**Fall 2014 CCSDS**

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

**BSI – London, UK,**

November 12-13, 2014

# Attendance:

|  |  |  |
| --- | --- | --- |
| Name | Organization | Email Address |
| Gilles Moury (Co-Chair) | CNES | gilles.moury@cnes.fr |
| Howard Weiss (Co-Chair) | NASA/SPARTA | howard.weiss@parsons.com |
| Ignacio Aguilar-Sanchez | ESA/ESTEC | ignacio.aguilar.sanchez@esa.int  |
| Brandon Bailey | NASA/GSFC | brandon.t.bailey@nasa.gov  |
| Gordon Black | UKSA/QinetiQ | gordon.black@outlook.com |
| Jian Chen | CNSA | chenjiach@gmail.com  |
| Matthew Cosby | UKSA/QinetiQ | mcosby@qinetiq.com  |
| Daniel Fischer | ESA/ESOC | daniel.fischer@esa.int  |
| Martin Pilgram | DLR | martin.pilgram@dlr.de |
| Dorothea Richter | DLR/GSOC | dorothea.richter@dlr.de  |
| Bruno Saba | CNES | bruno.saba@cnes.fr  |
| Greg Kazz | NASA/JPL | greg.j.kazz@jpl.nasa.gov  |
| Charles Sheehe | NASA/GRC | charles.j.Sheehe@nasa.gov  |
| Gian-Paolo Calzolari | ESA/ESOC | gian.paolo.calzolari@esa.int  |
| Thomas Ganett | NASA/AIAA | tomg@aiaa.org  |
| Ed Greenberg | NASA/JPL | egreenberg@jpl.nasa.gov  |
| Jin-Ho Jo | ETRI | jhjo@etri.re.kr  |
| R.Lee Pitts | NASA/MSFC | Robert.l.pitts@nasa.gov  |
| Aydar Vildanov | FSA/JSC | vildanov@iss-reshtnev.ru  |
| Lorenzo Marchetti | ESA/VEGA | lorenzo.marchetti@esa.int  |

# 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)
 |
| 3 – SDLS protocol draft blue book:* Status of document
* Coordination of publication with TM, TC and AOS Space Link Protocols revised blue books
 |
| 4 – SDLS Protocol green book :* Review of contributions (action items SDLS 1111/07, 0414/04)
* Review of document
	+ Objective : simultaneous publication with blue book
 |
| 5 – SDLS Protocol extension (extended procedures) :* Review of inputs (action items SDLS 0412/07, 1012/10, 1013/07, 0414/03)
* Discussion of specification for
	+ Security Control Directives and Monitoring Data
	+ Real-time reporting of SDLS (CLSR)
* 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:

* + - ESA presentation “SDLS interoperability testing” (**attachment 2 )**
		- NASA plan for SDLS testing (**attachment 4**)
		- CNES presentation “SDLS AOS protocol simulator” (**attachment 5**)
		- CNES SDLS implementation surprises (**attachment 6**)
		- CNES presentation – SDLS Monitoring & Control services (**attachment 9**)

The list of input documents is the following:

* SDLS interoperability test report ESA-CNES (**attachment 3**)
* NASA SDLS prototype plan (**attachment 7**)
* SDLS interoperability testing yellow book (**attachment 8** )

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) > [november 2014 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** |
| --- | --- | --- | --- |
| SDLS0414/01 | G.Moury & C.BIggerstaff | Finalize disposition of all RIDs on SDLS core protocol and issue review package (red-4 v4 + dispositioned RIDs) for WG final approval and for further transmission to CCSDS Technical Editor with appropriate resolution for preparing Blue Book |  April 30,2014closed |

Closed: red-4 v4 + dispositionned RIDs approved by WG and sent to CCSDS editor (mail 5/7/14)

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0414/02 | B.Saba | Propose content of configuration file for exchange of configuration parameter between simulators. |  May 30,2014closed |

Closed : proposal sent to ESA for interoperability testing

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0414/03 | G.Moury | Propose text for Type-2 SDLS OCF insertion in TM/AOS books. Investigate possibility to insert type-2 OCF, without agency review, in the revised version of TM/AOS books to be published simultaneously with SDLS Core Protocol book. |  June 30,2014closed |

Closed: done – sent by mail to SDLS and SLS WGs – 24/10/14 – presented at both meetings

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

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

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1013/05 | B.Saba & D.Fischer | Exchange simulators specifications. |  1st version : Dec 30, 2013Final version: Apr 30, 2014closed |

Closed: simulators specs exchanged between ESA and CNES

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1013/07 | G.Moury | Investigate modifications needed to AOS and TM specs to accommodate type-2 (SDLS) OCF |  Mar 15, 2014closed |

Closed: modification to TM and AOS blue books drafted and proposed to SLP WG for potential inclusion in on-going revision of TM and AOS blue books. Proposal rejected at this stage since it would require an additional agency review and referencing an unpublished blue book (SDLS extended procedures) for the specification of the content of the SDLS OCF (CLSR). Subject to be further discussed at spring 2015 meeting with SLP WG (operational aspects: multiplexing CLCW and CLSR, hot redundancy and cross-strapping of SDLS Processor)

|  |  |  |  |
| --- | --- | --- | --- |
| A.I. | Actionee | Action | Deadline |
| SDLS1013/10 | G.Moury | Forward to CESG the question of the acceptatbility to limit SDLS interoperability testing to TC and AOS |  Mar 15, 2014closed |

Closed : Interoperability testing of SDLS should cover TM, TC and AOS.

| **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 2013open |

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

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0412/07 | B.Saba | Propose SDLS Management & Control functions and directives, including : rationale, function, action, response  | oct 2013closed |

Closed: see point 5 of the agenda – presentation “Monitoring and control messages proposal” – attachment xx

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1012/10 | B.Saba | Develop specification for one SDLS Monitoring & Control directive following agreed framework and book structure for extended procedures |  oct 2013closed |

Closed: see point 5 of the agenda – presentation “Monitoring and control messages proposal” – attachment 9

## SDLS prototyping and interoperability testing

### SDLS interoperability testing over TM/TC by ESA-CNES

See ESA presentation “SDLS interoperability testing” – **attachment 2**

ESA/ESOC prototype/implementation covers more than the SDLS core protocol but also part of the extended procedures (key management, …).

SDLS can be tested locally with the SCOS ground system connected to a spacecraft simulator and the SDLS security unit simulator. The ESA Test Environment uses software modules to simulate the entire space communication chain “MCS-satellite”.

Interoperability tests have been performed between ESA and CNES where ESA simulates the ground part and CNES the on-board part:

* ESA generates secured TC frames with or without security errors. CNES decodes those TC frames emulating the on-board receiving part.
* CNES generates TM secured transfer frames, without or with security errors, emulating the on-board TM/SDLS part. ESA decodes those TM frames emulating the ground receiving part.

Four test cases where defined to cover the various type of traffic (see test report in **attachment 3**):

* Test case #1: TC link – SDLS baseline mode - BD frames only – security errors: invalid SPI, SN out of range, replay, invalid MAC
	+ OK: all frames correctly decoded. All errors detected
* Test case #2: TC link – SDLS baseline mode - AD frames + BC frames – security errors: replay, invalid MAC – transmission errors: single bit errors, burst errors, errors on AD and BC frames
	+ OK: all frames correctly decoded. All errors detected: transmission errors detected by the COP, security errors detected by SDLS receiver
	+ Test case #2 enabled to detect that both implementations added a Security Header and Trailer to BC frames. Apparently the fact that BC frames are not protected and therefore do not carry Security Header and Trailer is not emphasized enough. Should be highlighted in the Green Book (see action SDLS 1114/01).

| **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 |

* Test case #3: TM link – baseline mode: Authenticated encryption – security errors: invalid SPI, replay, invalid MAC
	+ OK: all frames correctly decoded. All security errors detected.
	+ SN out of window not tested in TM 🡺 to be added for completeness.
* Test case #4: concurrent execution of TC (with COP) and TM link. This is equivalent to the concurrent execution of test cases #2 and #3. It is a closed loop test that ideally requires real-time connection of ground simulator with on-board simulator. This real-time connection through internet poses 2 problems :
	+ Getting a common working configuration of SLE protocol between the sending and receiving end
	+ Direct network connection by-passing the firewalls or co-location of implementation

In terms of test coverage and SDLS validation, test cases #2 and #3 are complete. Nevertheless a close loop TC/TM test would complete the validation of the non-interaction of the COP with SDLS. A work-around for test case #4 implementation could be e-mail exchange of a sequence of TC and TM frames, frame by frame. This would take much longer but still would serve the purpose.

| **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 |

To avoid the firewall issues or the colocation cost for interoperability testing, a solution could be to use virtual machines on a Cloud Services like Amazon Web Services. CCSDS could investigate to use/provide such a service to perform the interoperability testing of protocols which is required by CCSDS rules.

| **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 |

### SDLS interoperability testing over AOS

NASA ITC (Independent Test Capability) (Brandon Bailey) made a presentation on its capacity in terms of TM/TC systems simulation (see presentation “NASA plan for SDLS testing” – **attachment 4**). In general they perform independent validation of Flight Software and Ground SW. NASA ITC made also a proposal for an SDLS prototype plan (**attachment 7**).

Since interoperability of SDLS over AOS is presently missing, the WG proposes that NASA ITC concentrates on simulating SDLS Secured AOS transfer frames, that CNES could decode with its own AOS simulator (see CNES presentation “SDLS AOS protocol simulator” – **attachment 5**). A JWST SW/simulator could be used to generate AOS frames.

SDLS interoperability testing over AOS could be limited to test case #3. Close loop test (test case #4) is not necessary for AOS, especially if it is done for TM in close loop with TC-COP. In any case, close loop testing will really be mandatory only for extended procedures.

### Test findings

CNES made a short presentation (CNES SDLS implementation surprises – **Attachment 6**) pointing out 2 mistakes made by the implementers:

* Segment header placed after the Security Header in TC
* BC frames protected in TC, therefore unduly carrying security header and trailer.

Those mistakes were made by two independent developers. This maybe shows that those specifications are not clear enough in the blue book or at least should be emphasized in the green book. Action 01 was set up to answer this concern.

### Way forward

The SDLS yellow book (**attachment 8**) on interoperability testing of SDLS should be completed with the elements in the test report (**attachment 3**) covering SDLS testing over TM/TC. It should also be completed with the results of the SDLS over AOS interoperability testing to be performed by NASA-CNES.

| **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 |

## SDLS protocol draft blue book

### Status of document

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 once interoperability testing has been completed. CCSDS editor is waiting for SDLS testing yellow book and SLS AD resolution to publish.

### 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. One final edit was done at this 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** |
| --- | --- | --- | --- |
| SDLS1114/05 | G.Moury | Post final version of TM, TC and AOS revised blue books on SDLS CWE. |  Feb 30,2015 |

## SDLS protocol green book

Text missing in a few places:

* Recovery SA scenarios (§4.7.5): inputs in TAS presentation on SDLS red-2 comments
* For Annex D (interaction with data link performances), a short summary text for SDLS interaction with TM. Present text of annex D deals only with TC interaction.
* Sections 4 & 5 of annex A (justification of baseline mode)
* Sections 4.2 (Concept of operation: synchronization IV, SN), 4.3 (Concept of operation: authentication), 4.4 (concept of operation: encryption), 4.5 (concept of operation: authenticated encryption)
* …

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

## SDLS Protocol Extension (extended procedures)

### Security Control Directives and Monitoring Data

CNES (B.Saba) made a presentation on Security Control Directives (SCD) and Monitoring Data (SMD) (see **attachment 9**):

* SCD/SMD messages transmission could be either:
	+ CCSDS packets with a mission defined APID
	+ Specific control frames in TC
* There might be the need for a timestamp instead or in addition to the packet counter
* Internal format of SCD/SMD:
	+ Proposal to use a TLV format (Tag, Length, Value) which offers a lot of flexibility for SDLS future evolutions and for user specific needs

**Conclusion on formatting:**

* **TLV formatting rules would be specified in the extended procedures BB**
* **Bit level format specifications for the minimal set of SCD/SMD would be specified in baseline mode annex of extended procedures BB**

### Monitoring & Control services:

The list of M&C directives has been agreed from the CNES presentation (see **attachment 9**):

* Security Log status request (nb of reports in log, capacity left, full flag, …) + response
* Dump log + response
* Erase log + response
* Self-test (should be specified in a very general manner)+response
* NOP (is only meaningful if you have real-time reporting mechanism like CLSR to see the ARC incrementing)
* Security event : generated automatically, not necessarily transmitted but put in the log file
* Read ARC + response

**Real-time reporting of SDLS on-board security processor**:

* It is proposed to defined a CLSR (Command Link Security Report) following the model of CLCW (Command Link Control Word – reporting from the TC-COP) and transmitted real-time in the OCF field of TM transfer frames. CLSR is updated regularly each time there is a TC frame received by the SDLS processor.
* A proposal is made in CNES presentation (**Attachment 9**) which has been extensively discussed:
	+ CLSR in 2 parts (CLSR1 & 2) of 32 bits each carrying alarm flags (MAC, ARC, SPI), SPI and ARC
* A simplified approach would be to concentrate CLSR into one 32-bit word only by transmitting only the 8-LSB of the ARC, with the following content:
	+ Control word type (3 bits)
	+ Alarm bit (1 bit): persistent (would have to be reset by SCD from the ground)
	+ Error flags (MAC, SPI, ARC): not persistent – relative to current reported TC frame – updated at each received TC frame
	+ SPI (16 bits)
	+ ARC 8-LSB (8 bits)

**Conclusion on CLSR:**

* **CLSR bit level specification to be inserted in SDLS extended procedures BB in section 4.2.2., specifiying format + behavior**

| **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 |

### Extended procedures white book

It is agreed to proceed in 2 stages:

1. Complete the generic part of the extended procedures (main text) specifying services, directives, procedures and PDU
2. Develop a baseline mode to enable full interoperability of the extended procedures in identified cross-support scenario(s), as an annex to the document. This annex should provide bit level specification for the directives & reports strictly needed for the scenario(s) and the associated transport mechanism(s) (packets, control frames, OCF, …)

Cross-support scenario(s) should be defined in extended procedures Green Book. Potential definition:

* + Agency A operating Agency B spacecraft in SDLS secure mode
	+ Predefined set of keys
	+ No OTAR
	+ Predefined set of SA.

For the extended procedures BB it is decided to retain the level of details of the Key management services (§3.2 & 5.4) and to apply it to:

* SA management services
* Monitoring and Control services

With respect to the update of the extended procedures white book, 3 action items have been agreed:

* + SDLS1114/07 : provide CLSR specification in §4.2.2.

| **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 |

| **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 |

## Overall Planning

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

SDLS core protocol:

* AOS Interoperability testing (NASA-CNES) : Jan-Feb 2015
* Yellow book : March 2015
* Blue book publication : june 2015
* Green book publication: November 2015

 SDLS extended procedures:

* White book V1 completed : June 2015
* Red book 1 (including baseline configuration): November 2015

## AOB

None

# List of decisions and action items agreed at this meeting

| **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 |

| **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 |

| **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 |

| **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 |

| **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 |

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

| **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 |

| **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 |

| **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 |