**May 2024 CCSDS**

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

Washington DC, USA

May 1-2, 2024

# 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 |
| Brent Andres | NASA | Brent.r.andres@nasa.gov | 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 |
| Josiah Johnson | NASA | josiah.m.johnson@nasa.gov | On-site |
| Tanja Lange | TU Eindhoven / ESA | tanja@hyperelliptic.org | Remote |
| Jérome Merle | CNES | jerome.merle@cnes.fr | On-site |
| Joost Oranje | ESA | joost.oranje@esa.int | On-site |
| Yohann Roiron | ESA | yohann.roiron@esa.int | Remote |
| Bruno Saba | CNES | bruno.saba@cnes.fr | On-site |
| Charles Sheehe | NASA/GRC | charles.j.sheehe@nasa.gov | On-site |
| Marcus Wallum | ESA/ESOC | marcus.wallum@esa.int | On-site |

# Agenda :

The agenda of the meeting was the following:

**Wednesday May 1, 2024 all day, Thursday May 2 morning only**

|  |  |  |
| --- | --- | --- |
| **Date/time** | **Room** | **Agenda Item** |
| **May 1**  08:45 -17:30  (EDT) | TBD | 1 - Action items review |
| 2 – [Update of SDLS Core Protocol Green Book (350.5-G-2)](https://public.ccsds.org/Pubs/350x5g2.pdf):  Issue 2 published : January 2024 |
| 3 – SDLS Extended Procedures Green Book:  Disposition of comments received from SEA and SLS ADs  Resolution to publish |
| 4 – “ [Triple Key Encapsulation Mechanisms (KEM) Profile “ project](https://cwe.ccsds.org/fm/Lists/Projects/DispFormDraft.aspx?ID=788&Source=http://cwe.ccsds.org/fm/Lists/Projects/AllOpenChartersWithDraftProjects.aspx):  Review of project definition in CWE to be submitted to CMC approval  Outline of document and review of contributors  Discussion of the KEM profile to be selected for SDLS  Coordination with related projects:   * Crypto algorithms BB update * SDLS Extended Procedures update |
| **May 2**  08:45-12:45  (EDT) | TBD | 5 – “ [Revise SDLS Extended Procedures BB to adress constellations “ project](https://cwe.ccsds.org/fm/Lists/Projects/DispFormDraft.aspx?ID=789&Source=http://cwe.ccsds.org/fm/Lists/Projects/AllOpenChartersWithDraftProjects.aspx):  Review of project definition in CWE to be submitted to CMC approval  Outline of document and review of contributors  Discussion of the procedures to be added for symmetric key exchange and secure channel establishment between peers  Coordination with related projects:   * Triple Key Encapsulation Mechanisms (KEM) Profile * Crypto algorithms BB update |
| 6 – AOB: |

# Presentations and documents:

The list of presentations made is the following:

* Quantum Resistant CCSDS SDLS – Way forward – ESA presentation (**attachment 1**)
* Triple-KEM and Extended Procedures update projects – CNES presentation (**attachment 2**)

The list of input/output documents is the following:

* Update of SDLS Core Protocol Green Book 350.5-G-2
  + Final version published: 350x5g2.pdf (**attachment 3**)
* Final draft green book for SDLS EP 350.11-G:
  + Final version submitted to CMC poll for publication: 350x11xg1 - clean.docx (**attachment 4**)
* Final report from ESA study with TU Eindhoven: an asymmetric-based PQC algorithm for space mission (**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 2024 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** |
| --- | --- | --- | --- |
| SDLS1123/01 | Howie Weiss | Create 2 draft projects for:   * Revision of the crypto BB (352.0-B) to include asymmetric crypto primitives needed for Triple-KEM * Developing new BB for Triple-KEM procedure.   Submit projects to CMC approval, once agreed at Security WG level. | 15/12/2023  done |

Status: closed

* “Revision of Crypto BB” project was approved by CMC on 06/12/2024 – project to be handled by SEC WG
* “Triple-KEM BB” project was approved by CMC on 06/12/2024 – project to be handled by SDLS WG

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1123/02 | Gilles Moury | Create 1 draft project for:   * Revision of SDLS Extended Procedures (355.1-B) to include procedure for symmetric key exchange.   Submit project to CMC approval, once agreed at SDLS WG level. | 15/12/2023  done |

Status: closed

* “Revision of SDLS Extended Procedures BB to address constellations” project approved by CMC on 04/05/2024 – project to be handled by SDLS WG

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1123/03 | Gilles Moury | Issue WG resolution to publish SDLS EP Green Book and send to SLS and SEA ADs for review and approval. | 15/12/2023  done |

Status: closed – WG resolution to publish SDLS EP GB sent to SEA and SLS ADs on 11/09/2023.

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

The final version of the document has been published January 2024 (**attachment 1**).

## SDLS Extended Procedures Green Book

SDLS Extended Procedures final draft Green Book was updated by C.Biggerstaff before the meeting, including all the dispositions of the comments received from SEA and SLS ADs. Final edits were reviewed by the WG during the meeting. The resulting document is in **attachment 4**.

It will be submitted to CESG/CMC poll for publication following an SEA/SLS areas resolution to publish.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0524/01 | Gilles Moury | Issue SLS/SEA areas resolution to publish SDLS EP Green Book. | 15/06/2024 |

Many thanks to the book technical editor Craig Biggerstaff for his continuous commitment during this long drafting process.

## Triple-KEM project

* Presentation by Antonios Atlasis: Quantum Resistant CCSDS SDLS – Way forward – 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). This hierarchy does not fit with space-to-space links. 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 session 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).

To cover these new mission scenarios, 3 new projects have been approved to:

* Standardize a key establishment mechanism so-called Triple-KEM (Key Encapsulation Mechanism) to generate symmetric session keys needed to establish an SDLS secure channel between 2 peers at the data link layer.
* Revise the Crypto algorithms BB to include the asymmetric PQC primitives needed for the Triple-KEM
* Revise the Extended Procedures BB to include the procedures for session keys establishment and traffic SA instantiation between two peers.

The presentation (see **attachment 1**) discusses possible way forward for the 3 projects. The following points have been addressed:

* Study of PQC algos & protocols for SDLS initiated by ESA with experts from TU Eindhoven
* Trade-off performed to select best scheme for key establishment, so-called Triple-KEM
* Final report provided by ESA for circulation among the WG (see **attachment 5**)
* 2 other ESA activities could support the Triple-KEM project:
  + Development of a simulator for SDLS PQC implementations
  + Development of a first SDLS PQC implementation which could provide one of the 2 independent implementations needed for interoperability testing
* The Crypto algorithms GB will need to be updated to include justification for the introduction and selection of PQC algorithms + considerations on True Random Number Generators
* The Crypto algorithm BB will need to include the selected PQC KEM algorithms: Kyber, Classic McEliece (for cases where long term public key does not need to be renewed, or it is expected to be renewed very rarely, or throughput is big enough to accommodate its renewal), and FrodoKEM (for more conservative missions) (section 5) and introduce the concept of hybrid implementations (pre-post quantum) for asymmetric crypto protocol + crypto agility (section 2 – overview)
* For interoperability testing, reference implementations exist for PQC primitives. Therefore, no specific development is needed.
* Two approaches can be envisaged: with or without Pre-Shared Symmetric Keys: the latter is the preferred solution
* The Triple-KEM BB should be ideally written as cryptoagnostic but including a non-normative annex specifying a baseline mode with the preferred (hybrid) configuration.
* The Triple-KEM procedure could be potentially used also by BPSec. Therefore, *ideally*, the specification should also be generic with no SDLS specific features (TBC)
* The triple-KEM messages for key establishment need to be transmitted over the space link with appropriate security. This can be done:
  + using SDLS over the relevant data link protocol (AOS, TC, TM or USLP) by adding new procedures + associated messages to the Extended Procedures BB.
  + or by defining a dedicated transmission protocol for “space key exchange” procedures (i.e. like IKE for IPSec)
* Triple-KEM procedure will negotiate/establish only symmetric keys. Initiator/Recipient determination + SA parameters will preferably not be negotiated but possibly preset (e.g. according to the SCID for the I/R determination).

The 2 related draft projects need to be submitted to CMC approval:

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0524/02 | Gilles Moury | Request CCSDS Secretariat to submit “Triple-KEM” project to CMC poll for approval | 15/06/2024  done |

AI closed: Project submitted to CMC approval on 05/29/2024. Approved on 06/12/2024.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0524/03 | Howie Weiss | Request CCSDS Secretariat to submit “Update of crypto book” project to CMC poll for approval | 15/06/2024  done |

AI closed: Project submitted to CMC approval on 05/29/2024. Approved on 06/12/2024.

## [Revise SDLS Extended Procedures BB to address constellations “ project](https://cwe.ccsds.org/fm/Lists/Projects/DispFormDraft.aspx?ID=789&Source=http://cwe.ccsds.org/fm/Lists/Projects/AllOpenChartersWithDraftProjects.aspx)

* Presentation by Gilles Moury (CNES) : **Triple-KEM and Extended Procedures update projects – Attachment 2.**

SDLS Extended Procedures BB needs to be updated to include procedures for symmetric key exchange and secure link establishment between peers. Project has been approved by CMC on 04/05/2024.

Extended Procedures directives (Command and Reply) are normally transferred using packets over an SDLS secure channel. To instantiate this SA, a shared symmetric key needs to be exchanged between to 2 peers. To achieve this, two new procedures could be specified:

* Key exchange procedure:
  + Hypothesis: Bi-directional unsecure communication link already established (physical + data link): e.g. through Session Access Control procedure (Prox-1)
  + One peer starts the procedure by sending a query (hailing sequence)
  + Authentication of the parties
  + Key establishment/exchange by Triple-KEM: one set of symmetric traffic key(s)
* SA establishment procedure:
  + needs to create a common SA between the 2 peers
  + to be keyed with the ephemeral traffic key exchanged as a result of the KE procedure
  + negotiation/setting of the SA parameters

The feasibility of this approach needs to be confirmed taking into account the security requirements for the Triple-KEM messages transmission.

## AOB

**Next meeting: November 6-7 2024, in London, UK.**

**Intermediate webconf:** to be organized end September to discuss Triple-KEM procedures and specific requirements regarding data link protocol and security.