CCSDS
The Consultative Committee for Space Data Systems

Draft Recommendation for
Space Data System Standards

CCSDS BUNDLE PROTOCOL SECURITY SPECIFICATION

DRAFT RECOMMENDED STANDARD

CCSDS 734.5-R-2

RED BOOK
September 2023

The Consultative Committee for Space Data Systems

Draft Recommendation for
Space Data System Standards

CCSDS BUNDLE PROTOCOL SECURITY SPECIFICATION

DRAFT RECOMMENDED STANDARD

CCSDS 734.5-R-2

RED BOOK
September 2023

AUTHORITY

Issue:	Red Book, Issue 2
Date:	September 2023
Location:	Not Applicable

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

This document has been approved for publication by the Management Council of the Consultative Committee for Space Data Systems (CCSDS) and represents the consensus technical agreement of the participating CCSDS Member Agencies. The procedure for review and authorization of CCSDS documents is detailed in *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-4), and the record of Agency participation in the authorization of this document can be obtained from the CCSDS Secretariat at the email address below.

This document is published and maintained by:

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

STATEMENT OF INTENT

(WHEN THIS RECOMMENDED STANDARD IS FINALIZED, IT WILL CONTAIN THE FOLLOWING 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.

FOREWORD

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 the *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-4). Current versions of CCSDS documents are maintained at the CCSDS Web site:

http://www.ccsds.org/

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

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

Member Agencies

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

Observer Agencies

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

PREFACE

This document is a draft CCSDS Recommended Standard. Its 'Red Book' status indicates that the CCSDS believes the document to be technically mature and has released it for formal review by appropriate technical organizations. As such, its technical contents are not stable, and several iterations of it may occur in response to comments received during the review process.

Implementers are cautioned **not** to fabricate any final equipment in accordance with this document's technical content.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

DOCUMENT CONTROL

Document	Title	Date	Status
CCSDS 734.5-R-1	CCSDS Streamlined Bundle Security Protocol Specification, Draft Recommended Standard, Issue 1	March 2018	Original draft issue, superseded
CCSDS 734.5-R-2	CCSDS Bundle Protocol Security Specification, Draft Recommended Standard, Issue 2	September 2023	Current draft

CONTENTS

CONTENTS (continued)

Section Page

Figure

Table

1 INTRODUCTION

1.1 PURPOSE

This document defines a Recommended Standard for the CCSDS Bundle Protocol Security Protocol (BPSec), based on the Bundle Protocol Security Protocol of RFC 9172 (reference [1]). BPSec defines Bundle Protocol version 7 (RFC 9171) (reference [2]) extension blocks with associated procedures that may be used with BPv7 bundles. These extension blocks provide a structured method for applying data integrity, authenticity, and/or confidentiality to blocks within a bundle.

1.2 SCOPE

This Recommended Standard defines BPSec in terms of:

- the protocol data units employed by the service provider; and
- the procedures performed by the service provider.

It does not specify:

- individual implementations or products;
- the implementation of service interfaces within real systems;
- the methods or technologies required to perform the procedures; or
- the management activities required to configure and control the service.

This Recommended Standard does not mandate the operational use of any particular cryptographic algorithm with BPSec. Reference [E3] provides a listing of algorithms recommended by CCSDS and those algorithms should be preferred by security contexts defined by CCSDS; any organization should conduct a risk assessment before choosing to substitute other algorithms.

The protocol specified here applies only to the Bundle Protocol version 7 and does not interact with other CCSDS protocols. BPSec applies to the Session and Presentation Layers of the Open Systems Interconnection (OSI) model as it relates to the Bundle Protocol.

1.3 APPLICABILITY

This Recommended Standard applies to the creation of Agency standards and for secure data communications over space networks 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 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.

BPv7 requires that inter-bundle security services (as opposed to the security services provided by overlying application protocols or underlying convergence-layer protocols) be provided in accordance with the BPSec Recommended Standard. BPv7 also requires that any BPv7 Agent (BPA) which sources, cryptographically verifies, and/or accepts a bundle must implement support for the BPSec Recommended Standard. The use of BPSec for any particular transmission of BPv7 bundles is optional for CCSDS missions.

1.4 RATIONALE

The goals of this Recommended Standard are to:

- provide a standard method of applying block-specific security for bundle transport, independent of the underlying cryptographic algorithms employed by any particular space mission; and
- facilitate the development of common commercial implementations to improve interoperability across agencies.

1.5 ORGANIZATION OF THIS RECOMMENDED STANDARD

The remainder of the document is then structured as follows:

- Section 2 introduces the need for security measures at the bundle protocol and showcases the main concepts and features of BPSec.
- Section 3 defines a profile of BPSec defined in IETF RFC 9172 (reference [1]).
- Section 4 provides the service specification for this protocol.
- Annex A addresses the Implementation Conformance Statement (ICS) PROFORMA.
- Annex C discussed any implications related to Space Assigned Numbers Authority (SANA), patent, or security aspects.
- Annex B defines the security contexts to use for interoperability testing.
- Annex D addresses the management information for the BPSec.
- Annex E lists the informative references.
- Annex F defines the acronyms used throughout this Recommended Standard.

Comments in the form of notes and figures have been inserted to clarify the specifications.

1.6 DEFINITIONS

This subsection provides references to terms and definitions necessary for understanding this Recommended Standard. Additional terms and definitions related to this Recommended Standard can be found in references [1], [2], [3], [4], and [5].

In particular, this document follows RFC 9172 in that it defines an integrity security operation. Depending on the mechanism used to provide integrity, such operations may also provide authenticity. In some cases the input data to an encryption function may itself be encrypted. This is referred to as superencryption.

BP may be deployed in scenarios that prohibit establishing relationships between two or more entities prior to exchanging information. BPSec defines a new term, security context, to refer to the practice of annotating a bundle with contextual information that would otherwise be used to establish a security association. Security associations may still be used with BPSec under the auspices of BPSec security contexts that allow them.

1.7 NOMENCLATURE

1.7.1 NORMATIVE TEXT

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.

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] E. Birrane and K. McKeever. *Bundle Protocol Security (BPSec)*. RFC 9172. Reston, Virginia: ISOC, January 2022.

[2] S. Burleigh, K. Fall, and E. Birrane. *Bundle Protocol Version 7*. RFC 9171. Reston, Virginia: ISOC, January 2022.

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

[4] “CCSDS Terms.” Space Assigned Numbers Authority. https://sanaregistry.org/r/terms.

[5] R. Shirey. *Internet Security Glossary*. Version 2. RFC 4949. Reston, Virginia: ISOC, August 2007.

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

[7] *Symmetric Key Management*. Issue 2. Draft Recommendation for Space Data System Practices (Red Book), CCSDS 354.0-R-2. Washington, D.C.: CCSDS, February 2022.

[8] E. Birrane, A. White, and S. Heiner. *Default Security Contexts for Bundle Protocol Security (BPSec)*. RFC 9173. Reston, Virginia: ISOC, January 2022.

[9] C. Bormann and P. Hoffman. *Concise Binary Object Representation (CBOR)*. STD 94. Reston, Virginia: ISOC, December 2020.

2 OVERVIEW

2.1 SECURITY NEEDS FOR BUNDLE PROTOCOL VERSION 7

The Bundle Protocol (BP) provides end-to-end communications across many networking environments, including Delay/Disruption Tolerant Networks (DTNs). The BPv7 specification refers to a DTN as ‘a networking architecture providing communications in and/or through highly stressed environments’ (reference [2]). In this context, the term ‘highly stressed environment’ can refer to multiple challenging conditions including intermittent connectivity, large and/or variable delays, asymmetric data rates, and high bit error rates. Whether deployed in a DTN or some other networking environment, ‘BP may be viewed as sitting at the Application Layer of some number of constituent networks, forming a store-carry-forward overlay network’ (reference [2]).

BP is presumed to be deployed in circumstances where the networking environment is not trusted, which requires consideration of usual security challenges related to confidentiality, integrity, and authenticity.

Networks may be untrusted for a variety of reasons. Different nodes in a network may cross multiple administrative boundaries (such as on the Internet) such that not every administrative entity is given the same level of trust. Within a given administrative boundary such as an enterprise intranet, nodes may have different physical or logical access controls and policies which may affect trust. Similarly, individual nodes may incorporate components (convergence layers, virtual machines, open source libraries) with differing levels of trust.

The stressed nature of certain networks where BP may be deployed may impose constraints that break or otherwise impede the use of usual transport security mechanisms. BPSec specifies unique security features inherent in securing a store-and-forward-based transport protocol, including protecting data at rest, preventing unauthorized consumption of critical resources such as storage space, and operating without regular contact with a centralized security oracle (such as a certificate authority).

Because transport security mechanisms that require multiple handshakes may not be feasible in the environments where BP functions, new end-to-end security services that can secure bundles in all DTN environments are needed.

2.2 CONCEPT OF BUNDLE PROTOCOL SECURITY

2.2.1 GENERAL

BPSec is a protocol by which space missions can apply security services to individual blocks that make up a BPv7 bundle. BPSec data units are codified as extension blocks within the BP and exist only in the context of a bundle.

2.2.2 BPSEC SECURITY SERVICES

BPSec provides two security services for blocks within a BPv7 bundle:

a) Bundle Integrity Block (bib-integrity). This service specifies an integrity mechanism over the block-type-specific data of a target block. This service also supports the inclusion of additional data beyond the plaintext of the block-type-specific data of the target block. Integrity mechanisms (absent confidentiality mechanisms) detect changes resulting from processing errors, environmental conditions, or intentional manipulation. With appropriate mechanisms such as digital-signature-based authentication, integrity can also provide data authentication/authenticity.

b) Bundle Confidentiality Block (bcb-confidentiality). This service specifies authenticated confidentiality over the plaintext block-type-specific data of a target block. This service also supports the inclusion of additional authenticated data beyond the plaintext of the block-type-specific data of the target block.

2.2.3 SECURITY CONTEXTS

Security contexts in BPSec differ from security associations in IPsec.

Internet IPsec uses the term ‘security association’ defined as:

> a one-way (inbound or outbound) agreement between two communicating peers that specifies the IPsec protections to be provided to their communications. This includes the specific security protections, cryptographic algorithms, and secret keys to be applied, as well as the specific types of traffic to be protected.

The specifics of a security association are often negotiated and maintained as state at the endpoints. As a result, endpoints can use a security parameters index (an integer), which, together with the destination IP address and security protocol, uniquely identifies a single (active) security association.

RFC 9172 uses the term ‘security context’ to refer to the set of assumptions, algorithms, configurations, and policies used to implement security services. One of the main differences between security contexts and security associations is that with security contexts, the specifics needed to invoke the security services (the assumptions, algorithms, configurations and policies) may be predefined so that no negotiated state is required at the endpoints.

Security contexts:

– are parameterizable; for instance, a single security context might be configurable to, for example:

  - allow the use of different cipher suites/key lengths (signaled as part of the block containing the security operation),

  - specify a set of ‘scope’ flags specifying which parts of the target Bundle Block are to be covered by the security operation (e.g., to block-type-specific data only, to include the header of the target block),
  - include an optional parameter that is the encrypted version of a symmetric key used to encrypt block context;
- include configuration and policy information; for example:
  - specify what actions should be taken if particular security measures are not present in the bundle or fail acceptance,
  - specify which blocks should be included in outbound bundles to particular next hops (e.g., previous-hop-block).

For example, one mission may use a 256-bit Advanced Encryption Standard (AES) cipher suite for confidentiality with a negotiated Security Association IDentifier (SAID) (similar to the security parameters index in IPsec). In this case, at most the SAID must be communicated in the bundles that use confidentiality to process security at a security acceptor. Another mission may use the same 256-bit AES cipher without the ability to negotiate (or sustain) a security association. In this case, cipher suite parameters (possibly included a wrapped key) may be encoded with a symmetric key and included in the security block. In both cases, the same cipher suite is used, but the security context surrounding the cipher suite is very different.

BPSec security blocks identify the security context used in the handling of cryptographic materials associated with the security operations represented by these blocks. Different security contexts can be used for different bundles and for different security operations within a single bundle. The application of a given security context to a security operation is defined by BPA local node policy on the security source.

CCSDS recommended cryptographic algorithms as specified in reference [E3] should be used in the definition of security contexts unless a specific reason exists that does not allow them.

2.2.4 BPSEC SECURITY OPERATIONS AND BLOCKS

BPSec security services can be applied to individual blocks within a bundle, providing fine-grained security in a bundle.

Blocks in a bundle may carry different types of information. Payload blocks carry application data. Extension blocks may carry network information, annotative information related to the payload, or special processing instructions for the bundle itself. This combination of network-focused, bundle-focused, and application-data-focused information often requires different security services with different shared secrets (keys), different policies, and different accesses.

BPSec specifies the application of a security service to a specific target block within a bundle. This operation is notated as OP(service, target). For example, applying the of bib-integrity service to a bundle's primary block would be notated as:

OP(bib-integrity, primary block)

BPSec requires that all security operations in a bundle be unique. This means that the same security service cannot be applied to the same target block multiple times. Such a situation would create ambiguity in the order of operation of verifying integrity and cases where some integrity mechanisms succeed and others fail verification.

BPSec security services (such as bib-integrity) use security contexts to define cipher suites, parameters, and results. It is possible to define a security context which would calculate multiple integrity results over a single target block. In this case, there is still a single operation, OP(bib-integrity, target block), with that operation carrying multiple security results from the generating security context. This avoids the ambiguity of having multiple security services, because this single security service generates all integrity results at the same time, processes all integrity results at the same time, and provides a single mechanism to dispose multiple integrity results that pass/fail verifications.

Security operations for a particular target block are instantiated in a bundle by their inclusion in a security block. Every security block contains at least one, and possible many, security operations.

When multiple security operations share certain common attributes (e.g., the same security source, security service, and parameters) they may be aggregated into a single security block. In this case, there is a one-to-many relationship between a security block and the security operations it carries.

The relationship between security blocks and target blocks is illustrated in figure 2-1. The figure illustrates a bundle containing six blocks: the required primary and payload block and four extension blocks. Security block (1) provides a security service for target block (1) and security block (2) provides a security service for target block (2).

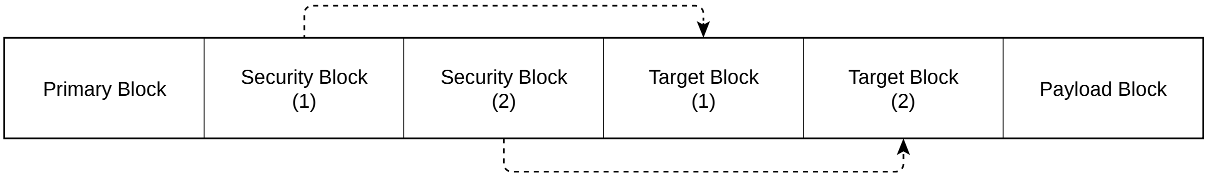

Figure 2-1: Security Block Targets

2.2.5 BPSEC ROLES AND RESPONSIBILITIES

BPSec defines three functions associated with the processing of security operations within security blocks:

– the security source;

– security verifier;

– and security acceptor.

These roles are defined per security operation. This means that different security operations in the same bundle might have different security sources, verifiers, and acceptors.

The security source of a security operation is the BPA that added the security block. The source is identified as the Node ID of the BPA. Security sources must ensure that security operations in a security block would not violate any constraints imposed by BPSec. When a security block contains multiple security operations, all operations share the same security source.

The security verifier of a security operation is one or more BPAs that verify a security operation as a bundle transits through the BPA. If the verification succeeds, the security blocks remains in the bundle. If the verification fails, the security block and bundle will be processed in accordance with the local BPA security policy.

A given BPA might be identified as a security verifier for some, but not all, of the security operations in a security block. For example, if a security block contains two security operations: OP(bib-integrity, primary block) and OP(bib-integrity, payload block), a BPA might be configured as the security verifier for the integrity results over the primary block but not the payload block.

A common use of security verifiers is to verify the integrity and/or authenticity of blocks in a bundle prior to its delivery to its destination. Detecting corrupted data quickly (and removing corrupted bundles early) helps reduce congestion and resource utilization within the network.

The security acceptor of a security operation refers to the single BPA that both verifies and removes a security operation from a bundle. When the last security operation is removed from a security block, the security block is removed from the bundle.

A security acceptor does not have to be the bundle destination. Security operations may be terminated prior to a bundle's reaching a destination, particularly when some security results are processed at administrative boundaries in a network.

The bundle destination is considered to be the default security acceptor for any security operations remaining in a bundle when it reaches its destination.

Figure 2-2 illustrates the operational concepts associated with BPSec, where BN denotes a ‘bundle node’. Bundles are created at BN1 and BN2 and received by BN2 and BN3. The BPAs at these nodes serve as the security source, verifier, and acceptor. A BPA may perform multiple functions as shown by BN2, which acts as the security source for Bundle 3, security verifier for Bundle 2, and security acceptor for Bundle 1.

Each security service is added for a target block by a security source and removed by a security acceptor. Some bundles may encounter security verifiers in transit such as Bundle 2 at BN2.

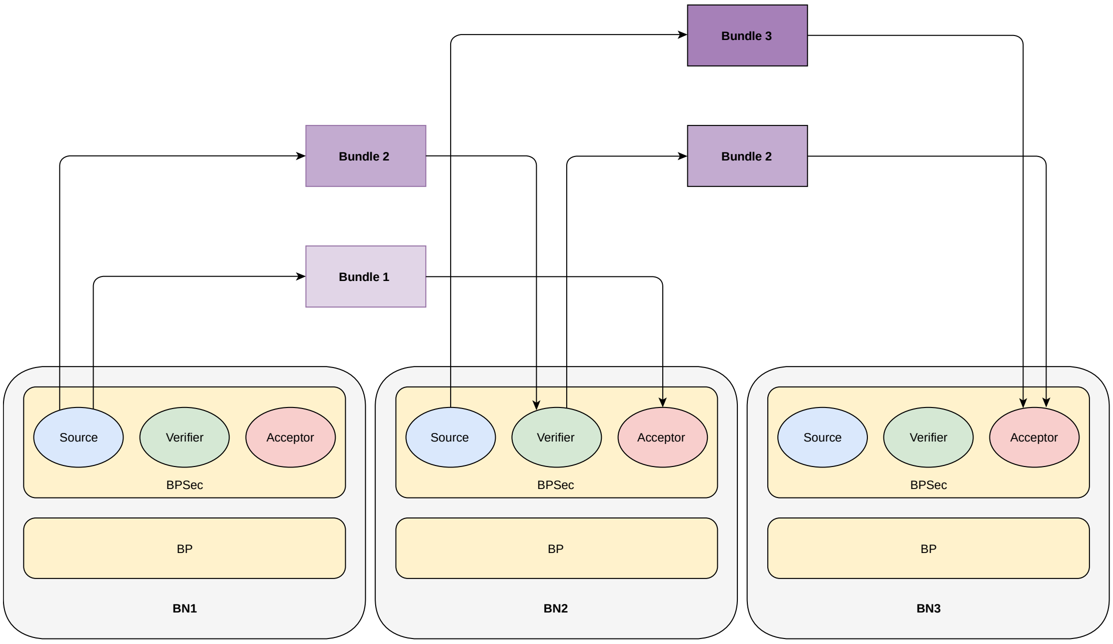

Figure 2-2: BPA Security Functions

Figure 2-3 illustrates the operations of a security source, verifier, and acceptor on an integrity security block.

At step 1, the security source identifies a target block in the bundle. By policy, integrity must be applied before the bundle is transmitted. At step 2, the security source computes an integrity result and adds it to the bundle in the form of a BPSec block.

Steps 3 and 4 occur at a security verifier. In step 3, the node is identified as the security block security verifier. The security verifier verifies the integrity of the target of the security block at step 4.

Steps 5, 6, and 7 occur at the security acceptor. Step 5 identifies the node as the security block’s security acceptor. The integrity of the target block is verified in step 6. The security block is removed from the bundle in step 7.

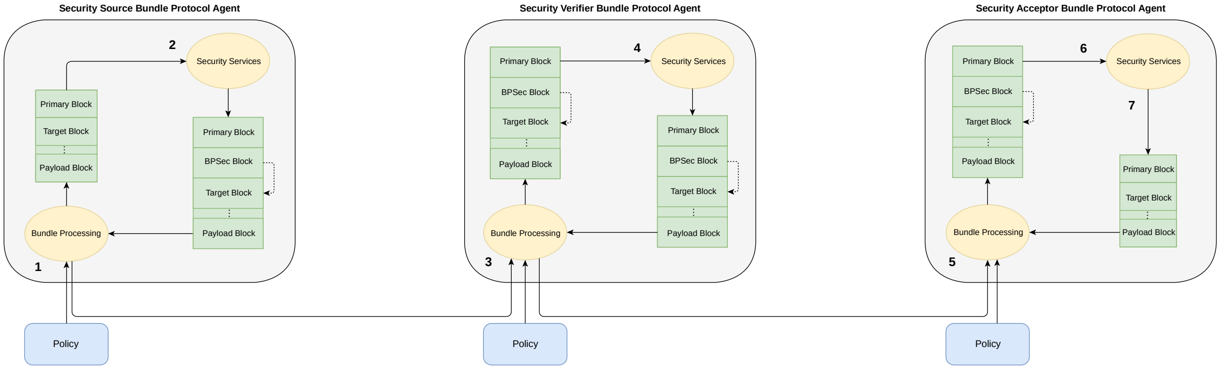

Figure 2-3: Security Operations Processing

2.3 NOTABLE FEATURES OF BPSEC

2.3.1 OVERVIEW

This subsection describes those features of BPSec that distinguish it from security mechanisms in existing network architectures (such as the Internet).

2.3.2 GENERAL

BPSec provides security services to assure the confidentiality, integrity, and/or authenticity of the contents of blocks in a bundle. Specifically, BPSec provides the following capabilities:

- Security blocks may be added to a bundle by the source BPA or downstream BPAs.
- Security blocks may be modified or removed from a bundle by security verifiers and security acceptors.
- A security block may represent either a collection of data integrity or a collection of confidentiality security operations.

NOTE – A block may represent a collection of operations because, according to the security policy, it might apply security operations (e.g., confidentiality) to a set of target blocks within the bundle, not just a single target block.

- A security operation may be added to a security block if it represents a unique security operation.
- Security mechanisms use a security context that specifies the cipher suite, user parameters for the cipher suite, and any special processing rules related to the use of the cipher suite.
- Multiple security blocks of the same block type may exist in a bundle.

2.3.3 AUTHENTICATION

BPSec can provide authentication via a combination of BPSec block types and the security context(s) in which they are used. Authentication can be applied to a single target block or to some set of cryptographically bound target blocks. There are four mechanisms for authenticating data provided by BPSec, as follows.

First, BPSec provides a mechanism for signature-based authentication of target block plaintext through the application of a Block Integrity Block (BIB), which calculates a security result over the contents of a target block. The calculated security result is defined by the security context being applied. For example, a security context might specify that the BIB security result be calculated as a SHA-2 signature combined with a keyed hash over the block-type-specific data field of the target block. The authenticity of the target block could be assessed by a receiving node by locally calculating the security result using a key associated with the expected information source. If the computed result matches the result in the BIB, there is evidence that the target block was both unchanged and created by the expected information source.

Second, BPSec provides a mechanism for signature-based authentication of target block ciphertext through the application of the Block Confidentiality Block (BCB). The application of a BCB causes the block-type-specific data of a target block to be replaced by ciphertext generated by a given cipher suite. BPSec requires the use of Authenticated Encryption with Associated Data (AEAD) cipher suites. The BCB carries with it an authentication security result associated with the ciphertext placed in the target block. Decryption of the target block requires an authentication operation. Similar to the BIB, authentication is provided through data signatures.

Third, BPSec provides a mechanism for authentication of information within BIB and BCB blocks. Each BPSec security block contains a series of security context parameters, and individual security contexts both define these parameters and define ways in which these parameters must be authenticated. For example, if a security context defines a session key as a parameter carried in a BIB or BCB, it may also specify that the session key be wrapped using a long-term key encryption key using a specific key wrapping algorithm.

Fourth, by providing block-level granularity and the ability to define security contexts, BPSec allows for the authentication of multiple blocks in a bundle (or the bundle itself) through combinations of the above capabilities. For example, a signature-based integrity check over the Primary Block (which includes the source and destination of the bundle) may authenticate that a bundle should be processed by a BPA because the bundle was sourced by an authorized bundle source. Alternatively, individual target blocks may include the Primary Block (or other blocks) as part of their Additional Authenticated Data (AAD) in either integrity or confidentiality operations. This effectively binds a given target block to a given bundle and prevents blocks from being taken out of one bundle and included in another.

Finally, the security context mechanism defined by BPSec allows for the specification of non-signature-based authentication mechanisms. It is conceivable that multi-factor authentication mechanisms or non-signature based mechanisms can be applied to bundles and associated behavior can be captured in a custom security context. This is possible because the BIB and BCB blocks defined by BPSec carry security context parameters and security context results, but how that information is used at a BPA is given by the behavior of the individual security context.

2.3.4 BLOCK-LEVEL GRANULARITY

The target block of any security operation is another block in the bundle. The ability to ‘target’ individual blocks enables BPSec to secure information uniquely.

BPSec provides the ability to secure individual target blocks. This requirement is derived from the BPv7 feature allowing extension blocks containing different types of information.

Some blocks carry information about the bundle itself. Other blocks carry application data or annotations related to the application data. Yet other blocks might carry information relevant to the state of the network itself. Block-level granularity allows multiple security services to be applied to blocks with the level(s) of security the target blocks require.

2.3.5 MULTIPLE SECURITY SOURCES

BPSec allows a bundle to contain multiple security blocks from different security sources.

This is a unique provision because blocks might be added to a bundle after the bundle creation and may need security applied.

BPv7 allows extension blocks to be added to a bundle at any node. A downstream node may add a security block to a bundle, in which case that node is the security source for the added security block.

2.3.6 MIXED SECURITY POLICY

BPSec allows different security operations to be governed by different security policies. The determination of security source, security verifier, and security acceptor roles is a function of local policy and information resident in the received bundle. This is a unique ability as it allows elements of policy determination to be driven by security parameters and annotations carried in security blocks within a bundle.

The topology of a DTN might evolve over the lifetime of a bundle such that different nodes along a bundle path have different security capabilities and roles from those that existed at the time of bundle creation. Therefore the determination of which BPAs have which security roles is made as part of the configuration of the BPA.

2.3.7 DETERMINISTIC PROCESSING

BPSec ensures that the creation, verification, and acceptance of security services within a bundle always produce deterministic results. To accomplish this, BPSec imposes a strict ordering of operations and restricts features or feature combinations that could endanger this ordering.

3 CCSDS PROFILE OF RFC 9172

3.1 ADOPTION OF MECHANISMS FROM RFC 9172

This document adopts the Bundle Protocol Security Protocol as specified in Internet RFC 9172 (reference [1]), with the constraints and exceptions specific in section 3 of this document.

3.2 USE OF APPROVED SECURITY CONTEXTS

3.2.1 Implementations of this Recommended Standard shall use Security Context Identifiers (SCIs) that have been assigned by Internet Assigned Numbers Authority (IANA).

3.2.2 SCIs approved by CCSDS are those that are listed in the CCSDS approved security contexts registry.

NOTES

1 IANA assigns BPSec Security Context Identifiers using the registry located at: https://www.iana.org/assignments/bundle/bundle.xhtml#bpsec-security-context. This registry is expected to include a range of context identifiers to be assigned and managed by SANA.

2 Wherever possible, missions are expected to use security contexts that are either approved by the CCSDS or otherwise allocated from the SANA-assigned portion of the BPSec Security Context Identifiers registry.

3 Security contexts are defined in normative specifications, to include the default context provided in annex B of this document. The appropriateness of a security context for any particular mission use is at the sole discretion of the mission as a function of its own security and threat analysis.

4 Missions can characterize their security requirements as low, medium, or high in accordance with reference [E2]. This characterization refers to the scope of security and associated policy. There is not a direct correlation between a specific security context and a specific mission security characterization.

3.3 USE OF CCSDS-APPROVED KEY MANAGEMENT

3.3.1 SECURITY CONTEXTS

Security contexts approved by the CCSDS shall support CCSDS-approved key management mechanisms.

3.3.2 USE OF SANA-REGISTERED SECURITY CONTEXTS

Key management mechanisms for SANA-registered security contexts shall conform to reference [6].

3.3.3 USE OF SYMMETRIC KEY MANAGEMENT MECHANISMS FOR SANA-REGISTERED SECURITY CONTEXTS

Symmetric key management mechanisms for SANA-Registered security contexts shall conform to reference [7].

NOTE – Key management mechanisms may be specified separately from the definition of a security context in cases where multiple security contexts might use the same key management mechanisms (such as exchanging keys) or in cases where missions may choose to employ different mechanisms based on considerations outside of the scope of the security context itself.

3.4 APPLICATION OF CCSDS POLICY CONSIDERATIONS

The specification and management of security policy on BPAs is necessary but outside the scope of this document.

3.5 SANA REGISTRY CONSIDERATIONS

3.5.1 The recommendations of this document require the creation of a BPSec Approved Security Contexts SANA registry. New entries require an approved CCSDS document specifying the IANA-assigned Security Context Identifier.

NOTE – As indicated in 3.2.2, IANA assigns BPSec Security Context Identifiers using the registry located at:
https://www.iana.org/assignments/bundle/bundle.xhtml#bpsec-security-context.
This registry is expected to include a range of context identifiers to be assigned and managed by SANA.

3.5.2 Security contexts that CCSDS defines for space missions must be registered with IANA.

4 BPSEC SERVICE DEFINITION

4.1 OVERVIEW

This section provides the service definition for BPSec.

The definitions of these functions are logical and do not presuppose any specific BPA, security context definition, or cipher suite implementation. Function behaviors do not presuppose any configuration approach, policy approach, or method for generating cryptographic material.

This specification allows for the concurrent execution of these functions such that one function can be started prior to completion of some other function, regardless of whether these functions operate on different blocks within a bundle or different bundles within the BPA.

The parameters for these functions are documented in an abstract sense and specify the information passed between the BPA entity that calls the function and the BPSec entity that executes the function. The way in which a specific implementation makes this information available is not constrained by this specification. In addition to the parameters specified in this section, an implementation may provide other parameters on the function interface (e.g., parameters for controlling the service, monitoring performance, diagnosis, and so on).

4.2 BPSEC SERVICES

BPSec shall provide the following services:

a) ApplyBIB;

b) ApplyBCB;

c) VerifyBIB;

d) VerifyBCB;

e) AcceptBIB;

f) AcceptBCB.

4.3 SUMMARY OF PRIMITIVES

4.3.1 REQUEST PRIMITIVES

The BPSec service shall consume the following request primitives:

a) ApplyBIB.request;

b) ApplyBCB.request;

c) VerifyBIB.request;

d) VerifyBCB.request;

e) AcceptBIB.request;

f) AcceptBCB.request.

4.3.2 INDICATION PRIMITIVES

The BPSec service shall provide the following indication primitives.

a) ApplyBIB.indication;

b) ApplyBCB.indication;

c) VerifyBIB.indication;

d) VerifyBCB.indication;

e) AcceptBIB.indication;

f) AcceptBCB.indication.

4.4 SUMMARY OF PARAMETERS

4.4.1 TARGET BUNDLE

The Target Bundle parameter shall consist of the bundle containing one or more blocks for which a BPSec service is being requested. The calling BPA must be the BPA identified as the security source for security blocks being added.

4.4.2 TARGET BLOCK IDENTIFIERS

The Target Block Identifiers parameter shall uniquely identify the target block(s) within the target bundle being used by the ApplyBIB or ApplyBCB functions.

4.4.3 MODIFIED BUNDLE

4.4.3.1 Modified bundles shall be returned as results of security operations that add or remove security blocks from bundles.

4.4.3.2 The Modified Bundle parameter shall contain a copy of the target bundle that includes any changes made by the BPSec service.

4.4.4 NEW BIB BLOCK IDENTIFIER

The New BIB Block Identifier paramter shall contain the block ID of the BIB block added as a result of an ApplyBIB.request.

4.4.5 NEW BCB BLOCK IDENTIFIER

The New BCB Block Identifier paramenter shall contain the block ID of the BCB block added as a result of an ApplyBCB.request.

4.4.6 SECURITY CONTEXT IDENTIFIER

4.4.6.1 The Security Context Identifier parameter shall identify the security context used to generate cryptographic material associated with the ApplyBIB and ApplyBCB functions.

4.4.6.2 In the context of ApplyBCB, this parameter must reference an AEAD cipher suite.

4.4.7 SECURITY CONTEXT PARAMETERS

4.4.7.1 The Security Context Parameters parameter shall consist of a set of parameters associated with the security context identified by the Security Context Identifier.

4.4.7.2 These parameters must be provided as inputs to the algorithms used to produce cryptographic material for the bundle.

NOTE – In addition to being input to the suite of algorithms, some of these parameters may also be recorded in the BPSec security blocks added to the bundle for use by downstream security verifiers and security acceptors.

4.4.8 LOCAL SECURITY CONTEXT PARAMETERS

4.4.8.1 The Local Security Context Parameters parameter shall consist of the information configured at a security verifier BPA for the security context specified in the security block identified in the Security Block parameter.

4.4.8.2 These local security context parameters must be provided as inputs to the security context used to verify the integrity or confidentiality of the target block.

NOTE – The security block’s security context parameters and Local Security Context Parameters may provide conflicting values for the same parameter. When such conflicts exist, local node policy must specify how conflicts are resolved.

4.4.9 SECURITY SOURCE

The Security Source parameter shall consist of the Endpoint IDentifier (EID) of the node that is inserting the security block into the bundle.

4.4.10 VERIFICATION BLOCK IDENTIFIERS

The Verification Block Identifiers parameter shall uniquely identify the block(s) within the target bundle being used by the VerifyBIB or VerifyBCB functions.

4.4.11 VERIFICATION RESULT

The Verification Result parameter shall indicate whether the verification operations passed or failed.

NOTE – The verification result may include ancillary information such as error codes.

4.5 CCSDS BPSEC SERVICE PRIMITIVES

4.5.1 OVERVIEW

A security block is added to a bundle by the BPA serving as the security source for that block. Each security block may contain one or more related security operations, with each security operation applied to a different target block in the bundle. The BPSec defines two security blocks: BIB and BCB, and these blocks are added to a bundle using two functions: ApplyBIB and ApplyBCB.

4.5.2 ApplyBIB.request

4.5.2.1 Function

4.5.2.1.1 The ApplyBIB.request primitive shall be used to apply a BIB integrity operation to one or more target blocks in a bundle.

4.5.2.1.2 All blocks that are targets of the BIB operation must be present in the target bundle before invoking ApplyBIB.request.

4.5.2.2 Semantics

ApplyBIB.request shall provide parameters as follows:

```
ApplyBIB.request (Target Bundle,
                  Target Block Identifiers,
                  Security Context Identifier,
                  Security Context Parameters)
```

4.5.2.3 When Generated

This function shall be invoked on a BPA when local security policy determines that the BPA is the security source of a bib-integrity service for one or more target blocks in the bundle.

4.5.2.4 Effect on Receipt

4.5.2.4.1 When invoked, this function shall provide all input parameters to the selected security context, capture the results generated by the security context, and insert the results into the target bundle in the form of a new security block.

4.5.2.4.2 The modified target bundle (with the new BIB block) shall be returned to the caller in the ApplyBIB.indication.

4.5.2.5 ApplyBCB.request

4.5.2.6 Function

4.5.2.6.1 The ApplyBCB.request primitive shall be used to apply a BCB integrity operation to one or more target blocks in a bundle.

4.5.2.6.2 All blocks that are targets of the BCB operation must be present in the target bundle before invoking ApplyBCB.request.

4.5.2.7 Semantics

ApplyBCB.request shall provide parameters as follows:

```
ApplyBCB.request  (Target Bundle,
                   Target Block Identifiers,
                   Security Context Identifier,
                   Security Context Parameters)
```

4.5.2.8 When Generated

This function shall be invoked on a BPA when local security policy determines that the BPA is the security source of a bcb-confidentiality service for one or more target blocks in the bundle.

4.5.2.9 Effect on Receipt

4.5.2.9.1 When invoked, this function shall provide all input parameters to the selected security context, capture the results generated by the security context, and insert these results into the bundle in the form of a new security block.

4.5.2.9.2 When the ApplyBCB Function has completed the processing, it shall return the modified bundle with the new BCB block and any other changes via the ApplyBCB.indication.

4.5.3 ApplyBIB.indication

4.5.3.1 Function

The ApplyBIB.indication primitive shall be used to provide the BPA the contents of the bundle after the requested BIB security operation has been applied.

4.5.3.2 Semantics

ApplyBIB.indication shall provide parameters as follows:

ApplyBIB.indication (Modified Bundle,
New BIB Block Identifier)

4.5.3.3 When Generated

ApplyBIB.indication shall be generated by the BPSec service once the requested BIB security operation has been applied to the target bundle and the contents of the modified bundle have been computed.

4.5.3.4 Effect on Receipt

On receipt of ApplyBIB.indication, the BPA shall replace the original bundle with the modified bundle.

4.5.4 ApplyBCB.indication

4.5.4.1 Function

The ApplyBCB.indication primitive shall be used to provide the BPA the contents of the bundle after the requested BCB security operation has been applied.

4.5.4.2 Semantics

ApplyBCB.indication shall provide parameters as follows:

```
ApplyBCB.indication  (Modified Bundle,
                      New BCB Block Identifier)
```

4.5.4.3 When Generated

ApplyBCB.indication shall be generated by the BPSec service once the requested BCB security operation has been applied to the target bundle and the contents of the modified bundle have been computed.

4.5.4.4 Effect on Receipt

On receipt of ApplyBCB.indication shall replace the original bundle with the modified bundle.

4.5.5 VerifyBIB.request

4.5.5.1 Function

The VerifyBIB.request primitive shall be used to verify a particular BIB.

4.5.5.2 Semantics

VerifyBIB.request shall provide parameters as follows:

```
VerifyBIB.request    (Target Block Identifiers,
                      Verification Block Identifiers,
                      Security Context Identifier,
                      Local Security Context Parameters)
```

4.5.5.3 When Generated

VerifyBIB.request shall be generated by a BPA that is configured to be a security verifier for the particular BIB instance provided.

4.5.5.4 Effect on Receipt

When invoked, VerifyBIB shall do the following in sequence:

a) provide all input parameters to the selected security context;

b) capture the results generated by the security context;

c) determine if the integrity verification succeeded; and

d) generate a VerifyBIB.indication.

4.5.6 VerifyBCB.request

4.5.6.1 Function

The VerifyBCB.request primitive shall be used to verify a particular BCB.

4.5.6.2 Semantics

VerifyBCB.request shall provide parameters as follows:

```
VerifyBCB.request   (Target Block Identifiers,
                    Verification Block Identifiers,
                    Security Context Identifier,
                    Local Security Context Parameters)
```

4.5.6.3 When Generated

VerifyBCB.request shall be generated by a BPA that is configured to be a security verifier for the particular BCB instance provided.

4.5.6.4 Effect on Receipt

When invoked, VerifyBCB shall do the following in sequence:

a) provides all input parameters to the selected security context;

b) captures the results generated by the security context;

c) determines if the confidentiality verification succeeded; and

d) generate a VerifyBCB.indication.

4.5.7 VerifyBIB.indication

4.5.7.1 Function

The VerifyBIB.indication primitive shall be used to provide information about the verification of a particular BIB.

4.5.7.2 Semantics

VerifyBIB.indication shall provide parameters as follows:

VerifyBIB.indication (Verification Result)

4.5.7.3 When Generated

VerifyBIB.indication shall be generated by a CCSDS BPSec implementation once it has verified a particular BIB.

4.5.7.4 Effect on Receipt

The effect on receipt of VerifyBIB.indication by the BP application is undefined.

4.5.8 VerifyBCB.indication

4.5.8.1 Function

The VerifyBCB.indication primitive shall be used to provide information about the verification of a particular BCB.

4.5.8.2 Semantics

VerifyBCB.indication shall provide parameters as follows:

VerifyBCB.indication (Verification Result)

4.5.8.3 When Generated

VerifyBCB.indication shall be generated by a CCSDS BPSec implementation once it has verified a particular BCB.

4.5.8.4 Effect on Receipt

The effect on receipt of VerifyBCB.indication by the BP application is undefined.

4.5.9 AcceptBIB.request

4.5.9.1 Function

The AcceptBIB.request primitive shall be used by a security acceptor to verify the integrity of security operations within the BIB for which the BPA is configured as a security acceptor.

4.5.9.2 Semantics

AcceptBIB.request shall provide parameters as follows:

```
AcceptBIB.request   (Target Bundle,
                     Verification Block Identifiers,
                     Security Context Identifier,
                     Local Security Context Parameters)
```

4.5.9.3 When Generated

AcceptBIB.request shall be generated by a CCSDS BPSec implementation that is a security acceptor for a bundle containing the BIB to verify.

4.5.9.4 Effect on Receipt

When invoked, AcceptBIB provides all input parameters to the selected security context, captures the results generated by the security context, determines if the confidentiality verification succeeded, and generates an AcceptBIB.indication.

4.5.10 AcceptBCB.request

4.5.10.1 Function

The AcceptBCB.request primitive shall be used by a security acceptor to verify the integrity of security operations within the BCB for which the BPA is configured as a security acceptor.

4.5.10.2 Semantics

AcceptBCB.request shall provide parameters as follows:

```
AcceptBIB.request   (Target Bundle,
                     Verification Block Identifiers,
                     Security Context Identifier,
                     Local Security Context Parameters)
```

4.5.10.3 When Generated

AcceptBCB.request shall be generated by a CCSDS BPSec implementation that is a security acceptor for a bundle containing the BCB to verify.

4.5.10.4 Effect on Receipt

When invoked, AcceptBCB.request provides all input parameters to the selected security context, captures the results generated by the security context, determines if the confidentiality verification succeeded, and generates an AcceptBCB.indication. If the verification succeeded, the AcceptBCB.indication shall include decrypted versions of any encrypted blocks.

4.5.11 AcceptBIB.indication

4.5.11.1 Function

The AcceptBIB.indication primitive shall be used to verify a particular BIB.

4.5.11.2 Semantics

4.5.11.2.1 AcceptBIB.indication shall provide parameters as follows:

```
AcceptBIB.indication (Verification Result,
                      Modified Bundle)
```

4.5.11.2.2 The modified bundle shall be such that accepted security operations are removed from the BIB.

4.5.11.2.3 If all security operations are removed from a BIB, that the BIB shall be removed from the bundle.

4.5.11.3 When Generated

AcceptBIB.indication shall be generated by a CCSDS BPSec implementation once it has completed processing of an AcceptBIB.request.

4.5.11.4 Effect on Receipt

The effect on receipt of AcceptBIB.indication by the BP application is undefined.

4.5.12 AcceptBCB.indication

4.5.12.1 Function

The AcceptBCB.indication primitive shall be used to verify a particular BCB.

4.5.12.2 Semantics

4.5.12.2.1 AcceptBCB.indication shall provide parameters as follows:

```
AcceptBCB.indication  (Verification Result,
                       Modified Bundle)
```

4.5.12.2.2 Accepted security operations shall be removed from the BCB and, if all security operations are removed from a BCB, the BCB will be removed from the bundle.

4.5.12.2.3 The target blocks of the confidentiality service shall be modified based on whether confidentiality was successfully removed.

4.5.12.2.4 If confidentiality removal was successful, the ciphertext contents of the target blocks shall be replaced by the plaintext outputs from the security context.

4.5.12.2.5 If confidentiality removal was not successful, the target block shall be removed from the bundle.

4.5.12.3 When Generated

AcceptBCB.indication shall be generated by a CCSDS BPSec implementation once it has completed processing of an AcceptBCB.request.

4.5.12.4 Effect on Receipt

The effect on receipt of AcceptBCB.indication by the BP application is undefined.

ANNEX A

IMPLEMENTATION CONFORMANCE STATEMENT PROFORMA

(NORMATIVE)

A1 INTRODUCTION

A1.1 OVERVIEW

This annex provides the ICS Requirements List (RL) for an implementation of BPSec for CCSDS. The ICS for an implementation is generated by completing the RL in accordance with the instructions below. An implementation claiming conformance must satisfy the mandatory requirements referenced in the RL.

A1.2 ABBREVIATIONS AND CONVENTIONS

The RL consists of information in tabular form. The status of features is indicated using the abbreviations and conventions described below.

Item Column

The item column contains sequential numbers for items in the table.

Feature Column

The feature column contains a brief descriptive name for a feature. It implicitly means ‘Is this feature supported by the implementation?’

Status Column

The status column uses the following notations:

– M	mandatory;
– O	optional;
– C	conditional;
– X	prohibited;
– I	out of scope;
– N/A	not applicable.

Support Column Symbols

The support column is to be used by the implementer to state whether a feature is supported by entering Y, N, or N/A, indicating:

Y	Yes, supported by the implementation.
N	No, not supported by the implementation.
N/A	Not applicable.

The support column should also be used, when appropriate, to enter values supported for a given capability.

A1.3 INSTRUCTIONS FOR COMPLETING THE RL

An implementer shows the extent of compliance to the Recommended Standard by completing the RL; that is, the state of compliance with all mandatory requirements and the options supported are shown. The resulting completed RL is called an ICS. The implementer shall complete the RL by entering appropriate responses in the support or values supported column, using the notation described in A1.2. 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 X*i*, where *i* is a unique identifier, to an accompanying rationale for the noncompliance.

A2 ICS PROFORMA FOR BPSEC FOR CCSDS

A2.1 GENERAL INFORMATION

A2.1.1 Identification of ICS

Date of Statement (DD/MM/YYYY)	
ICS serial number	
System Conformance statement cross-reference	

A2.1.2 Identification of Implementation Under Test

Implementation Name	
Implementation Version	
Special Configuration	
Other Information	

A2.1.3 Identification of Supplier

Supplier	
Contact Point for Queries	
Implementation Name(s) and Versions	
Other information necessary for full identification, for example, name(s) and version(s) for machines and/or operating systems; System Name(s)	

A2.1.4 Identification of Specification

CCSDS 734.5-R-2	
Have any exceptions been required? NOTE – A YES answer means that the implementation does not conform to the Recommended Standard. Non-supported mandatory capabilities are to be identified in the ICS, with an explanation of why the implementation is non-conforming.	Yes [ ] No [ ]

A2.2 REQUIREMENTS LIST

Item	Description	Reference	Status	Support
1	The same security service MUST NOT be applied to a security target more than once in a bundle.	RFC 9172 Section 3.2	M	
2	A single security block MAY represent multiple security operations.	RFC 9172 Section 3.3	O	
3	A security target in a security block MUST be represented as the block number of the target block.	RFC 9172 Section 3.4	M	
4	The fields of the ASB SHALL be as specified in RFC 9172, Section 3.6.	RFC 9172 Section 3.6	M	
5	The block type code value of a BIB SHALL be as specified in Section 11.1 of RFC 9172.	RFC 9172 Section 3.7	M	
6	The block-type-specific data field of a BIB SHALL follow the structure of the ASB.	RFC 9172 Section 3.7	M	

Item	Description	Reference	Status	Support
7	A security target listed in the Security Targets field of a BIB MUST NOT reference a security block defined in RFC 9172 (e.g., a BIB or a BCB).	RFC 9172 Section 3.7	M	
8	The security context MUST utilize an authentication mechanism or an error detection mechanism.	RFC 9172 Section 3.7	M	
9	The block type code value of a BCB SHALL be as specified in Section 11.1 of RFC 9172	RFC 9172 Section 3.8	M	
10	BCBs MUST have the ‘Block must be replicated in every fragment’ flag set if one of the targets is the payload block.	RFC 9172 Section 3.8	M	
11	BCBs MUST NOT have the ‘Block must be removed from bundle if it cannot be processed’ flag set.	RFC 9172 Section 3.8	M	
12	The block-type-specific data fields of a BCB SHALL follow the structure of the ASB.	RFC 9172 Section 3.8	M	
13	A security target listed in the Security Targets field of a BCB SHALL be able to reference the payload block, a non-security extension block, or a BIB.	RFC 9172 Section 3.8	M	
14	A BCB MUST NOT include another BCB as a security target.	RFC 9172 Section 3.8	M	
15	A BCB MUST NOT target the primary block.	RFC 9172 Section 3.8	M	
16	A BCB MUST NOT target a BIB unless it shares a security target with that BIB.	RFC 9172 Section 3.8	M	
17	BCBs MUST utilize a confidentiality cipher that provides AEAD.	RFC 9172 Section 3.8	M	
18	Additional information created by a cipher suite MAY be placed either in a security result field or in the generated ciphertext.	RFC 9172 Section 3.8	O	
19	When a BCB is applied, the security target body data SHALL be encrypted ‘in-place’.	RFC 9172 Section 3.8	M	
20	When adding a BCB to a bundle, if some (or all) of the security targets of the BCB match all of the security targets of an existing BIB, then the existing BIB MUST also be encrypted.	RFC 9172 Section 3.9	M	

Item	Description	Reference	Status	Support
21	When adding a BCB to a bundle, if some (or all) of the security targets of the BCB match some (but not all) of the security targets of a BIB, then that BIB MUST be altered in the following way. Any security results in the BIB associated with the BCB security targets MUST be removed from the BIB and placed in a new BIB. This newly created BIB MUST then be encrypted.	RFC 9172 Section 3.9	M	
22	A BIB MUST NOT be added for a security target that is already the security target of a BCB	RFC 9172 Section 3.9	M	
23	A BIB integrity value MUST NOT be checked if the BIB is the security target of an existing BCB.	RFC 9172 Section 3.9	M	
24	A BIB integrity value MUST NOT be checked if the security target associated with that value is also the security target of a BCB.	RFC 9172 Section 3.9	M	
25	A BIB MUST NOT have a BCB as its security target.	RFC 9172 Section 3.9	M	
26	The canonical form of the primary block is as specified in reference [2] with the following constraint: CBOR values from the primary block MUST be canonicalized using the rules for Deterministically Encoded CBOR, as specified in [9].	RFC 9172 Section 4	M	

Item	Description	Reference	Status	Support
27	All non-primary blocks share the same block structure and are canonicalized as specified in reference [2] with the following constraints. CBOR values from the non-primary block MUST be canonicalized using the rules for Deterministically Encoded CBOR, as specified in [9]. Only the block-type-specific data field may be provided to a cipher suite for encryption as part of a confidentiality security service. Fields other than the block-type-specific data within a non-primary block MUST NOT be encrypted or decrypted and MUST NOT be included in the canonical form used by the cipher suite for encryption and decryption	RFC 9172 Section 4	M	
28	An integrity-protection mechanism MAY be applied to fields other than the block-type-specific data within a non-primary block as supported by the security context.	RFC 9172 Section 4	O	
29	Reserved and unassigned flags in the block processing control flags field MUST be set to 0 in a canonical form.	RFC 9172 Section 4	M	
30	If a received bundle contains a BCB, the receiving node MUST determine whether it is the security acceptor for any of the security operations in the BCB.	RFC 9172 Section 5.1.1	M	
31	If the receiving node is the security acceptor for any of the security operations in the BCB, the node MUST process those operations and remove any operation-specific information from the BCB prior to delivering data to an application at the node or forwarding the bundle.	RFC 9172 Section 5.1.1	M	
32	If processing a security operation fails, the target SHALL be processed according to the security policy.	RFC 9172 Section 5.1.1	M	

Item	Description	Reference	Status	Support
33	If processing a security operation fails, a bundle status report indicating the failure MAY be generated.	RFC 9172 Section 5.1.1	O	
34	When all security operations for a BCB have been removed from the BCB, the BCB MUST be removed from the bundle.	RFC 9172 Section 5.1.1	M	
35	If the receiving node is the destination of the bundle, the node MUST decrypt any BCBs remaining in the bundle.	RFC 9172 Section 5.1.1	M	
36	If the receiving node is not the destination of the bundle, the node MUST process the BCB if directed to do so as a matter of security policy.	RFC 9172 Section 5.1.1	M	
37	If the security policy of a node specifies that a node should have applied confidentiality to a specific security target and no such BCB is present in the bundle, then the node MUST process this security target in accordance with the security policy.	RFC 9172 Section 5.1.1	M	
38	If the payload block is removed as a result of security processing, the bundle MUST be discarded.	RFC 9172 Section 5.1.1	M	
39	If an encrypted payload block cannot be decrypted (i.e., the ciphertext cannot be authenticated), then the bundle MUST be discarded and processed no further.	RFC 9172 Section 5.1.1	M	
40	If an encrypted security target other than the payload block cannot be decrypted, then the associated security target and all security blocks associated with that target MUST be discarded and processed no further.	RFC 9172 Section 5.1.1	M	
41	As a result of security operations, if a block is deleted from a bundle or if a bundle is dropped, requested status reports (see reference [2]) MAY be generated to reflect bundle or block deletion.	RFC 9172 Section 5.1.1	O	

Item	Description	Reference	Status	Support
42	When a BCB is decrypted, the recovered plaintext for each security target MUST replace the ciphertext in each of the security targets’; block-type-specific data fields.	RFC 9172 Section 5.1.1	M	
43	If the plaintext is of a different size than the ciphertext, the framing of the CBOR byte string of this field MUST be updated to ensure this field remains a valid CBOR byte string.	RFC 9172 Section 5.1.1	M	
44	If a BCB contains multiple security operations, each operation processed by the node MUST be treated as if the security operation has been represented by a single BCB with a single security operation for the purposes of report generation and policy processing.	RFC 9172 Section 5.1.1	M	
45	If a received bundle contains a BIB, the receiving node MUST determine whether it is the security acceptor for any of the security operations in the BIB.	RFC 9172 Section 5.1.2	M	
46	If the receiving node is the security acceptor for any security operations in a BIB, the node MUST process those operations and remove any operation-specific information from the BIB prior to delivering data to an application at the node or forwarding the bundle.	RFC 9172 Section 5.1.2	M	
47	If processing a security operation fails, the target SHALL be processed according to the security policy.	RFC 9172 Section 5.1.2	M	
48	If processing a security operation fails, a bundle status report indicating the failure MAY be generated.	RFC 9172 Section 5.1.2	O	
49	When all security operations for a BIB have been removed from the BIB, the BIB MUST be removed from the bundle.	RFC 9172 Section 5.1.2	M	
50	A BIB MUST NOT be processed if the security target of the BIB is also the security target of a BCB in the bundle.	RFC 9172 Section 5.1.2	M	

Item	Description	Reference	Status	Support
51	If the security policy of a node specifies that a node should have applied integrity to a specific security target and no such BIB is present in the bundle, then the node MUST process this security target in accordance with the security policy.	RFC 9172 Section 5.1.2	M	
52	If the security policy of a node specifies that a node should have applied integrity to a specific security target and no such BIB is present in the bundle, it is RECOMMENDED that the node remove the security target from the bundle if the security target is not the payload or primary block.	RFC 9172 Section 5.1.2	O	
53	If a the security target is the payload or primary block, the bundle MAY be discarded. This action can occur at any node that has the ability to verify an integrity signature, not just the bundle destination.	RFC 9172 Section 5.1.2	O	
54	If a receiving node is not the security acceptor of a security operation in a BIB, it MAY attempt to verify the security operation anyway to prevent forwarding corrupt data.	RFC 9172 Section 5.1.2	O	
55	If a verification security operation fails, the node SHALL process the security target in accordance with local security policy.	RFC 9172 Section 5.1.2	M	
56	If a payload integrity check fails at a waypoint, it is RECOMMENDED that it be processed in the same way as a failure of a payload integrity check at the bundle destination.	RFC 9172 Section 5.1.2	O	
57	If a BIB integrity check passes at waypoint, the node MUST NOT remove the security operation from the BIB prior to forwarding.	RFC 9172 Section 5.1.2	M	

Item	Description	Reference	Status	Support
58	If a BIB contains multiple security operations, each operation processed by the node MUST be treated as if the security operation has been represented by a single BIB with a single security operation for the purposes of report generation and policy processing.	RFC 9172 Section 5.1.2	M	
59	If it is necessary for a node to fragment a bundle payload, and security services have been applied to that bundle, the fragmentation rules described in reference [2] MUST be followed.	RFC 9172 Section 5.2	M	
60	A BCB or BIB MUST NOT be added to a bundle if the ‘Bundle is a fragment’ flag is set in the bundle processing control flags field.	RFC 9172 Section 5.2	M	

ANNEX B

CCSDS PROFILE OF DEFAULT IANA SECURITY CONTEXTS

(NORMATIVE)

B1 OVERVIEW

A default set of BPSec security contexts that can be used for integrity and confidentiality security operations has been defined in RFC 9173 (reference [8]).

B2 CCSDS USE OF SECURITY CONTEXTS FROM RFC 9173

B2.1 SECURITY CONTEXTS FOR INTEROPERABILITY TESTING

For the purposes of CCSDS interoperability testing, implementations shall use security contexts defined in reference [8].

B2.2 MISSION USE OF SECURITY CONTEXTS FROM RFC 9173

Missions are not required to implement the security contexts defined in reference [8].

NOTE – CCSDS intends to define a set of security contexts for space missions; those documents will state whether implementation of those contexts by missions is mandatory or not.

ANNEX C

SECURITY, SANA, AND PATENT CONSIDERATIONS

(INFORMATIVE)

C1 SECURITY CONSIDERATIONS

C1.1 SECURITY CONCERNS WITH RESPECT TO THE CCSDS DOCUMENT

C1.1.1 Data Privacy

Malicious nodes may examine the contents of a bundle and attempt to recover protected data or cryptographic keying material from the blocks contained within. The BPSec BCB protects against this action by enciphering the contents of its target block thereby providing data privacy via a confidentiality service.

Malicious nodes may continue to examine bundles offline in an attempt to recover encrypted data. The security contexts used by the BCB should be selected to provide suitable protection over the useful lifetime of the information being protected.

To provide verifiable integrity checks, the security contexts used by the BCB should utilize encryption schemes that are ‘indistinguishable under adaptive chosen ciphertext attack’ (IND-CCA2) secure. Such schemes guard against signature substitution.

Irrespective of whether BPSec is used, traffic analysis will be possible.

C1.1.2 Data Integrity

Malicious nodes may modify blocks within a bundle, to include replacing existing blocks, adding new blocks, and removing blocks. BPSec can detect these activities using both the BIB and BCB blocks, depending on whether plaintext or ciphertext integrity is required.

The integrity mechanisms used by the BIB and BCB should be strong against collision attacks and malicious nodes should be prevented from accessing the cryptographic material used by the security source. If these conditions can be met, malicious nodes will be unable to modify the target block without being detected.

BPSec does not support an in-bundle mechanism to detect (or correct) cases where a malicious node removes a block from a bundle. If a target block is removed, then any security block associated with that target block will fail to validate. If a security block is removed from the bundle, some other policy must be in place at the security verifier or security acceptor to note that a security block was expected to exist in the bundle.

The implementation of BPSec must be combined with a policy configuration at BPAs which describes the expected and required security operations that must be applied to, or expected to be present for, blocks in bundles processed by the BPA.

C1.1.3 Control of Access to Resources

Resource access controls are not directly addressed by this specification.

C1.1.4 Availability of Resources

No mechanisms are defined in this specification to verify or assist with the verification of availability of resources.

C1.1.5 Auditing of Resource Usage

No mechanisms are defined in this specification to audit or assist with the auditing of resource usage by the protocol.

C1.2 POTENTIAL THREATS AND ATTACK SCENARIOS

Malicious actors might attempt to disrupt network operations in a number of ways, including but not limited to:

- injecting bundles with malicious or intentionally incorrect information in their payloads;
- injecting bundles with intentionally malformed structure;
- replaying previously transmitted bundles;
- adding, removing, or modifying blocks to/from/in bundles;
- flooding the network with garbage traffic (denial-of-service attack).

This specification provides protocol mechanisms to defend against information-based attacks (replay, impersonation of senders, and denial-of-service attacks). To be effective against these attacks, the protocol mechanisms described here need to be combined with security policy that states how to react to certain security events. Security policy will be discussed in a separate document.

(See reference [E1] for a fuller description of potential threats against space missions.)

C1.3 CONSEQUENCES OF NOT APPLYING SECURITY TO THE TECHNOLOGY

If BPSec is not used, bundle delivery must rely on security measures provided by the convergence layer adapter(s) and/or lower layers. For space applications these alternative security measures may be non-existent or shared across a large group of applications and application domains.

The consequence of not using BPSec is that bundle exchange has to rely on security mechanisms either at the Data Link Layer or the Application Layer. Data Link Layer security might be present on some links and not on others.

C2 SANA CONSIDERATIONS

In addition to the required SANA action identified in 3.5.1, SANA is requested to update the CCSDS Abbreviations Registry (OID: 1.3.112.4.14) with the terms found in annex F.

C3 PATENT CONSIDERATIONS

There are no known patents covering Bundle Protocol Security as described in this document and its normative references.

ANNEX D

CONSIDERATIONS FOR BUNDLE PROTOCOL SECURITY MANAGED INFORMATION

(INFORMATIVE)

D1 OVERVIEW

Managed parameters are those parameters provided by management rather than being included in the on-the-wire BPSec protocol. Because BP bundles may be stored in a network for extended periods of time, parameters that identify the state of the network must be provided by management as part of the policy or technical configuration of BPAs in the network.

This annex contains a set of suggested management parameters for BPSec implementations to support. A future normative CCSDS document will provide a BPSec application data model in the context of the BP network management framework currently under development.

D2 MANAGED PARAMETERS

The managed parameters listed in table D-1 are relevant to the overall configuration of a BPSec implementation.

NOTES

1 The detailed specification of some managed parameters must occur in the context of a specific security context. Such detail is not provided here.

2 These parameters are defined in an abstract sense, and are not intended to imply any particular implementation of a management system.

Table D-1: Recommended BPSec Managed Parameters

Bundle Security Roles		What security roles does this node implement, for example: Security Source Security Verifier Security Acceptor	
Supported cipher suites		Cipher suites supported by this node	
Expected security blocks		Security blocks expected to be present in incoming bundles	
Cipher suite keys		Key material for the cipher suites implemented by this node	

D3 BPSEC APPLICATION DATA MODEL

The information elements described in table D-2 below are relevant to the operational state of a BPSec instance. How such values are managed and/or requested/conveyed by any particular network management system is not defined here.

Table D-2: Recommended BPSec Information Elements

Name	Type	Parameters	Description
num_good_tx_sec_blk	Unsigned integer	Block type (BIB, BCB, Both)	Total successfully transmitted security blocks
num_bad_tx_sec_blk	Unsigned integer	Block type (BIB, BCB, Both)	Total unsuccessfully transmitted security blocks
num_good_rx_sec_blk	Unsigned integer	Block type (BIB, BCB, Both)	Total successfully received security blocks
num_bad_rx_sec_blk	Unsigned integer	Block type (BIB, BCB, Both)	Total unsuccessfully received security blocks
num_missing_rx_sec_blks	Unsigned integer	Block type (BIB, BCB, Both)	Total missing-on-RX security blocks
num_fwd_sec_blks	Unsigned integer	Block type (BIB, BCB, Both)	Total forwarded security blocks
num_good_tx_sec_bytes	Unsigned integer	Block type (BIB, BCB, Both)	Total successfully transmitted security blocks
num_bad_tx_sec_bytes	Unsigned integer	Block type (BIB, BCB, Both)	Total unsuccessfully transmitted security block bytes
num_good_rx_sec_bytes	Unsigned integer	Block type (BIB, BCB, Both)	Total successfully received security block bytes
num_bad_rx_sec_bytes	Unsigned integer	Block type (BIB, BCB, Both)	Total unsuccessfully received security block bytes
num_missing_rx_sec_bytes	Unsigned integer	Block type (BIB, BCB, Both)	Total missing-on-Rx security block bytes
num_fwd_sec_bytes	Unsigned integer		Total forwarded security block bytes
last_update_src	Time	Security source	Last BPSEC update
last_reset	Time	Security source	Last reset

D4 SECURITY CONTEXT MANAGED PARAMETERS

Future normative books on security contexts will provide the managed parameters for those specific security context definitions.

NOTE – Security context managed parameters are those parameters associated with the security context of a BPSec block, but managed and provided by the BPAs comprising the security source, security verifier (as appropriate) and security acceptor of the security block as part of their local security context parameters.

ANNEX E

INFORMATIVE REFERENCES

(INFORMATIVE)

[E1] *Security Threats against Space Missions*. Issue 3. Report Concerning Space Data System Standards (Green Book), CCSDS 350.1-G-3. Washington, D.C.: CCSDS, February 2022.

[E2] *The Application of Security to CCSDS Protocols*. Issue 3. Report Concerning Space Data System Standards (Green Book), CCSDS 350.0-G-3. Washington, D.C.: CCSDS, March 2019.

[E3] *CCSDS Cryptographic Algorithms*. Issue 2. Recommendation for Space Data System Standards (Blue Book), CCSDS 352.0-B-2. Washington, D.C.: CCSDS, August 2019.

ANNEX F

ABBREVIATIONS

(INFORMATIVE)

Term	Meaning
AAD	Additional Authenticated Data
AEAD	Authenticated Encryption with Associated Data
BCB	Block confidentiality block
BIB	Block integrity block
BN	Bundle Node
BP	Bundle Protocol
BPA	Bundle Protocol agent
BPSec	Bundle Protocol Security
DTN	Delay-Tolerant Networking
EID	endpoint identifier
IANA	Internet Assigned Numbers Authority
ICS	Implementation Conformance Statement
ID	Identifier
IETF	Internet Engineering Task Force
IP	Internet Protocol
IV	initialization vector
OP	Operation
OPA	on path attacker
OSI	Open Systems Interconnect
RFC	Request for Comments
RL	requirements list
SANA	Space Assigned Numbers Authority
SCI	security context identifier