CESG POLL ITEM DISPOSITION (PID) INITIATION FORM

AREA PID NUMBER: SLS-01
SUBMITTING AREA: Space Link Services

REVIEWER'S NAME: Gian Paolo Calzolari
E-MAIL ADDRESS: Gian.Paolo.Calzolari@esa.int

DOCUMENT NUMBER: CCSDS 734.5-R-0
DOCUMENT NAME: CCSDS Streamlined Bundle Security Protocol
DATE ISSUED: September 2017
PAGE NUMBER: 1-1   PARAGRAPH NUMBER: 1.1
PID SHORT TITLE: Why streamlined?

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

FROM:
This document defines a Recommended Standard for the CCSDS Streamlined Bundle
Security Protocol (SBSP) specification to define security features for the
CCSDS Bundle Protocol (BP) (reference [1]) intended for use in delay-tolerant
networks in order to provide Delay-Tolerant Networking (DTN) security
services. SBSP provides authentication, integrity, and confidentiality for
bundles along a path through a DTN and is based upon the IETF Bundle Protocol
Security Specification (reference [2]).

TO:
This document defines a Recommended Standard for the CCSDS Streamlined Bundle
Security Protocol (SBSP) specification to define security features for the
CCSDS Bundle Protocol (BP) (reference [1]) intended for use in delay-tolerant
networks in order to provide Delay-Tolerant Networking (DTN) security
services.

SBSP provides authentication, integrity, and confidentiality for bundles
along a path through a DTN. SBSP is based upon the IETF Bundle Protocol
Security Specification (reference [2]) and it is defined streamlined because
<include rationale>.

CATEGORY OF REQUESTED CHANGE: Technical Fact

SUPPORTING ANALYSIS:
   1) Splitting into two paragraphs increases readability. (EDITORIAL)
   2) Splitting the second sentence into two sentences splits two different
      subjects (what is provided vs. origins) and increases readability.
      (RECOMMENDED)
   3) Nowhere it is stated why this protocol is funny preceded by the
      appellation "streamlined". A short rationale is definitively required.
      (TECHNICAL FACT)

DISPOSITION:

```
            CESG POLL ITEM DISPOSITION (PID) INITIATION FORM


AREA PID NUMBER:        SLS-02
SUBMITTING AREA:        Space Link Services
-------------------------------------------------------------------
REVIEWER'S NAME:        Gian Paolo Calzolari
E-MAIL ADDRESS:         Gian.Paolo.Calzolari@esa.int
-------------------------------------------------------------------
DOCUMENT NUMBER:   CCSDS 734.5-R-0
DOCUMENT NAME:     CCSDS Streamlined Bundle Security Protocol
DATE ISSUED:       September 2017
PAGE NUMBER:       1-1        PARAGRAPH NUMBER:  1.2
PID SHORT TITLE:   What is not addressed
-------------------------------------------------------------------
```

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

FROM:

This specification does not address individual cipher suite implementations. The definition and enumeration of cipher suites should be undertaken in separate specification documents. This specification does not address the implementation of security policy and does not provide a security policy for SBSP. Security policies are typically based on the nature and capabilities of individual networks and network operational concepts. However, this specification does recommend policy considerations when building a security policy. This specification does not address how to combine SBSP security blocks with other protocols, other BP extension blocks, or other best practices to achieve security in any particular network implementation.

To (e.g.):

This specification does not address

- individual cipher suite implementations as the definition and enumeration of cipher suites should be undertaken in separate specification documents;
- implementation of security policy;
- any security policy for SBSP, but only recommends policy considerations when building a security policy, as security policies are typically based on the nature and capabilities of individual networks and network operational concepts;
- how to combine SBSP security blocks with other protocols, other BP extension blocks, or other best practices to achieve security in any particular network implementation.

```
-------------------------------------------------------------------
```
CATEGORY OF REQUESTED CHANGE: Recommended
```
-------------------------------------------------------------------
```
SUPPORTING ANALYSIS:

Presentation with bullet lists is clearer and immediately draw readers attention on items not addressed in this book.

```
-------------------------------------------------------------------
```
DISPOSITION:

```
            CESG POLL ITEM DISPOSITION (PID) INITIATION FORM

AREA PID NUMBER:        SLS-03
SUBMITTING AREA:        Space Link Services
----------------------------------------------------------------
REVIEWER'S NAME:        Gian Paolo Calzolari
E-MAIL ADDRESS:         Gian.Paolo.Calzolari@esa.int
----------------------------------------------------------------
DOCUMENT NUMBER:   CCSDS 734.5-R-0
DOCUMENT NAME:     CCSDS Streamlined Bundle Security Protocol
DATE ISSUED:       September 2017
PAGE NUMBER:       1-1         PARAGRAPH NUMBER:  1.2
PID SHORT TITLE:   SBSP vs. other protocols
----------------------------------------------------------------
DESCRIPTION OF REQUESTED CHANGE:  (Use From: "..." To "..." format)

I am not sure the sentence below is fully correct and it should be improved.
```

This specification does not address how to combine SBSP security blocks with other protocols, other BP extension blocks, or other best practices to achieve security in any particular network implementation.

```
----------------------------------------------------------------
CATEGORY OF REQUESTED CHANGE:  Recommended
----------------------------------------------------------------
SUPPORTING ANALYSIS:
```

I think that this specification **does address** how to combine SBSP security blocks with the Bundle protocol. Therefore it should be remarked that it addresses only BP and no other protocols.

```
----------------------------------------------------------------
DISPOSITION:
```

CESG POLL ITEM DISPOSITION (PID) INITIATION FORM

AREA PID NUMBER: SLS-04
SUBMITTING AREA: Space Link Services

REVIEWER'S NAME: Gian Paolo Calzolari
E-MAIL ADDRESS: Gian.Paolo.Calzolari@esa.int

DOCUMENT NUMBER: CCSDS 734.5-R-0
DOCUMENT NAME: CCSDS Streamlined Bundle Security Protocol
DATE ISSUED: September 2017
PAGE NUMBER: 2-1   PARAGRAPH NUMBER: 2.1
PID SHORT TITLE: key properties of a security system

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

I fail in understanding which key properties of a security system are
described by this book.
Do you refer to the subsections in chapter 2 or to other items in the
following chapters.

Please make it clearer, possibly with an explicit list.

CATEGORY OF REQUESTED CHANGE: Technical fact

SUPPORTING ANALYSIS:

The word property/properties is only present in section 2.1 and no other
section says that a property is defined there.

DISPOSITION:

CESG POLL ITEM DISPOSITION (PID) INITIATION FORM

AREA PID NUMBER: SLS-05
SUBMITTING AREA: Space Link Services

REVIEWER'S NAME: Gian Paolo Calzolari
E-MAIL ADDRESS: Gian.Paolo.Calzolari@esa.int

DOCUMENT NUMBER: CCSDS 734.5-R-0
DOCUMENT NAME: CCSDS Streamlined Bundle Security Protocol
DATE ISSUED: September 2017
PAGE NUMBER: 4-x   PARAGRAPH NUMBER: 4.x
PID SHORT TITLE: Normative Chapter 4

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

If this chapter is normative (as it looks to me), add its clauses to Annex
for PICs.

In the unlikely case that this chapter is NOT normative reword clauses and
move all to a non-normative Annex.

CATEGORY OF REQUESTED CHANGE: Technical Fact

SUPPORTING ANALYSIS:

PICS do not list any clause from Chapter 4.

DISPOSITION:

CESG POLL ITEM DISPOSITION (PID) INITIATION FORM

```
AREA PID NUMBER:        SLS-06
SUBMITTING AREA:        Space Link Services
------------------------------------------------------------------
REVIEWER'S NAME:        Gian Paolo Calzolari
E-MAIL ADDRESS:         Gian.Paolo.Calzolari@esa.int
------------------------------------------------------------------
DOCUMENT NUMBER:   CCSDS 734.5-R-0
DOCUMENT NAME:     CCSDS Streamlined Bundle Security Protocol
DATE ISSUED:       September 2017
PAGE NUMBER:       5-1        PARAGRAPH NUMBER:  5
PID SHORT TITLE:   Why do you have chapter 5
------------------------------------------------------------------
DESCRIPTION OF REQUESTED CHANGE:  (Use From: "..." To "..." format)
```

Delete chapter 5 and move the comment to any other suitable (non-normative) chapter.

```
------------------------------------------------------------------
CATEGORY OF REQUESTED CHANGE:     Technical Fact
------------------------------------------------------------------
SUPPORTING ANALYSIS:
```

Chapter 5 should be normative but it only contains a comment.

```
------------------------------------------------------------------
DISPOSITION:
```

CESG POLL ITEM DISPOSITION (PID) INITIATION FORM

AREA PID NUMBER: SLS-07
SUBMITTING AREA: Space Link Services

REVIEWER'S NAME: Gian Paolo Calzolari
E-MAIL ADDRESS: Gian.Paolo.Calzolari@esa.int

DOCUMENT NUMBER: CCSDS 734.5-R-0
DOCUMENT NAME: CCSDS Streamlined Bundle Security Protocol
DATE ISSUED: September 2017
PAGE NUMBER: 6-x   PARAGRAPH NUMBER: 6.x
PID SHORT TITLE: Normative Chapter 6

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

If this chapter is normative (as it looks to me), add its clauses to Annex
for PICs.

In the unlikely case that this chapter is NOT normative reword clauses and
move all to a non-normative Annex.

CATEGORY OF REQUESTED CHANGE: Technical Fact

SUPPORTING ANALYSIS:

PICS do not list any clause from Chapter 6.

DISPOSITION:

```
              CESG POLL ITEM DISPOSITION (PID) INITIATION FORM

AREA PID NUMBER:       SLS-08
SUBMITTING AREA:       Space Link Services
-----------------------------------------------------------------
REVIEWER'S NAME:       Gian Paolo Calzolari
E-MAIL ADDRESS:        Gian.Paolo.Calzolari@esa.int
-----------------------------------------------------------------
DOCUMENT NUMBER:   CCSDS 734.5-R-0
DOCUMENT NAME:     CCSDS Streamlined Bundle Security Protocol
DATE ISSUED:       September 2017
PAGE NUMBER:       7-x           PARAGRAPH NUMBER:  7
PID SHORT TITLE:   Normative Chapter 7
-----------------------------------------------------------------
DESCRIPTION OF REQUESTED CHANGE:  (Use From: "..." To "..." format)

If this chapter is NOT normative (as it looks to me), move all to a non-
normative Annex.


In the unlikely case that this chapter is normative reword clauses to
normative form and add them to Annex for PICs.



-----------------------------------------------------------------
CATEGORY OF REQUESTED CHANGE:     Technical Fact
-----------------------------------------------------------------
SUPPORTING ANALYSIS:




-----------------------------------------------------------------
DISPOSITION:
```

```
            CESG POLL ITEM DISPOSITION (PID) INITIATION FORM

AREA PID NUMBER:        SLS-09
SUBMITTING AREA:        Space Link Services
-----------------------------------------------------------------
REVIEWER'S NAME:        Gian Paolo Calzolari
E-MAIL ADDRESS:         Gian.Paolo.Calzolari@esa.int
-----------------------------------------------------------------
DOCUMENT NUMBER:   CCSDS 734.5-R-0
DOCUMENT NAME:     CCSDS Streamlined Bundle Security Protocol
DATE ISSUED:       September 2017
PAGE NUMBER:       A-1            PARAGRAPH NUMBER:  A
PID SHORT TITLE:   Annex A incomplete
-----------------------------------------------------------------
DESCRIPTION OF REQUESTED CHANGE:  (Use From: "..." To "..." format)

Complete Annex as required.




-----------------------------------------------------------------
CATEGORY OF REQUESTED CHANGE:     Technical Fact
-----------------------------------------------------------------
SUPPORTING ANALYSIS:


Annex A looks incomplete as it only contains clauses from chapter 3.



-----------------------------------------------------------------
DISPOSITION:
```