**May 2022 CCSDS**

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

May 25, June 10, 2022

# Attendance:

**SDLS WG virtual 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  |
| Craig Biggerstaff | NASA/JSC | craig.biggerstaff@nasa.gov  |
| Daniel Fischer | ESA/ESOC | daniel.fischer@esa.int  |
| Greg Kazz | NASA/JPL | greg.j.kazz@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 Green Book:* Review of contributions
* Review of document
 |
| 3 – SDLS Core Protocol (355.0-B-2):* Status of publication poll
 |
| 4 – Update of SDLS Core Protocol Green Book* Finalization of document
 |

The list of presentations made is the following:

The list of input/output documents is the following:

* Draft green book for SDLS EP 350.11-G:
	+ Edited during the meeting : SDLS EP Green v3 2022-06-10.docx (**attachment 1**)
* Update of SDLS Core Protocol Green Book 350.5-G-1:
	+ Revised SDLS Green Book as finalized during the meeting: 350x5g1\_final update\_g2 2022-05-25.doc (**attachment 2**)
* Update of SDLS Core protocol BB (355.0-B-2)
	+ Mail concerning requirement for IV authentication (**attachment 3**)
	+ Approved version for publication (**attachment 4**)

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 2022 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** |
| --- | --- | --- | --- |
| SDLS1121/01 | I. Aguilar | Check with Oana Gaur if she has specific examples of crypto modes where IV is authenticated. |  30/12/2021Closed 04/05/22 |

**Closed :** by mailof I.Aguilar (04/05/2022) **– (Attachment 3).** IV authentication is notrecommended by the standard but not forbidden for a given project.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1121/02 | G.Moury | check SDLS GB if non-authentication of Frame Sequence Number is correctly explained in GB. |  30/12/2021Closed04/05/2022 |

Closed : non-authentication of Master Frame Counter is explained in SDLS GB in section 3.2.5.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1121/03 | G.Moury | Generate revised SDLS blue book and generate resolution for 355.0-B-2 publication |  30/12/2021Closed 11/02/2022 |

Closed: done

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1121/04 | G.Moury | Return RIDs disposition to originators. |  30/12/2021Closed15/01/2022 |

Closed : done

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1121/05 | G.Moury | Send back SDLS WG responses to CSS-CSTS WG. |  30/12/2021Closed 03/05/2022 |

Closed : done

## SDLS Extended Procedures draft Green Book review

The resulting document as edited during the meeting is in **Attachment 1**.

The following points were discussed and agreed:

* Definition of Secure Channels was added in §2.5 SA Management – same definition as in §3.2.2 and 3.5.2 of SDLS GB: “All Transfer Frames that share the same SA on a physical channel constitute a Secure Channel. A Secure Channel consists of one or more Global Virtual Channels or Global MAPIDs (TC and USLP only) assigned to an SA at the time of its creation.”
* §3.1.1.3 Protection of EP PDUs : text is needed in this section to discuss the necessity to partition the IV for Key Verification directives and TC authentication to guarantee that the same IV will not be used on-board and on-ground for the same key, since the IV is likely to be generated for the same key on-board (key verification reply PDU) and on-ground (SDLS authentication of TC).

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0522/01 | I. Aguilar | Provide text for §3.1.1.3 explaining necessity of not repeating same IV for the same key although IV might be generated on-board and on-ground for the same key. Add a pointer to section 4.4.1.2 Implications for key verification. Add the same text in §3.2.5.1 Key verification. |  15/09/2022 |

* §4.2.2 Logical cross-strapping: text should be modified to mention the use of APID to route EP PDUs to the appropriate security unit on-board in the logical cross-strapping architecture.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0522/02 | C. Biggerstaff | Modify text in §4.2.2 to mention the use of APID to route EP PDUs to the appropriate security unit on-board in the logical cross-strapping architecture. |  15/09/2022 |

* Draft edited at the meeting (Attachment 1), besides the 2 additions identified above, is considered complete. A final draft should be produced for WG review before or at the next meeting.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0522/03 | C. Biggerstaff | Perform an overall check of the document. Provide a clean version of the final draft EP GB for review by the WG. |  30/09/2022 |

## SDLS Core Protocol pink sheets (355.0-B-2 revision):

SDLS Core protocol pink sheets (**attachment 4**) have been submitted to agency review. All RIDs were disposed satisfactorily. Publication was approved by CESG and CMC (June 2022).

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

The resulting document as edited during the meeting is in **Attachment 2**.

The following points were discussed and agreed:

* Text was added to section A2.3 to justify the increase of the key size in baseline mode from 128 to 256-bit: “Since the first publication of this report, the quantum computing threat to cryptographic algorithms has become more credible. In the case of symmetric algorithms, the well-known Grover algorithm divides by 2 the exponent of the number of trials for brute force attack. The proposed mitigation is to simply multiply by 2 the key length. Therefore, the key length for baseline mode of SDLS was doubled to 256-bit.”
* Draft edited at the meeting (**Attachment 2**) is considered complete. A final draft will be generated for circulation and review by the WG before next meeting.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0522/04 | G. Moury | Perform an overall check of the document. Provide a clean version of the final draft SDLS GB v2 for review by the WG. |  15/08/2022 |

## AOB

**Next meeting: October 17-21 2022, hopefully face-to-face in Toulouse, France.**