The Consultative Committee for Space Data Systems

Research and Development for
Space Data System Standards

CUSTODY TRANSFER AND COMPRESSED BUNDLE STATUS REPORTING

EXPERIMENTAL SPECIFICATION

CCSDS 734.6-O-1

ORANGE BOOK

June 2026

The Consultative Committee for Space Data Systems

Research and Development for
Space Data System Standards

CUSTODY TRANSFER AND COMPRESSED BUNDLE STATUS REPORTING

EXPERIMENTAL SPECIFICATION

CCSDS 734.6-O-1

ORANGE BOOK

June 2026

AUTHORITY

Issue:	Experimental Specification, Issue 1
Date:	June 2026
Location:	Not Applicable

This document has been approved for publication by the Consultative Committee for Space Data Systems (CCSDS). 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).

This document is published and maintained by:

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

FOREWORD

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

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

https://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

- 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.
- State Space Corporation (Roscosmos)/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.
- Taiwan Space Agency (TASA)/ Taiwan.
- 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.
- SSC Space/Sweden.
- Swiss Space Office (SSO)/Switzerland.
- United States Geological Survey (USGS)/USA.

PREFACE

This document is a CCSDS Experimental Specification. Its Experimental status indicates that it is part of a research or development effort based on prospective requirements, and as such it is not considered a Standards Track document. Experimental Specifications are intended to demonstrate technical feasibility in anticipation of a 'hard' requirement that has not yet emerged. Experimental work may be rapidly transferred onto the Standards Track should a hard requirement emerge in the future.

DOCUMENT CONTROL

Document	Title and Issue	Date	Status
CCSDS 734.6-O-1	Custody Transfer and Compressed Bundle Status Reporting, Experimental Specification, Issue 1	June 2026	Original issue

CONTENTS

1 INTRODUCTION

1.1 PURPOSE

The purpose of this document is to define Custody Transfer (CT) and Compressed Bundle Status Reporting (CBSR) extensions for Bundle Protocol version 7 (BPv7).

1.2 SCOPE

This Experimental Specification defines necessary structures and procedures required for Custody Transfer (CT) and CBSR for BPv7. It recommends implementation mechanics and describes use cases enabled by these extensions.

1.3 APPLICABILITY

The specification is applicable to Disruption Tolerant Networks (DTN) based on BPv7 where CT or CBSR are not part of the core specification. They do not require implementation on all DTN nodes as these new extension blocks can be forwarded transparently. However, non-supporting nodes reduce efficiency, which may lead to unintended behavior.

1.4 RATIONALE

The regular Bundle Status Reporting (BSR) defined in the BPv7 specification is generally discouraged due to its impact on bandwidth: each requested report results in a new bundle. Compressed reporting solves this by reporting on multiple bundles in a single report.

CT was supported in Bundle Protocol Version 6 (BPv6) [E1] but removed from version 7. Nevertheless, many missions consider it useful for optimizing bundle transfer by shifting bundle responsibility between nodes. However, CT can be complicated by reforwarding timer estimations and custody acceptance timing. This experimental specification acknowledges these issues but does not address large-scale, open DTNs. Instead, it provides flexibility to address these complications in smaller, tightly managed networks expected in near-term deployments.

CT and CBSR use the same underlying approach for bundle sequence identification. The approach based on sequence numbers provides an efficient way to refer to sets of bundles and may apply beyond this specification.

1.5 DOCUMENT STRUCTURE

This Experimental Specification is organized as follows:

- Section 2 provides an overview of the approach and the underlying concepts.
- Section 3 specifies the general concepts for bundle sequence identification.
- Section 4 specifies CT in terms of the extension block, custody signal, and associated procedures.

– Section 5 specifies CBSR in terms of the extension block, reporting signal, and associated behavior.

– Section 6 discusses how end-to-end services can be realized based on CBSR.

– Annex A provides the Protocol Implementation Conformance Statement (PICS).

– Annex B contains Security, SANA/IANA and patent considerations.

– Annex C describes prototyping activities supporting this experimental specification.

– Annex D contains Concise Data Definitions Language (CDDL) expressions for the extension blocks and administrative records defined in this specification.

– Annex E provides informative references.

– Annex F provides a list of abbreviations and acronyms.

1.6 REFERENCES

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

[1] CCSDS *Bundle Protocol Specification*. Issue 1. CCSDS Experimental Specification (Orange Book), CCSDS 734.20-O-1. Washington, D.C.: CCSDS, April 2025.

[2] Burleigh, S., Fall, K., and Birrane, E. III. RFC 9171: *Bundle Protocol Version 7*. IETF, 2022.

2 OVERVIEW

This specification defines the following constructs:

- **CT** is driven by the Custody Transfer Extension Block (**CTEB**), inserted into bundles to request custody. Nodes respond with a Compressed Custody Signal (**CCS**), an administrative record that signals the disposition of multiple bundles in a single transmission. The disposition of a single bundle can be acceptance or rejection, but the specification is extensible.
- **CBSR** is driven by the Compressed Reporting Extension Block (**CREB**), inserted into bundles to provide information about bundle sequences and, optionally, to request status reports. Nodes respond with a Compressed Reporting Signal (**CRS**), which is an administrative record that reports on the sequence and, when requested, the status of multiple bundles in a single transmission.

Both processes rely on a common bundle sequence numbering mechanism, described below, but maintain separate counters. The processes are independent but can be combined to aid both hop-by-hop and end-to-end reliability.

2.1 BUNDLE SEQUENCE NUMBERS

Bundle sequence numbers (BSN) are generated by bundle sequence counters (BSC) that are incremented to a maximum value and included in the proposed extension blocks. A single node can create multiple sequences by using multiple BSCs, e.g., one per destination. These counters are identified either by a destination Endpoint ID (EID) or bundle sequence ID (BSID), a positive integer.

2.2 CUSTODY TRANSFER

A node requests CT by inserting a CTEB into a bundle. A receiving node becomes the bundle's custodian by sending an acceptance CCS to the current custodian identified in the CTEB. A custodian stores and re-forwards a bundle until it receives an acceptance signal or the bundle expires. The acceptance signal uses bundle sequences to indicate custody acceptance or refusal for multiple bundles. A bundle sequence refers to intervals of sequence numbers and the node that assigned them, extracted from the CTEB of received bundles. A custodian receiving a CCS uses bundle sequences to identify which bundles it no longer needs to store and re-forward.

2.3 COMPRESSED BUNDLE STATUS REPORTING

CBSR uses a CREB to provide sequence numbers and request bundle status reports such as reception, deletion, or delivery. Status reports are delivered by a CRS. A CREB is inserted into a bundle to provide sequence numbering and request reporting on the status of that bundle as it traverses the network. The receiving node sends this status information via a CRS either to the requester or to a report-to node explicitly specified in CREB. CBSR enables additional services based on the information provided in the extension block and reporting signals, such as reliable end-to-end or in-sequence delivery of bundles.

2.4 BUNDLE RE-FORWARDING

Unlike BPv6, the CT mechanism defined in this specification does not prescribe a specific trigger for initiating bundle re-forwarding. Depending on the implementation and specific use cases, re-transmission can be based on received custody signals, explicit commands, reliable convergence layers, or timers (as in BPv6 custody). These mechanisms also apply to CBSR to enable reliable bundle delivery. CT can be combined with CSR to provide both efficiency and full reliability. CT enables efficient hop-by-hop retransmission between custodians with compressed delivery reporting, but cannot guarantee end-to-end reliability if bundles are lost at a custodial node due to storage constraints or other problems. CSR provides end-to-end delivery confirmation to address this limitation.

2.5 DISCUSSION: FRAGMENTATION

Bundle fragmentation is problematic for bundles that request custody or compressed reporting because the fragments can no longer be uniquely identified by the combination of BSN, BSID, and administrative endpoint ID (AEID). Currently, no mechanism for bundle reassembly is defined or even required by RFC 9171 [2], which only addresses Application Data Unit reassembly.

Therefore, fragmentation of bundles containing any of the specified extension blocks should be avoided. If possible, this should be enforced at bundle creation by setting the ‘Bundle must not be fragmented’ in the bundle processing control flag. Since this flag can only be set at a bundle’s source, it is not always possible to guarantee that it is set when an intermediate node adds an extension block.

In addition, intermediate nodes that do not implement this specification may inadvertently fragment a bundle. Thus, if the bundle is a fragment, the current specification prohibits adding or processing any of the specified extension blocks. Conforming implementations also shall not fragment any bundle containing these extension blocks. Due to the recently discovered issues with bundle fragmentation in RFC 9171 [2], errata have been reported, and bundle fragmentation is expected to be deprecated in favor of convergence layer segmentation.

3 BUNDLE SEQUENCE IDENTIFICATION

3.1 INTRODUCTION

This section defines an efficient way to refer to sequences of bundles using numbers provided by counters. These BSN are used in the extension blocks and administrative records defined in this specification. Sequence numbering enables efficient reference to multiple bundles in a series and supports gap detection. However, in many use cases a single counter per bundle node is not sufficient. Therefore, multiple sequences can be used per bundle node, with each sequence identified by a BSID or destination EID.

3.2 BUNDLE IDENTIFICATION

Bundle identification mechanisms enable references to specific bundles in extension blocks and administrative records, supporting services such as gap detection and in-sequence delivery.

3.2.1 A BSC shall generate a sequence of positive integer values which start at zero and increase by one each time its current value is included into an extension block as a BSN.

3.2.2 A bundle node may maintain multiple counters for different purposes. Each counter shall be identified by a BSID (positive integer) or destination EID.

NOTE – The assignment of BSIDs is determined by mission or network design to optimize for different use cases. For example, they may be set based on a service number (if using the InterPlanetary Network [IPN] naming scheme) or the next-hop node ID.

3.2.3 Separate counters must be maintained for CT and CBSR.

3.2.4 The BSID ‘0’ shall be reserved to indicate that different counters are maintained for each destination EID.

NOTE – When the BSID is ‘0’, the applicable counter is identified by the bundle's destination EID.

3.2.5 When a BSN is included in an extension block, it shall take the current value of a BSC, which is then increased by one.

3.2.6 If a BSN is included in an extension block, the related BSID shall be included as well if non-zero.

3.2.7 The block source AEID shall be an EID of the administrative element of the Bundle Protocol Agent inserting an extension block with BSN.

3.2.8 The same AEID shall always be used for the same BSC if generated BSN are inserted in an extension block.

NOTES

1 The AEID identifies the block source node. It may be expressed in different naming schemes (e.g., IPN or DTN) or forms within a naming scheme (e.g., the 2-tuple or the 3-tuple form in the IPN naming scheme). It can therefore be difficult for receiving and processing nodes to recognize that different AEIDs refer to the same node.

2 This requirement also applies when the AEID is given implicitly by the bundle source node ID in the primary header.

3.2.9 If a BSN is included in an extension block, an AEID shall be included as well unless it is the same as the source node ID in the primary block.

3.2.10 If a counter reaches a maximum value of 2^8, 2^{16}, 2^{32} or 2^{64}, it may be reset to zero.

NOTES

1 Having defined maximum values allows processing nodes to detect possible sequence counter wraparounds.

2 The maximum value should be managed in the node's Management Information Base (MIB).

3.2.11 The maximum value of a BSC must be set high enough to prevent BSN reuse in administrative records or during the lifetime of a bundle with an extension block carrying that BSN.

NOTES

1 While maximum values might be straightforward in limited mission scenarios, for larger and more heterogeneous networks they can be based on internal policies defining maximum bundle lifetimes and estimated traffic volumes.

2 Bundles are uniquely identified during their lifetime in a given context (such as CT or CBSR) by the combination of their block source AEID, BSN, and:

   a. Destination EID if BSID = '0';

   b. BSID if BSID ≠ '0'.

3.3 SEQUENCES AND COLLECTIONS

Bundle sequences and collections identify multiple bundles using the mechanisms described above and are typically used in administrative records.

3.3.1 A bundle **sequence** shall be a Concise Binary Object Representation (CBOR) definite-length array of three or four items:

1 **identifier**, either:

   a. BSID (CBOR unsigned integer) as defined in 3.2; or

   b. Destination EID (CBOR encoded endpoint ID);

2 **first sequence number** (CBOR unsigned integer), which is the starting BSN of the first subsequence in the range of bundles to which the sequence is referring;

3 **range**, which is one of:

   a. sequence range as defined in 3.3.2;

   b. CBOR unsigned integer representing the length of the sequence if there is only one to include;

4 **block source AEID** (CBOR encoded endpoint ID), if required.

NOTES

1 The range specifies which subsequence of bundles are included in and excluded from the report. The range field alternatingly encodes the lengths of both included and excluded sub sequences.

2 The extension block definition or the administrative records explicitly state whether a block source AEID is required. It is omitted when the sequence receiver is the node that provided the sequence number, since that node was the source of the extension block. For example, custody signals (as defined in Section 4) never carry the block source AEID.

3 Later versions of this specification may include additional optional elements, such as status report reason codes as registered in the IANA 'Bundle Status Report Reason Codes' subregistry of the 'Bundle Protocol' registry or time spans to which the reports relate.

3.3.2 A sequence **range** shall be a CBOR definite-length array with uneven length of unsigned integers that specify the varying lengths of alternating included and excluded subsequences:

– 1st *included* subsequence length;

– 1st excluded subsequence length;

– 2nd *included* subsequence length;

– 2nd excluded subsequence length;

– 3rd *included* subsequence length, etc.

NOTE – Bundle sequences report on subsequences in the overall range of 'First Sequence Number – Total Sequence Length-1', where the Total Sequence Length is not part of a bundle sequence, but the sum of the lengths of all included and excluded subsequences in that range.

3.3.3 A bundle sequence **collection** shall be a CBOR definite-length array of bundle sequence(s), which may be empty (e.g., periodically generated signals).

NOTE – Unlike bundle sequences, collections do not need to share the same BSID or destination EID.

3.4 BUNDLE FRAGMENTATION

3.4.1 Bundles containing any extension blocks from this specification shall not be fragmented.

NOTE – The reporting mechanism in this specification cannot report on individual fragments. To prevent fragmentation by non-compliant intermediate nodes, it is recommended to set the 'Bundle Must Not be Fragmented' flag at the bundle's source node.

3.4.2 Extension blocks defined in this specification shall only be added to bundles that are not fragments.

3.4.3 Specified extension blocks shall not be processed if the bundle is a fragment.

NOTE – The extension blocks specified in this specification may be present in fragments if intermediate nodes that do not comply with this specification fragment the bundle.

4 CUSTODY TRANSFER

This section defines the CTEB and CCS formats and the procedures governing custody transfer between nodes. This specification does not prescribe specific triggers for bundle re-forwarding, allowing implementations to adapt CT to their specific network constraints.

4.1 CUSTODY TRANSFER EXTENSION BLOCK

4.1.1 A Custody Transfer Extension block (CTEB) shall follow the canonical bundle block format according to RFC 9171 [2] section 4.3.2.

4.1.2 The Bundle Block Type code shall be 13.

4.1.3 A bundle shall never contain more than one CTEB.

4.1.4 The block-type-specific data shall be a definite-length CBOR byte string containing a definite-length CBOR array of three elements, according to 3.2:

- BSN (CBOR unsigned integer);
- BSID (CBOR unsigned integer);
- block source AEID (endpoint).

NOTE – The BSID may be '0,' indicating that sequence numbers are provided according to the destination

4.2 COMPRESSED CUSTODY SIGNAL

4.2.1 A CCS shall be an administrative record according to RFC 9171 [2] section 6.1.

4.2.2 The Bundle Administrative Record Type code shall be 13.

4.2.3 A CCS shall contain a CBOR map composed of key/value pairs as record content:

- **Disposition Code**: a key of the map shall be the custody signal disposition code:
  - 1 – *Acceptance* with no further information: an unsigned CBOR integer (values above 1 reserved for future use);
  - -1 – *Rejection* with no further information: a negative CBOR integer (values below -1 reserved for future use).
- **Bundle Sequence Collection**: as defined in 3.2.2 and subject to the constraints defined in 4.2.4.

NOTE – Later versions of this specification may define additional positive values for custody acceptance (e.g., 'custody acceptance – duplicate reception') or negative values for custody rejection (e.g., 'custody rejection – bundle forwarded'). To maintain compatibility with future extensions, implementations may find it useful to test positive or negative values in general and not only 1 or -1.

4.2.4 The bundle sequences in sequence collections (4.2.3) shall never contain a block source AEID.

NOTE – The CCS is sent to the AEID contained in the CTEB, so the receiving administrative element is the one that provided the BSN.

4.3 CUSTODY PROCEDURES

4.3.1 Any node can request CT by inserting a CTEB into a bundle.

NOTE – The CT requesting node does not have to be the source node.

4.3.2 A node that is not the destination of a received bundle shall decide whether to accept or refuse its custody upon receiving a CTEB.

NOTE – The custody decision will depend on mission or local network policies and other constraints. A node may take custody of a bundle when there is reasonable likelihood that it can be forwarded to a next custodian successfully, based on a bundle lifetime, upcoming contacts, past experiences, etc. At a minimum, the node must be capable of storing the bundle for eventual re-transmission. The conditions for accepting or rejecting bundle custody should be clearly documented.

4.3.3 When a node takes custody, it shall store the required information for creating an acceptance CCS and delete the current CTEB.

4.3.4 Unless the bundle will be reliably forwarded to the bundle's destination, a node taking custody shall:

- add a new CTEB requesting custody transfer with its own AEID as the block source AEID before forwarding the bundle;
- store the bundle until a custody acceptance signal is received or the bundle lifetime has expired.

NOTES

1 Reliable forwarding to bundle destination can typically only be determined when the exact route and convergence layer adapters (CLA) are known (e.g., direct forwarding via Transmission Control Protocol convergence layer). While CT is not mandatory in such cases, a CTEB can be added and the bundle retained until an acceptance signal is received for additional delivery assurance.

2 To get informed about any bundle deletion that occurred after custody acceptance, compressed bundle deletion reports can be requested.

4.3.5 The destination of a bundle with a CTEB shall not deliver the bundle without accepting custody.

4.3.6 If the custodian detects a duplicated bundle based on the sequence number in the CTEB, it must (re-)send the acceptance signal and discard the duplicate.

NOTE – A node may maintain a list of bundles for which it has accepted and transferred custody. This enables the node to suppress delayed re-forwarded bundles by resending an acceptance signal and discarding the bundle.

4.3.7 If a node refuses custody, it should store all required information for creating a refusal CCS.

NOTE – A node refusing custody may delete or forward the bundle. When forwarding without taking custody, the node may not store refusal information and thus will not generate a refusal signal. Combining CT with compressed reporting (as defined in Section 5) provides additional tracking of bundle reception, deletion, and forwarding.

4.3.8 A node shall send a CCS based on the stored information (per MIB configuration) or external events.

NOTE – CCS transmission timing is an implementation matter that can be based on:

a) periodic timers (when CTEB requests exist);

b) size constraints (bundle size or count), supplemented by a timer to prevent indefinite delays when the size limit is not reached but there are no additional bundles to report;

c) external events (link establishment, explicit command).

4.3.9 If a custodian does not receive a CCS acceptance signal for a specific bundle, the bundle should be re-forwarded.

NOTES

1 The decision to re-forward a bundle is an implementation matter and may be based on:

a) timers – if no custody signal is received within a specified time, the bundle may be re-forwarded;

b) received custody signals – if in-sequence reception of bundles can be assumed, gaps in reported accepted custody signals may indicate lost bundles and trigger re-forwarding;

c) explicit commands – all or specific bundles with pending custody acceptance may be re-forwarded by command;

d) other events, internal or external, such contact initiation;

e) convergence layer failures – reported failure to forward the bundle via a CLA.

2 A node may refrain from re-forwarding a bundle when it is its source and the bundle is no longer needed, or if an intermediate node estimates that the bundle cannot reach its destination before expiration. In such cases, the node should report bundle deletion (preferably via compressed deletion reporting) or inform the bundle source by other means.

5 COMPRESSED BUNDLE STATUS REPORTING

This section defines the CREB and CRS formats and the procedures governing compressed bundle status reporting. A CREB inserts information about bundle sequences and, optionally, requests compressed bundle status reports. To support these options, CREB formats vary in length based on the data included and whether a report is requested in response.

5.1 COMPRESSED REPORTING EXTENSION BLOCK

5.1.1 GENERAL REQUIREMENTS

5.1.1.1 A compressed reporting extension block shall follow the canonical bundle block format according to RFC 9171 [2] section 4.3.2.

5.1.1.2 The block type code shall be 14.

5.1.1.3 A bundle may contain one or more CREBs inserted at the same or different bundle nodes.

5.1.1.4 The block-type-specific data shall be a definite-length CBOR byte string containing a definite-length CBOR array of 1 to 5 elements as defined in the next sections.

5.1.1.5 Only the bundle's source node shall add CREBs with a definite-length CBOR array of length 1, 2, or 3.

5.1.2 ARRAY LENGTH 1–SEQUENCE NUMBER ONLY

This format provides simple sequential numbering of bundles according to the destination EID, enabling gap detection or in-sequence delivery at the bundle's destination.

5.1.2.1 When the array length is 1, the array element shall contain a BSN according to 3.2.

5.1.2.2 When the array length is 1, the block source shall be the source node of the bundle.

NOTE – In this case the CREB has been added by the bundle source. The AEID of the bundle source node may then not be known explicitly by extension block's receivers. For certain naming schemes, it could be inferred from the source node ID contained in the primary block. However, since array length 1 does not require creating and transmitting to the AEID, the EID of the administrative element is not needed for processing the extension block.

5.1.2.3 When the array length is 1, the bundle sequence ID '0' shall be implicitly assumed.

NOTE – According to 3.3.1, separate sequence counters are used per destination EID. This allows a destination node to detect gaps in bundle reception from a specific source node.

5.1.3 ARRAY LENGTH 2– SEQUENCE NUMBER AND ID

This format provides sequential numbering of bundles according to specific criteria. BSID could be set based on the source EID (e.g., the service number for the IPN naming scheme), or the next hop ID to enable gap detection.

5.1.3.1 If the array length is 2, the array elements shall be BSID and BSN (CBOR unsigned integer) according to 3.2.

5.1.3.2 If the array length is 2, the block source AEID shall default to the bundle source node's AEID (see note to 5.1.2.2).

5.1.4 ARRAY LENGTH 3–REPORTING REQUEST WITH IMPLICIT SOURCE

This format is used for CBSR when the bundle's source node is requesting reporting and the source node ID in the primary block is also the AEID for responses.

5.1.4.1 If the array length is 3, the array elements shall be:

- The items defined for an array of length 2 in 5.1.3.1;
- Status Report Request Flags: CBOR unsigned integer which shall be processed as bit field indicating the flag values for the following reporting requests:
  - Bit 0 – reception;
  - Bit 1 – forwarding;
  - Bit 2 – delivery;
  - Bit 3 – deletion;
  - Bit 4 - custody acceptance;
  - Bit 5 – custody rejection;
  - Bit 6 to 63 – reserved for future use.

NOTE – Custody-related reporting is for informational purposes only and should not be confused with custody signals that trigger the behavior defined in Custody Procedures (4.3). The intention is to enable the reporting of custody-related behavior to a report-to node that is different from the current custodian, which is the receiver of all custody signals.

5.1.4.2 When the array length is 3, the bundle source must use an AEID (in the primary block) to receive status reports.

5.1.4.3 When the array length is 3, the block source AEID must match the bundle source's AEID, indicating that the bundle source added the CREB.

5.1.5 ARRAY LENGTH 4– REPORTING REQUEST

This format allows a node to request CSR to the AEID of the CREB-inserting node.

5.1.5.1 If the array length is 4, the array elements shall be:

- The items defined for an array of length 3 in 5.1.4.1;
- Block source AEID – the EID of the administrative endpoint of the node that created the CREB and assigned the BSID and BSN. Reports are sent to this node by default if no report-to EID is specified (see length 5 below).

5.1.6 ARRAY LENGTH 5–REPORTING REQUEST WITH REPORT-TO EID

This format allows a node to request CSR to a specific report-to endpoint.

5.1.6.1 If the array length is 5, the array elements shall be:

- The items defined for an array of length 4 in 5.1.5.1;
- Report-to EID – the EID to which the reports shall be send.

5.2 COMPRESSED REPORTING SIGNAL

5.2.1 A CRS shall be an administrative record according to RFC 9171 [2] section 6.1.

5.2.2 The record type code shall be 14.

5.2.3 A CRS shall contain a CBOR map as its record content. The map shall consist of:

- *key*: the **reason** for the status report (a CBOR unsigned integer):
  - 0 – reception;
  - 1 – forwarding;
  - 2 – delivery;
  - 3 – deletion;
  - 4 – custody acceptance;
  - 5 – custody rejection;
  - Values above 6 – reserved for future use;
- *value*: bundle **sequence collection** as defined in 3.3, subject to the constraints defined below.

5.2.4 The bundle sequences in sequence collections shall include a block source AEID only when the report-to destination EID differs from the administrative element of the CREB-inserting node (i.e., case 5.1.6 above).

NOTE – When the receiving node inserted the CREB, the block source AEID is implicit and not required.

5.2.5 The CRS Destination shall be:

– the source node ID in the primary block for a three-element array (5.1.4);

– the block source AEID for a four-element array (5.1.5);

– the report-to endpoint for a five-element array (5.1.6).

5.2.6 Reception of a CREB with a three-, four- or five-element array shall cause the receiving bundle node to store all required information for generating a CRS, including status report reason, destination, BSN and BSID, as well as the block source AEID.

5.2.7 CRS shall be generated and transmitted to a common destination based on the stored information.

NOTE – The timing of CRS transmission is an implementation matter that can be based on:

- periodic timer (when CREB requests exist);
- size constraints (bundle size or count), supplemented by a timer to prevent indefinite delays when the size limit is not reached but there are no additional bundles to report;
- external events (link establishment, explicit command).

5.2.8 Once a CRS for a specific bundle has been transmitted, no other reporting signal for this bundle should be generated with the same reporting reason.

6 END-TO-END SERVICES

This section discusses how the mechanisms introduced in Section 5 realize end-to-end services between a bundle's source and destination. Some services offer functionality similar to the Delay-Tolerant Payload Conditioning (DTPC) Transport Service defined for BPv6 [E1] in CCSDS 734.2-B-1 Annex E. Unlike DTPC, which introduces a BP application layer protocol with protocol data units transmitted in the payload block, the services described here rely solely on extension blocks from this specification. However, DTPC offers additional features (such as topics and an aggregation service) that the mechanisms described here do not replace.

The services described in the following sections are not mutually exclusive, so they can be combined without the need for additional extension blocks. The mechanisms differ in their requirements:

- In-Sequence Delivery and Duplicate Suppression do not require the generation of CRSs and work with any type of CREB, even with the simple 1-element form as defined in 5.1.2.
- End-to-end Accounting and Reliability require the source node to insert a CREB that:
    - assigns BSN based on the destination EID;
    - requests delivery reporting;
    - indicates optional deletion reporting.

6.1 IN-SEQUENCE DELIVERY

CREB sequence numbers based on separate counters per destination EID (BSID '0') enable bundle re-ordering at destination. Lost or delayed bundles are typically handled using timeouts.

6.2 DUPLICATE SUPPRESSION

Duplicate suppression works similarly to the in-sequence delivery. When CREB sequence numbers use separate counters per destination EID (BSID '0'), duplicated bundles can be detected by the same sequence number and suppressed. This is more efficient than using time stamps, which would require storage.

6.3 GAP DETECTION

End-to-end gap detection can also be based on BSNs using separate counters per destination EID (i.e., Bundle Sequence ID '0'). Out-of-order bundle arrivals can be addressed by implementing a time window before reporting a gap, to wait for late arrivals with lower sequence numbers than the current maximum.

6.4 ACCOUNTING

The use of CSR for delivery or deletion of bundles allows for end-to-end accounting of bundles towards the source node (using the request format in 5.1.5) or a different report-to EID (using the request format in 5.1.6):

- For **delivery** reporting, only the **destination** node must support CRS.
- For **deletion** accounting, both the **destination** and **deleting** nodes must support CRS.

If the deleting node does not support CSR, failed delivery can still be inferred from a missing delivery report. However, cases where the reporting signal is lost may result in wrongly assumed delivery failure.

6.5 RELIABILITY

Using the end-to-end accounting mechanism described above, end-to-end reliability can be provided by re-forwarding a bundle when an expected delivery report has not been received or the bundle has been reported as deleted. Re-forwarding a bundle again over the full end-to-end path is usually inefficient, so this mechanism may be combined with Custody Transfer as specified in section 4. In this way, re-forwarding will typically happen between custodians with re-forwarding from the source required only if CT fails.

ANNEX A

PROTOCOL IMPLEMENTATION CONFORMANCE STATEMENT PROFORMA

(NORMATIVE)

A1 INTRODUCTION

A1.1 GENERAL

This annex provides the Protocol Implementation Conformance Statement (PICS) Requirements List (RL) for implementations of this experimental specification. Implementations may employ any combination of these features but need to state clearly which features are supported. Feature support requires implementation of all mandatory requirements, including those from the base standards referenced in the RL.

The PICS is generated by completing the RL in accordance with the instructions below. It states which capabilities, features, and options of the protocol have been implemented for use by the following:

- protocol implementer: as a checklist to reduce the risk of non-conformance through oversight;
- protocol tester: as the basis for selecting appropriate tests for assessing conformance claims for the implementation;
- supplier and acquirer of the implementation: as a detailed indication of the implementation's capabilities relative to the common basis for understanding provided by the standard PICS proforma;
- user of the implementation: as a basis for checking the possibility of interoperability with another implementation.

For this specification, four distinct features have been identified:

- Custody Transfer (A4);
- Compressed Reporting – CREB Sequence Numbering (A5);
- Compressed Reporting – CREB Reporting Requests (Annex A6);
- Compressed Reporting – Compressed Reporting Signal (Annex A7).

A1.2 NOTATION

The following are used to indicate the status of requirements in the RL:

Status Symbols

M mandatory;

O optional.

This PICS is organized into features (A4 to A7), so ‘mandatory’ applies if the specific feature is implemented and support is indicated in A3 below.

A1.3 SUPPORT COLUMN SYMBOLS

The implementer shall indicate support for each item by entering Y, N, or N/A in the support column:

Y Yes, supported by the implementation.

N No, not supported by the implementation..

A1.4 INSTRUCTIONS FOR COMPLETING THE REQUIREMENTS LIST

In the Support column, each response shall be either a code selected from the indicated set of responses or one or more parameter values. If a mandatory requirement is not satisfied, exception must be supplied by entering a reference Xi, where i is a unique identifier to an accompanying rationale for the noncompliance.

A1.5 REFERENCED BASE STANDARDS

The base standard referenced in the RL is this document.

A1.6 IDENTIFICATION OF PROTOCOL

Ref	Question	
1	Date of Statement (DD/MM/YYYY)	
2	CCSDS Reference	
3	Protocol Name	Custody Transfer and Compressed Bundle Status Reporting

A2 IDENTIFICATION OF THE IMPLEMENTATION

Implementation Name	
Implementation Version	
Special Configuration	

Supplier	
Contact Point for Queries	
Other information necessary for full identification, such as, project, name(s) and version(s) for machines and/or operating systems, system name(s).	

A3 IMPLEMENTATION SCOPE & FEATURES

The following features are identified and may be implemented separately. A 'YES' implies the applicability of all requirements contained in the referenced section.

Custody Transfer (A4)	YES / NO
Compressed Reporting – CREB Sequence Numbering (A5)	YES / NO
Compressed Reporting – CREB Reporting Requests (A6)	YES / NO
Compressed Reporting – CRS (A7)	YES / NO
Have any exceptions within the implementation scope been required? If yes, identify the affected feature and the exceptions. NOTE – A YES answer means that the implementation of a protocol feature does not conform to the specification. Non-supported mandatory capabilities are to be identified in the PICS, with an explanation of why the implementation is non-conforming.	YES / NO

A4 CUSTODY TRANSFER

Type ID	Requirements	Reference	Status	Support
CT-01	CTEB	4.1	M	
CT-02	CCS	4.2	M	
CT-03	Custody Procedures	4.3	M	

A5 COMPRESSED REPORTING – CREB SEQUENCE NUMBERING

Type ID	Requirements	Reference	Status	Support
SN-01	CREB – General Requirements	5.1.1	M	

Type ID	Requirements	Reference	Status	Support
SN-02	CREB – Array Length 1	5.1.2	M	
SN-03	CREB – Array Length 2	5.1.3	M	
SN-04	CREB – Array Length 3	5.1.4	M	

A6 COMPRESSED REPORTING – CREB REPORTING REQUESTS

Type ID	Requirements	Reference	Status	Support
RR-01	CREB – General Requirements	5.1.1	M	
RR-02	CREB – Array Length 4	5.1.5	M	
RR-03	CREB – Array Length 5	5.1.6	M	

A7 COMPRESSED REPORTING – COMPRESSED REPORTING SIGNAL

Type ID	Requirements	Reference	Status	Support
RS-01	CRS	5.2	M	

ANNEX B

SECURITY, SANA/IANA, AND PATENT CONSIDERATION

(INFORMATIVE)

B1 SECURITY CONSIDERATIONS

B1.1 INTRODUCTION

Any deployment or use of DTN nodes and networks must consider security aspects based on a detailed security risk assessment of network specifics, involved parties, and criticality of data. Network operators must define security requirements and policies for participating nodes and their operations. The following sections address specific aspects related to CT and CSR, but they must be considered in the context of overall network security rather than in isolation.

B1.2 SECURITY CONCERNS WITH RESPECT TO THE CCSDS DOCUMENT

The mechanisms specified in this document have been designed for relatively small, well-managed DTN networks where all participating parties are known and agreements on the use of the network and its resources have been established. For security purposes, application of BP security (BPSec) [E2] is recommended.

B1.2.1 DATA PRIVACY

Data reported via CBSR may be considered sensitive. To prevent unauthorized or malicious nodes from requesting reports, the inserting node can authenticate the CREB using a BPSec Bundle Integrity Block (BIB). Reporting nodes can then verify that the CREB is authentic for the contained CREB Admin EID and apply policies to determine whether reporting to that node or report-to EID is allowed. CRS can be protected by a BPSEC bundle confidentiality block.

B1.2.2 DATA INTEGRITY

Data integrity of CTEB and CREB extension blocks can be provided by BIBs targeting these extension blocks. Similarly, data integrity of CCS and CRS can be provided by a BIB targeting the payload block of the signaling bundle, where signals are contained as administrative records.

B1.2.3 AUTHENTICATION OF COMMUNICATING ENTITIES

The block sources for CTEB and CREB extension blocks can be authenticated by a BIB. The source of CCS and CRS can be authenticated by a BIB targeting the bundle’s primary block.

B1.2.4 CONTROL OF ACCESS TO RESOURCES

For CT, custody acceptance can be based on the successful authentication of the bundle's source node or the previous CTEB-inserting custodian. To protect storage and communication resources, custody acceptance can be limited to specific bundle sources or previous custodians.

For CBSR, reporting can be based on the successful authentication of the CREB block source and limited to specific block sources or report-to EIDs to protect storage and communication resources.

NOTE – BIBs may have an impact on processing resources.

B1.2.5 AVAILABILITY OF RESOURCES

Availability of resources can be protected by the same means as described in the section above.

B1.2.6 AUDITING OF RESOURCE USAGE

Usage of processing, storage, and communication resources of bundles nodes should be monitored. Specifically for CT, monitoring parameters may include the amount of storage used for bundles in custody, potentially distinguished by bundle source or destination in the future. Total traffic generated by CT and CBSR should also be monitored.

B1.3 POTENTIAL THREATS AND ATTACK SCENARIOS

Malicious nodes may insert CTEB that require nodes to store bundles for extended periods. Nodes may protect against this by the authenticating and authorization as described in B1.2.4.

Malicious nodes may also take custody of a bundle and discard it silently, causing bundle loss. Compressed delivery reporting can detect such losses and trigger action to prevent further forwarding of bundles to those malicious nodes.

Finally, compressed reports may be exploited by malicious nodes to flood target nodes by inserting target EIDs as report-to EIDs. This can be mitigated by the mechanisms described in B1.2.4.

B1.4 CONSEQUENCES OF NOT APPLYING SECURITY TO THE TECHNOLOGY

If no security mechanisms are applied, malicious nodes may exhaust communication, storage, and processing resources by requesting CT, CBSR, or sending false custody refusal signals that cause unnecessary bundle re-forwarding. Bundles may be discarded and lost due to false custody acceptance signals.

B2 SANA/IANA CONSIDERATIONS

Since IANA have not delegated resources for block type or administrative record types to SANA, the registrations in the subsections below have been assigned by IANA.

B2.1 BUNDLE BLOCK TYPES

https://www.iana.org/assignments/bundle/bundle.xhtml#block-types

BP Version	Value	Description	Reference
7	13	Custody Transfer Extension Block	CCSDS 734.6-O-1 (this book)
7	14	Compressed Status Reporting Extension Block	CCSDS 734.6-O-1 (this book)

B2.2 BUNDLE ADMINISTRATIVE RECORD TYPES

https://www.iana.org/assignments/bundle/bundle.xhtml#admin-record-types

BP Version	Value	Description	Reference
7	13	Compressed Custody Signal	CCSDS 734.6-O-1 (this book)
7	14	Compressed Reporting Signal	CCSDS 734.6-O-1 (this book)

B3 PATENT CONSIDERATIONS

There are no patents that are known to apply to this specification.

ANNEX C

PROTOTYPING

(INFORMATIVE)

C1 ESA BUNDLE PROTOCOL IMPLEMENTATION

All features described in this specification have been implemented in ESA's Bundle Protocol Implementation and validated:

- To test the lower-level concepts like sequence number generation and conformance to structure definitions, unit tests have been employed to validate proper sequence number management as well as correct creation and proper encoding/decoding of structures (extension blocks, administrative records, sequence structures).
- The higher-level concepts have been validated through simulations and testing of the aspects outlined in the rest of this Annex. In the tests, a source node added extension blocks while other nodes in the network were configured for certain scenarios, e.g., nodes with artificially low storage capacity were used to test custody refusal.

Additional validation of custody transfer and compressed reporting has been performed in a simulated lunar communication scenario with a lunar relay orbiter, a lunar rover, a ground station, and related control centers. The rover control centers sent bundles to the lunar rover requesting delivery reporting and custody transfer for the compressed delivery reporting signals. This validation was fully successful in terms of custody transfer and generation of compressed reporting signals, although it did reveal a bug in ESA's BP implementation related to local endpoint registration. A brief description of implementation aspects is provided below.

C1.1 SEQUENCE NUMBER GENERATION

ESA BP implements the bundle sequence counters as two maps (one for CT and one for CBSR) of BSIDs: a wrapper for a destination EID or bundle Sequence ID mapped to sequence numbers. Each map is accessible through a function that accepts a sequence identifier and inserts a new mapping, increments the current count, or resets the count based on the configured maximum. The updated value is then used for the creation of extension blocks.

C1.2 CUSTODY ACCEPTANCE/REFUSAL

ESA BP evaluates whether to take custody of a bundle during reception. The destination node always accepts custody, while intermediate nodes may refuse custody if the bundle cannot be forwarded (e.g., when no next hop is known) or if a configurable storage threshold is reached.

When custody is accepted, a dedicated retention constraint is added to the bundle that is removed upon reception of an accepting CCS from a new custodian. When custody is refused due to inability to forward, the bundle is deleted. If custody is refused due to reaching the

storage threshold but the bundle can be forwarded immediately, it will be forwarded and deleted afterwards.

C1.3 RE-FORWARDING OF BUNDLES

Only bundles for which custody has been accepted will be re-forwarded. Re-forwarding will happen after a configurable timeout or upon reception of CCS. The timeout is realized by storing a dedicated re-forwarding time that is periodically checked against the current time.

When a refusing CCS is received, the re-forwarding time is reset for all refused bundles to try sending them later, eventually via another node. When an accepting CCS is received, all excluded bundles in the received bundle sequence ranges will be re-forwarded immediately based on reported gaps in the sequence.

C1.4 GENERATING AND SENDING COMPRESSED SIGNALS

When a bundle reaches certain stages in its lifecycle inside ESA BP (e.g., after reception or custody acceptance/refusal), all necessary information to generate a CCS or CRS is stored in a compressed item. These items are then stored in a temporary item buffer that is identified by the corresponding signal destination. When a new destination is added, it starts a timer that triggers the processing of items once it reaches a configurable timeout. Additionally, when a buffer accumulates a certain number of items, processing will be triggered prematurely. During processing, the buffer is removed and items are aggregated into a Compressed Signal that is sent to its destination.

C2 NASA GSFC BUNDLE PROTOCOL IMPLEMENTATION

Custody transfer as defined in this specification was tested onboard the Cislunar Autonomous Positioning System Technology Operations and Navigation Experiment (CAPSTONE) spacecraft during multiple uplink and downlink passes at lunar distances. These experiments used BPNode Build 7.0.5, a DTN BPv7 flight software node developed by the NASA Goddard Space Flight Center (GSFC) and running within the core Flight System (cFS).

After initial ground testing, the software, test tools, and scripts were released to the public in these NASA GitHub repositories:

– https://github.com/nasa/bplib;

– https://github.com/nasa/bp;

– https://github.com/nasa/dtn-tools.

C2.1 SOFTWARE INFORMATION

Date of Statement	5/5/2026
CCSDS Reference	CCSDS 734.6-O-1
Protocol Name	Custody Transfer and Compressed Bundle Status Reporting

Implementation Name	BPNode
Implementation Version	Build 7.0.5
Special Configuration	Flight Software DTN Node hosted on cFS
Supplier	NASA-GSFC
Contact Point for Queries	gsfc-dtn@nasa.onmicrosoft.com

C2.2 TEST COVERAGE

Type ID	Requirements	Reference	Status	Support	Tested/ Remarks
CT-01	CTEB	4.1	M	Yes	Yes
CT-02	CCS	4.2	M	Yes	Yes
CT-03	Custody Procedures	4.3	M	Yes	Yes

ANNEX D

CONCISE DATA DEFINITIONS LANGUAGE EXPRESSIONS

(INFORMATIVE)

For informational purposes, an expression of this specification in the Concise Data Definition Language (CDDL) is provided below. Where the CDDL expression disagrees with the textual representation in the earlier sections of this document, the textual representation takes precedence. The definitions below utilize CDDL expressions from RFC 9171 [2].

```
; Compressed Custody Signal
$admin-record /= [13, custody-signal-content]
custody-signal-content = {
  -1 => seq-collection; Custody rejected
  1 => seq-collection; Custody accepted
  * int => seq-collection; Reserved
}

; Bundle Sequence Collection
seq-collection = [+ seq]
; Bundle Sequence
seq = [
  seq-id-ref: (unit .gt 0) / eid,
  seq-start: seq-num,
  range: seq-range / seq-incl-len,
  ? blk-source
]

; Bundle Sequence Range
seq-range = [seq-incl-len, +(seq-exl-len, seq-incl-len)]
seq-incl-len = uint .gt 0; inclusive length
seq-exl-len = uint .gt 0; exclusive length

; Bundle Sequence Number
seq-num = uint

; Bundle Sequence ID
```

```
seq-id = uint

; Block Source Administrative Endpoint ID
blk-source = eid

; Compressed Reporting Signal
$admin-record /= [14, reporting-signal-content]
reporting-signal-content = {
  0 => seq-collection; Reception report
  1 => seq-collection; Forwarding report
  2 => seq-collection; Delivery report
  3 => seq-collection; Deletion report
  4 => seq-collection; Custody acceptance report
  5 => seq-collection; Custody rejection report
  * int  => seq-collection; reserved
}

; CTEB
$extension-block /= extension-block-use<13, embedded-cbor<ext-data-custody-transfer>>
ext-data-custody-transfer = [
  seq-num,
  seq-id,
  blk-source
]

; CREB
$extension-block /= extension-block-use<14, embedded-cbor<ext-bundle-reporting>>
ext-bundle-reporting /= [
  seq-num,
  ?(
    seq-id,
    ?(
      status-report-request-flags,
      ?(
        blk-source,
        ? report-to-eid: eid
      )
```

```
    )
  )
]


status-report-request-flags = uint .bits statusrequestbits
statusrequestbits = &(
  reception: 0,
  forwarding: 1,
  delivery: 2,
  deletion: 3,
  custody-accepted: 4,
  custody-rejected: 5,
  reserved: 6..63
)
```

ANNEX E

INFORMATIVE REFERENCES

(INFORMATIVE)

[E1] CCSDS *Bundle Protocol Specification*. Issue 1. CCSDS Recommendation (Blue Book), CCSDS 734.2-B-1. Washington, DC.: CCSDS, September 2015.

[E2] CCSDS *Bundle Protocol Security Specification*. Issue 2. CCSDS Report (Red Book), CCSDS 734.5-R-2. Washington, DC.: CCSDS, September 2023.

ANNEX F

ABBREVIATIONS AND ACRONYMS

(INFORMATIVE)

AEID	Administrative Endpoint ID
BIB	Bundle Integrity Block
BP	Bundle Protocol
BPv6, BPv7	Bundle Protocol version 6, 7
BSC	Bundle Sequence Counter
BSID	Bundle Sequence ID
BSN	Bundle Sequence Number
BSR	Bundle Status Report
CBOR	Concise Binary Object Representation
CBSR	Compressed Bundle Status Report(ing)
CCS	Compressed Custody Signal
CDDL	Concise Data Definition Language
cFS	core Flight System
CLA	Convergence Layer Adaptor
CREB	Compressed Reporting Extension Block
CRS	Compressed Reporting Signal
CT	Custody Transfer
CTEB	Custody Transfer Extension Block
DTN	Disruption/Delay Tolerant Networking
DTPC	Delay-Tolerant Payload Conditioning
EID	Endpoint ID

IANA	Internet Assigned Numbers Authority
IPN	InterPlanetary Network
MIB	Management Information Database
PICS	Protocol Implementation Conformance Statement
RFC	Request For Comments
RL	Requirements List
SANA	Space Assigned Numbers Authority