**May 2020 CCSDS**

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

May 6-7, 2020

# Attendance:

**SDLS WG webmeeting:**

|  |  |  |
| --- | --- | --- |
| 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) |
| Gian-Paolo Calzolari | ESA/ESOC | [gian-paolo.calzolari@esa.int](mailto:gian-paolo.calzolari@esa.int) |
| 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) |
| Bradley Myers | NASA/IVV | [bradley.a.myers@nasa.gov](mailto:bradley.a.myers@nasa.gov) |
| Joost Oranje | CGI Netherland BV | joost.oranje@cgi.com |
| Dorothea Richter | DLR/GSOC | [dorothea.richter@dlr.de](mailto:dorothea.richter@dlr.de) |
| Michael Pajevski | NASA/JPL | [michael.j.pajevski@jpl.nasa.gov](mailto:michael.j.pajevski@jpl.nasa.gov) |
| 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 Blue Book:   * + Published February 2020 |
| 3 – SDLS Extended Procedures Green Book:   * Review of contributions * Review of document |
| 4 – SDLS Core Protocol (355.0-B-1) pink sheets   * 5-year review of the SDLS blue book |

The list of presentations made is the following:

* none

The list of input/output documents is the following:

* Draft green book for SDLS EP:
  + SDLS EP Green v1 - virtual WG 20200507.docx (**attachment 1**)
* Pink sheets to SDLS BB (355.0-B-1) to introduce USLP, SDLS EP, extended key size for baseline mode, etc:
  + 355x0b1\_pink sheets for USLP insertion 20200507.doc (**attachment 2**)

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) > [May 2020 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  open |

* Open: security WG considers developing a Green Book on physical layer security including potential user requirements and solutions (see §3.5).

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0418/05 | C.Biggerstaff Ignacio Aguilar | Develop scenarios including ISL and constellations in §4.2 scenarios of EP GB | Sept  2018  closed |

* Closed: 2 scenarios were developed by C.Biggerstaff in § 4.4.3 Inter-satellites links. Those ISL scenarios were discussed at length during the meeting. The conclusion of the WG was that the SDLS EP being a unidirectional protocol (Initiator to Recipient) is not well suited for ISL and constellations of satellites. Therefore, it was decided to remove section 4.4.3 altogether from the GB and avoid discussing application of EP to constellations.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1018/02 | C. Biggerstaff | Add a text discussing EP PDU protection over the spacelink in EP GB . | April  2019  closed |

* Closed: text on EP PDU protection over the spacelink developed by C. Biggerstaff in §3.1.1.3 Protection of Protocol Data Units

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1018/08 | C. Biggerstaff | Add a justification in EP GB why key derivation (scheme 3) is not included in EP. | Mar  2019  closed |

* Closed : justification added in §4.5.2.1 Key Management schemes not implemented

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1018/12 | G. Moury | Develop Annex A Baseline mode to justify Baseline Mode settings. | Mar  2019  closed |

* Closed: text of Annex A provided by G.Moury and reviewed during the meeting.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0519/01 | G. Moury | Justify in EP GB the set of Space Data Link protocols allowed for forward and return links (as specified in §4.2.2). | Sept  2019  closed |

* Closed: text added in §3.5.3.1

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0519/06 | G. Moury | Update pink sheets to SDLS BB to introduce USLP and the above mentioned edits. | 31/07/2019  closed |

* Closed: SDLS BB pink sheets updated for the meeting and discussed: see file in **Attachment 2**.

## SDLS EP draft Green Book review

An updated draft was provided before the meeting by C. Biggerstaff. This draft was reviewed during the meeting. The resulting document including all the modifications and comments done during the meeting is in **Attachment 1**.

The following points were discussed and agreed:

* Figures 2-2 and 3-3 could be updated to include a continuous dashed line showing SDLS secured transfer frames and EP PDUs data path. To be done if it does not overload the figures. **AI CB**
* Wording to be improved for §3.1.1.3 (Protection of Protocol Data Units) to indicate that mission specific protection of EP PDUs for their on-board transfer might be needed to guarantee integrity. **AI CB**
* Introduce text in § 3.2.4.2 to indicate that integrity & confidentiality protection might be needed for OTAR PDUs during their transfer on-board but also during their transfer on the ground in the MOC. **AI CB**
* Add text in §3.3.4.1 about Recovery SA: check text already available in SDLS Core Protocol GB (350.5-G). **AI GM**
* §4.2.1 Physical cross-strapping / §4.2.2 Logical cross-strapping: 2 different architectures for EP PDU distribution and routing on-board are described. I.Aguilar will raise questions and make proposals to improve text provided by C.Biggerstaff. **AI IA**
* §4.3 Contingency and off-nominal scenarios: text from SDLS GB (350.5-G-1) §3.5.1.1 (Clear Mode) and §3.5.1.2 (Recovery SA) could be partly reused to discuss the interest of EP for dealing with contingency scenarios. **AI CB**
* §4.4.3 Inter-Satellite links: after lengthy discussion, recognizing that SDLS EP is not well suited for Inter-satellite links due to its unidirectional and master-slave operation between an Initiator and a Recipient, it was decided not to develop ISL scenarios in the EP GB. Section §4.4.3 should be removed from the GB. **AI CB**
* Annex A: A5.2.2. Justification of key length (AES-GCM) for OTAR and Key Verification PDUs. Justification for 256-bit key length needs to be improved. **AI IA**

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0520/01 | C. Biggerstaff | Provide updates to EP GB as mentioned above. | 30/09/2020 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0520/02 | G. Moury | Provide updates to EP GB as mentioned above. | 30/09/2020 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0520/03 | I. Aguilar | Provide updates to EP GB as mentioned above. | 30/09/2020 |

## Pink sheets to SDLS BB (355.0-B-1)

An updated draft was provided before the meeting by G. Moury. This draft was reviewed during the meeting. The resulting document including all the modifications and comments done during the meeting is in **Attachment 2**:

* §1.6 Definitions: add definition for Service Provider, Initiator and Recipient
* §2.2.6 : modify figure to show the 2 COPs : COP-1 and COP-P
* §3.2.2.7 : stipulate in NOTES 2 that condition : “the Virtual Channel specified by the GVCID is using segment headers” is only applicable to TC and not to USLP (there is no segment in USLP).
* §4.2.2.6.2: in TM and AOS blue books, there is no clause stipulating that: “Transfer Frames with an invalid MCID/VCID shall be discarded”. There is only a non prescritive NOTE (linked to clause 4.3.6.2 or 4.3.6.3) stating that: “Transfer Frames with an invalid MCID are discarded”. In USLP and TC, this normative clause exists in § 4.3.9.4 and §4.4.6.3 respectively:
  + Transfer Frames with an invalid MCID shall be discarded (USLP)
  + Transfer Frames with an invalid VCID shall be discarded (TC)

If transfer frames with invalid MCID/VCID are not discarded at the receiving end by the space data link protocol, SDLS needs to authenticate the MCID/VCID field(s) of the transfer frame header to be able to reject those invalid frames. Therefore, the authentication bit mask needs to be set to “1” for those fields.

Two courses of action for this issue :

* Include a normative clause in TM and AOS stating : “Transfer Frames with an invalid MCID/VCID shall be discarded”, in the pink sheets in preparation for those 2 documents
* Modify default authentication bit mask in SDLS Core protocol to include MCID/VCID field(s) specifically for TM and AOS (clause 4.2.2.6.2)

Preferred solution is to align TM and AOS with USLP and TC, and add normative clause in respective pink sheets.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0520/04 | G. Moury | Insert normative clause for invalid MCID in TM and AOS pink sheets | 30/09/2020 |

|  |  |  |  |
| --- | --- | --- | --- |
| SDLS0520/05 | G. Moury | Insert modifications agreed above in SDLS Core protocol pink sheets | 30/09/2020 |

## AOB

**Next meeting (hopefully face-to-face): 28-29 October 2020, CNES Toulouse, France.**