**May 2023 CCSDS**

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

Huntsville, AL, USA

May 10-11, 2023

# Attendance:

**SDLS WG hybrid meeting:**

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Organization | Email Address | Participation |
| Gilles Moury (Co-Chair) | CNES | [gilles.moury@cnes.fr](mailto:gilles.moury@cnes.fr) | On-site |
| Howard Weiss (Co-Chair) | NASA/SPARTA | [howard.weiss@parsons.com](mailto:howard.weiss@parsons.com) | On-site |
| Julien Airaud | CNES | julien.airaud@cnes.fr | On-site |
| Antonios Atlasis | ESA/ESTEC | antonios.atlasis@esa.int | Remote |
| Craig Biggerstaff | NASA/JSC | [craig.biggerstaff@nasa.gov](mailto:craig.biggerstaff@nasa.gov) | Remote |
| Matt Cosby | Goonhilly Earth Station / UKSA | matt.cosby@goonhilly.org | On-site |
| Wesley Hovis | NASA/SAIC | [wesley.a.hovis@nasa.gov](mailto:wesley.a.hovis@nasa.gov) | On-site |
| Jérome Merlet | CNES | jerome.merlet@cnes.fr | On-site |
| Joost Oranje | ESA | joost.oranje@esa.int | On-site |
| Bruno Saba | CNES | bruno.saba@cnes.fr | On-site |
| Charles Sheehe | NASA/GRC | charles.j.sheehe@nasa.gov | On-site |
| Paul Thompson | QinetiQ/UKSA | pbthompson@qinetiq.com | Remote |
| Takayuki Wada | JAXA | Wada.takayuki@jaxa.jp | On-site |
| Marcus Wallum | ESA/ESOC | marcus.wallum@esa.int | Remote |

# Agenda :

The agenda of the meeting was the following:

**May 10, 2023 all day, May 11 morning only**

|  |  |  |
| --- | --- | --- |
| **Date/time** | **Room** | **Agenda Item** |
| **May 10**  all day | TBD | 1 - Action items review |
| 2 – Update of SDLS Core Protocol Green Book (350.5-G-2):  Finalization of document (taking into account SEA AD comments – AI SDLS1022/01-04) |
| 3 – PQC Asymmetric Key Exchange and Authentication Protocol for CCSDS SDLS:  Discussion of WG feedback (AI SDLS1022/02-03) |
| 4 – Review of proposed revised text for SDLS-COP-1 ordering in TC and USLP pink sheets (response to G.Kazz mail dated 23/01) |
| **May 11**  morning | TBD | 5 – SDLS Extended Procedures Green Book:   * Review of contributions * Review of document (AI SDLS1022/05) |

# Presentations and documents:

The list of presentations made is the following:

* Key Establishment Mechanism for SDLS – ESA presentation – F.Weber (**attachment 1**)

The list of input/output documents is the following:

* Update of SDLS Core Protocol Green Book 350.5-G:
  + Edited during the meeting: SDLS 350x5g2 revised draft 2023-05-10 (**attachment 2**)
* SDLS/COP ordering in TC and USLP issue:  
  + Edited during the meeting (modified text in §6.5.2.2):  
    232x0b4\_final\_GK\_Jan 23\_2023 SDLS WG 2023-05-10 (**attachment 3**)
  + Edited during the meeting (modified text in §6.5.2.2):  
    732x1b2\_draft\_Jan\_23\_2023 SDLS WG 2023-05-10 (**attachment 4**)
* Draft green book for SDLS EP 350.11-G:
  + Edited during the meeting: SDLS EP Green v3 2023-05-11 - WG final review.docx (**attachment 5**)

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 2023 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** |
| --- | --- | --- | --- |
| SDLS1022/01 | G. Moury | Answer SEA AD general observations on the SDLS Core protocol GB-2 and edit final draft of document for WG and ADs approval | 15/12/2022  open |

Status : on-going action. SDLS GB-2 draft has been finalized during the meeting. A mail will be sent to SEA and SLS AD together with the final draft for approval.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1022/02 | SDLS WG | Contribute/comment on use use cases for asymmetric cryptography related to SDLS (link layer security) | 15/04/2023  open |

Status: on-going action. Feedback received during the meeting.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1022/03 | SDLS WG | Provide feedback of protocol design considerations and selection criteria for PQC algorithms. | 15/04/2023  open |

Status: on-going action.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1022/04 | Gilles Moury | Add text in Annex D of SDLS GB to warn user against operational sequences where SDLS will interfere and block the COP. | 15/12/2022  closed |

Status: closed: Note added in §3.1.1 and 3.3.2 of SDLS GB to warn user against operational sequences where SDLS will interfere and block the COP.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1022/05 | C. Biggerstaff | Perform an overall check of the document. Provide a clean version of the final draft EP GB for review and approval for publication by the WG. | 15/02/2023  closed |

Status: closed: final draft of EP GB provided for review at the meeting (see **attachment 5**).

## Update of SDLS Core protocol Green Book (350.5-G-2)

The final draft of the document taking into account all the comments made by SEA/AD has been reviewed during the meeting. The document taking into account all the edits made at this meeting is in **attachment 2** (SDLS 350x5g2 revised draft 2023-05-10).

A mail will be sent to SEA and SLS AD together with the final draft for approval (AI SDLS1022/01). Pending approval for publication by SEA and SLS AD, issue a resolution for SDLS GB-2 publication.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0523/01 | G.Moury | Pending approval for publication by SEA and SLS AD, issue a resolution for SDLS GB-2 publication. | 15/09/2023 |

## PQC Asymmetric Key Exchange and Authentication Protocol for CCSDS SDLS

* Presentation by Florian Weber: Key Update Mechanism for SDLS – ESA presentation (**attachment 1**)

SDLS currently relies on pre-shared symmetric keys. This is applicable to the most common scenario of space operation: i.e.: a Mission Control Center communicating securely with a given spacecraft. Besides, SDLS Extended procedures introduce a hierarchy in SDLS secured links with the notion of Initiator (typically MCC) and Recipient (typically Spacecraft). Finally, SDLS being based on pre-shared symmetric keys requires the management of one set of secret keys per communicating pair, which does not scale when the number of communicating pairs in the system increases.

However, future spacelink scenarios include, among others:

* Space to space communication between spacecrafts, links for which no implicit hierarchy exists and number of communicating pairs can be significant
* Operation of large constellations (potentially with Inter-Satellite Links), where the number of communicating pairs is inherently very high and fluctuating

The use of asymmetric cryptography to exchange symmetric keys whenever an SDLS secure spacelink is needed would provide scalability (large number of communicating pairs can be handled) and flexibility (no need to define a hierarchy among the communicating nodes).

The presentation proposes to introduce a post-quantum, forward-secure asymmetric key-update mechanism (slide 5) in SDLS EP. Long-term key-pair would be needed to perform authenticated key exchange. This long-term key pair should preferably be updatable (slide 8). To perform this update, different KEM and signature schemes are proposed and evaluated in terms of overhead (slides 9-18).

The action items SDLS1022/02 and 03 (listed hereafter) are still pending.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1022/02 | SDLS WG | Contribute/comment on use use cases for asymmetric cryptography related to SDLS (link layer security) | 15/04/2023 |

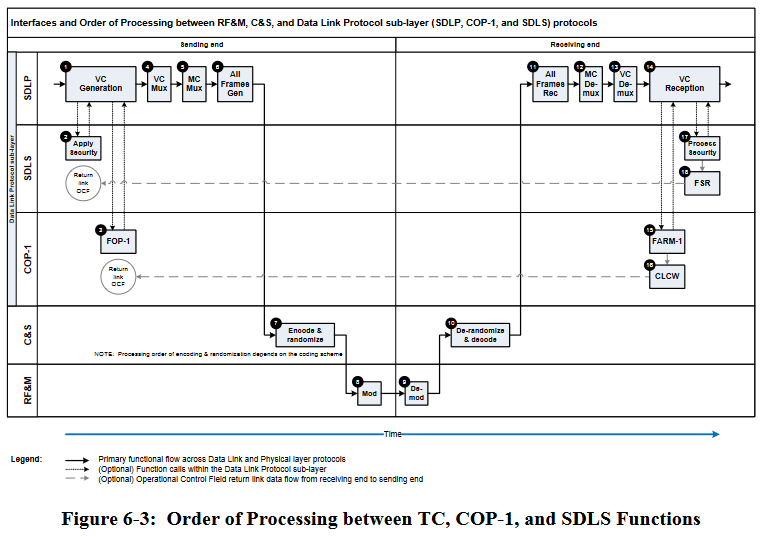
| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1022/03 | SDLS WG | Provide feedback of protocol design considerations and selection criteria for PQC algorithms. | 15/04/2023 |

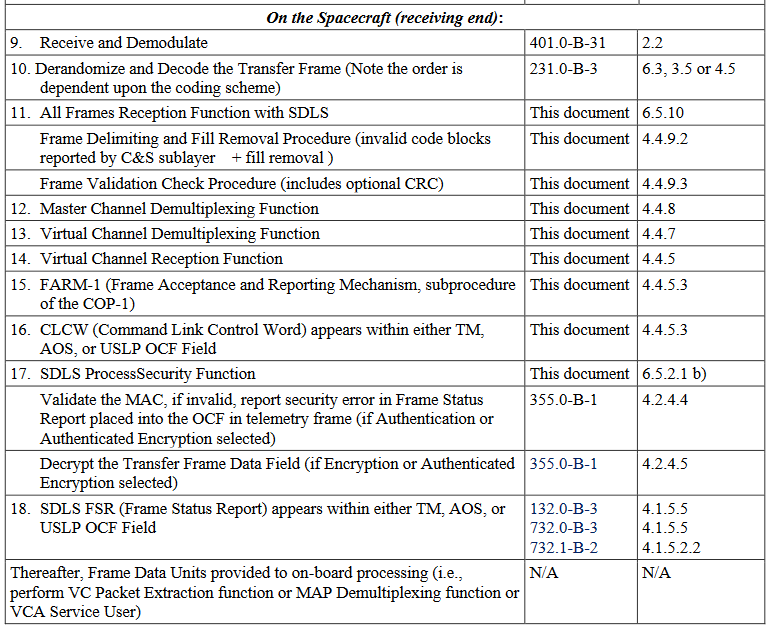
An SDLS draft project could be proposed, if agencies interest is confirmed for extending SDLS and SDLS EP to space-to-space communication scenarios (ISL, constellations), to develop additional procedures for establishing dynamically secure channels at the data link layer between pair of satellite within a fleet. End-to-end security at the network layer can also be considered for this scenario.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0523/02 | SDLS WG | Indicate interest of respective agencies for developing SDLS extension to inter-satellites links and constellation scenarios. | 15/10/2023 |

## Revised text for SDLS-COP1 ordering in TC and USLP data link recommendations

NASA GSFC & JPL have raised issues regarding the order of processing between COP and SDLS functions in TC. The current specified order (§ 6.4.2.6 of TC Space Data Link Protocol BB) is : SDLS-FOP-SpaceLink-FARM-SDLS. The detailed ordering of the functions is depicted in Figure 6-3 and table 6-1 of TC and USLP SDLP BB and reproduced below:







The pros and cons of both orders of processing have been exchanged by mail before the fall 2022 meeting. During the meeting, it was decided to confirm the order of processing currently specified and to clarify the text of section 6.5.2 of TC and USLP SDLP BB (Order of processing between TC/USLP, COP-1 and SDLS Protocols). In particular, the text of the NOTE in §6.5.2.2 was modified by the WG during the meeting as follows:

“*Whenever Type-AD and Type-BD frames are mixed on the same VC, then the SDLS ProcessSecurity Anti-Replay function will reject retransmitted frames older that the last accepted Type-BD frame. This is due to their lower anti-replay sequence count in comparison to the Type-BD anti-replay sequence count. As a result, they are falsely labelled as SDLS security failures. Therefore, mixing Type-AD and Type-BD frames on the same VC secured by SDLS is generally not advised while acceptance of Type-AD frames are pending*.”

The same warning text has been added to SDLS Green Book (§3.1.1 and 3.3.2).

The modified TC and USLP pink sheets have been sent back to SLP WG Chairman (G.Kazz) **(attachments 3 and 4**) for further review by the SLP WG.

## SDLS Extended Procedures Green Book

SDLS Extended Procedures draft Green Book was updated by C.Biggerstaff before the meeting and reviewed by the WG. The resulting document is in **attachment 5**. Craig Biggerstaff will edit the final draft and circulate the document for approval by the WG before resolution for publication is issued to SLS and SEA AD.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0523/03 | C. Biggerstaff | Perform an overall check of the document. Provide the final draft EP GB for review and approval for publication by the WG. | 15/07/2023 |

## AOB

**Next meeting: November 6-10 2023, in The Hague, Netherlands.**