**June 2025 CCSDS**

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

JHU-APL, Laurel, MD, USA

June 11-12, 2025

# 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/JPL/Parsons | [howard.weiss@parsons.com](mailto:howard.weiss@parsons.com) | On-site |
| Antonios Atlasis | ESA/ESTEC | antonios.atlasis@esa.int | On-site |
| Craig Biggerstaff | NASA/JSC/KBR | [craig.biggerstaff@nasa.gov](mailto:craig.biggerstaff@nasa.gov) | Remote |
| Daniel Fischer | ESA/ESOC | Daniel.fischer@esa.int | On-site |
| Oana-Alexandra Graur | ESA/ESTEC | Oana-Alexandra.Graur@esa.int | Remote |
| Tanja Lange | TU Eindhoven / ESA | tanja@hyperelliptic.org | Remote |
| Jérome Merle | CNES | jerome.merle@cnes.fr | On-site |
| Matthias Mueller | OHB | Mathias.mueller@ohb.de | Remote |
| Dorothea Richter | DLR | dorothea.richter@dlr.de | On-site |
| Bruno Saba | CNES | bruno.saba@cnes.fr | On-site |
| Paul Thompson | RedSpace / UKSA | paul@redspace.ltd | On-site |
| Marcus Wallum | ESA/ESOC | marcus.wallum@esa.int | On-site |

# Agenda :

The agenda of the meeting was the following:

**Wednesday June 11, 2025 all day, Thursday June 12 afternoon only**

|  |  |  |
| --- | --- | --- |
| **Date/time** | **Room** | **Agenda Item** |
| **June 11**  08:45 -17:30  (EDT) | KC-4 | 1 - Action items review (see [MoM Nov 2024](https://spacecomm.sharepoint.com/sites/SLS/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2FSLS%2FShared%20Documents%2FSLS%2DSEA%2DDLS%2FCWE%20Private%2Fmeeting%20material%2FNov%202024%20meeting%2FMoM&FolderCTID=0x01200016AEFAC54964424C9CD979137E2A1E8A&View=%7B2BE46707%2D54B3%2D4558%2DB9B5%2D1A581FDDD2F7%7D)) |
| 2 – “[Revise Cryptographic Algorithm BB to add PQC algorithms” project](https://spacecomm.sharepoint.com/sites/FM/Lists/Projects/DispForm.aspx?ID=372&pa=1&e=PN4788):  Status of project  Selection of PQC primitives needed for Triple-KEM asymmetric key exchange  Recommended hybrid implementations |
| 3 – “ [Triple Key Encapsulation Mechanisms (KEM)” project](https://spacecomm.sharepoint.com/sites/FM/Lists/Projects/DispForm.aspx?ID=373&pa=1&e=kHW9vO):  Outline/scope/applicability of document  Review of the 3KEM procedure selected for SDLS:   * 3KEM (by Oana Alexandra Graur, A. Atlasis).   + 3KEM definition progress (detailed definition, software implementation, formal verifications)   + Preliminary identification of 3KEM managed parameters   Status of draft specification  Coordination with related projects:   * Crypto algorithms BB revision * SDLS Extended Procedures update |
| **June 12**  13:30-17:30  (EDT) | KC-4 | 4 – “ [Revise SDLS Extended Procedures BB to adress constellations “ project](https://spacecomm.sharepoint.com/sites/FM/Lists/Projects/DispForm.aspx?ID=375&pa=1&e=GvypPC):  Outline/scope of revision  Review of the key management procedure(s) to be added for symmetric key exchange (using 3KEM procedure) and secure channel establishment between peers:   * SDLS Extended Procedure for KEM Exchange (by Craig Biggerstaff) * Integration into SDLS and SDLS EP (by Oana Alexandra Graur, A. Atlasis)   + Preliminary trade-off (reusing existing SDLS PDUs and defining new ones). How to achieve rekeying of SDLS SAs when 3KEM is used   + Generic pool of 3KEM symmetric keys vs keys assigned automatically for SAs within the 3KEM at runtime   + Perfect Forward Secrecy (PFS) vs Contingency Operations - concept of sessions when it comes to integration into SDLS / SDLS EP and how to ensure that the operator does not use old keys from older 3KEM sessions, despite new keys having been generated by 3KEM in newer runs (yet not compromise on safety)   + Construction of KEY IDs for 3KEM keys   Status of draft specification  Coordination with related projects:   * Triple Key Encapsulation Mechanisms (KEM) * Crypto algorithms BB revision |
| 5 – revise security annex of [131.2-B](https://ccsds.org/wp-content/uploads/gravity_forms/5-448e85c647331d9cbaf66c096458bdd5/2025/01/131x2b2.pdf) and [131.3-B](https://ccsds.org/wp-content/uploads/gravity_forms/5-448e85c647331d9cbaf66c096458bdd5/2025/01/131x3b2e1.pdf) to mention specific security threats linked to Adaptive Coding and Modulation (ACM) systems |
| 6 – AOB: |

# Presentations and documents:

The list of presentations made is the following:

* CCSDS Cryptographic Algorithms – Proposed Updates and Rationale (for 3KEM Needs) – Oana Graur, Antonios Atlasis / ESA presentation (**attachment 1**)
* A post-Quantum Authenticated Key Exchange (3KEM) – Current State – Oana Graur & al. / ESA presentation (**attachment 2**)
* 3KEM Integration into SDLS EP – Oana Graur & al. / ESA presentation (**attachment 3**)
* SDLS Extended Procedure for KEM Exchange – Craig Biggerstaff / NASA presentation (**attachment 4**)

The list of input/output documents is the following:

* ESA proposed updates to the Cryptographic Algorithms Blue Book (352.0-B) to add PQC primitives to support Triple-KEM (**attachment 5**)
* CNES proposed updates to the security annexes of 131.2-B and 131.3-B to cover threats related to ACM mode of operation (**attachment 6**)

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) > [June 2025 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** |
| --- | --- | --- | --- |
| SDLS1124/01 | Oana Graur | Draft a first version of the Triple-KEM blue book. | ~~15/04/2025~~  15/11/25 |

AI open – Protocol steps of Triple KEM, prototyping and validation were discussed in detail at this meeting (see §4.3) to finalize the definition of the protocol and pave the way to the writing of the specification (Triple-KEM blue book). Deadline for the first draft is extended.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1124/02 | Craig Biggerstaff | Draft an update of the SDLS EP BB with a proposal for the additional KEM procedure(s) needed. | ~~15/04/2025~~  15/11/25 |

AI open: SDLS Extended Procedures needed to support 3-KEM were discussed in details at this meeting (see §4.4). Deadline for the first draft of updates to SDLS EP BB is extended.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1124/03 | Gilles Moury | Draft update of security annexes of 131.2 and 131.3 to include specific security threats to ACM. | 15/04/2025  closed |

AI closed at this meeting: see §4.5

## “Revise Cryptographic Algorithm BB to add PQC algorithms” project

An update of the CCSDS cryptographic algorithm BB has been drafted by ESA (**attachment 5**) to add Post Quantum Crypto primitives that can be used for key agreement purposes. It also introduces the concepts of crypto agility and hybrid implementations. Crypto algorithms Green Book will also need to be updated to discuss KEM, new primitives, crypto agility, hybrid.

More specifically the following post-quantum crypto algorithms have been proposed to support Key Exchange mechanism:

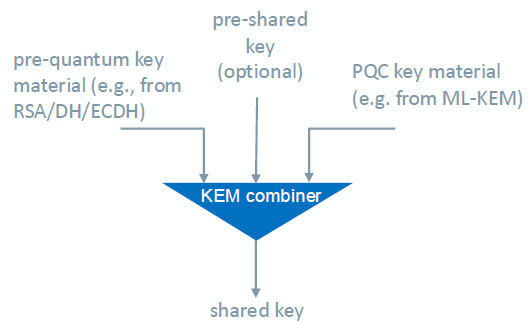
* ML-KEM (Module Lattice based Key Encapsulation Mechanism (ML-KEM also known as Kyber)) standardized by NIST as FIPS203. Is proposed for the baseline mode of 3KEM.
* FrodoKEM (under discussion for standardization by ISO)
* Classic McEliece (under discussion for standardization by ISO)

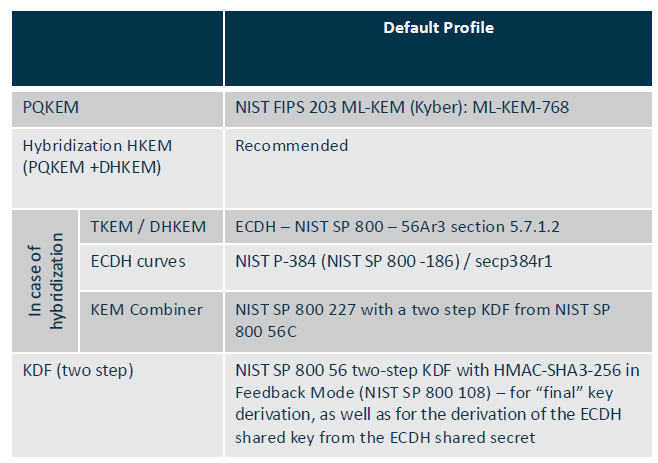
To support hybrid implementations, the following alternative pre-quantum algorithm has been also proposed: Elliptic Curve Cryptography (ECC) using ECDH (Elliptic Curve Diffie-Hellman)

Hybrid implementations enable to use post-quantum schemes in combination with classical schemes, thus mitigating the security risk stemming from a potential break of the relatively new post-quantum algorithms.

Four points have been discussed at the SEA-Security WG meeting and summarized at this meeting (see **attachment 1**):

* Curve selection for ECDH: NIST P-384 (FIPS PUB 800-186) is proposed for 3-KEM baseline mode
* Key Derivation Function (KDF):
  + Is needed to derive as many final keys as needed from the shared secret generated by KEM. Is also needed for hybrid implementation of KEM
  + NIST SP800-56C two step KDF is proposed for 3KEM baseline mode
* KEM combiner:
  + Is needed to combine the inputs from the pre- and post-quantum schemes (hybrid implementations) and produce a common shared secret



* + NIST SP800-227 KDF is proposed for 3KEM baseline mode.
* 3KEM – Default profile (baseline mode):
  + The baseline mode is proposed by ESA as follows:
  + 

ESA is currently prototyping in SW the 3 post-quantum algorithms proposed (ML-KEM, FrodoKEM and Classic McEliece) to check the suitability of those algorithms for implementation on space HW. This activity also covers SW implementation of the Triple-KEM.

## Triple-KEM project

* Presentation by Oana Graur: A post-Quantum Authenticated Key Exchange (3KEM) – Current State - ESA presentation (**attachment 2**)

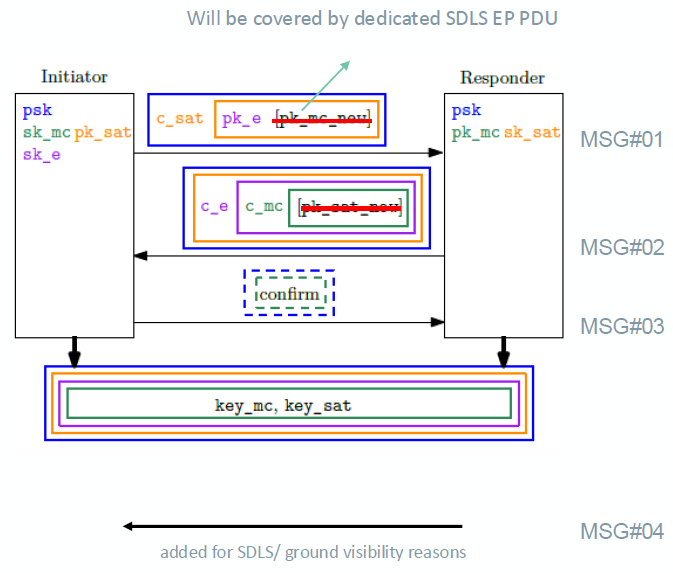
3KEM is a protocol for Authenticated Key Agreement tailored for space and SDLS, which provides:

* Perfect Forward Secrecy (PFS)
* Post-Quantum crypto (preferably hybridized with pre-quantum)
* Post Compromise Security

It should be suitable for a FIPS 140-3 certification or CC evaluation.

It should be easily executed on standard space hardware.

Slide #5: a fourth message/step is needed to confirm that the satellite (responder) has correctly received the 3rd message and the correct computation of all derived keys. It is a final bilateral key confirmation (see figure below).



The number of keys derived will be a managed parameter.

A set of public-private keys (so-called “long term key”) needs to be loaded on-board before flight. A specific EP procedure is needed for the update of the long term key. The update of the long term key requires the capability to generate autonomously on-board a set of public-private keys which in turn requires the implementation of a Random Number Generator (RNG) on-board. A RNG is also needed for 3KEM.

Slides 8-11 introduce the 3 steps/KEM of the 3KEM: IKEM, RKEM, EKEM enabling authentication of both parties and Key transport.

Given the complexity of the 3KEM protocol, a 3KEM Green Book is definitely needed.

Slides 13-20 detail the 3KEM protocol steps:

* Initiator ID, Responder ID and session # are needed
* Initiator ID and responder ID should identify the security unit addressed both on-board and on-ground. The notion of session should be introduced to allow PFS.
* A PROTOCOL\_TOKEN identifies the profile/configuration of the 3KEM used. It is a managed parameter of the protocol available at both ends of the link.
* PROTOCOL\_TOKEN is public information and can be transmitted in clear.
* Long term keys are also managed parameters of the protocol and needs to be loaded before flight.
* No negotiation of the cypher suite, it is too difficult to secure. 3KEM is an opinionated protocol where both parties need to have the same PROTOCOL\_TOKEN (managed parameter) to operate.
* The # of keys finally generated will be also a managed parameter of the protocol.

Formal Verification of 3KEM (slide 26):

* Will be done using Tamarin Prover as a formal verification tool using symbolic model
* Will also be done using Computational Model
* 2 independent teams working on validation. Some proofs already provided in study report.

Test vectors (slide 27):

* Include: inputs, outputs, randomness at every single steps of the protocol
* Could be provided as a 3KEM BB annex (possibly pointing to a SANA registry) for implementers to use for validation.

Prototyping:

* 2 Python implementations already exist: one by ESA, one by TU Eindhoven. 4th step/message needs to be added. KEM combiner still to be decided.
* An implementation over an FPGA (Microsemi PolarFire) is on-going at OHB (Matthias Mueller)

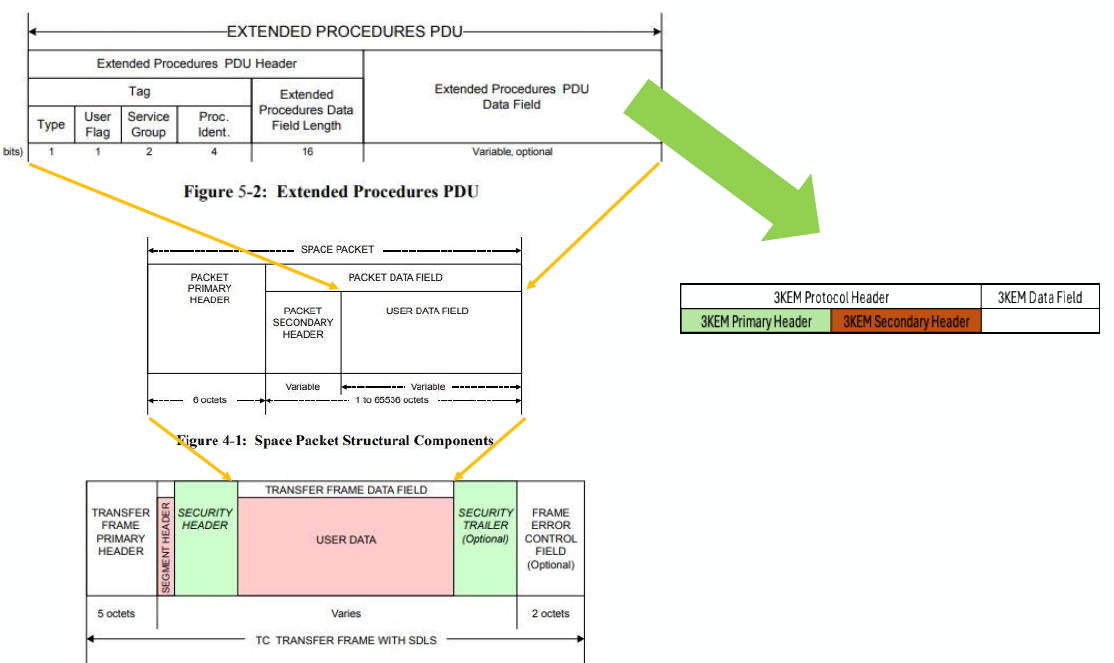
Way forward for the 3KEM BB:

* Slides and excel tables detailing the protocol steps will be distributed to the WG
* Draft specification (white book) to be circulated to the WG, ideally for the next meeting (mid-September). But given the very short period of time between this meeting and the next, this might not be possible.
* The 3KEM BB shall specify a generic 3KEM protocol allowing various configurations and crypto suites. An informative annex will specify a so-called “baseline mode/profile” that will be recommended for interoperability. It will correspond to a specific PROTOCOL\_TOKEN to be used as a default (see §4.2). The 3KEM messages will be specified in the 3KEM BB.

## [Revise SDLS Extended Procedures BB to support 3KEM and address constellations scenarios](https://cwe.ccsds.org/fm/Lists/Projects/DispFormDraft.aspx?ID=789&Source=http://cwe.ccsds.org/fm/Lists/Projects/AllOpenChartersWithDraftProjects.aspx)

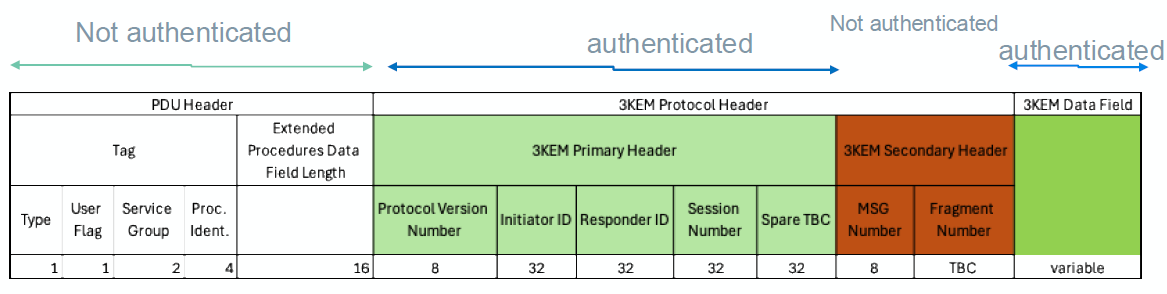
* 3KEM Integration into SDLS EP – Oana Graur & al. / ESA presentation (**attachment 3**)
* SDLS Extended Procedure for KEM Exchange – Craig Biggerstaff / NASA presentation (**attachment 4**)

3KEM messages are encapsulated in SDLS EP PDUs which are encapsulated in CCSDS packets inserted in Transfer Frames data field. The overhead is considered acceptable since the 3KEM protocol will be executed only once to establish secure channels between two entities.

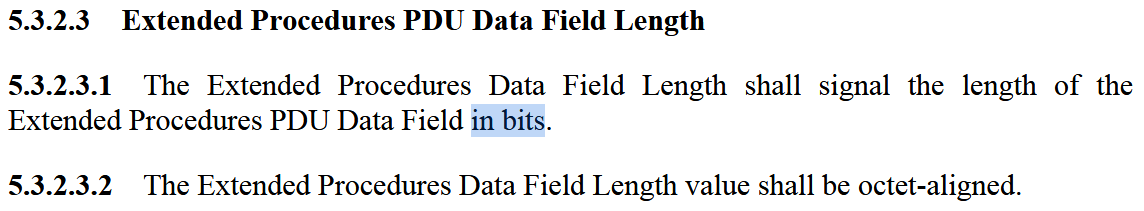


3KEM protocol header definition:

* Needs to include InitiatorID and ResponderID to identify target security unit (nominal/redundant) inside the spacecraft or ground segment (could be: SCID + @unit). Point to a set of long term keys (private, public) pre-loaded in the target unit.
* Needs to include a session number (32-bit to allow for random number)
* Needs to include a Protocol Version number to allow for further evolution of the protocol
* Secondary eaderHeaHHeader identifies the message # (1 to 4 for 3KEM) in the sequence and the fragment number (if 3KEM PDU fragmentation is needed).



As currently written in the SDLS EP BB (355.1-B-1), the EP PDU length is limited to 64Kbits, since the EP PDU length field is 16-bit and signals the length in bits (and not in bytes as it should be, since the data field length shall be octet-aligned) (§5.3.2.3.1):



This “typo” cannot be corrected without impacting existing SDLS EP implementations. Therefore, we are limited to 64Kbits for the 3KEM messages length. This might not be sufficient for all crypto suites. Estimation for:

* FrodoKEM: 25 kbytes
* ML-KEM Kyber : 3 kbytes

Fragmentation of 3KEM PDUs is therefore needed. Appropriate signalling of the fragment position should be put into the PDU secondary header (i.e. “fragment number” or “fragment offset”, …).

In terms of protection, the proposal is to have:

* EP PDU header not protected
* 3KEM message header authenticated
* 3KEM message secondary header not protected (authenticating secondary header adds complexity since this header changes for each message of the sequence)
* 3KEM message data field authenticated

Slide#15: proposal to have seven 3KEM messages defined:

* 4 for the 3KEM protocol itself (symmetric keys establishment)
* 1 to upload new long term public key
* 1 to ask the satellite to generate new long term public key and confirm generation
* 1 to downlink satellite/responder public key

Consideration for integrating 3KEM in EP (slides 21-29):

* SDLS EP designed for the management of purely symmetric systems. The concept of sessions (needed for PFS) does not exist.
* To leverage the provided PFS of the 3KEM protocol, it is proposed that:
  + New keys are derived in a new session
  + SAs are replicated and associated with fresh keys at every key negotiation session
  + The SPI definition is extended to include: Session ID and Context ID
* More generally, a specific mode for SDLS EP could be specified suited for 3KEM operation.

Way forward for the update (pink sheets) of the SDLS EP BB:

* Slides detailing the various proposals for the SDLS EP update to support 3KEM protocol will be distributed to the WG.
* The SDLS EP update will specify the additional procedure(s) and mode needed to execute sessions of 3KEM, refresh symmetric keys, rekey SAs and potentially renew long term keys (asymmetric keys).
* Draft specification of the updates (pink sheets) to be initiated once the 3KEM protocol draft specification is available.

## Revise security annex of [131.2-B](https://ccsds.org/wp-content/uploads/gravity_forms/5-448e85c647331d9cbaf66c096458bdd5/2025/01/131x2b2.pdf) and [131.3-B](https://ccsds.org/wp-content/uploads/gravity_forms/5-448e85c647331d9cbaf66c096458bdd5/2025/01/131x3b2e1.pdf) to mention specific security threats linked to Adaptive Coding and Modulation (ACM) systems

* CNES proposed updates to the security annexes of 131.2-B and 131.3-B to cover threats related to ACM mode of operation (**attachment 6**)

As a response to AI1124/03, a proposal for the update of security annexes to the 2 CCSDS standards which include ACM mode of operation, has been drafted. It has been discussed and updated during the meeting. The resulting text is in **attachment 6.** It details security threats, attack scenarios and countermeasures specific to the ACM mode of operation.

The update will be forwarded to the C&S WG who is in charge of those 2 standards.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0625/01 | Gilles Moury | Forward modified security annexes of 131.2 and 131.3 to C&S WG for further processing. | 15/07/2025 |

## AOB

The SDLS WG mailing list will be refreshed. Please send a confirmation mail to [gilles.moury@cnes.fr](mailto:gilles.moury@cnes.fr) if you wish to stay on the mailing list.

**Next meeting: 17-18 September 2025, TU Hamburg, Germany.**