

Delay-Tolerant Networking
Internet-Draft
Intended status: Experimental
Expires: January 3, 2019

E. Birrane
E. DiPietro
D. Linko
Johns Hopkins Applied Physics Laboratory
July 2, 2018

Bundle Protocol Security Application Data Model
draft-birrane-dtn-adm-bpsec-01

Abstract

This document describes the Application Data Model (ADM) for the Bundle Protocol Security (BPSEC) in compliance with the template provided by [[I-D.birrane-dtn-adm](#)].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 3, 2019.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
1.1.	Technical Notes	2
1.2.	Scope	3
1.3.	Requirements Language	3
2.	Structure and Design of this ADM	3
3.	Naming and Identification	4
3.1.	Namespace and Nicknames	4
4.	BPSEC Agent ADM JSON Encoding	5
5.	IANA Considerations	23
6.	References	23
6.1.	Informative References	23
6.2.	Normative References	23
	Authors' Addresses	23

[1.](#) Introduction

An Application Data Model (ADM) provides a guaranteed interface for the management of an application or protocol in accordance with the Asynchronous Management Architecture (AMA) defined in [\[I-D.birrane-dtn-ama\]](#). This document is in compliance with the template provided by [\[I-D.birrane-dtn-adm\]](#).

BPSEC ([\[I-D.ietf-dtn-bpsec\]](#)) defines integrity and confidentiality mechanisms for securing extension blocks within a Bundle Protocol bundle. The BPSEC Agent ADM provides the set of information used to monitor and configure common aspects of any BPSEC software implementation.

[1.1.](#) Technical Notes

- o This document describes Version 1.0 of the BPSEC Agent ADM.
- o The Asynchronous Resource Identifier (ARI) for this ADM is NOT correctly set. A sample ARI is used in this version of the specification and MAY change in future versions of this ADM until an ARI registry is established. This notice will be removed at that time.
- o Agent applications MAY choose to ignore the name, description, or other annotative information associated with the component definitions within this ADM where such items are only used to

provide human-readable information or are otherwise not necessary to manage a device.

[1.2.](#) Scope

This ADM specifies those components of the Asynchronous Management Model (AMM) common to the BPSEC management of any instance of a BPA.

Any Manager software implementing this ADM MUST perform the responsibilities of an AMA Manager as outlined in [\[I-D.birrane-dtn-adm\]](#) as they relate to the objects included in this document.

Any Agent software implementing this ADM MUST perform the responsibilities of an AMA Agent as outlined in [\[I-D.birrane-dtn-adm\]](#) as they relate to the objects included in this document.

[1.3.](#) Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](#) [[RFC2119](#)].

[2.](#) Structure and Design of this ADM

The BPSEC Agent ADM's structure is in accordance to [\[I-D.birrane-dtn-adm\]](#). This ADM contains metadata, edd, variables, table templates, report templates, and controls. Externally Defined Data (EDD) are values that are calculated external to the ADM system. Table Templates are column templates that will be followed by any instance of this table available in the network. They may not be created dynamically within the network by Managers. Controls are predefined and sometimes parameterized opcodes that can be run on an Agent. Controls are preconfigured in Agents and Managers as part of ADM support. Variables are values that are statically defined in an ADM or dynamically by Managers in a network deployment. There are no constants, macros, or operators in this ADM at this time. The contents of this ADM are derived from the main functions and data that are needed to configure and manage BPSEC.

All ADMs have metadata that includes the name, namespace, and version of the ADM, as well as the name of the organization that is issuing that particular ADM. This is important for identification purposes of the ADMs and to ensure version control. The EDDs chosen deal with bundle integrity blocks and bundle confidentiality blocks, the most important concepts from the Bundle Security Protocol. This ADM additionally incorporates a "uses statement." The purpose of this statement is to pull in the information present in another ADM. In this case, this ADM "uses" the AMP Agent ADM.

[3.](#) Naming and Identification

This section outlines the namespaces used to uniquely identify ADM objects in this specification.

[3.1.](#) Namespace and Nicknames

In accordance with [[I-D.birrane-dtn-adm](#)], every ADM is assigned a moderated Namespace. In accordance with [[I-D.birrane-dtn-amp](#)], these namespaces may be enumerated for compactness. The namespace and ADM identification for these objects is defined as follows.

Identifier	Value
Namespace	DTN/bpsec
ADM Enumeration	4

Table 1: Namespace Information

Given the above ADM enumeration, in accordance with [[I-D.birrane-dtn-amp](#)], the following AMP nicknames are defined.

+-----+-----+	
Nickname	Collection
+-----+-----+	
80	DTN/bpsec/Const
81	DTN/bpsec/Ctrl
82	DTN/bpsec/Edd
83	DTN/bpsec/Mac
84	DTN/bpsec/Oper
85	DTN/bpsec/Rptt
87	DTN/bpsec/Tblt
89	DTN/bpsec/Var
90	DTN/bpsec/Mdat
91-99	DTN/bpsec/Reserved

Table 2: BPSEC ADM Nicknames

4. BPSEC Agent ADM JSON Encoding

The following is the JSON encoding of the BPSEC Agent ADM:

```
{
  "uses":["Amp:Agent"],
  "Mdat": [
    {
      "name": "name",
      "type": "STR",
      "value": "bpsec",
      "description": "The human-readable name of the ADM."
    },
    {
      "name": "namespace",
      "type": "STR",
      "value": "DTN:BundleProtocolSecurity",
      "description": "The namespace of the ADM."
    },
    {
      "name": "version",
      "type": "STR",

```

```
      "value": "v1.0",
      "description": "The version of the ADM."
    },
    {
      "name": "organization",
      "type": "STR",
      "value": "JHUAPL",
      "description": "The name of the issuing organization of the ADM."
    }
  ],
  "Edd": [
    {
      "name": "num_good_tx_bcb_blk",
      "type": "UINT",

```

```

    "description": "Total successfully Tx Bundle Confidentiality blocks"
  },
  {
    "name": "num_bad_tx_bcb_blk",
    "type": "UINT",
    "description": "Total unsuccessfully Tx Block Confidentiality Block
      (BCB) blocks"
  },
  {
    "name": "num_good_rx_bcb_blk",
    "type": "UINT",
    "description": "Total successfully Rx BCB blocks"
  },
  {
    "name": "num_bad_rx_bcb_blk",
    "type": "UINT",
    "description": "Total unsuccessfully Rx BCB blocks"
  },
  {
    "name": "num_missing_rx_bcb_blks",
    "type": "UINT",
    "description": "Total missing-on-RX BCB blocks"
  },
  {
    "name": "num_fwd_bcb_blks",
    "type": "UINT",
    "description": "Total forward BCB blocks"
  },
  {
    "name": "num_good_tx_bcb_bytes",
    "type": "UINT",
    "description": "Total successfully Tx BCB bytes"
  },
  },

```

```

  {
    "name": "num_bad_tx_bcb_bytes",
    "type": "UINT",
    "description": "Total unsuccessfully Tx BCB bytes"
  },
  {
    "name": "num_good_rx_bcb_bytes",
    "type": "UINT",

```

```

    "description": "Total successfully Rx BCB bytes"
  },
  {
    "name": "num_bad_rx_bcb_bytes",
    "type": "UINT",
    "description": "Total unsuccessfully Rx BCB bytes"
  },
  {
    "name": "num_missing_rx_bcb_bytes",
    "type": "UINT",
    "description": "Total missing-on-Rx BCB bytes"
  },
  {
    "name": "num_fwd_bcb_bytes",
    "type": "UINT",
    "description": "Total forwarded BCB bytes"
  },
  {
    "name": "num_good_tx_bib_blks",
    "type": "UINT",
    "description": "Total successfully Tx Block Integrity Block (BIB)
      blocks"
  },
  {
    "name": "num_bad_tx_bib_blks",
    "type": "UINT",
    "description": "Total unsuccessfully Tx BIB blocks"
  },
  {
    "name": "num_good_rx_bib_blks",
    "type": "UINT",
    "description": "Total successfully Rx BIB blocks"
  },
  {
    "name": "num_bad_rx_bib_blks",
    "type": "UINT",
    "description": "Total unsuccessfully Rx BIB blocks"
  },
  {
    "name": "num_miss_rx_bib_blks",

```

"type": "UINT",


```

    "description": "Total missing-on-Rx BIB blocks"
  },
  {
    "name": "num_fwd_bib_blks",
    "type": "UINT",
    "description": "Total forwarded BIB blocks"
  },
  {
    "name": "num_good_tx_bib_bytes",
    "type": "UINT",
    "description": "Total successfully Tx BIB bytes"
  },
  {
    "name": "num_bad_tx_bib_bytes",
    "type": "UINT",
    "description": "Total unsuccessfully Tx BIB bytes"
  },
  {
    "name": "num_good_rx_bib_bytes",
    "type": "UINT",
    "description": "Total successfully Rx BIB bytes"
  },
  {
    "name": "num_bad_rx_bib_bytes",
    "type": "UINT",
    "description": "Total unsuccessfully Rx BIB bytes"
  },
  {
    "name": "num_miss_rx_bib_bytes",
    "type": "UINT",
    "description": "Total missing-on-Rx BIB bytes"
  },
  {
    "name": "num_fwd_bib_bytes",
    "type": "UINT",
    "description": "Total forwarded BIB bytes"
  },
  {
    "name": "last_update",
    "type": "TV",
    "description": "Last BPSEC update"
  },
  {
    "name": "num_known_keys",
    "type": "UINT",
    "description": "Number of known keys"
  },

```

```
{
  "name": "key_names",
  "type": "STR",
  "description": "Known key names"
},
{
  "name": "ciphersuite_names",
  "type": "STR",
  "description": "Known ciphersuite names"
},
{
  "name": "rule_source",
  "type": "STR",
  "description": "Known rule sources"
},
{
  "name": "num_good_tx_bcb_blks_src",
  "type": "UINT",
  "parmspec": [{"type": "STR", "name": "Src"}],
  "description": "Number of successfully Tx BCB blocks from SRC"
},
{
  "name": "num_bad_tx_bcb_blks_src",
  "type": "UINT",
  "parmspec": [{"type": "STR", "name": "Src"}],
  "description": "Number of failed TX BCB blocks from SRC"
},
{
  "name": "num_good_rx_bcb_blks_src",
  "type": "UINT",
  "parmspec": [{"type": "STR", "name": "Src"}],
  "description": "Number of successfully Rx BCB blocks from SRC"
},
{
  "name": "num_bad_rx_bcb_blks_src",
  "type": "UINT",
  "parmspec": [{"type": "STR", "name": "Src"}],
  "description": "Number of failed RX BCB blocks from SRC"
},
{
  "name": "num_missing_rx_bcb_blks_src",
  "type": "UINT",
  "parmspec": [{"type": "STR", "name": "Src"}],
  "description": "Number of missing-onRX BCB blocks from SRC"
},
{
```

```
"name": "num_fwd_bcb_blks_src",  
"type": "UINT",
```

```
  "parmspec": [{"type": "STR", "name": "Src"}],  
  "description": "Number of forwarded BCB blocks from SRC"  
},  
{  
  "name": "num_good_tx_bcb_bytes_src",  
  "type": "UINT",  
  "parmspec": [{"type": "STR", "name": "Src"}],  
  "description": "Number of successfully Tx bcb bytes from SRC"  
},  
{  
  "name": "num_bad_tx_bcb_bytes_src",  
  "type": "UINT",  
  "parmspec": [{"type": "STR", "name": "Src"}],  
  "description": "Number of failed Tx bcb bytes from SRC"  
},  
{  
  "name": "num_good_rx_bcb_bytes_src",  
  "type": "UINT",  
  "parmspec": [{"type": "STR", "name": "Src"}],  
  "description": "Number of successfully Rx bcb bytes from SRC"  
},  
{  
  "name": "num_bad_rx_bcb_bytes_src",  
  "type": "UINT",  
  "parmspec": [{"type": "STR", "name": "Src"}],  
  "description": "Number of failed Rx bcb bytes from SRC"  
},  
{  
  "name": "num_missing_rx_bcb_bytes_src",  
  "type": "UINT",  
  "parmspec": [{"type": "STR", "name": "Src"}],  
  "description": "Number of missing-on-Rx bcb bytes from SRC"  
},  
{  
  "name": "num_fwd_bcb_bytes_src",  
  "type": "UINT",  
  "parmspec": [{"type": "STR", "name": "Src"}],  
  "description": "Number of forwarded bcb bytes from SRC"  
},
```

```

{
  "name": "num_good_tx_bib_blks_src",
  "type": "UINT",
  "parmspec": [{"type": "STR", "name": "Src"}],
  "description": "Number of successfully Tx BIB blocks from SRC"
},
{
  "name": "num_bad_tx_bib_blks_src",
  "type": "UINT",

```

```

  "parmspec": [{"type": "STR", "name": "Src"}],
  "description": "Number of failed Tx BIB blocks from SRC"
},
{
  "name": "num_good_rx_bib_blks_src",
  "type": "UINT",
  "parmspec": [{"type": "STR", "name": "Src"}],
  "description": "Number of successfully Rx BIB blocks from SRC"
},
{
  "name": "num_bad_rx_bib_blks_src",
  "type": "UINT",
  "parmspec": [{"type": "STR", "name": "Src"}],
  "description": "Number of failed Rx BIB blocks from SRC"
},
{
  "name": "num_miss_rx_bib_blks_src",
  "type": "UINT",
  "parmspec": [{"type": "STR", "name": "Src"}],
  "description": "Number of missing-on-Rx BIB blocks from SRC"
},
{
  "name": "num_fwd_bib_blks_src",
  "type": "UINT",
  "parmspec": [{"type": "STR", "name": "Src"}],
  "description": "Number of forwarded BIB blocks from SRC"
},
{
  "name": "num_good_tx_bib_bytes_src",
  "type": "UINT",
  "parmspec": [{"type": "STR", "name": "Src"}],
  "description": "Number of successfully Tx BIB bytes from SRC"

```

```

},
{
  "name": "num_bad_tx_bib_bytes_src",
  "type": "UINT",
  "parmspec": [{"type": "STR", "name": "Src"}],
  "description": "Number of failed Tx BIB bytes from SRC"
},
{
  "name": "num_good_rx_bib_bytes_src",
  "type": "UINT",
  "parmspec": [{"type": "STR", "name": "Src"}],
  "description": "Number of successfully Rx BIB bytes from SRC"
},
{
  "name": "num_bad_rx_bib_bytes_src",
  "type": "UINT",

```

```

  "parmspec": [{"type": "STR", "name": "Src"}],
  "description": "Number of failed Rx BIB bytes from SRC"
},
{
  "name": "num_missing_rx_bib_bytes_src",
  "type": "UINT",
  "parmspec": [{"type": "STR", "name": "Src"}],
  "description": "Number of missing-on-Rx BIB bytes from SRC"
},
{
  "name": "num_fwd_bib_bytes_src",
  "type": "UINT",
  "parmspec": [{"type": "STR", "name": "Src"}],
  "description": "Number of forwarded BIB bytes from SRC"
},
{
  "name": "last_update_src",
  "type": "TV",
  "parmspec": [{"type": "STR", "name": "Src"}],
  "description": "Last BPSEC update from SRC"
},
{
  "name": "last_reset",
  "type": "TV",
  "parmspec": [{"type": "STR", "name": "Src"}],

```

```

        "description": "Last reset"
    }
],
"Tblt" : [
    {
        "name": "keys",
        "columns": [{"type": "STR", "name": "key_name"}],
        "description": "This table lists all keys in the security policy
            database."
    },
    {
        "name": "ciphersuites",
        "columns": [{"type": "STR", "name": "csname"}],
        "description": "This table lists supported ciphersuites."
    },
    {
        "name": "bib_rules",
        "columns": [{"type": "STR", "name": "SrcEid"},
            {"type": "STR", "name": "DestEid"},
            {"type": "UINT", "name": "TgtBlk"},
            {"type": "STR", "name": "csName"},
            {"type": "STR", "name": "keyName"}
        ]
    }
]

```

```

    ],
    "description": "BIB Rules."
},
{
    "name": "bcb_rules",
    "columns": [{"type": "STR", "name": "SrcEid"},
        {"type": "STR", "name": "DestEid"},
        {"type": "UINT", "name": "TgtBlk"},
        {"type": "STR", "name": "csName"},
        {"type": "STR", "name": "keyName"}
    ],
    "description": "BCB Rules."
}
],
"Var": [
    {
        "name": "total_bad_tx_blks",
    }
]

```

```

    "type": "UINT",
    "initializer": {
      "type": "UINT",
      "postfix-expr": [{
        "ns": "DTN/bpsec",
        "nm": "Edd.num_bad_tx_bib_blks_src",
      }, {
        "ns": "DTN/bpsec",
        "nm": "Edd.num_bad_tx_bcb_blks_src",
      }, {
        "ns": "Amp/Agent",
        "nm": "Oper.plusUINT",
      }]
    },
    "description": "This is the number of failed TX blocks (# failed BIB +
      # failed bcb).",
  }
],
"Rptt": [
  {
    "name": "full_report",
    "definition" : [
      {
        "ns": "DTN/bpsec",
        "nm": "Edd.num_good_tx_bcb_blk",
      },
      {
        "ns": "DTN/bpsec"

```

```

    "nm": "Edd.num_bad_tx_bcb_blk",
  },
  {
    "ns": "DTN/bpsec",
    "nm": "Edd.num_good_rx_bcb_blk",
  },
  {
    "ns": "DTN/bpsec",
    "nm": "Edd.num_bad_rx_bcb_blk",
  },
  {

```

```

        "ns": "DTN/bpsec"
        "nm": Edd.num_missing_rx_bcb_blks",
    },
    {
        "ns": "DTN/bpsec"
        "nm": Edd.num_fwd_bcb_blks",
    },
    {
        "ns": "DTN/bpsec"
        "nm": Edd.num_good_tx_bcb_bytes",
    },
    {
        "ns": "DTN/bpsec"
        "nm": Edd.num_bad_tx_bcb_bytes",
    },
    {
        "ns": "DTN/bpsec"
        "nm": Edd.num_good_rx_bcb_bytes",
    },
    {
        "ns": "DTN/bpsec"
        "nm": Edd.num_bad_rx_bcb_bytes",
    },
    {
        "ns": "DTN/bpsec"
        "nm": Edd.num_missing_rx_bcb_bytes",
    },
    {
        "ns": "DTN/bpsec"
        "nm": Edd.num_fwd_bcb_bytes",
    },
    {
        "ns": "DTN/bpsec"
        "nm": Edd.num_good_tx_bib_blks",
    },
    {
        "ns": "DTN/bpsec"

```

```

        "nm": Edd.num_bad_tx_bib_blks",
    },
    {
        "ns": "DTN/bpsec"

```



```

        "nm": Edd.num_good_rx_bib_blks",
    },
    {
        "ns": "DTN/bpsec"
        "nm": Edd.num_bad_rx_bib_blks",
    },
    {
        "ns": "DTN/bpsec"
        "nm": Edd.num_miss_rx_bib_blks",
    },
    {
        "ns": "DTN/bpsec"
        "nm": Edd.num_fwd_bib_blks",
    },
    {
        "ns": "DTN/bpsec"
        "nm": Edd.num_good_tx_bib_bytes",
    },
    {
        "ns": "DTN/bpsec"
        "nm": Edd.num_bad_tx_bib_bytes",
    },
    {
        "ns": "DTN/bpsec"
        "nm": Edd.num_good_rx_bib_bytes",
    },
    {
        "ns": "DTN/bpsec"
        "nm": Edd.num_bad_rx_bib_bytes",
    },
    {
        "ns": "DTN/bpsec"
        "nm": Edd.num_miss_rx_bib_bytes",
    },
    {
        "ns": "DTN/bpsec"
        "nm": Edd.num_fwd_bib_bytes",
    },
    {
        "ns": "DTN/bpsec"
        "nm": Edd.last_update",
    },
    {
        "ns": "DTN/bpsec"

```

```
        "nm": Edd.num_known_keys",
    },
    {
        "ns": "DTN/bpsec"
        "nm": Edd.key_names",
    },
    {
        "ns": "DTN/bpsec"
        "nm": Edd.ciphersuite_names",
    },
    {
        "ns": "DTN/bpsec"
        "nm": Edd.rule_source",
    }
],
"description": "all known meta-data, externally defined data, and
    variables"
},
{
    "name": "source_report",
    "parmspec": [{ "type": "STR", "name": "Source" }],
    "definition": [{
        "ns": "DTN/bpsec",
        "nm": "Edd.num_good_tx_bcb_blks_src",
        "ap": [{
            "type": "ParmName",
            "value": "Source"
        }]
    },
    {
        "ns": "DTN/bpsec",
        "nm": "Edd.num_bad_tx_bcb_blks_src",
        "ap": [{
            "type": "ParmName",
            "value": "Source"
        }]
    },
    {
        "ns": "DTN/bpsec",
        "nm": "Edd.num_good_rx_bcb_blks_src",
        "ap": [{
            "type": "ParmName",
            "value": "Source"
        }]
    },
    {
        "ns": "DTN/bpsec",
```

"nm": "Edd.num_bad_rx_bcb_blks_src",

Internet-Draft

BPSEC ADM

July 2018

```
    "ap": [{
      "type": "ParmName",
      "value": "Source"
    }]
  },
  {
    "ns": "DTN/bpsec",
    "nm": "Edd.num_missing_rx_bcb_blks_src",
    "ap": [{
      "type": "ParmName",
      "value": "Source"
    }]
  },
  {
    "ns": "DTN/bpsec",
    "nm": "Edd.num_fwd_bcb_blks_src",
    "ap": [{
      "type": "ParmName",
      "value": "Source"
    }]
  },
  {
    "ns": "DTN/bpsec",
    "nm": "Edd.num_good_tx_bcb_bytes_src",
    "ap": [{
      "type": "ParmName",
      "value": "Source"
    }]
  },
  {
    "ns": "DTN/bpsec",
    "nm": "Edd.num_bad_tx_bcb_bytes_src",
    "ap": [{
      "type": "ParmName",
      "value": "Source"
    }]
  },
  {
    "ns": "DTN/bpsec",
    "nm": "Edd.num_good_rx_bcb_bytes_src",
```

```

        "ap": [{
            "type": "ParmName",
            "value": "Source"
        }]
    },
    {
        "ns": "DTN/bpsec",
        "nm": "Edd.num_bad_rx_bcb_bytes_src",

```

```

        "ap": [{
            "type": "ParmName",
            "value": "Source"
        }]
    },
    {
        "ns": "DTN/bpsec",
        "nm": "Edd.num_missing_rx_bcb_bytes_src",
        "ap": [{
            "type": "ParmName",
            "value": "Source"
        }]
    },
    {
        "ns": "DTN/bpsec",
        "nm": "Edd.num_fwd_bcb_bytes_src",
        "ap": [{
            "type": "ParmName",
            "value": "Source"
        }]
    },
    {
        "ns": "DTN/bpsec",
        "nm": "Edd.num_good_tx_bib_blks_src",
        "ap": [{
            "type": "ParmName",
            "value": "Source"
        }]
    },
    {
        "ns": "DTN/bpsec",
        "nm": "Edd.num_bad_tx_bib_blks_src",
        "ap": [{

```

```

        "type": "ParmName",
        "value": "Source"
    }
  ],
  {
    "ns": "DTN/bpsec",
    "nm": "Edd.num_good_rx_bib_blks_src",
    "ap": [
      {
        "type": "ParmName",
        "value": "Source"
      }
    ]
  },
  {
    "ns": "DTN/bpsec",
    "nm": "Edd.num_bad_rx_bib_blks_src",

```

```

        "ap": [
          {
            "type": "ParmName",
            "value": "Source"
          }
        ]
      },
      {
        "ns": "DTN/bpsec",
        "nm": "Edd.num_miss_rx_bib_blks_src",
        "ap": [
          {
            "type": "ParmName",
            "value": "Source"
          }
        ]
      },
      {
        "ns": "DTN/bpsec",
        "nm": "Edd.num_fwd_bib_blks_src",
        "ap": [
          {
            "type": "ParmName",
            "value": "Source"
          }
        ]
      },
      {
        "ns": "DTN/bpsec",
        "nm": "Edd.num_good_tx_bib_bytes_src",
        "ap": [
          {
            "type": "ParmName",

```

```

        "value": "Source"
    }
  ],
  {
    "ns": "DTN/bpsec",
    "nm": "Edd.num_bad_tx_bib_bytes_src",
    "ap": [{
      "type": "ParmName",
      "value": "Source"
    }]
  },
  {
    "ns": "DTN/bpsec",
    "nm": "Edd.num_good_rx_bib_bytes_src",
    "ap": [{
      "type": "ParmName",
      "value": "Source"
    }]
  },
  {
    "ns": "DTN/bpsec",
    "nm": "Edd.num_bad_rx_bib_bytes_src",

```

```

    "ap": [{
      "type": "ParmName",
      "value": "Source"
    }]
  },
  {
    "ns": "DTN/bpsec",
    "nm": "Edd.num_missing_rx_bib_bytes_src",
    "ap": [{
      "type": "ParmName",
      "value": "Source"
    }]
  },
  {
    "ns": "DTN/bpsec",
    "nm": "Edd.num_fwd_bib_bytes_src",
    "ap": [{
      "type": "ParmName",
      "value": "Source"
    }]
  },

```

```

    ]]
  },
  {
    "ns": "DTN/bpsec",
    "nm": "Edd.last_update_src",
    "ap": [{
      "type": "ParmName",
      "value": "Source"
    }]
  },
  {
    "ns": "DTN/bpsec",
    "nm": "Edd.last_reset",
    "ap": [{
      "type": "ParmName",
      "value": "Source"
    }]
  }
],
"description": "security info by source"
}
],

"Ctrl": [
{
  "name": "rst_all_cnts",
  "description": "This control causes the Agent to reset all counts
    associated with block or byte statistics and to set the Last
    Reset Time of the BPsec EDD data to the time when the control

```

```

    was run."
  },
  {
    "name": "rst_src_cnts",
    "parmspec": [{"type": "STR", "name": "src"}],
    "description": "This control causes the Agent to reset all counts
      (blocks and bytes) associated with a given bundle source and set
      the Last Reset Time of the source statistics to the time when
      the control was run."
  },
  {
    "name": "delete_key",

```

```

    "parmspec": [{"type": "STR", "name": "key_name"}],
    "description": "This control deletes a key from the BPsec system."
  },
  {
    "name": "add_key",
    "parmspec": [
      {"type": "STR", "name": "key_name"},
      {"type": "BYTESTR", "name": "keyData"}
    ],
    "description": "This control adds a key to the BPsec system."
  },
  {
    "name": "add_bib_rule",
    "parmspec": [
      {"type": "STR", "name": "source"},
      {"type": "STR", "name": "destination"},
      {"type": "INT", "name": "target"},
      {"type": "STR", "name": "ciphersuiteId"},
      {"type": "STR", "name": "key_name"}
    ],
    "description": "This control configures policy on the BPsec protocol
      implementation that describes how BIB blocks should be applied to
      bundles in the system. This policy is captured as a rule which
      states when transmitting a bundle from the given source endpoint
      ID to the given destination endpoint ID, blocks of type target
      should have a BIB added to them using the given ciphersuite and the
      given key."
  },
  {
    "name": "del_bib_rule",
    "parmspec": [
      {"type": "STR", "name": "source"},
      {"type": "STR", "name": "destination"},
      {"type": "INT", "name": "target"}
    ],
    "description": "This control removes any configured policy on the

```

```

    BPsec protocol implementation that describes how BIB blocks should
    be applied to bundles in the system. A BIB policy is uniquely
    identified by a source endpoint Id, a destination Id, and a target
    block type."
  },

```



```

{
  "name": "list_bib_rules",
  "description": "This control returns a table describinng all of the
    BIB policy rules that are known to the BPsec implementation."
},
{
  "name": "add_bcb_rule",
  "parmspec": [
    {"type": "STR", "name": "source"},
    {"type": "STR", "name": "destination"},
    {"type": "INT", "name": "target"},
    {"type": "STR", "name": "ciphersuiteId"},
    {"type": "STR", "name": "key_name"}
  ],
  "description": "This control configures policy on the BPsec protocol
    implementation that describes how BCB blocks should be applied to
    bundles in the system. This policy is captured as a rule which
    states when transmitting a bundle from the given source endpoint id
    to the given destination endpoint id, blocks of type target should
    have a bcb added to them using the given ciphersuite and the given
    key."
},
{
  "name": "del_bcb_rule",
  "parmspec": [
    {"type": "STR", "name": "source"},
    {"type": "STR", "name": "destination"},
    {"type": "INT", "name": "target"}
  ],
  "description": "This control removes any configured policy on the
    BPsec protocol implementation that describes how BCB blocks should
    be applied to bundles in the system. A bcb policy is uniquely
    identified by a source endpoint id, a destination endpoint id, and
    a target block type."
},
{
  "name": "list_bcb_rules",
  "description": "This control returns a table describing all of the bcb
    policy rules that are known to the BPsec implementation"
}
]
}

```

[5.](#) IANA Considerations

At this time, this protocol has no fields registered by IANA.

[6.](#) References

[6.1.](#) Informative References

[I-D.birrane-dtn-ama]
Birrane, E., "Asynchronous Management Architecture",
[draft-birrane-dtn-ama-07](#) (work in progress), June 2018.

[6.2.](#) Normative References

[I-D.birrane-dtn-adm]
Birrane, E., DiPietro, E., and D. Linko, "AMA Application
Data Model", [draft-birrane-dtn-adm-02](#) (work in progress),
June 2018.

[I-D.birrane-dtn-amp]
Birrane, E., "Asynchronous Management Protocol", [draft-
birrane-dtn-amp-04](#) (work in progress), June 2018.

[I-D.ietf-dtn-bpsec]
Birrane, E. and K. McKeever, "Bundle Protocol Security
Specification", [draft-ietf-dtn-bpsec-06](#) (work in
progress), October 2017.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
Requirement Levels", [BCP 14](#), [RFC 2119](#),
DOI 10.17487/RFC2119, March 1997,
<<https://www.rfc-editor.org/info/rfc2119>>.

Authors' Addresses

Edward J. Birrane
Johns Hopkins Applied Physics Laboratory

Email: Edward.Birrane@jhuapl.edu

Evana DiPietro
Johns Hopkins Applied Physics Laboratory

Email: Evana.DiPietro@jhuapl.edu

Internet-Draft

BPSEC ADM

July 2018

David Linko
Johns Hopkins Applied Physics Laboratory

Email: David.Linko@jhuapl.edu

