**May 2021 CCSDS**

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

May 19-20, 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) |
| 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) |
| Greg Kazz | NASA/JPL | [greg.j.kazz@jpl.nasa.gov](mailto:greg.j.kazz@jpl.nasa.gov) |
| Joost Oranje | CGI Netherland BV | joost.oranje@cgi.com |
| 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:   * Status of agency review |
| 4 – Future work:   * Update of SDLS Core Protocol Green Book   + Clarification of order of processing between SDLS and COP   + Alignment with TC SLP pink sheets |

The list of presentations made is the following:

* CYSAT presentation (commented by ESA): Cybersecurity challenges of IP-based spacelinks and COTS oriented architectures: available in CWE private: [https://cwe.ccsds.org/sls/docs/SLS-SEA-DLS/CWE Private/meeting material/May 2021 virtual meeting/CYSAT'21\_ReOrbit\_Ignacio Chechile.pdf](https://cwe.ccsds.org/sls/docs/SLS-SEA-DLS/CWE%20Private/meeting%20material/May%202021%20virtual%20meeting/CYSAT'21_ReOrbit_Ignacio%20Chechile.pdf)

The list of input/output documents is the following:

* Draft green book for SDLS EP:
  + SDLS EP Green v2 2021-05-19.docx (**attachment 1**)
  + SDLS EP Green v2 fig 3-1.png (**attachment 2**)
  + SDLS EP Green v2 fig 4-1.png (**attachment 6**)
  + SDLS EP Green v2 fig 4-2.png (**attachment 7**)
* 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**)
* Update of SDLS Core Protocol Green Book in coherency with TC SLP pink sheets:
  + Pink sheets to Space Data Link Protocols BB (TC 232.0-B) to introduce Frame Security Header (FSH), SDLS EP, etc.. :
    - 232x0b3\_Changes\_2021\_May\_18\_SDLS rev2021-05-19.docx (**attachment 4**)
  + Proposed new figure and text for replacement of Figure 3-3 of SDLS GB and Figure 6-3 of TC SLP BB:
    - Table6\_1\_TC\_SDLP\_2021\_May\_18.docx (**attachment 5**)
  + Justification for not protecting BC frames – mail (**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) > [May 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  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** |
| --- | --- | --- | --- |
| SDLS1020/01 | C. Biggerstaff | Provide updates to EP GB as mentioned above. | 30/04/2021  closed |

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 Superseded by other actions

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1020/03 | I. Aguilar | Provide updates to EP GB as mentioned above. | 30/04/2021  closed |

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

## SDLS EP draft Green Book review

The resulting document including all the modifications and comments done during the meeting are in **Attachment 1**.

The following points were discussed and agreed:

* §1.1: SDLS EP can also be operated on space-to-space links but not peer-to-peer. SDLS EP can only operate in a master-slave configuration. For space-to-space links, it means there is a hierarchy between the communicating nodes which in some case exists (e.g. orbiter-lander). When there is no hierarchy (e.g. constellations), higher layer end-to-end security might be preferable to hop by hop SDLS and SDLS EP. Space-to-space links can be mentioned in section 1.1, 2.1 and 2.3.2.
* Figure 2-2: should be updated to show the data path for the EP directives as a dash line. **Action CB**
* §3.1.1.3 : add a figure to show the various layers of protection for EP PDUs. Explain that OTAR command PDU and Key Verification Reply PDUs protection is not done necessarily using SDLS SA. If a project wants to protect all EP directives, this is equivalent to a second layer of SDLS security. **Action CB**
* §2.7 and 3.5: add 2 subsections on User defined procedures: 2.7 overview, 3.5 details. SDLS EP framework can be used to define mission specific procedures augmenting SDLS EP. **Action IA**
* Figure 3-1 and 3-3: add a legend for significance of the solid and dashed arrows. Action IA. Done see **attachment 2**.
* §3.3.1.2: text missing on number of Control SAs needed for each traffic SA. **Action IA**.
* §3.3 SA management: add a text to explain how starting/stopping an SA can be used to open and close a Secure Channel. **Action IA**.
* §3.3.2.1: Text to be added to explain that authentication bit mask has to be tailored for a given Space Link Protocol. **Action IA**.
* §3.3.2.4: Seamless key change: develop a diagram to illustrate. **Action CB.**
* §4.2.1 et 4.2.2: Redundancy: improve figures 4-1 and 4-2 to illustrate the 2 redundancy/cross-strapping implementation scheme: physical and logical. Security units can be addressed using VC, MAP or APID. Action CB. Done (**see attachment 6,7**). Additional text can be provided if needed. I.Aguilar will raise questions and make proposals to improve text provided by C.Biggerstaff. **AI IA**
* Discussion about clear mode: clear mode is mentioned in SDLS BB and SDLS GB but not in SDLS EP BB nor SDLS EP GB. Should we remove completely clear mode from SDLS documents? could be done through the on-going revision of SDLS BB and GB.
* 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** |
| --- | --- | --- | --- |
| SDLS0521/01 | C. Biggerstaff | Provide updates to EP GB as mentioned above. | 30/09/2021 |

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

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

SDLS Core protocol pink sheets (**attachment 3**) will be submitted to agency review shortly. An interim telecon will be organized to disposition the collected RIDs.

A RID should be generated (**AI GM**) to add an item in requirement 4.2.2.6.2 stating:

* (TC with COP only): Frame count field shall be all zeros in the authentication bit mask (i.e. Frame Count shall not be authenticated due to order of processing between SDLS and COP at sending end)

| **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 |

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

Interface of SDLS with TC space data link protocol and associated COP has been the subject of misinterpretations by projects especially regarding the order of processing between SDLS and COP functions. A diagram and a table have been developed for insertion in the TC Space Data Link protocol pink sheets (232.0-B) (**see attachments 4 and 5**) This diagram with the associated table will be used as figure 6-3 in the TC SLP BB and also in SDLS Green Book to replace figure 3-3.

The TC SDLP pink sheets have been discussed with SLP WG with the following conclusions (reflected in **attachment 4):**

* 2 specific subsections for Frame Initialization Procedure (6.4.2.2) and Frame finalization procedure (6.4.2.3). The text of those 2 subsections have been reviewed.

Modifications to be introduced in SDLS GB:

* Replace figure 3-3 by new diagram showing order of processing at both ends of the link + associated table (attachment 5)
* 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 Extended Procedures as appropriate
* Complete §3.1.1 with justification for not protecting BC frames (see **attachment 8**)

| **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 |

## AOB

Comment by ESA of a CYSAT conference presentation made by ReOrbit about vulnerabilities of IP and COTS based spacelinks. Analysis of CCSDS standards vs COTS based internet solutions. Suitability of CCSDS/SDLS for massive LEO constellation ?

Presentation on CWE : [https://cwe.ccsds.org/sls/docs/SLS-SEA-DLS/CWE Private/meeting material/May 2021 virtual meeting/CYSAT'21\_ReOrbit\_Ignacio Chechile.pdf](https://cwe.ccsds.org/sls/docs/SLS-SEA-DLS/CWE%20Private/meeting%20material/May%202021%20virtual%20meeting/CYSAT'21_ReOrbit_Ignacio%20Chechile.pdf)

**Next meeting: October 2021, hopefully face-to-face in Toulouse.**

**Interim telecon to be scheduled to disposition 355.0-B pink sheets RIDs.**