CCSDS Space Data Link Security WG

November 08-09, 2017 meeting in Den Haag Mariott (NL)

AGENDA

November 08, 09 AM

Date/time	Room	Agenda Item
Wed 08 08H45-17H30	Vermeer	**1- Action items review**
		2 – SDLS Core protocol Green Book: • Review of final draft submitted to CCSDS TE • Review of Annex 2.3 (design of cryptographic parameters) o See AI SDLS0517/02

		3 – SDLS Protocol extension (extended procedures):
		• Finalization of Red Book v4
		   o Review of SDLS Extended Procedures Red 1 v3
		   o Discussion of open points (see May 2017 MoM):
		      ▪ AI 0517/03 : FSR specification and flag definition (update of§4.2.2)
		      ▪ Rekey PDU and optional ARC parameter
		      ▪ Use of master keys : precisions to be added in §4.3.1
		      ▪ Association of ARC to key instead of SPI
		      ▪ OTAR/key verification procedure
		      ▪ Unique identification of source and target SPI (AI SDLS0517/04)
		      ▪ Unique identification of sender and receiver VCs (using Service Group field in PDU header)
		      ▪ Specification of uniqueness of SA database for bi-directional links.
		• Interoperability testing
		   o Test of procedures modified at last meeting (OTAR, key verification, key verification, ARC field in rekey PDU, identification of direction in subgroup field of PDU header (SA management), SA direction identification, "bad SPI" flag redefinition)
		   o Final results of interoperability testing and associated report (yellow book).

Thu 09 08H45-12H30	Dali	4 – <u>SDLS Extended Procedures Green Book:</u>
		
		   • Refinement of structure (AI SDLS0517/09)
		
		   • Review of contributions
		
		5 – <u>Physical layer security:</u>
		
		   • White paper on physical layer security:
		
		      o Threats that could be mitigated by physical layer security and corresponding security services
		
		      o Way forward.
		
		6 – <u>Meeting conclusions</u>