**November 2024 CCSDS**

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

London, UK

November 6-7, 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 |
| Antonios Atlasis | ESA/ESTEC | antonios.atlasis@esa.int | On-site |
| Brandon Bailey | AerospaceCorp / NASA | [Brandon.bailey@aero.org](mailto:Brandon.bailey@aero.org) | 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 |
| Angel Custodio Espinar | OESIA / ESA | acustodio@oesia.com | On-site |
| Oana-Alexandra.Graur@esa.int | 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 |
| Dorothea Richter | DLR | dorothea.richter@dlr.de | On-site |
| Bruno Saba | CNES | bruno.saba@cnes.fr | On-site |
| Xisen Tian | Naval Post Graduate School / NASA | charles.j.sheehe@nasa.gov | On-site |
| Marcus Wallum | ESA/ESOC | marcus.wallum@esa.int | On-site |
| Cheon Yee Jin | KARI | yjcheon@kari.re.kr | On-site |

# Agenda :

The agenda of the meeting was the following:

**Wednesday Nov 6, 2024 all day, Thursday Nov 7 afternoon only**

|  |  |  |
| --- | --- | --- |
| **Date/time** | **Room** | **Agenda Item** |
| **Nov 6**  08:45 -17:00  (GMT) | Devonshire (Clayton hotel) | 1 - Action items review (see [MoM May 2024](https://cwe.ccsds.org/sls/docs/Forms/AllItems.aspx?RootFolder=%2Fsls%2Fdocs%2FSLS%2DSEA%2DDLS%2FCWE%20Private%2Fmeeting%20material%2FMay%202024%20meeting%2FMoM&FolderCTID=0x012000439B56FF51847E41B5728F9730D7B55F&View=%7BAE8FB44C%2DE80A%2D42CF%2D8558%2DFB495ABB675F%7D)) |
| 2 – [SDLS Extended Procedures Green Book](https://public.ccsds.org/Pubs/350x11g1e1.pdf):  Issue 1 published : July 2024 |
| 3 – [“Revise Cryptographic Algorithm BB to add PQC algorithms” project](https://cwe.ccsds.org/fm/Lists/Projects/DispForm.aspx?List=bc2d6e0f%2D3242%2D46e3%2Da13d%2D3d907343af44&ID=787&Source=https%3A%2F%2Fcwe%2Eccsds%2Eorg%2Ffm%2FLists%2FProjects%2FAllItems%2Easpx&ContentTypeId=0x0100B63160D64FE81342BE42A874DE7E703D):  Status of project  Selection of PQC primitives needed for Triple-KEM asymmetric key exchange  Possible/recommended hybrid implementations |
| 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):  Outline/scope/applicability of document  Discussion of the KEM profile to be selected for SDLS  Need for a dedicated “Space Key Exchange” protocol  Coordination with related projects:   * Crypto algorithms BB revision * SDLS Extended Procedures update |
| 5 – Presentation “Security assessment of SDLS implementation” (A.Atlasis - ESA) |
| 6 – Presentation “Unveiling Vulnerabilities in TT&C to Cyber Attacks” (B. Bailey - Aerospace Corp) |
| **Nov 7**  13:30-14:30  (GMT) | BSI G1 | 7 – Presentation of “[Adaptive Coding & Modulation (ACM) security issues](https://indico.esa.int/event/528/attachments/5988/10196/Security_Risks_of_Adaptive_Coding_and_Modulation_in_Space_Systems.pdf)” – Security Systems Lab (Oxford University)  Joint session with SLP/C&S/RFM WGs |
| **Nov 7**  14:30-17:30  (GMT) | Devonshire (Clayton hotel) | 8 – “ [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):  Outline/scope of revision  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 revision |
| 9 – AOB: |

# Presentations and documents:

The list of presentations made is the following:

* Using SPACE-SAT to find vulnerabilities in SDLS implementations– Antonios Atlasis / ESA presentation (**attachment 1**)
* Covert Control: Unveiling Vulnerabilities in TTC to Cyber Attacks – Brandon Bailey / Aerospace Corp presentation (**attachment 2**)
* 3KEM and KEM-Sign Integration in SDLS: brainstorming – Oana-Alexandra Graur / ESA presentation (**Attachment 3**)

The list of input/output documents is the following:

* Published Green Book for SDLS Extended Procedures 350.11-G-1 (**attachment 4**)
* Final report from ESA study with TU Eindhoven: an asymmetric-based PQC algorithm for space mission (**attachment 5**)
* ESA proposed update to the Cryptographic Algorithms Blue Book to add PQC primitives to support Triple-KEM (**attachment 6**)
* Paper from Security Lab / university of Oxford : Security Risks of Adaptive Coding and Modulation (ACM) in Space Systems (**attachment 7**)
* Presentation Paper from Security Lab / university of Oxford : Security Risks of Adaptive Coding and Modulation (ACM) in Space Systems (**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) > [Nov 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** |
| --- | --- | --- | --- |
| SDLS0524/01 | Gilles Moury | Issue SLS/SEA areas resolution to publish SDLS EP Green Book. | 15/06/2024  closed |

AI closed – resolution issued – Green Book published July 2024.

| **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  closed |

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  closed |

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

## SDLS Extended Procedures Green Book

SDLS Extended Procedures Green Book was published. The published document is in **attachment 4**. Many thanks to all the contributors and in particular to the editor Craig Biggerstaff.

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

An update of the CCSDS cryptographic algorithm BB has been drafted by ESA (**Attachment 6**) 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
* 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)

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.

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

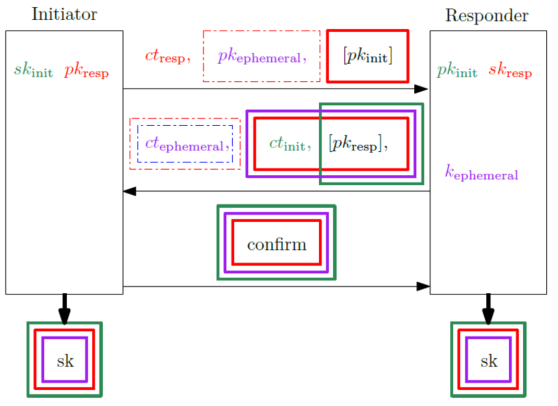
* Presentation by Oana-Alexandra Graur: 3KEM and KEM-Sign Integration in SDLS: brainstorming – ESA presentation (**attachment 3**)
* Final report from ESA study with TU Eindhoven: an asymmetric-based PQC algorithm for space mission (**attachment 5**)

The cryptographic primitives used in the key negotiation protocol needs to be mature and standardized and if possible approved by the national security agencies (NIST, BSI, ANSSI, …).

A validated/standardized KEM combiner should be specified to support an hybrid scheme (a KEM combiner uses a Key Derivation Function to combine the inputs from the pre- and post-quantum schemes and produce a common shared secret). Different solutions exist like: CHEMPAT, X-wing, …

Should certification according to NIST FIPS140-3 be considered for protocol and implementation?

Triple-KEM is a modular stand-alone protocol to establish symmetric keys between two parties (so-called Initiator and Responder). This protocol needs to exchange messages across the spacelink. The block diagram of the exchange is as follows (extract from ESA/TU Eindhoven report):

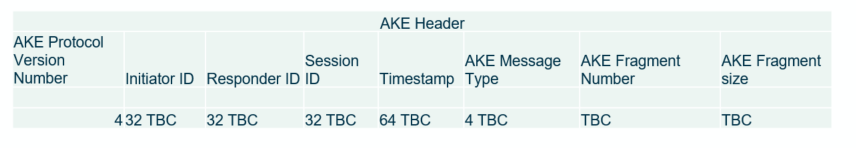


The KEM messages can be exchanged over an unprotected channel like an SDLS SA operating in clear mode. This dedicated SA in clear mode could be limited to the exchange of KEM messages. Denial of service is the only risk of operating the Triple-KEM procedure over an unprotected channel.

The KEM procedures generates a set of symmetric keys that can be used to key a so-called bootsrap SA that in turn will be used to instantiate one or several traffic SAs. All those SAs will be keyed by the symmetric keys generated by the Triple-KEM procedure.

The KEM messages provide their own protection using the private/public keys of the Initiator and the Responder. Those private/public keys should be pre-exiting in all the in-orbit assets. Distribution can be done pre-flight or in-orbit using SDLS.

A format is proposed for the KEM PDU (so-called AKE PDU):



This AKE PDU can be transmitted inside an SDLS EP PDU using the TLV format. A dedicated extended procedure (under Key Management) can be defined for KEM, enabling the exchange of KEM messages over an SDLS channel. The limitation in terms of PDU size is 64Ko (max CCSDS packet size).

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).

As a conclusion, KEM messages can be exchanged on the spacelink using a dedicated SDLS extended procedure that needs to be further specified in the revised SDLS EP BB. This limits the extent of the SDLS EP update needed to accommodate KEM.

The Triple-KEM Blue Book will specify the procedure and the AKE PDUs. The SDLS EP Blue Book will specify the procedure to transmit the AKE PDUs across the spacelink.

The Triple-KEM Blue Book will be ideally written as crypto agnostic with the addition of a non-normative annex specifying a baseline mode. This baseline mode will foster interoperability.

Oana Graur will draft a first version of the Triple-KEM blue book with an emphasis on the normative part: protocol specification and message (AKE PDU) format.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1124/01 | Oana Graur | Draft a first version of the Triple-KEM blue book. | 15/04/2025 |

## [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)

At least, one additional procedure needs to be defined for the transmission of KEM messages. Other might be needed to instantiate/key traffic SAs with the keys produced by the KEM procedure.

Error cases should be considered. KEM procedure should include error messages and “restart” directive in case of message not received or not received correctly, to avoid deadlock situations.

Craig Biggerstaff will draft an update of the SDLS EP BB with a proposal for the additional procedure(s) needed.

| **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 |

## Presentation “Security assessment of SDLS implementation” (A.Atlasis - ESA)

* Using SPACE-SAT to find vulnerabilities in SDLS implementations– Antonios Atlasis / ESA presentation (**attachment 1**)

SPACE-SAT is a security assessment toolset for CCSDS and ECSS protocols implementations (including SDLS). It was used to assess NASA Cryptolib implementation of SDLS and demonstrate the value of security assessment of implementations.

3 vulnerabilities were identified. They have been disclosed and have been fixed in new releases.

Implementation security considerations could be added in the SDLS Green Book together with a list of potential pitfalls.

## Presentation “Unveiling Vulnerabilities in TT&C to Cyber Attacks” (B. Bailey - Aerospace Corp)

* Covert Control: Unveiling Vulnerabilities in TTC to Cyber Attacks – Brandon Bailey / Aerospace Corp presentation (**attachment 2**)

This presentation made at CYSAT 2024 conference demonstrates through simulation of various attack scenarios (Man In the Middle, Rogue Ground Station) the value of SDLS to mitigate most of them. The simulation is performed using:

* + NASA Core Flight Software Simulator
  + and SPARTA Cyber Exploiter (SPACE) Invader to simulate the attacker (implementing SPARTA TTPs)

## Joint session with RFM/C&S/SLP WGs - Presentation of “[Adaptive Coding & Modulation (ACM) security issues](https://indico.esa.int/event/528/attachments/5988/10196/Security_Risks_of_Adaptive_Coding_and_Modulation_in_Space_Systems.pdf)” – Security Systems Lab (Oxford University)

* Paper from Security Lab / university of Oxford : Security Risks of Adaptive Coding and Modulation (ACM) in Space Systems (**attachment 7**)
* Presentation from Security Lab / university of Oxford : Security Risks of Adaptive Coding and Modulation (ACM) in Space Systems (**attachment 8**)

The objective of the attacker is to decrease the power requirements of performing a radio interference attack on the downlink by hijacking the ACM control channel on the return link. Specifically, the adversary aims to weaken the downlink channel to jamming and overshadowing interference by selecting less resilient modulation and coding parameters,

and by preventing the ground terminal from successfully requesting more resilient parameters.

Different types of attacks have been successfully experimented:

* Hijacking the ACM control channel on the uplink and select the least resilient MODCOD (for DVB-S2: 32-APSK 9/10). The attacker can then jam easily the communication downlink. Victim receiver’s requests to switch to a more resilient MODCOD are ignored. This type of attack can be avoided by protecting the ACM control channel uplink using SDLS to authenticate and anti-replay.
* Transmitting interference at a carefully selected power level, such that the victim’s receiver detects the interference and selects via the control channel a sufficiently robust MODCOD which implies a significant data rate reduction on the downlink communication channel. So with very limited power you are able to force the victim to a very low data rate transmission. This type of attack can be countered by implementing at the receiver a signal quality measurement resilient to radio interference.

Considering the security threats to ACM exemplified in this presentation, it is necessary to update the security annexes of the CCSDS Blue Books that cover ACM systems, namely:

* 131.3-B-2: CCSDS Space Link Protocols over ETSI DVB-S2 Standard
* 131.2-B-2: Flexible Advanced Coding and Modulation Scheme for High Rate Telemetry Applications

to include all the attack scenarios listed in the presentation.

| **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 |

## AOB

**Next meeting: 7-8 May 2025, APL, Laurel, USA (TBC).**

**Intermediate webconf:** TBD