**Nov 2021 CCSDS**

**Space Data Link Security WG Minutes of virtual meeting**

Nov 8-9, 2021

# Attendance:

**SDLS WG virtual meeting:**

|  |  |  |
| --- | --- | --- |
| 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) |
| Craig Biggerstaff | NASA/JSC | [craig.biggerstaff@nasa.gov](mailto:craig.biggerstaff@nasa.gov) |
| Matthew Cosby | UKSA | [matt.cosby@goonhilly.org](mailto:matt.cosby@goonhilly.org) |
| Daniel Fischer | ESA/ESOC | [daniel.fischer@esa.int](mailto:daniel.fischer@esa.int) |
| Ohad Newton | NASA/MSFC | [ohad.newton@nasa.gov](mailto:ohad.newton@nasa.gov) |
| Dorothea Richter | DLR/GSOC | [dorothea.richter@dlr.de](mailto:dorothea.richter@dlr.de) |
| Bruno Saba | CNES | bruno.saba@cnes.fr |
| Marcus Wallum | ESA/ESOC | marcus.wallum@esa.int |

# Agenda :

The agenda of the meeting was the following:

|  |  |  |
| --- | --- | --- |
| **Date/time** | **Room** | **Agenda Item** |
|  |  | 1 - Action items review |
| 2 – SDLS Extended Procedures Green Book:   * Review of contributions * Review of document |
| 3 – SDLS Core Protocol (355.0-B-1) pink sheets:   * Disposition of agency review RIDs |
| 4 – Update of SDLS Core Protocol Green Book:   * Clarification of order of processing between SDLS and COP * Alignment with TC SLP revised Blue Book * Add USLP * Add SDLS Extended Procedures |
|  |  | 5 – Update of SLE ROCF and FCLTU service Blue Books:   * Impact of SDLS FSR |

The list of presentations made is the following:

The list of input/output documents is the following:

* Draft green book for SDLS EP:
  + SDLS EP Green v2 2021-11-08.docx (**attachment 1**)
  + Figure PDU protection §3.1.1.3 .vsdx (**attachment 2**)
* Pink sheets to SDLS BB (355.0-B-1) to introduce USLP, SDLS EP, extended key size for baseline mode, etc:
  + 355x0p11\_CMC\_Approval.doc (**attachment 3**)
  + 355x0p11.ESA-RID\_ESA dispositions.docx (**attachment 4**)
  + 355x0-B-1 pink sheets CNES RIDs disposition.docx (**attachment 5**)
  + CCSDS-355.0-P-1.1-NASA RID disposition.docx (**attachment 6**)
* Update of SDLS Core Protocol Green Book 350.5-G-1:
  + Revised SDLS Green Book as input to the meeting: SDLS Green Book 350.5-G-0 final draft\_Rev\_16-11-2017\_revision 2021-11-04.docx (**attachment 7**)
* Update of SLE ROCF and FCLTU service Blue Books:
  + PIDs SLE BBs SLP Sept 30-CSTS-WG\_\_Rev-IAS.xlsx (**attachment 8**)
  + MeetingMinutes\_SLP\_CS\_TIM\_Sept30\_2021\_Final SDLS edits 2021-11-09.docx (**attachment 9**)

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 2021 virtual 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) > MoM

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

* Open: security WG considers developing a Green Book on physical layer security including potential user requirements and solutions.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0521/01 | C. Biggerstaff | Provide updates to EP GB as mentioned above. | 30/09/2021  closed |

* Closed: discussed during the meeting. Superseded by other actions.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0521/02 | I. Aguilar | Provide updates to EP GB as mentioned above. | 30/09/2021  closed |

* Closed: discussed during the meeting. Superseded by other actions

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0521/03 | G.Moury | Submit RID to complete req 4.2.2.6.2 (355.0-B). | 30/06/2021  closed |

* Closed: RID has been submitted to 355.0-B pink sheets review.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0521/04 | G.Moury | Generate SDLS GB revised draft (350.5-G-2) with above mentioned updates. | 30/06/2021  closed |

* Closed: SDLS GB proposed revised draft (**attachment 7**)

## SDLS Extended Procedures draft Green Book review

The resulting document including all the modified figures (3-1, 2-2, 3-3, 3-7, 4-1, 4-2) at the meeting are in **Attachment 1**.

The following points were discussed and agreed:

* Figure 2-2: this figure was updated by Craig Biggerstaff to show the EP directive data path (red dash line) emphasizing the fact that EP directives are all SDLS protected on the link.
* Figure 3-1: this figure was reorganized by Craig Biggerstaff to show:
  + Logical sequence of EP directives
  + Optional flows for less frequent situations
  + Logical sequence of interaction between EP directive families
* Figure 3-3: this figure was modified to show legend of the different types of lines:
  + EP directive interfaces
  + EP directive data path

and Packet Routing taking place in C&DH

* §3.1.1.3 Protection of Protocol Data Units: proposal to add a simple drawing showing two concentric security domains:
  + one outside circle for traffic protection
  + one inner circle for EP directives protection

Proposed draft figure by Ignacio Aguilar in **attachment 2**, with 2 configurations:

* + TC protected/TM unprotected
  + TC protected/TM protected.
* §3.3.2.4: specific diagrams (figure 3-7 and 3-8) for seamless key change have been inserted by Craig Biggerstaff to show the logical flow of SA management directives at the sending and receiving end. The timeline is shown.
* Figures 4-1 and 4-2 were updated to illustrate both types of redundancy scheme: physical cross-strapping and logical cross-strapping.

## SDLS Core Protocol pink sheets (355.0-B revision) agency review:

SDLS Core protocol pink sheets (**attachment 3**) have been submitted to agency review. The following RIDs have been received:

* 11 RIDs from ESA (**attachment 4**)
* 1 RID from CNES (**attachment 5**)
* 1 RID from NASA (**attachment 6**)

All RIDs have been disposed. The following actions have been noted:

* **AI ESA**: RID ESA-OG-01: check with Oana Gaur if she has specific examples of crypto modes where IV is authenticated.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1121/01 | I. Aguilar | Check with Oana Gaur if she has specific examples of crypto modes where IV is authenticated. | 30/12/2021 |

* **AI CNES**: RID CNES-GM-01: check SDLS GB if non-authentication of Frame Sequence Number is correctly explained in GB.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1121/02 | G.Moury | check SDLS GB if non-authentication of Frame Sequence Number is correctly explained in GB. | 30/12/2021 |

For the SDLS 355.0-B, the non-authentication of the Frame Sequence Number is covered by requirement **4.2.2.6.2 h) now j)** in pink sheets, and reads:

* the mask bits corresponding to all other Transfer Frame header fields should contain ‘all zeros’, unless otherwise specified according to mission requirements.

The RIDs disposition will be inserted in the revised version of the SDLS blue book. The RIDs dispositions will be sent back to the originators.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1121/03 | G.Moury | Generate revised SDLS blue book and generate resolution for 355.0-B-2 publication | 30/12/2021 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1121/04 | G.Moury | Return RIDs disposition to originators. | 30/12/2021 |

## Update of SDLS Core protocol Green Book (350.5-G)

The following modifications have been introduced in SDLS GB (**attachment 7**):

* Replace figure 3-3 by new diagram showing order of processing at both ends of the link + associated table
* Add § 3.3.5 for USLP
* Explain why Frame Count field should not be authenticated in TC (due to order of processing between SDLS and COP)
* Add reference to Extended Procedures as appropriate
* Complete §3.1.1 with justification for not protecting BC frames

Annex A2.3 – Table A-1 should be revised to mention 256-bit key length as the recommended key length.

## Update of SLE ROCF and FCLTU service Blue Books:

SLE services blue books are being revised by the CSS-CSTS WG. During the CESG review of the revised SLE Blue Books for publication, SLS AD raised PIDs (see **attachment 8**) related to possible interaction between SLE ROCF and FCLTU services on one side and SLS Space Data link protocols as well as SDLS.

A list of questions for the SDLS WG to answer was established during a joint meeting between SLS-SLP and CSS-CSTS WGs related to those PIDs (see **attachment 9**). The output of the SDLS WG discussion resulted in the following responses:

* Is timely delivery of the FSR required ? Yes, if the TM frames are not transmitted real-time to the Mission Operation Center (MOC)
* Currently the ROCF service does not deliver the OCF. Is that acceptable or not ? no, ROCF service should be able to deliver FSR as type-2 OCF if needed by the mission.
* If certain flags are set in the FSR, such as a security error has been detected on-board the spacecraft, what behavior should the ground station take? ROCF does not have to check the fields of FSR but to send it back to originator of uplink (usually MOC).
* For example, should the FCLTU service interrupt the uplink when such a security error is detected on-board and reported in the FSR ? No automatic action can be envisaged when security error is reported in FSR. Human analysis is needed at the MOC.
* Which fields in the FSR should the ROCF service examine in order for the FCLTU or Forward Frame Services to take appropriate action ? No FSR field check is needed from ROCF service. No automatic action in Ground Station can be envisaged from analysis of FSR fields.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1121/05 | G.Moury | Send back SDLS WG responses to CSS-CSTS WG. | 30/12/2021 |

## AOB

**Next meeting: May 2022, hopefully face-to-face in Huntsville, Alabama.**