**October 2022 CCSDS**

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

Toulouse, France

October 19-20, 2022

# 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) | Remote |
| Ignacio Aguilar-Sanchez | ESA/ESTEC | [ignacio.aguilar.sanchez@esa.int](mailto:ignacio.aguilar.sanchez@esa.int) | On-site |
| Antonios Atlasis | ESA/ESTEC | antonios.atlasis@esa.int | On-site |
| Craig Biggerstaff | NASA/JSC | [craig.biggerstaff@nasa.gov](mailto:craig.biggerstaff@nasa.gov) | On-site |
| Matt Cosby | Goonhilly Earth Station / UKSA | matt.cosby@goonhilly.org | On-site |
| Daniel Fischer | ESA/ESOC | [daniel.fischer@esa.int](mailto:daniel.fischer@esa.int) | On-site |
| Greg Kazz | NASA/JPL | greg.j.kazz@jpl.nasa.gov | Remote |
| Franck Keck | Secunet | franck.keck@secunet.com | Remote |
| David Koisser | ESA/TUD | david.koisser@ext.esa.int | Remote |
| Ohad Newton | Barrios Technology/NASA | ohad.newton@nasa.gov | Remote |
| Dorothea Richter | DLR/GSOC | [dorothea.richter@dlr.de](mailto:dorothea.richter@dlr.de) | On-site |
| Bruno Saba | CNES | bruno.saba@cnes.fr | On-site |
| Charles Sheehe | NASA/GRC | charles.j.sheehe@nasa.gov | Remote |
| Marcus Wallum | ESA/ESOC | marcus.wallum@esa.int | On-site |

# Agenda :

The agenda of the meeting was the following:

|  |  |  |
| --- | --- | --- |
| **Date/time** | **Room** | **Agenda Item** |
| **Oct 19**  14:00-17:00  CEST | WE WORK | 1 - Action items review |
| 2 – Update of SDLS Core Protocol (355.0-B-2):  Status of publication |
| 3 – Update of SDLS Core Protocol Green Book (350.5-G-2):  Review comments from SEA-AD |
| 4 – PQC Asymmetric Key Exchange and Authentication Protocol for CCSDS SDLS:   * Considerations, Challenges, and Way Forward (A.Atlasis - ESA) |
| **Oct 19**  17:00-18:00  CEST | WE WORK | 5 – Joint session with SLP WG: SDLS/COP ordering in TC:   * Shall we allow both ordering? |
| **Oct 20**  14:00–18:00  CEST | WE WORK | 6 – SDLS Extended Procedures Green Book:   * Review of contributions * Review of document |

# Presentations and documents:

The list of presentations made is the following:

* Post Quantum Cryptography for Space Missions – ESA presentation – A.Atlasis (**attachment 1**)

The list of input/output documents is the following:

* Post Quantum Cryptography for Space Missions\_1.0 – ESA Technical Note – A.Atlasis (**attachment 2**)
* Draft green book for SDLS EP 350.11-G:
  + Edited during the meeting : SDLS EP Green v3 2022-10-20.docx (**attachment 3**)
* Update of SDLS Core Protocol Green Book 350.5-G:
  + Mail of comments of SEA AD : Re EXTERNAL SDLS Green Book issue 2 WG resolution to publish for area approval.msg (**attachment 4**)
  + SDLS 350x5g2 SEA-AD comments disposition by WG 2022-10-20.docx : Revised SDLS Green Book resulting from SEA/AD comments disposition by WG during the meeting (**attachment 5**)
* SDLS/COP ordering in TC issue :
  + Reordering the COP and SDLS Functions in TC Space Data Link Protocol.docx (**attachment 6**)
  + SDLS COP-1 Order Of Operations NASA (**attachment 7**)
  + SDLS COP-1 Order Of Operations CNES (**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) > [October 2022 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** |
| --- | --- | --- | --- |
| 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  Closed |

* Closed : Note added in §4.4.1.2 Implications for Key Verification, and referred to in §3.1.1.3 Protection of PDU and 3.2.5.1 Key Verification

| **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  Closed |

* Closed : text modified to mention the use of a unique identifier (e.g. APID) to route EP PDUs to the appropriate security unit on-board in the logical cross-strapping architecture.

| **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  Closed  Replaced by AI 1022/05 |

| **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  closed |

* Closed : final draft submitted to the WG and to the SLS and SEA ADs. Comments received from the SEA AD were discussed and dispositioned at this meeting.

## Update of SDLS Core Protocol (355.0-B-2)

The updated SDLS Core protocol blue book has been published – July 2022



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

The final draft reviewed by the WG at the last meeting was submitted to the SLS and SEA ADs together with a WG resolution to publish the document. Comments were received from the SEA AD. Those comments were discussed at this meeting and dispositioned. The resulting document (SDLS 350x5g2 SEA-AD comments disposition by WG 2022-10-20.docx) is in **attachment 5**.

The document still needs to be reviewed to answer the high level observations mentioned in the mail (13-10-2022 – **Attachment 4**) of SEA AD, reproduced hereafter:

1. It appears that the inclusion of AOS and USLP in this discussion is less than thorough.  Since both of them are now documented for use on the forward link, for “telecommanding” the treatment of them in that context should, in my opinion, be more thorough and careful.
2. There is a lot of casual use of TC and TM when it appears that telecommand and telemetry are really mean.  Likewise these words appear capitalized, implying the protocols, rather than lower case, implying the functions.  This should be cleared up.
3. There are a lot of references to the use of Reed Solomon which appear to make the assumption that this is the only forward coding allowed.  I believe that we now allow LDPC as well on the forward path, so this should be cleaned up too.
4. There is a fair amount of “we may do this” language in the document which seems to be a hold-over from White Book days.  This should be cleaned up.  It makes the document sound tentative.
5. It is not clear from the document if it is possible to apply these same link layer security approaches over an inter satellite link (ISL).  That kind of deployment, of course, would bring all kinds of key management complexities, and the whole use of terms like “telemetry” vs “telecommand” would need to be clarified, but in principle, given the essential protocol features, it should be possible to use it in this way.  Is this intended, or even possible?

Observation #2 has been taken care of by the modifications introduced in the document each time TC or TM is mentioned to clarify whether it is TC/TM protocols, or telecommand/telemetry functions which are meant.

The other observations will be dealt with further review of the document by Gilles Moury.

| **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 |

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

* Presentation by Antonios Atlasis: Post Quantum Cryptography for Space Missions – ESA presentation (**attachment 1**).
* ESA Technical note: Post Quantum Cryptography for Space Missions\_1.0 (**attachment 2**)

Discussion on slide #3: 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).

SDLS WG is invited to contribute/comment on use cases for asymmetric cryptography (slide #3 of presentation).

| **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 |

Slide #9: Asymmetric crypto can be used for:

* Public key encryption
* Session symmetric Keys establishment
* Digital signature

The application to SDLS would be : establishment of symmetric keys for each pair of communicating nodes.

For asymmetric crypto, Post Quantum Crypto (PQC) algorithms need to be considered given the risk of Quantum Computers maturity. NIST PQC competition is on-going (slide #9).

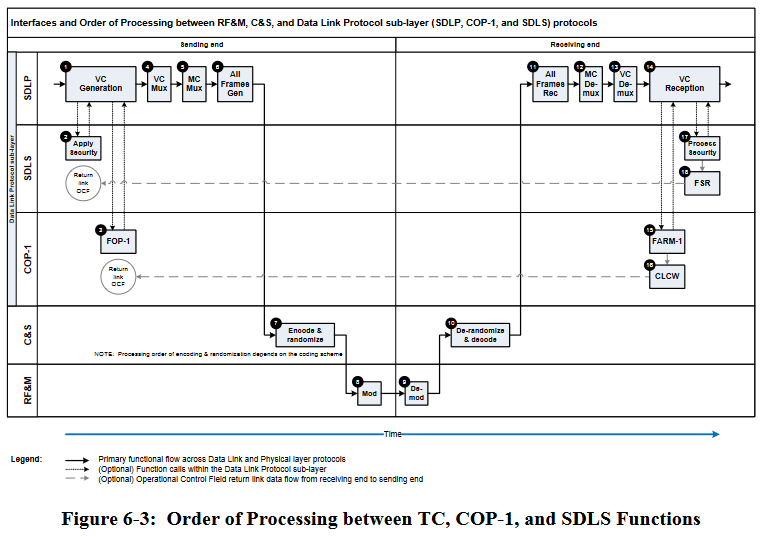
Security protocol (SDLS) needs to be adapted/augmented to benefit from asymmetric crypto/ PQC. Asymmetric crypto would be used to establish session keys to support symmetric crypto operational for data exchange.

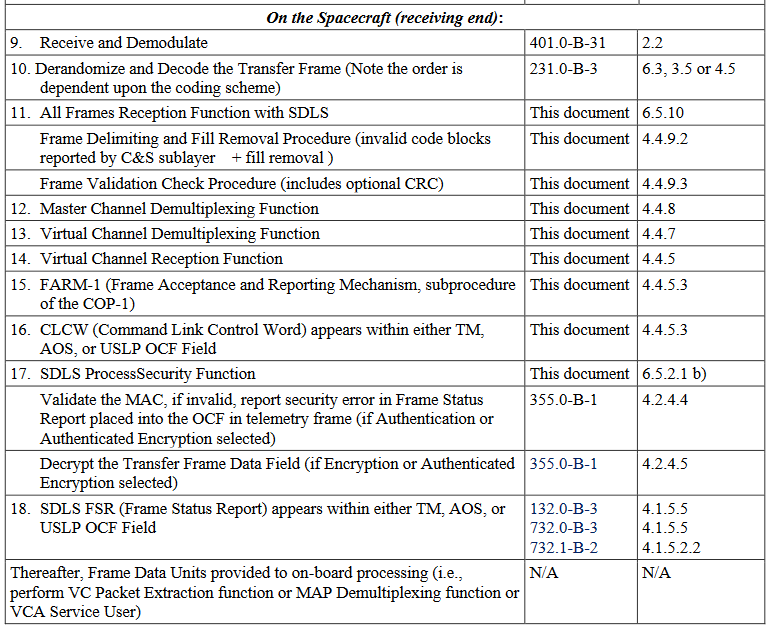
Slide #15: a number of criteria have to be taken into account for the trade-off on PQC algorithm selection and protocol design. Feedback of the WG on trade-off criteria / design considerations for PQC algorithm and protocol is welcome.

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

## Joint session with SLP WG: SDLS/COP ordering in TC

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 SDLP BB and reproduced below:







The pros and cons of both orders of processing have been exchanged by mail before the meeting (see **attachment 6**). Various considerations have been discussed during the meeting:

* Error detection and Frame validation (at the receiving side) are based on the channel code and the frame CRC (optional). This allows for a reliable transmission error detection. This transmission error detection occurs before SDLS function, whichever the order of processing between COP(FARM) and SDLS at the receiving side (see table 6-1 above).
* A specific sequence of operation is disrupting the COP with the current order of processing (see **attachment 7**):
  + A sequence of AD frames (one of which is discarded by Frame Validation due to transmission error) followed by a BD frame which bypass the COP. In that case, SDLS will accept the BD frame (provided its anti-replay sequence number window is sufficiently large) but rejects all the AD frames replayed by the COP (because of unvalid anti-replay counter – only upcounting ARC is allowed). In that case, COP will need to be reinitialized.
* Reversing the order of processing to :

FOP – SDLS – Encoding < Physical Channel > Decoding – SDLS – FARM

Raises the following problem (see **attachment 8** for details):

* + SDLS function operating before COP at the receiving end, and COP commands (BC frames) not being protected by SDLS, requires that BC frames bypass security. This bypass has to be based on the Bypass and Control Command flags of the Frame Header which is not authenticated. This is unacceptable since it introduces a security breach (backdoor) by allowing attacker to generate frames that will bypass security.
  + At the sending end, implementing SDLS function after FOP means that SDLS function has to be located in Ground Station in case COP is managed in G/S:
    - Implementing SDLS centrally at the MOC was a design criteria to avoid spreading security functions and keys to G/S.

Conclusion of the discussion:

* Reversing the order of processing to :

FOP – SDLS – Encoding < Physical Channel > Decoding – SDLS – FARM

would imply modifying SDLS protocol to include protection (in particular authentication) of BC frames. This is considered major modification that would impact existing implementations.

* For the reason explained above, decision of the WG was not to modify the order of processing between COP and SDLS but to document in SDLS GB the potential interference between COP and SDLS : e.g. sequence of operation depicted in **attachment 7.** This warning could be placed in SDLS GB annex D (Interaction of SDLS with data link protocol).

| **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 |

## SDLS Extended Procedures Green Book

SDLS Extended Procedures draft Green Book was reviewed. Text was added to §3.1.1.3, 3.2.5.1, 4.2.2, 4.4.1.2 to answer AI 0522/01 and 02. The resulting document is in **attachment 3**. Craig Biggerstaff will review and 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** |
| --- | --- | --- | --- |
| 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 |

## AOB

**Next meeting: May 8-12 2023, in Huntsville, AL, USA.**