**Spring 2015 CCSDS**

**Space Data Link Security WG Minutes of Meeting**

**Caltech – Pasadena, USA,**

March 25-26, 2015

# Attendance:

|  |  |  |
| --- | --- | --- |
| Name | Organization | Email Address |
| Gilles Moury (Co-Chair) | CNES | [gilles.moury@cnes.fr](mailto:gilles.moury@cnes.fr) |
| Howard Weiss (Co-Chair) | NASA/SPARTA | [howard.weiss@parsons.com](mailto:howard.weiss@parsons.com) |
| Ignacio Aguilar-Sanchez | ESA/ESTEC | [ignacio.aguilar.sanchez@esa.int](mailto:ignacio.aguilar.sanchez@esa.int) |
| Brandon Bailey | NASA/GSFC | [brandon.t.bailey@nasa.gov](mailto:brandon.t.bailey@nasa.gov) |
| Craig Biggerstaff | NASA/JSC | [Craig.biggerstaff@nasa.gov](mailto:Craig.biggerstaff@nasa.gov) |
| Gian-Paolo Calzolari | ESA/ESOC | [Gian-Paolo.calzolari@esa.int](mailto:Gian-Paolo.calzolari@esa.int) |
| Jian Chen | CNSA | [chenjiach@gmail.com](mailto:chenjiach@gmail.com) |
| Matthew Cosby | UKSA/QinetiQ | [mcosby@qinetiq.com](mailto:mcosby@qinetiq.com) |
| Daniel Fischer | ESA/ESOC | [daniel.fischer@esa.int](mailto:daniel.fischer@esa.int) |
| Dorothea Richter | DLR/GSOC | [dorothea.richter@dlr.de](mailto:dorothea.richter@dlr.de) |
| Charles Sheehe | NASA/GRC | [charles.j.Sheehe@nasa.gov](mailto:charles.j.Sheehe@nasa.gov) |
| Aydar Vildanov | FSA/JSC | [vildanov@iss-reshtnev.ru](mailto:vildanov@iss-reshtnev.ru) |

# Agenda :

The agenda of the meeting was the following (**attachment 1**):

|  |
| --- |
| **Agenda Item** |
| 1 – Action items review |
| 2 – SDLS prototyping and interoperability testing :   * Interoperability testing results (ESA, CNES, NASA) * Interoperability test report (yellow book) finalization * Interoperability testing over the cloud |
| 3 – SDLS protocol draft blue book:   * Coordination of publication with TM, TC and AOS Space Link Protocols revised blue books * Prepare resolution for publication |
| 4 – SDLS Protocol green book :   * Review of contributions (AI 1114/01&06, 0414/04, 1111/07) * Completing missing sections   + Objective : publication November 2015 |
| 5 – SDLS Protocol extension (extended procedures) :   * Review of inputs (action items 1114/07, 08, 09) * Finalization of White Book v1   + Main text (generic specification)   + “Baseline mode” annex enabling bit-level interoperability |
| 6 – Action items and meeting wrap-up |

The list of presentations made is the following:

* + - Keith Scott presentation “CCSDS Cloud based interoperability testing” , CESG presentation, 02/02/2015 (**attachment 2)**
    - CNES presentation – SDLS Monitoring & Control messages, nov 2014 **(attachment 5)**

The list of input documents is the following:

* SDLS core protocol interoperability test report (yellow book), 355.1-Y-1 (**attachment 3**)
* SDLS Extended Proceduresv04.doc (**attachment 4**)

All presentations and attachments are on the SDLS WG CWE private page : <http://cwe.ccsds.org> : [The CCSDS Collaborative Work Environment (CWE)](http://cwe.ccsds.org/) > [Space Link Services Area (SLS)](http://cwe.ccsds.org/sls) > [Documents](http://cwe.ccsds.org/sls/docs/Forms/AllItems.aspx?View=%7b16ACDA38%2dFFA3%2d4657%2d8F27%2dB166C23C24A2%7d) > [SLS-SEA-DLS](http://cwe.ccsds.org/sls/docs/Forms/AllItems.aspx?RootFolder=%2Fsls%2Fdocs%2FSLS%2DSEA%2DDLS&View=%7b16ACDA38%2dFFA3%2d4657%2d8F27%2dB166C23C24A2%7d) > [CWE Private](http://cwe.ccsds.org/sls/docs/Forms/AllItems.aspx?RootFolder=%2Fsls%2Fdocs%2FSLS%2DSEA%2DDLS%2FCWE%20Private&View=%7b16ACDA38%2dFFA3%2d4657%2d8F27%2dB166C23C24A2%7d) > [meeting material](http://cwe.ccsds.org/sls/docs/Forms/AllItems.aspx?RootFolder=%2Fsls%2Fdocs%2FSLS%2DSEA%2DDLS%2FCWE%20Private%2Fmeeting%20material&View=%7b16ACDA38%2dFFA3%2d4657%2d8F27%2dB166C23C24A2%7d) > [march 2015 meeting](http://cwe.ccsds.org/sls/docs/Forms/AllItems.aspx?RootFolder=%2Fsls%2Fdocs%2FSLS%2DSEA%2DDLS%2FCWE%20Private%2Fmeeting%20material%2Fnovember%202011%20meeting&View=%7b16ACDA38%2dFFA3%2d4657%2d8F27%2dB166C23C24A2%7d)

# Agenda points

## Action items review

Review of open action items from previous meetings & telecons (action items closed at this meeting are highlighted in red. Action items remaining open are highlighted in yellow):

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0414/04 | G.Moury | Review and complete text for Recovery SA discussion | June 30,  2014  closed |

Closed: text of section 3.5.1.2 completed (Recovery SA in Telecommand) – text of section 4.7.5 (Recovery SA scenario) completed.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1111/07  (supersedes SDLS0511/12) | I.Aguilar, C.Biggerstaff, G.Moury, B.Saba | Provide missing subsections of the green book taking into account miscellaneous points listed in section 6. | oct 2013  open |

Open: on-going see point 4 of the agenda : SDLS green book

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1114/01 | I.Aguilar | Emphasize in Green Book the fact that BC frames are not protected and therefore do not carry Security Header nor Trailer. | April 30,  2015  open |

Open: BC not protected already specified in §5.2 of Blue Book. No need to duplicate requirements. Statement to be inserted in GB to emphasize this point.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1114/02 | D.Fischer / B.Saba | Investigate feasibility of real-time implementation through the network of test case #4 (close loop). In particular: firewall issue, SLE configuration, TCP/IP sockets. If not feasible, investigate co-location testing or, as a last resort, through e-mail exchange (frame by frame). | March 30,  2015  closed |

Closed: close-loop testing (test case #4) abandoned. Test objectives already covered by other test cases. Feasibility questionable.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1114/03 | G.Moury | Investigate possibility at CCSDS level to provide Cloud Based virtual machines to perform interoperability testing | March 30,  2015  closed |

Closed: see point 2 of the agenda: interoperability testing over the cloud. Action to Brandon Bailey to write a white paper on the subject. Keith Scott (CESG) prepared a briefing for the CESG on interoperability testing over the Cloud (see **attachment 2**). The scenario we want to cover is only : interoperability testing between 2 member agencies implementations of a standard.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1114/04 | G.Moury | Complete the yellow book on SDLS core protocol interoperability testing with the testing results available. | March 30,  2015  closed |

Closed: yellow book completed – see point 2 of the agenda (interoperability test report (yellow book) finalization)

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1114/05 | G.Moury | Post final version of TM, TC and AOS revised blue books on SDLS CWE. | Feb 30,  2015  closed |

Closed: final version of Space Data Link Protocols books integrating SDLS function, posted in [The CCSDS Collaborative Work Environment (CWE)](http://cwe.ccsds.org/) > [Space Link Services Area (SLS)](http://cwe.ccsds.org/sls) > [Documents](http://cwe.ccsds.org/sls/docs/Forms/AllItems.aspx?View=%7b16ACDA38%2dFFA3%2d4657%2d8F27%2dB166C23C24A2%7d) > [SLS-SEA-DLS](http://cwe.ccsds.org/sls/docs/Forms/AllItems.aspx?RootFolder=%2Fsls%2Fdocs%2FSLS%2DSEA%2DDLS&View=%7b16ACDA38%2dFFA3%2d4657%2d8F27%2dB166C23C24A2%7d) > [Draft Documents](http://cwe.ccsds.org/sls/docs/Forms/AllItems.aspx?RootFolder=%2Fsls%2Fdocs%2FSLS%2DSEA%2DDLS%2FDraft%20Documents&View=%7b16ACDA38%2dFFA3%2d4657%2d8F27%2dB166C23C24A2%7d) > SDLP books

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1114/06 | I.Aguilar | Add short summary text in annex D of GB for SDLS potential interaction with TM performances. | March 30,  2015  open |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1114/07 | G.Moury | Provide specification of CLSR for §4.2.2 of extended procedures book (model after CLCW specification). | March 30,  2015  closed |

Closed: specification provided – see point 5 of the agenda – review of inputs

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1114/08 | B.Saba | Provide specification for Monitoring & Control services (services, directives, procedures, SCD/SMD definition) – text for §3.4 and 5.6 | March 30,  2015  open |

Open: to be completed for section 5.6 with bit level specification of PDU formats and corresponding diagrams – see point 5 of the agenda

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1114/09 | D.Fischer | Introduce the TLV format as agreed at this meeting for the SCD/SMD format (extended procedures PDU spec) | March 30,  2015  open |

Open: TLV format to be further specified in a dedicated section (§2.4) of extended procedures book with additional figures – see point 5 of the agenda

## SDLS prototyping and interoperability testing

### Interoperability testing results (ESA, CNES, NASA)

Interoperability testing of SDLS Core protocol has been completed in 2 steps:

* CNES – ESA : for test cases #1 (TC without COP), 2 (TC with COP) and 3 (TM) where ESA implemented/simulated the ground part and CNES the on-board part.
* CNES – NASA : for test case #4 (AOS) where NASA implemented/simulated the on-board part and CNES the ground part.

Close-loop testing where an SDLS secured TC link is looped back with a TM secured TM link, once envisaged for SDLS Core protocol interoperability testing, has been deferred to the interoperability testing of the extended procedures, for which it is mandatory.

### Interoperability test report (yellow book) finalization

The interoperability test report has been finalized (**attachment 3**) and will be forwarded to the CCSDS technical editor to support the CESG/CMC poll asking for SDLS core protocol blue book publication.

### Interoperability testing over the cloud

The scenario considered for the use of cloud based services is the following:

* 2 or more agencies interconnecting implementations of a given recommendation to be validated by interoperability testing
* Each agency uses its own certified cloud services provider satisfying its own security policies wrt SW protection. CNES and NASA have a number of trusted providers. Nevertheless the type of SW that can be installed on those cloud based virtual machines is to be investigated.

A presentation was made by Keith Scott (NASA/MITRE) in the frame of CESG to investigate the various types of services and the confidentiality clauses (**attachment 2**). The IAAS (Infrastructure as a Service) enabling complete control over a machine and segregation from other users seems to be the appropriate service model for interagency testing.

Brandon Bailey has taken the action to write a white paper (technical note) on cloud based interoperability testing taking as an example the extended procedures interoperability testing.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0315/01 | B. Bailey | Write a white paper on interoperability testing over the cloud applied to extended procedures. | 15 October,  2015 |

## SDLS protocol draft blue book

### Status of draft blue book

Draft blue book (red-4 v4) incorporating all RIDs dispositions from final agency review has been delivered to CCSDS editor together with RIDs dispositions. This book is ready for publication now that interoperability testing has been completed. CCSDS editor is waiting for SDLS testing yellow book and SLS AD resolution to publish.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0315/02 | G.Moury | Prepare resolution for publication of SDLS blue book and forward to SLS Area Director for initiating CESG/CMC poll. Forward interoperability test report to CCSDS technical editor. | 15 May,  2015 |

### Coordination of publication with TM, TC and AOS Space Link Protocols revised Blue Books

TM, TC and AOS space data link protocols revised blue books are finalized in the form of pink sheets. One final edit was done at the last meeting by the SLP WG. Objective is to publish simultaneously those 3 books with the SDLS by next spring meeting.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0315/03 | G.Moury | Coordinate publication resolution for TC, TM and AOS recommendations with SDLS one. | 15 May,  2015 |

## SDLS protocol green book

Complete text was reviewed and completed in several sections during the meeting.

New template for Green Books has been taken into account.

In annex D (**action 1114/06**), a section on interaction between TM/AOS and SDLS will be added discussing:

* Necessity of frame CRC depending on channel code option used :
  + Uncoded, convolutional, R-S E=16, R-S E=8, Turbocodes, LDPCC
* Based on undetected frame error rates performances for the various codes with or without the frame CRC.

A table could be added recommending frame CRC depending on AOS/TM channel coding option: uncoded, convolutional, R-S E=8 and Turbo options require frame CRC since their undetected frame error rate is not perfect. For R-S E=16 it is useless given the code performance. For LDPCC it has to be checked.

Green book updated during this meeting will be distributed to the WG by Ignacio Aguilar (GB editor) and further elaborated before the fall meeting so as to target a finalization of this book at the next meeting.

## SDLS Protocol Extension (extended procedures)

### Review of inputs

Two inputs were received before the meeting and incorporated into the extended procedures document (SDLS Extended procedures v04 – **Attachment 4**):

* Addition of Frame Security Report/ Command Link Security Report specification (§4.2.2)
* Addition of Monitoring & Control Service specification (§ 2.3.3, 2.4, 3.4, 5.6 (partial))

The TLV (Tag Length Value) format specification proposed as a generic format for all extended procedures PDUs should be moved from section 2.4 to section 5.3 and further developed. The specification of the TLV format should complemented with additional figures/diagrams to show the various possibilities (nested, …). A decision has to be taken on the size of the length field: at the moment it is proposed 16 bits allowing a TLV data unit up to 65535 octets in length.

### Review of extended procedures document v04

#### Review of main text (generic specification)

The document was reviewed linearly during the meeting. The following remarks, contributions were made :

**§2.3.1 :** insert in section 2 a state model for key management

**§3.4:** an introduction is needed.

ARC (Anti-Replay Counter) should be replaced by SN (Sequence Number) or anti-replay Sequence Number systematically in the section.

As a general rule, it should always be made clear whether it is the sending side or the receiving side that initiates or responds to the procedure.

§3.4.2.1: NOP directive

* Add procedural step even for this directive
* Add a parameter to this directive : the SA targeted

Daniel Fischer will review this M&C part to align level of spec to other service specifications (SA management, Key management)

§3.4.2.2.2: PING procedural steps

* Add a generic statement (either NOTE or requirement) stating that any report generated on-board shall be logged in the recipient log file.
* Ping request will just enable to check that the security unit is alive
* The specific SA reserved for extended procedures could be used to transmit that Ping request

§3.4.2.3: Security Log Status

* Add “capacity left” in the report

§3.4.2.4: Dump log:

* Do not specify the internal format of the log. Internal format is implementation specific. It is not possible to specify all possible entries.

§3.4.2.8: Write Security Message

* Directive not needed, no purpose for the sending side to write an entry into the security log of the receiving side.

A “Security Event” procedure is needed which enables automatic generation of security report whenever a security event occurs. This directive was proposed in CNES presentation at the last meeting (see slide 17 – **attachment 5**). This procedure should log entry for:

* Incorrect SN (replay, out of window)
* Incorrect MAC
* Invalid SPI
* SA unavailable (desactivated, unkeyed)
* Extended procedures white book

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0315/04 | B.Saba | Add subsection in 3.4 and 5.6 for specification of “Security Event” procedure and PDU | 15 Sept,  2015 |

§4.2.1.2: change to “SDLS extended procedures PDU shall be protected by authentication a s a minimum” instead of “ … shall be protected by the SDLS protocol”. The rationale is that for hosted payload or earth observation payloads, the SDLS extended procedures directives might be transmitted using secured packet transmission to recipient on-board and not SDLS. Therefore, there are 2 cases for the transmission scenario for transmission of EP directives to security unit:

* In-band signaling: i.e. transmission using reserved SA over SDLS protected space data link protocol.
* Out of band signaling : i.e. secured packet transmission to recipient on-board (end-to-end authentication required as a minimum)

§4.2.2.4.7: need for an FSR alarm field reset directive, this field being remanent.

§5.3.1: full specification of the TLV format should be inserted in that section with:

* 16-bit Tag
* 16-bit length field

#### Review of baseline mode annex (Annex E – as for SDLS blue book)

The following agreement was reached on the perimeter/parameters for the baseline mode for EP:

* Key size : 128 bits
* Algorithm to encrypt the key should be specified
* Key ID : 16-bit
* Master key ID : [0-255]
* Session key ID: [256-65535]
* Challenge/response (key verification procedure §5.4.3.5.2): scheme to be specified
* Key DB status request:
  + DB integrity check method left to the implementers
  + Request 🡺 TAG
  + Response 🡺 OK/NOK
* Load SA: need to define format for each internal parameter of SA
  + Anti replay sequence number : 32 bits
  + Anti replay window : 32 bits
* “SA self-test” not needed if the NOP directive (of the M&C services) addresses a specific SA
  + Add a parameter to the NOP directive : SA
* Log status request: OK
* Dump log (not necessarily needed):
  + No specification of security messages and log entries
  + Description of security messages (typical) should be in GB
* Self test:
  + No specification of the test to be performed
  + Result : OK/NOK
* Read Anti-Replay Sequence Number
* Set Anti-Replay Sequence Number
* Set anti-replay window

For the baseline mode (Annex E), two cases would be covered:

1. Baseline mode for TC link only:
   * TC uplink authenticated
   * TM unprotected
2. Baseline mode for full configuration TC/TM/AOS(PLTM)
   * TC uplink authenticated
   * TM downlink (TM Space Data Link Protocol) authenticated and encrypted
   * PLTM downlink (AOS Space Data Link Protocol) authenticated and encrypted

The objective is to finalize a first version of Extended Procedures White Book for next meeting, integrating:

* All 6 sections of the main body of the document
* Annex E defining baseline mode

To achieve this, the following action items have been set up:

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0315/05 | Daniel Fischer | Update extended procedures book to include generic PDU format definition/specification (TLV format) | 15 June,  2015 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0315/06 | B.Saba  Craig Biggerstaff | Provide detailed specifications for the SA Management (CB) and the M&C (BS) directives/reports procedures and PDUs (§3.3, 3.4, 5.5, 5.6) | 15 Sept,  2015 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0315/07 | B.Saba  Craig Biggerstaff  Daniel Fischer | Define directives/procedures/parameters needed for baseline mode (i.e. text for annex E) | 15 Sept,  2015 |

## Overall Planning

The target planning (which will be put on the CWE framework for the SDLS project) is:

SDLS core protocol:

* Yellow book : March 2015
* Blue book publication : june 2015
* Green book publication: November 2015

SDLS extended procedures:

* White book V1 completed : Nov 2015
* Red book 1 (including baseline configuration): January 2016

## AOB

None

# List of decisions and action items agreed at this meeting

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0315/01 | B. Bailey | Write a white paper on interoperability testing over the cloud applied to extended procedures. | 15 October,  2015 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0315/02 | G.Moury | Prepare resolution for publication of SDLS blue book and forward to SLS Area Director for initiating CESG/CMC poll. Forward interoperability test report to CCSDS technical editor. | 15 May,  2015 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0315/03 | G.Moury | Coordinate publication resolution for TC, TM and AOS recommendations with SDLS one. | 15 May,  2015 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0315/04 | B.Saba | Add subsection in 3.4 and 5.6 for specification of “Security Event” procedure and PDU | 15 Sept,  2015 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0315/05 | Daniel Fischer | Update extended procedures book to include generic PDU format definition/specification (TLV format) | 15 June,  2015 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0315/06 | B.Saba  Craig Biggerstaff | Provide detailed specifications for the SA Management (CB) and the M&C (BS) directives/reports procedures and PDUs (§3.3, 3.4, 5.5, 5.6) | 15 Sept,  2015 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0315/07 | B.Saba  Craig Biggerstaff  Daniel Fischer | Define directives/procedures/parameters needed for baseline mode (i.e. text for annex E) | 15 Sept,  2015 |