerland

Foreword

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

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

International Standard ISO 15892 was prepared by the Consultative Committee for Space Data Systems (CCSDS) (as CCSDS 713.5-B-1) and was adopted (without modifications except those stated in clause 3 of this International Standard) by Technical Committee ISO/TC 20, *Aircraft and space vehicles*, Subcommittee SC 13, *Space data and information transfer systems*.

Space data and information transfer systems — Protocol specification for space communications — Security protocol

1 Scope

This International Standard specifies the requirements for the services and protocols of the space communications protocol specification (SCPS) security protocol (SP). These requirements are to allow independent implementations of this protocol to interoperate if they use compatible security service algorithms.

This International Standard is applicable to any kind of space mission or infrastructure, regardless of complexity.

2 Conformance

This International Standard is applicable to all systems that claim conformance to the ISO/CCSDS SCPS security protocol.

3 Requirements

Requirements are the technical recommendations made in the following publication (reproduced on the following pages), which is adopted as an International Standard:

CCSDS 713.5-B-1, May 1999, *Recommendation for space data system standards — Space communications protocol specification (SCPS) — Security protocol (SCPS-SP).*

For the purposes of international standardization, the modifications outlined below shall apply to the specific clauses and paragraphs of publication CCSDS 713.5-B-1.

Pages i to v

This part is information which is relevant to the CCSDS publication only.

Pages B-1 to B-2

Add the following information to the references indicated in annex B:

[B12] Document CCSDS 713.0-B-1, May 1999, is equivalent to ISO 15891:2000.

[B13] Document CCSDS 714.0-B-1, May 1999, is equivalent to ISO 15893:2000.

[B16] Document CCSDS 701.0-B-2, November 1992, is equivalent to ISO 13420:1997.

[B17] Document CCSDS 102.0-B-4, November 1995, is equivalent to ISO 13419:1997.

[B18] Document CCSDS 201.0-B-2, November 1995, is equivalent to ISO 12171:1998.

4 Revision of publication CCSDS 713.5-B-1

It has been agreed with the Consultative Committee for Space Data Systems that Subcommittee ISO/TC 20/SC 13 will be consulted in the event of any revision or amendment of publication CCSDS 713.5-B-1. To this end, NASA will act as a liaison body between CCSDS and ISO.

Consultative Committee for Space Data Systems

RECOMMENDATION FOR SPACE DATA SYSTEM STANDARDS

SPACE COMMUNICATIONS PROTOCOL SPECIFICATION (SCPS)—

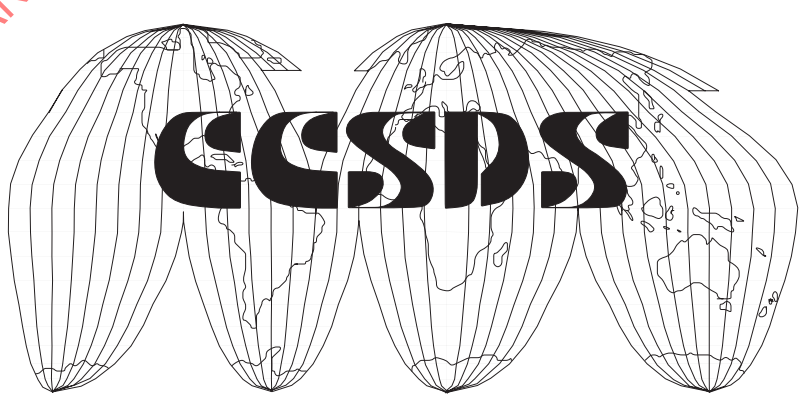
SECURITY PROTOCOL

(SCPS-SP)

CCSDS 713.5-B-1

BLUE BOOK

May 1999



(Blank page)

CCSDS RECOMMENDATION FOR SCPS SECURITY PROTOCOL (SCPS-SP)

AUTHORITY

Issue:	Blue Book, Issue 1
Date:	May 1999
Location:	Newport Beach, California, USA

This document has been approved for publication by the Management Council of the Consultative Committee for Space Data Systems (CCSDS) and represents the consensus technical agreement of the participating CCSDS Member Agencies. The procedure for review and authorization of CCSDS Recommendations is detailed in reference [B1], and the record of Agency participation in the authorization of this document can be obtained from the CCSDS Secretariat at the address below.

This Recommendation is published and maintained by:

CCSDS Secretariat
Program Integration Division (Code MT)
National Aeronautics and Space Administration
Washington, DC 20546, USA

STATEMENT OF INTENT

The Consultative Committee for Space Data Systems (CCSDS) is an organization officially established by the management of member space Agencies. 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 **Recommendations** and are not considered binding on any Agency.

This **Recommendation** is issued by, and represents the consensus of, the CCSDS Plenary body. Agency endorsement of this **Recommendation** is entirely voluntary. Endorsement, however, indicates the following understandings:

- o Whenever an Agency establishes a CCSDS-related **standard**, this **standard** will be in accord with the relevant **Recommendation**. Establishing such a **standard** does not preclude other provisions which an Agency may develop.

- o Whenever an Agency establishes a CCSDS-related **standard**, the Agency will provide other CCSDS member Agencies with the following information:

  - -- The **standard** itself.

  - -- The anticipated date of initial operational capability.

  - -- The anticipated duration of operational service.

- o Specific service arrangements shall be made via memoranda of agreement. Neither this **Recommendation** nor any ensuing **standard** is a substitute for a memorandum of agreement.

No later than five years from its date of issuance, this **Recommendation** 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 **Recommendation** is issued, existing CCSDS-related Agency standards and implementations are not negated or deemed to be non-CCSDS compatible. It is the responsibility of each Agency to determine when such standards or implementations are to be modified. Each Agency is, however, strongly encouraged to direct planning for its new standards and implementations towards the later version of the Recommendation.

FOREWORD

This Recommendation defines the services and protocols of the Space Communications Protocol Specification (SCPS) Security Protocol (SP).

Through the process of normal evolution, it is expected that expansion, deletion, or modification of this document may occur. This Recommendation is therefore subject to CCSDS document management and change control procedures as defined in reference [B1]. 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 addressed to the CCSDS Secretariat at the address indicated on page i.

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

Member Agencies

- British National Space Centre (BNSC)/United Kingdom.
- Canadian Space Agency (CSA)/Canada.
- Centre National d'Etudes Spatiales (CNES)/France.
- Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)/Germany.
- European Space Agency (ESA)/Europe.
- Instituto Nacional de Pesquisas Espaciais (INPE)/Brazil.
- National Aeronautics and Space Administration (NASA)/USA.
- National Space Development Agency of Japan (NASDA)/Japan.
- Russian Space Agency (RSA)/Russian Federation.

Observer Agencies

- Austrian Space Agency (ASA)/Austria.
- Central Research Institute of Machine Building (TsNIIMash)/Russian Federation.
- Centro Tecnico Aeroespacial (CTA)/Brazil.
- Chinese Academy of Space Technology (CAST)/China.
- Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
- Communications Research Laboratory (CRL)/Japan.
- Danish Space Research Institute (DSRI)/Denmark.
- European Organization for the Exploitation of Meteorological Satellites (EUMETSAT)/Europe.
- European Telecommunications Satellite Organization (EUTELSAT)/Europe.
- Federal Service of Scientific, Technical & Cultural Affairs (FSST&CA)/Belgium.
- Hellenic National Space Committee (HNSC)/Greece.
- Indian Space Research Organization (ISRO)/India.
- Industry Canada/Communications Research Centre (CRC)/Canada.
- Institute of Space and Astronautical Science (ISAS)/Japan.
- Institute of Space Research (IKI)/Russian Federation.
- KFKI Research Institute for Particle & Nuclear Physics (KFKI)/Hungary.
- MIKOMTEK: CSIR (CSIR)/Republic of South Africa.
- Korea Aerospace Research Institute (KARI)/Korea.
- Ministry of Communications (MOC)/Israel.
- National Oceanic & Atmospheric Administration (NOAA)/USA.
- National Space Program Office (NSPO)/Taipei.
- Swedish Space Corporation (SSC)/Sweden.
- United States Geological Survey (USGS)/USA.

CCSDS RECOMMENDATION FOR SCPS SECURITY PROTOCOL (SCPS-SP)

DOCUMENT CONTROL

Document	Title	Date	Status
CCSDS 713.5-B-1	Space Communications Protocol Specification (SCPS)—Security Protocol (SCPS-SP)	May 1999	Original issue

CCSDS RECOMMENDATION FOR SCPS SECURITY PROTOCOL (SCPS-SP)

CONTENTS

Section Page

1 INTRODUCTION 1-1

1.1 PURPOSE 1-1
1.2 SCOPE 1-1
1.3 APPLICABILITY 1-1
1.4 ORGANIZATION OF RECOMMENDATION 1-1
1.5 CONVENTIONS AND DEFINITIONS 1-2

2 OVERVIEW 2-1
3 PROTOCOL SPECIFICATION 3-1

3.1 SCPS-SP TYPES OF SECURITY SERVICES 3-1
3.2 SCPS-SP PROTOCOL DATA UNIT 3-2
3.3 SCPS-SP CLEAR HEADER 3-3
3.4 SCPS-SP PROTECTED HEADER 3-5
3.5 INTEGRITY CHECK VALUE FIELD 3-7

4 PROTOCOL FUNCTIONS 4-1

4.1 TRANSMISSION FUNCTIONS 4-1
4.2 RECEPTION FUNCTIONS 4-2
4.3 INTEGRITY SERVICE PROCESSING 4-4
4.4 AUTHENTICATION SERVICE PROCESSING 4-6
4.5 CONFIDENTIALITY SERVICE PROCESSING 4-7
4.6 END-SYSTEM TO INTERMEDIATE SYSTEM INTERACTIONS 4-11

5 SECURITY ASSOCIATION ATTRIBUTES 5-1

ANNEX A ACRONYMS AND ABBREVIATIONS A-1
ANNEX B INFORMATIVE REFERENCES B-1
ANNEX C PROTOCOL IMPLEMETATION CONFORMANCE STATMENT (PICS) PROFORMA C-1
ANNEX D SCPS SECURITY PROTOCOL SERVICE SPECIFICATION D-1

Figure

3-1 SCPS-SP Protocol Data Unit 3-2
3-2 SCPS-SP Clear Header 3-3
3-3 SCPS-SP Protected Header 3-5
3-4 Protected Header Encapsulated Address Field 3-6

CCSDS RECOMMENDATION FOR SCPS SECURITY PROTOCOL (SCPS-SP)

1 INTRODUCTION

1.1 PURPOSE

The purpose of this Recommendation is to define the services and protocols of the Space Communications Protocol Specifications (SCPS) Security Protocol (SP). This definition will allow independent implementations of the protocol to interoperate if they use compatible security service algorithms.

1.2 SCOPE

This Recommendation is intended to be applied to all systems that claim conformance to the SCPS Security Protocol.

1.3 APPLICABILITY

This Recommendation is designed to be applicable to any kind of space mission or infrastructure, regardless of complexity. It is intended that this should become a uniform standard among all CCSDS Agencies.

1.4 ORGANIZATION OF RECOMMENDATION

This document is organized as follows:

- Section 1 provides an introduction to the Recommendation;
- Section 2 provides an overview of the Security Protocol;
- Section 3 provides the protocol specification and the header layouts;
- Section 4 provides details on protocol processing;
- Section 5 provides information on Security Association Attributes;
- Annex A provides expansion of acronyms and abbreviations used in the document;
- Annex B lists informative references;
- Annex C provides the Protocol Implementation Conformance Statement (PICS);
- Annex D provides the Security Protocol's service specification.

1.5 CONVENTIONS AND DEFINITIONS

1.5.1 BIT NUMBERING CONVENTION AND NOMENCLATURE

In this document, the following convention is used to identify each bit in an N-bit field. The first bit in the field to be transmitted is drawn as the most left justified when drawing a figure, and is defined to be 'Bit 0'. The following bit is defined to be 'Bit 1' and so on, through 'Bit N-1'. The order in which multi-octet fields are transmitted is called 'Big-Endian' byte ordering. When applied to networking, this is called 'network byte order'. In this ordering scheme, bit 0 of a 32-bit value is the Most Significant Bit (MSB) and bit 31 is the least significant bit. The octet containing bits 0-7 is transmitted first, followed by the octet containing bits 8-15, followed by the octet containing bits 16-23, and finally the octet containing bits 24-31. Fields are sometimes drawn on more than one line in a figure. In this case, the uppermost line of a multi-line field is transmitted before subsequent lines in that field, and in the case of binary values, contains the bits of greater significance than those in following lines. Note that 'Big-Endian' byte ordering is NOT what some machines (notably the 80x86 class of machines) use internally. Implementers must ensure that headers are converted to network byte order for transmission.

The following conventions apply throughout this Recommendation:

- the words 'shall' and 'must' imply a binding and verifiable recommendation;
- the word 'should' implies an optional, but desirable, recommendation;
- the word 'may' implies an optional recommendation; and
- the words 'is', 'are', and 'will' imply statements of fact.

1.5.2 DEFINITIONS

Authentication: the assurance that information transmitted from a claimed source (such as the source's identity) in fact came only from that source.

Confidentiality: the disclosure of information only to those who are authorized and have been approved to receive it.

Confirm (primitive): a primitive issued by a service-provider to complete, at a particular service-access-point, some procedure previously invoked by a request at that service-access-point.

Decipherment: the mechanism by which coded text is transposed into plain text based on a predetermined key.

Encipherment: the mechanism by which plain text is transposed into a code based on a predetermined key.

End System: an addressable network entity within the SCPS Network.

Gateway: a network-addressable system that terminates a protocol at a given layer and invokes similar services at the same layer of an adjacent network.

Indication (primitive): a primitive issued by a service provider either to invoke some procedure or to indicate that a procedure has been invoked by the service user at a peer service-access-point.

Integrity: the assurance that information received from a source is in fact the information transmitted, without unauthorized modification.

Internet Protocol Number: the transport protocol identifier used by Internet Protocols. Values may range from 0 through 255, and valid values are defined in reference [B14].

N-Address: an address in the SCPS Network. The attributes of an N-Address are the Address Type and the Address Family.

N-Destination_Address: an N-Address that identifies the destination end system of a datagram in the SCPS Network. The N-Destination_Address is a parameter of all of the SCPS Network service primitives. It is an N-Address that identifies the destination end system of a datagram in the SCPS Network. The N-Destination_Address parameter must be of the Extended End System address type, and may be of either the IP or the SCPS address family.

Network-Service Data Unit (N-SDU): a variable-length, octet-aligned data unit of arbitrary format.. The Network Service Data Unit (N-SDU) is a parameter of the Unit Data service primitives.

N-Source_Address: an N-Address that identifies the end system originating a datagram in the SCPS Network. The N-Source_Address is a parameter to many of the primitives of the SCPS network service. The N-Source_Address must be of the Extended End System address type, and may be of either the IP or the SCPS address family. The N-Source_Address may not be a multicast or a broadcast address.

Primitive: (also known as service-primitive) an abstract, implementation-independent interaction between a service-user and the service-provider.

Request (primitive): a primitive issued by a service-user to invoke some procedure.

Response (primitive): a primitive issued by a service-user to complete, at a particular service-access-point, some procedure previously invoked by an indication at that service-access-point.

Security Association (SA): security management information used by the security mechanisms.

Security Association Identifier (SAID): the index into the SA database formed by the source and destination addresses of the communicating systems.

Service-Access-Point: a point at which the services of a layer are made available to the layer above it.

Service-Primitive: see Primitive.

Security Service Data Unit (S-SDU): a variable-length, octet-aligned data unit of arbitrary format. The S-SDU is a parameter of the Unit Data service primitives.

2 OVERVIEW

This document provides the framework for the SCPS-SP, which is a layer-3 subnetwork independent convergence security protocol.

The SCPS-SP provides the following connectionless security services on an end-to-end basis (where the service endpoints are defined by the implementer):

- confidentiality;
- integrity;
- authentication; or
- a combination of all of the above.

The basic mode of operation of SCPS-SP is encapsulation of a Transport Protocol Data Unit (T-PDU) into a Security Protocol Data Unit (S-PDU). The T-PDUs may be enciphered to provide confidentiality, may have an Integrity Check Value (ICV) calculated and appended to provide integrity (non-forgeability) of the T-PDU, or may both be enciphered and have an ICV applied. Explicit authentication in SCPS-SP requires the use of either the integrity and/or the confidentiality services. Implicit authentication is provided as a by-product of key management. In the case where both integrity and confidentiality are required, integrity is applied first, and then confidentiality.

The concepts for this specification are drawn from a number of sources (see annex B) such as *Secure Data Network Systems (SDNS) Security Protocol 3 (SP3)* (reference [B2]), *ISO Network Layer Security Protocol (NLSP)* (reference [B7]), *Internet Protocol Version 6 Encapsulating Security Payload* (reference [B3]), and *Integrated Network Layer Security Protocol* (reference [B5]). SCPS-SP's major point of departure from these other security protocols is the insistence on near-optimal bit efficiency, which was not a design requirement for the other protocols. The SCPS-SP has been refined to ensure minimal transmitted bit overhead.

The SCPS-SP assumes that it resides on top of a connectionless network service, known throughout this specification as the Underlying Network (UN). An example of such a protocol is the SCPS Network Protocol (SCPS-NP) (reference[B12]).

Processing within SCPS-SP is *security-critical*. Therefore, the Security Protocol is the only portion of the SCPS suite that, from a *security* perspective, must be *trusted* to perform its security functions correctly. This is not to imply that the other protocol layers do not have to operate correctly. However, only SCPS-SP has the responsibility to perform security-critical processing. The layers above SCPS-SP may handle classified or proprietary data, but it is SCPS-SP's job to ensure that the data is afforded the requisite security protections before forwarding the data to the lower layers and onto the network. Likewise, a protocol layer below SCPS-SP may handle sensitive data, but only SCPS-SP has the responsibility for ensuring that the required security services are applied.

The SCPS-SP employs both a *clear* and a *protected* header. The clear header, which must remain un-enciphered, provides a small amount of processing information to the security protocol. The protected header contains additional information which may be enciphered (along with the user data), depending upon the system security policy being enforced by the Security Protocol as well as the user's security services request. The security protection that the SCPS-SP attempts to provide is derived from a combination of the security services requested by the SCPS-SP user and the protection requirements imposed by the security domain administrator through the enforcement of the local security policy.

Although the degree of protection afforded by the security mechanisms depends on the use of specific cryptographic or digital signature secure hash techniques, correct operation of this protocol is *not* dependent on the choice of any particular encipherment, decipherment, or integrity algorithm. The choice of algorithms is left as a local security matter.

In order for SCPS-SP to provide end-to-end protection services and still operate across *security-unaware* networks, the addressing information in the UN layer must remain un-enciphered to allow PDU routing. Because the address information is not enciphered, SCPS-SP does not provide protection against traffic analysis, nor does it provide protection against jamming or low-probability-of-intercept (LPI). Traffic analysis protection must be provided at the link layer; jamming and LPI protection must be provided at the physical layer.[1] SCPS-SP also does not provide protection against replay attacks. It is assumed that either the encryption algorithm or a sequence number provided by an upper-layer transport protocol, such as SCPS-TP (reference [B13]), would protect against replay attacks.

Neither the choice nor the implementation of a specific security policy are within the scope of this specification. The choice of a specific security policy, and therefore the protection that will be achieved by the SCPS-SP user, is a local matter for determination by the security domain administration.

[1] Confidentiality, integrity, and authentication may also be provided at the physical layer. However, for store and forward systems, the security services at this layer can only be implemented on a hop-by-hop basis and not on an end-to-end basis. This means that when using link layer security services, the data must be deciphered, exposing the data, and then re-enciphered at each hop. This is not the case when using end-to-end security services such as those provided by SCPS-SP.

3 PROTOCOL SPECIFICATION

3.1 SCPS-SP TYPES OF SECURITY SERVICES

3.1.1 GENERAL

SCPS-SP shall support the following types of Security Services:

– integrity services;

– confidentiality services;

– authentication services.

3.1.2 INTEGRITY SERVICES

When *integrity services* are requested by a SCPS-SP user (e.g., an upper-layer protocol) or are required as a default action to enforce an administrative security policy,

a) SCPS-SP shall calculate an ICV over the SCPS-SP clear and protected headers, the user data, which includes any upper-layer protocol headers, and potentially a secret data stream (e.g., a 'secret key');

b) the size of the ICV shall be established in the SA database (*integ_alg_ICV_length*);

NOTE – The SCPS-SP operates with the assumption that there exists a Security Association (SA) database that contains pertinent security information, for use between the communicating entities, such as the encipher key, the key expiration, the key length, the Initialization Vector (IV) length, the encipherment algorithm, the integrity algorithm, and the ICV length. Example Security Association parameters are illustrated in section 5 (Security Association Attributes) of this Recommendation.

c) the specific manner in which the ICV is calculated shall be determined by the integrity algorithm as identified by *integ_alg_id* in the SA database.

3.1.3 CONFIDENTIALITY SERVICES

When *confidentiality services* are requested by a SCPS-SP user or are required as a default action to enforce an administrative security policy, the SCPS-SP shall use the encipherment key (*cipher_key*) in conjunction with the encipherment algorithm (*conf_alg_id*) and algorithm mode (*conf_alg_mode_id*) specified in the SA database to encipher the SCPS-SP protected header and the user data.

3.1.4 AUTHENTICATION SERVICES

When *authentication services* are requested by a SCPS-SP user,

a) the source and destination network addresses shall be encapsulated into the SCPS-SP protected header, and then either integrity and/or confidentiality services shall be applied, as above;

b) authentication *must* be requested with either integrity or confidentiality, or both; it cannot be provided without one or both of the other services.

3.1.5 SECURITY SERVICES PROCESSING

When both integrity and confidentiality services are requested, the SCPS-SP shall first perform the integrity service followed by the confidentiality service.

NOTE – As a result, the protected header, the user data, and the ICV generated by the integrity service are enciphered.

3.2 SCPS-SP PROTOCOL DATA UNIT

The SCPS-SP Protocol Data Unit (PDU) shall consist of the following parts in the following sequence:

	Length in bits
– Clear Header (mandatory)	variable
– Protected Header (mandatory)	variable
– User Data (optional)	variable
– Integrity Check Value (optional)	variable

NOTE – The SCPS-SP PDU is illustrated in figure 3-1.

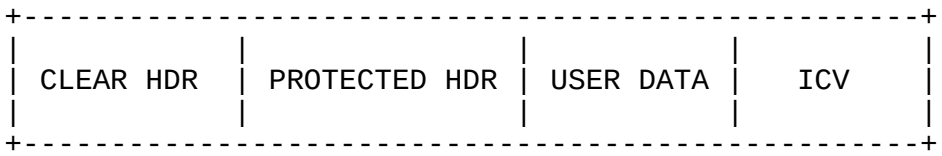


Figure 3-1: SCPS-SP Protocol Data Unit

3.3 SCPS-SP CLEAR HEADER

3.3.1 CLEAR HEADER FORMAT

The SCPS-SP Clear Header shall consist of the following fields in the following sequence:

	Length in bits
– Internet Protocol Number (mandatory)	8
– initialization vector (optional)	variable

NOTE – The SCPS-SP Clear Header is illustrated in figure 3-2.

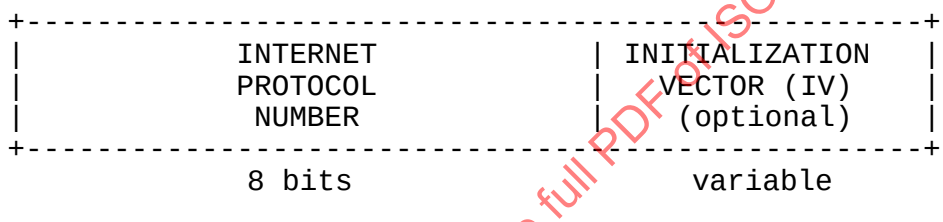


Figure 3-2: SCPS-SP Clear Header

3.3.2 CLEAR HEADER FIELDS

3.3.2.1 Internet Protocol Number

3.3.2.1.1 The Internet Protocol Number field shall be eight bits in length and shall occupy bits 0 through 7 of the SCPS-SP Clear Header.

3.3.2.1.2 The Internet Protocol Number field shall contain the Internet Assigned Numbers Authority (IANA) specified number of the next upper-layer to receive and process the PDU after SCPS-SP processing.

NOTE – Internet Protocol Number assignment is discussed in reference [B14].

3.3.2.2 Initialization Vector Option

3.3.2.2.1 The Initialization Vector Option field, if included, shall begin in bit 8 of the SCPS-SP Clear Header and shall end on an octet boundary.

NOTE – Some confidentiality algorithms require the use of an initialization vector (IV) for synchronization, while others do not. The key requirement for the generation of an IV is that it be pseudo-random and not repeat itself during the period an encipherment key is being used.

3.3.2.2.2 The contents of the Initialization Vector Option field shall be determined as follows:

a) If an Initialization Vector (IV) is explicitly transmitted:

1) the Security Association (SA) database entry *IV_explicit* shall be set to 'TRUE' during the SA establishment;

2) the IV, of *IV_length*, shall be constructed in accordance with the confidentiality algorithm's requirements and shall be placed into the clear header's optional IV field;

3) if an IV is not required, *IV_length* shall be set to zero (0).

b) If it is to be *reconstructed* by the receiver without being explicitly transmitted:

1) the SA database entry *IV_explicit* shall be set to 'FALSE' during the SA establishment;

2) the IV may be constructed using the (coarse and fine resolution) clocks available on the communicating end systems;

3) the IV shall be constructed of length *IV_length* through the combination of the source address, the destination address, and the clock outputs used to generate a UN timestamp;

4) the receiver shall reconstruct the IV as discussed in 4.5.2.

NOTE – In situations where transmitted bit overhead is a major concern, the explicit IV mode option should not be used. Additionally, in order to reduce processing overhead further, an encipherment algorithm should be chosen that affords the requisite protection, but does not require the use of an IV. Algorithm choices are not a part of this Recommendation and are left as a local security matter.

3.3.3 CLEAR HEADER PROCESSING

3.3.3.1 The Clear Header shall be used by the receiving SCPS-SP for routing and delivery of datagrams to an upper-layer protocol after security processing has been performed.

3.3.3.2 The Clear Header shall not be enciphered.

3.4 SCPS-SP PROTECTED HEADER

3.4.1 PROTECTED HEADER FORMAT

The SCPS-SP Protected Header shall consist of the following fields in the following sequence:

	Length in bits
– Protected Header Option Flags (mandatory)	8
– Security Classification Label (optional)	variable
– Encapsulated Address (optional)	variable
– Cipher Pad (optional)	variable

NOTE – The SCPS-SP Protected Header is illustrated in figure 3-3.

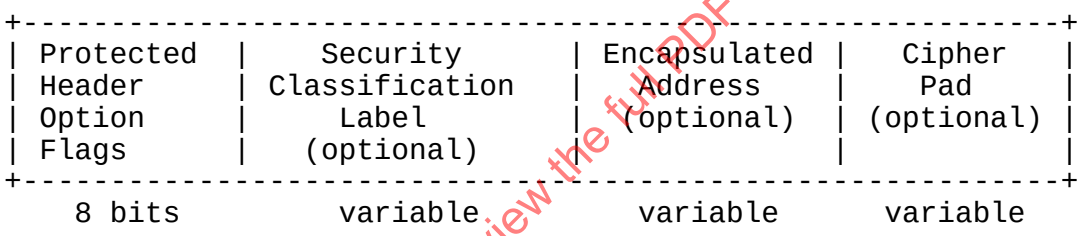


Figure 3-3: SCPS-SP Protected Header

3.4.2 PROTECTED HEADER FIELDS

3.4.2.1 Protected Header Option Flags Field

3.4.2.1.1 The Protected Header Option Flags field shall be eight bits in length and shall occupy bits 0 through 7 of the SCPS-SP Protected Header.

3.4.2.1.2 The Protected Header Option Flags field shall contain a value selected from the following list (no other flag-field bit combinations are currently defined):

Option	Binary Value
– ICV_present:	'00000001'
– cipher_padding_present:	'00000010'
– encapsulated_address_present:	'00000100'
– security_classification_label_present:	'00001000'

3.4.2.2 Security Classification Label Field

3.4.2.2.1 The Security Classification Label field shall, if used, begin in bit 8 of the SCPS-SP Protected Header and end on an octet boundary.

NOTE – The label may consist of any label format (e.g., IP Security Option, reference [B8]; Common Security Label, reference [B9]; Standard Security Label, reference [B11]). The label contents are dictated by the specific standard employed.

3.4.2.2.2 The Security Classification Label field shall consist of a label-length subfield followed by a label-contents subfield.

3.4.2.2.3 The label standard used shall be specified in the SA database (*label_standard_id*).

3.4.2.2.4 The length of this field will be determined by the specific label standard employed.

3.4.2.3 Encapsulated Address Field

3.4.2.3.1 The Encapsulated Address field shall, if included, begin on the next octet boundary following the locations of the Security Classification Label field, or the Protected Header Option Flags field if no Security Classification Label field is included, and end on an octet boundary.

NOTE – The Encapsulated Address option is used when *explicit* address authentication is required or when SCPS-SP is run at an Intermediate System (IS) (e.g., a security front-end device or security gateway). When addressing information is *sealed* into the protected header by the integrity or confidentiality services, the destination End System is assured that the PDU was transmitted from the claimed source. For a further discussion of the use of SCPS-SP at intermediate systems see reference [B15].

3.4.2.3.2 The Encapsulated Address field shall contain the following subfields in the following sequence:

	Length in bits
– destination addresses	variable
– source address	variable

NOTE – The Protected Header Encapsulated Address field is illustrated in figure 3-4.

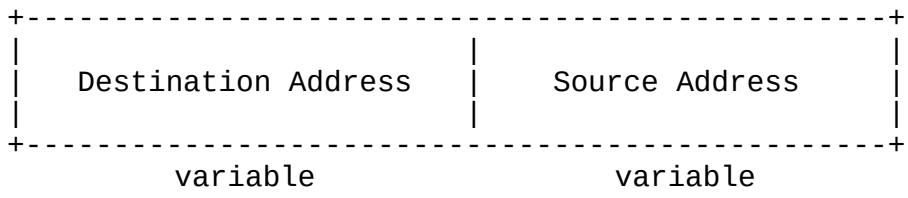


Figure 3-4: Protected Header Encapsulated Address Field

3.4.2.4 Cipher Pad Field

3.4.2.4.1 The Cipher Pad field shall, if included, begin on the next octet boundary following the location for the Encapsulated Address field, or the Security Classification Label field if the Encapsulated Address field is not included, or the Protected Header Option Flags field if neither the Encapsulated Address field nor the Security Classification Label field are included, and end on an octet boundary.

NOTE – The Cipher Pad field may be used when a particular encipherment or integrity algorithm requires data blocks to exist on even octet or word boundaries.

3.4.2.4.2 The Cipher Pad field shall contain pad octets each having a numeric value equal to the number of pad octets.

EXAMPLE – If seven pad octets are needed, the Cipher Pad Field will be filled with seven octets each having the decimal value seven.

3.4.3 PROTECTED HEADER PROCESSING

3.4.3.1 The protected header shall be enciphered along with the user data when the SCPS-SP user requests the confidentiality security service or when confidentiality is mandated to enforce the administrative security policy.

3.4.3.2 If the SCPS-SP user selects the integrity security service, SCPS-SP shall append an ICV to the PDU (see 3.5).

3.4.3.3 If the SCPS-SP user selects the authentication security service, a copy of the source and destination addressing information shall be placed into the protected header. This option shall only be used with the integrity service, confidentiality service, or both.

3.5 INTEGRITY CHECK VALUE FIELD

3.5.1 The Integrity Check Value field shall, if included, begin on an octet boundary following the location for the User Data field, or the Protected Header if no User Data field is included, and end on an octet boundary.

3.5.2 The Integrity Check Value field shall contain the results of the integrity algorithm, as defined by *integ_alg_id* in the SA database, run over the clear header, the protected header, the user data, and a secret key (if required).

3.5.3 The algorithm-dependent length of the ICV shall be stored in the SA database.

NOTE – The specific manner in which the integrity service operates is algorithm dependent.

(Blank page)

4 PROTOCOL FUNCTIONS

4.1 TRANSMISSION FUNCTIONS

4.1.1 In response to an S-UNITDATA.request primitive (request from an upper-layer protocol to the SCPS-SP to transmit a PDU), the SCPS-SP shall attempt to identify an SA database entry based on the source and destination address pair contained in the request.

NOTES

1 Details on the SCPS-SP service primitives are contained in annex D.

2 The SA attributes may be manually pre-placed into a static SA database in the SP-aware communicating end-points or negotiated through the use of a Security Association Protocol (SA-P) or a Key Management Protocol (KM-P). The SA-P (or KM-P) is a separate protocol, typically implemented at the application layer, used to provide security attribute management. The SA-P is mentioned within this document so that the relationship between it and SCPS-SP is better understood. The specification of an SA-P or KM-P is beyond the scope of this Recommendation.

4.1.2 If an SA database entry is not found, the SCPS-SP shall either refuse the request or invoke an SA-P or KM-P to establish an SA database entry for the communicating systems.

4.1.3 If an SA database entry is found, the SCPS-SP shall use the information contained in it to create an S-PDU made up of a clear header, a protected header, and the user data.

4.1.4 If authentication is requested, a copy of the source and destination addresses shall be placed in the protected header. Authentication shall only be used in conjunction with the integrity service, the confidentiality service, or both.

4.1.5 If a security label is requested (*label_req*),

a) the SCPS-SP shall ensure that the label's classification is within the range specified for the key (*key_class_range*) in the SA database;

b) the SCPS-SP shall construct the label using the label standard (*label_standard_id*) specified in the SA database (e.g., IPSO, CSL, SSL—references [B8], [B9], [B10], [B11]);

c) the label shall be placed in the protected header.

4.1.6 If integrity is requested,

a) the integrity algorithm (*integ_alg_id*), the ICV length (*integ_alg_ICV_length*), and the integrity key (*integ_key*), if required, shall be retrieved from the SA database;

b) the integrity algorithm shall be used to calculate an ICV over the clear header, the protected header, the user data, and, if required by the algorithm, the integrity key.

4.1.7 If confidentiality is requested, the encipherment algorithm (*conf_alg_id*) type and mode (*conf_alg_mode_id*), the encipherment key (*cipher_key*), the key expiration (*cipher_key_expire*), and its associated IV length (*IV_length*), if required, shall be retrieved from the SA database and used to encrypt the protected header and the user data.

4.1.8 If both confidentiality and integrity are requested, integrity shall be performed first followed by encipherment over the protected header, the user data, and the ICV.

4.2 RECEPTION FUNCTIONS

4.2.1 RECEPTION PROCEDURES

4.2.1.1 In response to an N-UNITDATA.indication primitive (indication from a lower-layer protocol to send an S-PDU to the SCPS-SP), the security protocol shall attempt to identify an SA database entry based on the source and destination address pair found in the Indication.

4.2.1.2 If no SA database entry is found,

a) the PDU shall be discarded;

b) a security audit log entry **may** be made;

c) an error indication shall **not** be returned to the source.

4.2.1.3 If an entry is found,

a) the SCPS-SP shall check the *confidentiality_on* attribute to determine if PDUs from the source address are enciphered;

b) if the *confidentiality_on* attribute is 'TRUE', the SCPS-SP shall decipher the S-PDU as described in 4.5.2;

c) the use of confidentiality shall be negotiated during the SA establishment.

4.2.1.4 After the PDU is deciphered, or if the PDU was not enciphered at its source, the SCPS-SP shall check the protected header flags to determine what additional security processing is necessary:

a) If the *ICV_present* flag is set, SCPS-SP shall calculate an ICV as described in 4.3.3 and compare it with the transmitted ICV:

1) if the ICVs match, the receiver is assured that the PDU has not been modified while in transit;

2) if the ICVs do not match exactly, indicating the PDU may have been modified without authorization,

   – the PDU shall be discarded,

   – a security audit log entry **may** be made,

   – an error indication shall **not** be returned to the source.

b) If the *encapsulated_address_present* flag is set, and if either the PDU was enciphered or an ICV was present, SCPS-SP shall compare the addresses embedded in the optional, encapsulated address field to the addresses found in the N-UNITDATA.indication:

   1) if the addresses match, the receiver has explicit assurance of the authenticity of the PDU;

   2) if the addresses do not match,

      – the PDU shall be discarded,

      – a security audit log entry **may** be made,

      – an error indication shall **not** be returned to the source;

   3) if the PDU had neither integrity nor confidentiality services applied,

      – the PDU shall be discarded,

      – a security audit log entry **may** be made,

      – an error indication shall **not** be returned to the source.

c) If the *security_classification_label_present* flag is set,

   1) SCPS-SP shall examine the label found in the optional security classification label field and compare it with the allowed classification range found in the SA database entry, *key_class_range*; [1]

   2) if the classification found in the label is within the allowable range, the receiver shall explicitly classify the PDU in accordance with the label;

   3) if the classification level of the label is out of range of the key,

      – the PDU shall be discarded,

      – a security audit entry **should** be made,

      – an error indication shall **not** be returned to the source.

[1] Classifications may be *military flavored* (e.g., secret, confidential) or may be *corporately flavored* (e.g., proprietary, company confidential, sensitive).

d) If the *cipher_padding_present* flag is set, the padding added for encipherment shall be removed from the PDU and discarded.

NOTE – Both the encipherment and decipherment algorithms may be the same. Both the encipherment and decipherment keys may be the same. These are local security policy and algorithm issues. If different encipherment and decipherment algorithms and/or keys are used, separate Security Association attributes are required for confidentiality algorithms and/or encipherment and decipherment keys.

4.2.2 ERROR PROCEDURES

4.2.2.1 Unless otherwise specified, whenever a condition check fails upon the receipt of an S-PDU, the SCPS security protocol shall discard the data currently being processed.

4.2.2.2 Optionally, SCPS-SP may log an audit record.

NOTE – Whether audit records are logged and the types of audit records logged are local security matters.

4.2.2.3 For security reasons, an error indication shall not be returned to the sender.

4.3 INTEGRITY SERVICE PROCESSING

4.3.1 GENERAL

4.3.1.1 Upon the request of an upper-layer protocol (S-UNITDATA.request) for integrity services, the SCPS-SP shall apply an integrity algorithm to generate an Integrity Check Value (ICV).

NOTE – The SCPS-SP protocol does not specify an integrity algorithm. Algorithm choices are a local matter for local security administration. The integrity algorithm identification (*integ_alg_id*) is assumed to be either manually pre-placed in the SA database or negotiated via an SA-P or KM-P.

4.3.1.2 The SA database entry shall contain information to be used between the communicating source and destination systems:

– the integrity algorithm identifier;

– an integrity key;

– the length of the ICV.

4.3.2 INTEGRITY SERVICE TRANSMISSION PROCESSING

4.3.2.1 The SCPS-SP shall generate an ICV of the length specified in the SA database (*integ_alg_ICV_length*) using the SA-specified integrity algorithm (*integ_alg_id*).

4.3.2.2 The ICV shall be appended to the end of the user data as specified in 3.5.

NOTE – The specific integrity algorithm governs the manner in which the ICV is generated.

4.3.3 INTEGRITY SERVICE RECEPTION PROCESSING

Upon the receipt of an N-UNITDATA.indication, the following shall be performed:

a) The SCPS-SP shall check the SA database to determine if confidentiality is being used between the communicating systems.

b) If confidentiality is being used, the PDU shall first be deciphered.

c) The SCPS-SP protected header flags shall be examined to determine if the *ICV_present* bit has been set:

   1) if set, indicating integrity had been applied at the PDU's source, the SCPS-SP shall generate an ICV, of the length specified (*integ_alg_ICV_length*) in the SA database, using the SA-specified integrity algorithm (*integ_alg_id*);

   2) the generated ICV shall be compared to the ICV transmitted in the S-PDU to ensure that the PDU has not been modified while in transit;

   3) if the transmitted and calculated ICVs match, the receiver is assured that the PDU has not been modified while in transit;

   4) if the ICVs do not match, indicating the PDU has undergone unauthorized modification during transmission,

      – the PDU shall be discarded,

      – depending on local security policy, an audit entry **may** be logged,

      – an error indication shall **not** be returned to the source.

4.4 AUTHENTICATION SERVICE PROCESSING

4.4.1 GENERAL

NOTE – Authentication provides a receiver with the ability to verify the true identity of the originator of the PDU. It also prevents spoofing by providing the ability to detect when someone is attempting to masquerade as someone else.

4.4.1.1 In SCPS-SP, *explicit* source authentication shall only be performed in conjunction with the integrity and/or confidentiality services.

4.4.1.2 Used in this manner, SCPS-SP shall provide authentication of the source of the PDU.

4.4.1.3 If the PDU contains a command, the receiver is assured that it came from an authentic, verified location.

NOTE – SCPS-SP provides an *implicit* authentication service by virtue of key management. If an end-system is attempting to masquerade as another system, that system will be able to generate a SCPS-SP PDU. However, the receiving system will not be able to authenticate or decipher the PDU because the incorrect key was used at the source (assuming strong key management is employed to protect keys from disclosure). From a security perspective, users should always assume that the encipherment algorithm is known and that the critical information that must be safeguarded is the encipher/decipher key.

4.4.2 AUTHENTICATION TRANSMISSION PROCESSING

4.4.2.1 If authentication and integrity are requested, processing shall be performed as stated in 4.3 (Integrity) with the source and destination addresses embedded into an optional address field in the SP-protected header.

4.4.2.2 If authentication and confidentiality are requested, the source and destination addresses shall be embedded into an optional address field in the SP-protected header and encipherment shall be performed as stated in 4.5 (Encipherment).

4.4.2.3 If authentication, integrity, and confidentiality are requested, address embedment shall take place, followed by integrity processing, followed by encipherment processing.

4.4.3 AUTHENTICATION RECEPTION PROCESSING

4.4.3.1 When a PDU is received by SCPS-SP, if SCPS-SP is running in an End System, the protected header shall be checked to see if the *encapsulated_address_present* flag is set (after deciphering, if necessary).

4.4.3.2 If the flag is set, the addresses embedded in the optional, encapsulated address field shall be compared to the addresses found in the N-UNITDATA.indication (e.g., the source and destination addresses from the underlying network-layer protocol):

a) if the addresses match, the receiver has explicit assurance of the authenticity of the PDU;

b) if the addresses do not match,

   1) the PDU shall be discarded;

   2) a security audit log entry **may** be made;

   3) an error indication shall **not** be returned to the source.

NOTES

1 If SCPS-SP is not running in an End System, but instead is running in an Intermediate System, the embedded addresses are used both as a means of authentication and onward routing into a secure enclave. See reference [B15] for an in-depth discussion of End System-Intermediate System interactions.

2 SCPS-SP assumes the use of Internet Protocol style addresses. It is also assumed that protocols above SCPS-SP are likewise using IP addresses. It is further assumed that any UN network protocol layers will provide any address mapping required between the IP addresses and the actual addresses used (if any) in the lower layers.

4.5 CONFIDENTIALITY SERVICE PROCESSING

4.5.1 ENCIPHERMENT TRANSMISSION PROCESSING

4.5.1.1 The SCPS-SP shall encipher PDUs when confidentiality services are requested by an upper-layer protocol.

NOTE – The SCPS-SP protocol does not specify an encipherment algorithm. Algorithm choices are a matter left for local security policy and are assumed to be manually pre-placed in a static SA database or negotiated via an SA-P or KM-P.

4.5.1.2 The encipherment function requires access to an SA database entry, indexed by a source and destination address pair, containing the following information to be used between the communicating source and destination systems:

– whether confidentiality shall be used between the communicating systems;

– the encipherment algorithm and mode;

– the key;

– the key expiration;

– the length of the initialization vector (IV) which provides encipherment synchronization.

NOTE – The need for an IV and its length are algorithm dependent.

4.5.1.3 If the algorithm in use requires an IV, the SA database entry *IV_length* shall be non-zero and shall indicate the length of the IV to be created.

NOTE – The major requirement for the generation of an IV is that it be pseudo-random and not repeat itself during the period an encipherment key is being used. SCPS-SP provides two means by which an IV may be communicated. It may be explicitly transmitted in an optional SCPS-SP clear header field or it may be *reconstructed* by the receiver without having been transmitted. The manner in which the IV is handled is determined through SA establishment.

4.5.1.4 If an IV is to be explicitly transmitted,

a) the SA database entry *IV_explicit* shall be set to 'TRUE' during the SA establishment;

b) the IV may be generated in accordance with the SA-specified confidentiality algorithm and mode;

c) an IV of length *IV_length* shall be transmitted in the SCPS-SP clear header IV option field.

4.5.1.5 If the IV is not to be explicitly transmitted,

a) the SA database entry *IV_explicit* shall be set to 'FALSE' during the SA establishment;

b) an IV may be constructed using the coarse and fine resolution clocks, if available, on the communicating end systems;

c) an IV, of length *IV_length*, may be constructed through the concatenation of the source address, the destination address, and the clock outputs used to generate a UN timestamp (such as found in SCPS-NP—see reference [B12]).

NOTE – The specific details of the IV construction are left as a local matter as they may vary from environment to environment depending on the algorithms used.

4.5.1.6 The SCPS-SP shall ensure that the confidentiality key in the SA database (*cipher_key*) has not expired:

a) it shall compare the current system time to the key expiration attribute (*cipher_key_expire*) in the SA database;

b) if the key has expired, a new key shall be established through the use of an SA-P/KM-P or via manual means;

c) if the key has not expired, the SCPS-SP shall employ the encipherment algorithm and mode, key, and the IV (if required) to encipher the protected header, the user data, and, if integrity has also been requested, the ICV.

4.5.2 DECIPHERMENT RECEPTION PROCESSING

4.5.2.1 In response to an N-UNITDATA.indication primitive the SCPS-SP shall decipher S-PDUs.

4.5.2.2 The SCPS-SP shall examine the SA database *confidentiality_on* attribute to determine whether encipherment has been used between the communicating systems:

– if *confidentiality_on* is 'TRUE', confidentiality services were applied at the PDU's source;

– if *confidentiality_on* is 'FALSE', confidentiality services were not applied at the PDU's source.

NOTE – The decipherment function requires access to an SA database entry indexed by a source and destination address pair.

4.5.2.3 The database entry shall contain at least the following information to be used between the communicating source and destination systems:

– the decipherment algorithm and mode;

– the key;

– the key expiration;

– the length of the IV.

NOTE – The need for an IV and its length is algorithm dependent.

4.5.2.4 If confidentiality services were applied to the PDU at its source, the receiving SCPS-SP shall examine the *IV_length* SA database attribute:

a) if *IV_length* is zero (0), then no IV processing is required;

b) if *IV_length* is non-zero, indicating that the use of an IV is required for the decipherment of the PDU, the SCPS-SP shall then examine the *IV_explicit* SA database attribute:

1) if *IV_explicit* is 'TRUE', indicating an IV of length *IV_length* has been transmitted in the optional IV field in the SCPS-SP clear header, the SCPS-SP shall retrieve the IV from the clear header and use it in the decipherment process described below;

2) if *IV_explicit* is 'FALSE', the SCPS-SP may combine the UN-layer timestamp (received in the N-UNITDATA.indication), and the source and destination addresses to reconstruct the IV that was used in the encipherment process.

NOTE – The UN timestamp (as received from SCPS-NP—see reference [B12]) contains only the low-order eight bits of the sender's coarse time-of-day clock, but the receiver may concatenate the received low-order bits with the high-order bits of its own time-of-day clock, taking into account the packet latency, to recreate the IV used in encipherment. This scheme may work if there is low packet latency in the network and there exists some degree of synchronized clocks. However, the specific details of such a scheme are environment and algorithm dependent and are left as a local implementation matter.

4.5.2.5 The SCPS-SP shall ensure that the confidentiality key in the SA database (*cipher_key*) has not expired:

a) it shall compare the current system time to the key expiration attribute (*cipher_key_expire*) in the SA database;

b) if the key has expired, a new key shall be established through the use of an SA-P/KM-P or via manual means.

4.5.2.6 If the confidentiality key has expired,

a) the S-PDUs may either be discarded or deciphered using the expired key, depending on the requirements of the local security policy;

b) if the expired key is allowed to be used, then the SCPS-SP shall employ the decipherment algorithm and mode, the expired key, and the IV (if required) to decipher the protected header contents, the S-PDU payload, and, if present, the ICV.

4.5.2.7 If the confidentiality key has not expired, the SCPS-SP shall employ the decipherment algorithm and mode, the key, and the IV (if required) to decipher the protected header contents, the S-PDU payload, and if present, the ICV.

4.6 END-SYSTEM TO INTERMEDIATE SYSTEM INTERACTIONS

4.6.1 When a PDU is received by a SCPS-SP-*aware* Intermediate System, the Intermediate System shall determine if security services were applied at the source by examining the UN layer's *Internet Protocol Number* field to identify the next protocol needed to process the PDU.

4.6.2 If SCPS-SP is identified in the SA as the required protocol, the PDU shall be handed to the Intermediate System's implementation of the Security Protocol.

4.6.3 The SCPS-SP shall perform security processing according to the information found in the SA database entry corresponding to the source of the PDU and the Intermediate System.

4.6.4 The SCPS-SP shall then examine the flags field in the SCPS-SP protected header and perform security processing as described in 4.2.

4.6.5 If the *encapsulated_address_present* flag is set, the SCPS-SP shall retrieve the addresses found in the Encapsulated Address field.

4.6.6 The Intermediate System implementation of SCPS-SP shall use the encapsulated addresses not only for explicit authentication checking, but also for onward routing of the PDU into the protected enclave after stripping away all vestiges of the security protocol.

4.6.7 The security protocol, using the addresses in the Encapsulated Address field, shall forward the PDU back down to the UN layer for routing onward to the non-SCPS-SP End-Systems within the enclave.

(Blank page)

5 SECURITY ASSOCIATION ATTRIBUTES

5.1 The source and destination addresses of the PDU shall act as the index into the local SA database.

5.2 In order to support the SCPS-SP security services, the following SA attributes are required (listed in no particular order):

a) encipher/decipher key: *cipher_key*;

b) encipher/decipher key expiration: *cipher_key_expire*;

c) confidentiality being used: *confidentiality_on* (Boolean);

d) key classification range: *key_class_range*;

e) explicit security label required, and if so, label standard:

- *label_req* (Boolean),
- *label_standard_id*;

f) encapsulated addressing required: *esp_addr* (Boolean);

g) confidentiality algorithm identifier: *conf_alg_id*;

h) confidentiality algorithm mode of operation: *conf_alg_mode_id*;

i) confidentiality IV length: *IV_length*;

j) IV explicitly transmitted: *IV_explicit* (Boolean);

k) integrity algorithm identifier: *integ_alg_id*;

l) integrity key: *integ_key*;

m) integrity key expiration: *integ_key_expire*;

n) integrity algorithm ICV length: *integ_alg_ICV_length*;

o) security protocol version number: *sp_version_number*.

5.3 All SA database attributes shall be at least 8 bits in size; however, the key attributes (e.g., *cipher_key*, *integ_key*) may be significantly larger depending on the algorithms used (e.g., 56 bits for DES, 128 bits for RSA).

5.4 Specific identification bits for algorithm and label identifiers shall be defined in the SA database.

(Blank page)

ANNEX A

ACRONYMS AND ABBREVIATIONS

(This annex **is not** part of the Recommendation.)

Term	Meaning
AOS	Advanced Orbiting Systems
APID	Application Process Identifier
DES	Data Encryption Standard
ES	End System
ESP	Encapsulating Security Payload (see reference [B3])
ICV	Integrity Check Value
IS	Intermediate System
IV	Initialization Vector
KM-P	key management protocol
LPI	low-probability-of-intercept
NP	Network Protocol
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
QOS	Quality of Service
RSA	Rivest-Shamir-Adleman Public Key Encryption
SA	Security Association
SA-P	SA protocol
SAID	Security Association Identifier
SCPS	Space Communications Protocol Specification
SCPS-NP	Space Communications Protocol Specification Network Protocol

SCPS-SP	Space Communications Protocol Specification Security Protocol
SCPS-TP	Space Communications Protocol Specification Transport Protocol
SDNS	Secure Data Network Systems (see reference [B2])
SP	Security Protocol
SP-3	Security Protocol at Layer 3 (see reference [B2])
S-PDU	Security Protocol Data Unit
SSL	Standard Security Label (see reference [B11])
T-PDU	Transport Protocol Data Unit
UN	Underlying Network

ANNEX B

INFORMATIVE REFERENCES

(This annex **is not** part of the Recommendation.)

[B1] *Procedures Manual for the Consultative Committee for Space Data Systems*. CCSDS A00.0-Y-7. Yellow Book. Issue 7. Washington, DC: CCSDS, November 1996.

[B2] *Secure Data Network Systems (SDNS) Security Protocol 3 (SP3).* SDN.301. Revision 1.5, 1989. Reprinted in Secure Data Network System (SDNS) Network, Transport, and Message Security Protocols. NIST-IR-90-4250. Gaithersburg, Maryland: NIST, 1990.

[B3] S. Kent and R. Atkinson. *IP Encapsulating Security Payload (ESP).* RFC 2406, November 1998.†

[B4] S. Kent and R. Atkinson. *IP Authentication Header*. RFC 2402, November 1998.

[B5] *Integrated Network Layer Security Protocol.* Internet Draft (deleted).

[B6] *Integrated Network Layer Security Protocol for TUBA.* Internet Draft (deleted).

[B7] *Information Technology—Open Systems Interconnection—Network Layer Security Protocol*. ISO/IEC 11577:1995. Geneva: ISO, 1995.

[B8] M. St. Johns. *Draft Revised IP Security Option*. RFC 1038, January 1988.

[B9] *Common Security Label (CSL).* MIL-STD-2045/48501. January 25, 1995.

[B10] S. Kent. *U.S. Department of Defense Security Options for the Internet Protocol*. RFC 1108, November 1991.

[B11] *Standard Security Label for Information Transfer*. FIPS PUB 188. Washington, D.C.: USDC/NIST, September 6, 1994.

[B12] *Space Communications Protocol Specification (SCPS)—Network Protocol (SCPS-NP)*. Recommendation for Space Data System Standards, CCSDS 713.0-B-1. Blue Book. Issue 1. Washington, D.C.: CCSDS, May 1999.

[B13] *Space Communications Protocol Specification (SCPS)—Transport Protocol (SCPS-TP)*. Recommendation for Space Data System Standards, CCSDS 714.0-B-1. Blue Book. Issue 1. Washington, D.C.: CCSDS, May 1999.

† Internet Request for Comments (RFC) texts are available on line in various locations (e.g., http://ietf.org/rfc/).

[B14] *Assigned Internet Protocol Numbers*. Internet Assigned Numbers Authority (IANA). <ftp://ftp.isi.edu/in-notes/iana/assignments/protocol-numbers>.

[B15] *Space Communications Protocol Specification (SCPS)—Rationale, Requirements, and Application Notes*. Report Concerning Space Data System Standards, CCSDS 710.0-G-1. Green Book. Issue 1. Washington, D.C.: CCSDS, May 1999.

[B16] *Advanced Orbiting Systems, Networks and Data Links: Architectural Specification*. Recommendation for Space Data Systems Standards, CCSDS 701.0-B-2. Blue Book. Issue 2. Washington, D.C.: CCSDS, November 1992.

[B17] *Packet Telemetry*. Recommendation for Space Data System Standards, CCSDS 102.0-B-4. Blue Book. Issue 4. Washington, D.C.: CCSDS, November 1995.

[B18] *Telecommand Part 1 — Channel Service*. Recommendation for Space Data System Standards, CCSDS 201.0-B-2. Blue Book. Issue 2. Washington, D.C.: CCSDS, November 1995.

ANNEX C

PROTOCOL IMPLEMETATION CONFORMANCE STATMENT PROFORMA

(This annex **is** part of the Recommendation.)

C1 INTRODUCTION

This annex provides the Protocol Implementation Conformance Statement (PICS) Requirements List (PRL) for implementations of SCPS-SP. The PICS for an implementation is generated by completing the PRL in accordance with the instructions below. An implementation shall satisfy the mandatory conformance requirements of the base standards referenced in the PRL.

An implementation's completed PRL is called the PICS. The PICS states which capabilities and options of the protocol have been implemented. The following can use the PICS:

- the protocol implementer, as a checklist to reduce the risk of failure to conform to the standard through oversight;
- the supplier and acquirer or potential acquirer of the implementation, as a detailed indication of the capabilities of the implementation, stated relative to the common basis for understanding provided by the standard PICS proforma;
- the user or potential user of the implementation, as a basis for initially checking the possibility of interworking with another implementation (note that, while interworking can never be guaranteed, failure to interwork can often be predicted from incompatible PICSes);
- a protocol tester, as the basis for selecting appropriate tests against which to assess the claim for conformance of the implementation.

C1.1 NOTATION

The following are used in the PRL to indicate the status of features:

Status Symbols

M mandatory.

M.<n> support of every item of the group labeled by the same numeral <n> required, but only one is active at a time.

O optional.

O.<n> optional, but support of at least one of the group of options labeled by the same numeral <n> is required.

C conditional.

- non-applicable field/function (i.e., logically impossible in the scope of the PRL).

I out of scope of PRL (left as an implementation choice).

X excluded or prohibited.

Two character combinations may be used for dynamic conformance requirements. In this case, the first character refers to the static (implementation) status, and the second refers to the dynamic (use) status; thus 'MO' means 'mandatory to be implemented, optional to be used'.

Notations for Conditional Status

The following predicate notations are used:

<predicate>:: This notation introduces a group of items, all of which are conditional on <predicate>.

<predicate>: This notation introduces a single item which is conditional on <predicate>.

In each case, the predicate may identify a protocol feature, or a Boolean combination of predicates. ('^' is the symbol for logical negation, '|' is the symbol for logical OR, and '&' is the symbol for logical AND.)

<index>: This notation indicates that the status following it applies only when the PICS states that the features identified by the index are supported. In the simplest case, <index> is the identifying tag of a single PRL item. The symbol <index> also may be a Boolean expression composed of several indices.

<index>:: This notation indicates that the associated clause should be completed.

Notations Used in the Protocol Feature Column

<r> Symbol used to denote the receiving system.

<t> Symbol used to denote the transmitting system.

Support Column Symbols

The support of every item as claimed by the implementer is stated by entering the appropriate answer (Y, N, or N/A) in the support column:

Y Yes, supported by the implementation.

N No, not supported by the implementation.

N/A Not applicable.

C2 REFERENCED BASE STANDARDS

SCPS-SP (this document) is the only base standard referenced in the PRL. In the tables below, numbers in the Reference column refer to applicable subsections within this document.

C3 GENERAL INFORMATION

C3.1 IDENTIFICATION OF PICS

Ref	Question	
1	Date of Statement (DD/MM/YYYY)	
2	PICS serial number	
3	System Conformance statement cross-reference	

C3.2 IDENTIFICATION OF IMPLEMENTATION UNDER TEST (IUT)

Ref	Question	Response
1	Implementation name	
2	Implementation version	
3	Machine name	
4	Machine version	
5	Operating System name	
6	Operating System version	
7	Special Configuration	
8	Other Information	

C3.3 IDENTIFICATION

Supplier	
Contact Point for Queries	
Implementation name(s) and Versions	
Other Information Necessary for full identification - e.g., name(s) and version(s) for machines and/or operating systems; System Name(s)	

C3.4 PROTOCOL SUMMARY

Protocol Version	
Addenda Implemented	
Amendments Implemented	
Have any exceptions been required? (Note: A YES answer means that the implementation does not conform to the protocol. Non-supported mandatory capabilities are to be identified in the PICS, with an explanation of why the implementation is non-conforming.	Yes_____ No_____
Date of Statement	

C4 INSTRUCTIONS FOR COMPLETING THE PICS

An implementer shows the extent of compliance to the protocol by completing the PRL; that is, compliance to all mandatory requirements and the options that are not supported are shown. The resulting completed PRL is called a PICS. In the Support column, each response shall be selected either from the indicated set of responses, or it shall comprise one or more parameter values as requested. If a conditional requirement is inapplicable, N/A should be used. If a mandatory requirement is not satisfied, exception information must be supplied by entering a reference Xi, where i is a unique identifier, to an accompanying rationale for the noncompliance. When the requirement is expressed as a two-character combination (as defined above), the response shall address each element of the requirement; e.g., for the requirement 'MO', the possible compliant responses are 'YY' or 'YN'.

C4.1 SCPS-SP PRIMITIVES

Item	Protocol Feature	Reference	Status	Support
A1	S-UNITDATA.request	D2.2	M	
A2	S-UNITDATA.indication	D2.4	M	

C4.1.1 S-UNITDATA.request

Item	Protocol Feature	Reference	Status	Support
B1	N-Destination_Address	D2.3	M	
B2	N-Source_Address		M	
B3	S-User_Internet_Protocol_Number		M	
B4	N-Source_Timestamp		M	
B5	S-Quality_of_Service		M	
B5a	confidentiality_requested		M	
B5b	integrity_requested		M	
B5c	authentication_requested		M	
B5d	security_label_requested		M	
B6	N-Basic_Quality_of_Service		M	
B7	N-Expanded_Quality_of_Service		O	
B8	S-SDU		M	

C4.1.2 S-UNITDATA.indication

Item	Protocol Feature	Reference	Status	Support
C1	N-Destination_Address	D2.5	M	
C2	N-Source_Address		M	
C3	S-User_Internet_Protocol_Number		M	
C4	N-Source_Timestamp		M	
C5	S-Quality_of_Service		M	
C6	N-Basic_Quality_of_Service		M	
C7	N-Extended_Quality_of_Service		O	
C8	S-SDU		M	

C4.1.3 Lower Layer Network Primitives

Item	Protocol Feature	Reference	Status	Support
D1	N-UNITDATA.request	D3.1	M	
D2	N-UNITDATA.indication		M	

C4.1.3.1 N-UNITDATA.request

Item	Protocol Feature	Reference	Status	Support
E1	N-Destination_Address	D3.2	M	
E2	N-Source_Address		M	
E3	S-Internet_Protocol_Number		M	
E4	N-Source_Timestamp		M	
E5	N-Basic_Quality_of_Service		M	
E6	N-Expanded_Quality_of_Service		O	
E7	S-PDU		M	