CCSDS Space Data Link Security WG

June 11-12, 2025 meeting – JHU-APL Laurel, MD, USA

AGENDA

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

Date/time	Room	Agenda Item
June 11 08:45 -17:30 (EDT)	TBD	1 - Action items review (see MoM Nov 2024)
		2 – "Revise Cryptographic Algorithm BB to add PQC algorithms" project: Status of project Selection of PQC primitives needed for Triple-KEM asymmetric key exchange Recommended hybrid implementations
		3 – " Triple Key Encapsulation Mechanisms (KEM)" project: Outline/scope/applicability of document Review of the 3KEM procedure selected for SDLS: - 3KEM (by Oana Alexandra Graur, A. Atlasis). o 3KEM definition progress (detailed definition, software implementation, formal verifications) o 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)	TBD	4 – " Revise SDLS Extended Procedures BB to adress constellations " project: 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: - Integration into SDLS and SDLS EP (by Oana Alexandra Graur, A. Atlasis) o Preliminary trade-off (reusing existing SDLS PDUs and defining new ones). How to achieve rekeying of SDLS SAs when 3KEM is used o Generic pool of 3KEM symmetric keys vs keys assigned automatically for SAs within the 3KEM at runtime o 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 and 131.3-B to mention specific security threats linked to Adaptive Coding and Modulation (ACM) systems
		6 – AOB: