**April 2018 CCSDS**

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

**NIST – Gaithersburg, USA**

April 11-12, 2018

# Attendance:

**SDLS WG meeting:**

|  |  |  |
| --- | --- | --- |
| 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  |
| Kenneth Andrews | NASA/JPL | andrews@shannon.jpl.nasa.gov  |
| Craig Biggerstaff | NASA/JSC | craig.biggerstaff@nasa.gov  |
| Matthew Cosby | UKSA | matt.cosby@goonhilly.org  |
| Daniel Fischer | ESA/ESOC | daniel.fischer@esa.int  |
| Anthony Scott Reeves | NASA/MSFC | scott.reeves@nasa.gov  |
| Dorothea Richter | DLR/GSOC | dorothea.richter@dlr.de  |
| Scott Schield | NASA/GSFC | scott.w.schield@ivv.nasa.gov  |

**Joint session with Space Data Link Protocol WG on interface between SDLS and USLP:**

* Participation from SDLP WG and SDLS WG

# Agenda :

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

|  |
| --- |
| **April 11-12**  |
|

|  |  |  |
| --- | --- | --- |
| **Date/time** | **Room** | **Agenda Item** |
|  |  | 1 - Action items review |
| 2 – SDLS Protocol extension (extended procedures):* Review of last modifications introduced in red book before Agency Review
* Interoperability testing
	+ Test of procedures modified at last meeting (OTAR, key verification, key verification, ARC field in rekey PDU, identification of direction in subgroup field of PDU header (SA management), SA direction identification, “bad SPI” flag redefinition)
	+ Final results of interoperability testing and associated report (yellow book).
 |
| 3 – SDLS / USLP compatibility / coherency:* Evolution of SDLS books to include USLP as SDLP
* USLP interaction with SDLS (edits to USLP red book for FSR and MC\_OCF, need for a UPID for SDLS EP directives)
* USLP interoperability testing with SDLS

  |
| 4 – SDLS Extended Procedures Green Book:* Review of contributions (AI SDLS 1117/02)
 |
| 5 - Physical layer security:* + Discussion of use case for bulk encryption (AI SDLS1117/03)
 |
| 5 – Meeting conclusions |

 |

The list of presentations made is the following:

* + - agenda (**attachment1)**

The list of input/output documents is the following:

* SDLS Extended Procedures Green v1 GM - BS - DF-20180411.docx (**attachment 2**)
* SDLS Extended Procedures Red 1v6 Clean 20171109-replytoPScomments modif 2018-04-11.docx (**attachment 3**)

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) > [april 2018 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** |
| --- | --- | --- | --- |
| SDLS0416/08 | B.Saba | Check suitability of Cloud Sigma as a cloud service provider for exporting code for interoperability testing. |  15 July,2016open |

* Daniel Fischer will transmit to Bruno Saba the ESA IT responsible contact for cloud testing contract.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0517/03 | D.Fischer | Introduce a subsection in SDLS Extended Procedures GB to describe CONOPS for switching keys on a secure channel “on the fly” vs “offline” |  30 Mar,2018closed |

* Section 3.2.5 “Seamless Key change (from frame to frame)” introduced in SDLS EP GB.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0517/10 | WG members | Provide refinements to GB outline : rationale + CONOPS parts |  30 Mar,2018closed |

* Done: SDLS extended Procedures GB outline was finalized before the meeting and reflected in the green book version reviewed during the meeting (**attachment 2**)

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1117/01 | G.Moury | Initiate agency poll at CMC level to determine potential interest in physical layer security (protection against jamming/interference) |  30 Dec.,2017open |

* Open: poll to be initiated. Formulation TBD to encompass both physical layer security and bulk encryption which was proposed by Victor Sank at the last meeting for possible standardization by CCSDS (§3.2.6 of Nov 2017 MoM).

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1117/02 | C.Biggerstaff | Distribute EP GB template |  30 Dec,2017closed |

* Done: EP GB template was distributed and used by contributors to provide their part.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1117/03 | V. Sank | Provide use cases for bulk encryption (missions requiring it) and associated interoperability and/or cross-support scenarios. |  30 March,2018open |

* Open : bulk encryption principles and advantages/drawbacks with respect to other security options are discussed in 350.0-G-2 (§5.2 and 6.4.1). Bulk encryption can be implemented in a black box inserted in an existing TC receiving chain provided that the bulk encryption is performed between frame generation and channel coding. It provides protection against traffic analysis but not against jamming which requires other techniques like spread spectrum, frequency hopping, antenna nulling, …

## SDLS extended procedures red book

Compared to the red book version that was finalized at the last meeting, a number of editorial modifications were introduced in the document as a result of disposition of comments received from SEA AD before CESG poll to initiate Agency Review for this SDLS EP red book. Those modifications are highlighted in the attached version of the document (**attachment 3**). Main editorial modifications are in sections 2.1, 2.2, 2.3.1 (Key lifecycle), 2.4 (FSR multiplexing scheme), 3.3 (clarification of SA management service), 4.1 (clarification of secure channel used to transport EP PDUs over the spacelink), annex E (acronyms list completed).

Additional editorial modifications were made during the meeting in §4.1. A RID should be made for agency review to introduce those modifications:

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0418/01 | G.Moury | Generate RID for SDLS EP red book agency review to introduce editorial modification made to §4.1 during meeting (see **attachment 3**) |  July,2018 |

Reference to type-2 OCF (i.e. FSR) should be added to TM and AOS Space Data Link Protocol blue books in §4.1.5.4 Operational Control Field (OCF). This should be inserted in TM and AOS SDLP pink sheets.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0418/02 | G.Moury | Submit input to TM and AOS SDLP BB upcoming pink sheets to introduce reference to FSR in §4.1.5 of those BB. |  July,2018 |

## SDLS Extended Procedures Intra & Interoperability testing

ESA/ESOC (David Koisser) and NASA/IVV (John Lucas) will resume and complete interoperability testing of Extended Procedures once the EP red-1 Agency Review is completed in order to take into account all technical modifications made in the standard as a result of RIDs dispositions.

USLP interoperability testing will cover only insertion/recovery of SDLS Security Header and Trailer. SDLS Core and extended procedures interoperability testing do not cover USLP because the simulation of the space data link protocol is only covering TM, TC and AOS (SCOS2000 for ESA). On NASA side, USLP simulation software for USLP interoperability testing has been developed at NASA/MSFC. Its integration with SDLS EP simulation SW developed at NASA/IVV to have a combined simulation of USLP and SDLS could be envisaged.

To take into account USLP in SDLS blue books (355.0 and 355.1), modifications need to be introduced in those 2 documents to reference USLP and specify parameters for operating SDLS over USLP (e.g. authentication mask to be adapted to USLP frame header). If USLP is published before Extended Procedures (355.1), EP BB can easily be updated to include USLP as a supported space link protocol.

## Extended Procedures Green Book

The reference of the document is: 350.11-G.

Craig Biggerstaff has distributed the template of the document that was used by the contributors to insert their part.

The document resulting from the various contributions and the modifications/additions made during the review of the document at the meeting is provided in**:**

SDLS Extended Procedures Green v1 GM - BS - DF-20180411.docx (**attachment 2**).

The various points discussed are the following:

**§1.1, 2.1, …:** the term “Security Unit” is used extensively in the EP green book. It is also mentioned in the EP red book but only in the definition of the Frame Security Report: FSR is the status word of the Security Unit. Security Unit concept should be defined in EP red book.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0418/03 | G.Moury | Issue RID against EP red-1 to add a definition of Security Unit. |  July2018 |

**§3.1:** Daniel Fischer provided text for Key management concept of operation.

A generic section should be added to discuss procedures failures (§3.5.1 Failure handling):

* Procedure failure will be reported through normal HK TM of the satellite
* A failed directive should not be executed
* The execution of EP directives following a procedure failure is to be handled through conditional logic as any other conditional commanding.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0418/04 | G.Moury | Provide text for §3.5.1 Failure handling |  Sept2018 |

**§3.5.2:** In that section the possible on-board architectures for EP security directives processing and reporting will be discussed. In particular:

* Discuss the 2 following implementation options:
	+ EP PDUs routed through the OBC back to the security unit
	+ EP PDUs intercepted by the Security Unit and executed locally

**§4.2 : Scenarios :** In that section, scenarios for Inter-Satellite Links (ISL), multi-hop, constellations should be discussed.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0418/05 | C.BiggerstaffIgnacio Aguilar | Develop scenarios including ISL and constellations in §4.2 scenarios |  Sept2018 |

## SDLS core protocol green book

SDLS green book should be submitted soon to CESG and CMC poll for publication.

## SDLS / USLP compatibility / coherency

A joint session with Space Link Protocol WG was held to discuss compatibility / coherency of USLP with SDLS. The following conclusions have been reached:

* Keep specific UPID for SDLS control commands in USLP spec and introduce it as an option in SDLS EP red book for transmitting EP directives over USLP
* Modify text for OCF in USLP to indicate: “SDLS secured link Recipient or Initiator”
* Update (insert in pink sheets) TM and AOS blue books to mention FSR as type 2 OCF defined by CCSDS (idem text already in USLP spec for FSR) (see AI SDLS 0418/02)

## AOB

**Next meeting: 17-18 October 2018, DIN/DLR – Berlin, Germany.**