November 2017 CCSDS
Space Data Link Security WG Minutes of Meeting
Mariott Hotel – Den Haag, NL

November 6-8-9, 2017

1 Attendance:

SDLS WG meeting:

Name	Organization	Email Address
Gilles Moury (Co-Chair)	CNES	gilles.moury@cnes.fr
Howard Weiss (Co-Chair)	NASA/SPARTA	howard.weiss@parsons.com
Ignacio Aguilar-Sanchez	ESA/ESTEC	ignacio.aguilar.sanchez@esa.int
Kenneth Andrews	NASA/JPL	andrews@shannon.jpl.nasa.gov
Craig Biggerstaff	NASA/JSC	craig.biggerstaff@nasa.gov
Matthew Cosby	UKSA	matt.cosby@goonhilly.org
Daniel Fischer	ESA/ESOC	daniel.fischer@esa.int
Chen Jia	CLTC/BITTT	chenjiach@gmail.com
Dorothea Richter	DLR/GSOC	dorothea.richter@dlr.de
Bruno Saba	CNES	bruno.saba@cnes.fr
Victor Sank	NASA/GSFC	victor.j.sank@nasa.gov
Charles Sheehe	NASA/GRC	charles.j.Sheehe@nasa.gov
Chen Taoming	CLTC/BITTT	chentaoming@bittt.cn

Joint session with RFM and C&S WG on physical layer security:

- Participation from RFM and C&S WG

2 Agenda :

The agenda of the meeting was the following (**attachment 1**):

November 6 AM, 08, 09 AM

Date/time	Room	Agenda Item
Mon 06 10H00- 12H00	Dali	1- Joint session RFM – SEC – SDLS WGs: • Physical layer security: o Threats that could be mitigated by physical layer security and corresponding security services o Way forward.
Wed 08 08H45- 17H30	Vermeer	2 - Action items review
		3 – 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
		4 – SDLS Protocol extension (extended procedures): o Finalization of Red Book v6 o Review of SDLS Extended Procedures Red 1 v6 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. o 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	5 – Discussion of bulk encryption 6 – Compatibility of SDLS with USLP: • USLP interoperability testing including or not SDLS • Compatibility of SDLS with USLP 7 – SDLS Extended Procedures Green Book: • Refinement of structure (AI SDLS0517/09) • Review of contributions 8 – Meeting conclusions

The list of presentations made is the following:

- agenda (**attachment1)**
- physical layer security presentation by NASA/ESA (**attachment2**)

The list of input/output documents is the following:

- "SDLS Extended Procedures Red 1v6 Clean 20171109.docx" (**attachment 3**)
- Resolution to submit Extended Procedures red-1 book to Agency Review - SLS-SEA-R-2017-11-001(355.1).v1.2 (**attachment 4**)
- SDLS Green Book 350.5-G-0 final draft_Rev_16-11-2017 (**attachment 5**)
- Extended Procedures Green Book outline v2 (**attachment 6**)
- Extended Procedures Green Book concept paper and resolution (**attachment 7**)

All presentations and attachments are on the SDLS WG CWE private page :
http://cwe.ccsds.org : The CCSDS Collaborative Work Environment (CWE) > Space Link Services Area (SLS) > Documents > SLS-SEA-DLS > CWE Private > meeting material > Nov 2017 meeting

3 Agenda points

3.1 Joint session with RFM/C&S WG: Physical layer security (6 Nov)

Presentation by Charles Sheehe and Ignacio Aguilar of the various threats that could be dealt with by physical layer security (see presentation **in attachment 2**). This presentation was made in response to action item AI SDLS0517/01.

- Data interception threat (slide #4):
  - Quantum computing will invalidate a number of cryptographic algorithm by typically 2023: for example : IP-sec, AES with 128-bit keys or shorter. Symmetric key algorithm like AES will require 256-bit keys by 2023 to protect against quantum computing.
- Traffic analysis threat (slide #4):
  - No traffic analysis possible if you have a bulk encryption of the data stream with continuous transmission or physical layer security (like spread spectrum)
- Jamming threat (slide #5):
  - Error Detecting Code (EDC) on the uplink detects transmission errors due to possible jamming or RFI, and rejects transfer frames. In the case of jamming, it results in denial of service.
  - EDC can saturate if the error density is too high and not detect all errors. In that case there is a possibility of undetected errors forwarded to the data link layer.
  - There are different levels of denial of service induced by jamming:
    - Loss or absence of synchronization
    - Detected by uncorrectable errors resulting in frame loss
    - Undetected errors resulting in corrupted frames being passed to the link layer with a probability of executing corrupted commands.
  - Characteristics of jamming signals would be needed to start the analysis of possible anti-jamming techniques.
- Replay threat (slide #6):
  - Recording and replaying the physical signal can be efficient if no replay protection is implemented at higher layer.

- Physical layer security options:
  - Crypto spreading techniques:
    - Symmetric key crypto to produce crypto sequence used in direct-sequence spread spectrum (DSSS)
    - Symmetric key crypto to produce crypto sequence used in frequency hopping system (FHSS). Another scheme for frequency hopping system is “detect & avoid” where the jamming signal is detected and avoided.
    - These techniques can protect against jamming, data interception and replay

  - Crypto information manipulation techniques:
    - Bulk encryption randomizes the full data stream but does not protect completely against denial of service but it does protect against data interception and replay.
  - RF fingerprinting:
    - Typically 50 distinct characteristics of a transmitter can be used to build a fingerprint
    - Will protect against data modification and replay (through authentication of sender).
  - Interference cancelling techniques (Active Noise Reduction):
    - Can be added to the list of physical layer security options as active techniques.
  - Optical communications will be inherently more resilient to jamming in uplink and downlink since it requires from the attacker the precise pointing of its laser beam to the targeted spacecraft or ground station.

- Possible new books:

  - CCSDS has a recommendation for CDMA DSSS for space to space links (415.1-B). It specifies spreading codes to be used for LEO to GEO links via relay satellites (forward links). Those codes have been optimized to limit Power Spectral Density and interference between users. They are public codes not meant for physical layer security (anti-jamming) although they provide protection against unintentional RFI. This standard can also be used for Direct To Earth links. One possibility would be to develop a CDMA DSSS recommendation (BB) for CCSDS modulations, providing anti-jamming through cryptographic PN spreading sequence. At the input of this development, interferer/jammers and channels characteristics would need to be defined. Use cases for unintentional and intentional jamming protection would be needed.

  - Secure broadcast channel minimum parameter recommendation (Green Book)

Way forward discussed and proposed:

- More results on this topic expected from ESA studies within 2 years
- Agencies to be formally polled for potential interest in physical layer security (more specifically jamming/interference resistant transmission)
- ESA to provide references on those physical layer security techniques and possible scenarios/use cases.
- Physical layer security will be kept as a subject to be monitored within SEA-SEC WG. No further work on physical layer security envisaged at SLS level for the time being unless interest expressed by agencies to start a project.

A.I.	Actionee	Action	Deadline
SDLS1117/01	G.Moury	Initiate agency poll at CMC level to determine	30 Dec., 2017

A.I.	Actionee	Action	Deadline
		potential interest in physical layer security (protection against jamming/interference)	

3.2 SDLS WG meeting (8-9 November)

3.2.1 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
SDLS0416/08	B.Saba	Check suitability of Cloud Sigma as a cloud service provider for exporting code for interoperability testing.	15 July, 2016 open

- Daniel Fischer will transmit to Bruno Saba the ESA IT responsible contact for cloud testing contract.

A.I.	Actionee	Action	Deadline
SDLS0416/10	I.Aguilar C.Sheehe	Draft white paper on opportunity to standardize Physical layer security in the frame of CCSDS	15 October, 2017 cancelled

- Presentation given on Nov 6 at the joint RFM-SDLS session, on threats relevant to physical layer security. No further work on physical layer security envisaged at SLS level for the time being unless interest expressed by agencies to start a project.

A.I.	Actionee	Action	Deadline
SDLS0517/01	I.Aguilar C.Sheehe	Prepare white paper on physical layer security	30 Oct., 2017 cancelled

- Presentation given on Nov 6 at the joint RFM-SDLS session, on threats relevant to physical layer security. No further work on physical layer security envisaged at SLS level for the time being unless interest expressed by agencies to start a project.

A.I.	Actionee	Action	Deadline
SDLS0517/02	I.Aguilar	Introduce synthesis of ESA security analysis report in SDLS GB A2.3 and reference.	30 June, 2017 closed

- This security analysis study report has been synthetized in an ESA TT&C workshop paper that will be added as reference document in SDLS GB. Section A2.3 will point to this reference document. See §3.2.2 of MOM hereafter.

A.I.	Actionee	Action	Deadline
SDLS0517/03	D.Fischer	Introduce a subsection in SDLS Extended Procedures GB to describe CONOPS for switching keys on a secure channel "on the fly" vs "offline"	30 Mar, 2018 open

A.I.	Actionee	Action	Deadline
SDLS0517/04	G.Moury	Update §4.2.2 FSR according to above mentioned decision	June, 2017 closed

- Done in last version of SDLS EP red book (SDLS Extended Procedures Red 1v6 Clean 20171109.docx – **Attachment 3**)

A.I.	Actionee	Action	Deadline
SDLS0517/05	D.Fischer	Circulate mail of industry on the above issue (identification of Source and Target SPI in EP PDUs).	June, 2017 closed

- Synthesis of exchanges with industry on this topic has been uploaded on CWE.

Two issues identified linked to this problem of identification of Source and target SPI in EP PDUs:

1. How do the Sender and Recipient of EP knows that the SA used for sending the command is not identical to the SA being acted upon?
   - Solution 1 : add an SPI to the EP PDU
   - Solution 2 : leave it to the implementation to solve
2. Is this requirement (4.3.1.4 - The Recipient of a SA Management Procedure shall reject any EP PDU affecting the same SA used to transmit the PDU) legitimate?
   - There are counter examples where this requirement would prevent legitimate usage like: limiting an SA to kill only its own key thus preventing an attacker to kill all keys on-board in case one key has been compromised.
   - The rationale for this requirement was that you could screw up an SA by sending wrong commands like setARC on the same SA.

Conclusion: **remove requirement 4.3.1.4 (SA cannot affect itself) and add a note in §4.3.1.3 to explain that it is not good practice to use an SA to control itself.**
Modify also 4.3.1.3 to "…. may be used for exchanging EP service PDUs.".
Modify also 4.3.1.2 to add "….or authenticated encryption.".

A.I.	Actionee	Action	Deadline
SDLS0517/06	D.Fischer	Circulate final draft of EP red book to the WG for approval	30 June, 2017 Closed

A.I.	Actionee	Action	Deadline
			during the meeting

A.I.	Actionee	Action	Deadline
SDLS0517/07	G.Moury	Issue resolution to CESG and CTA to submit EP red-1 to Agency Review.	30 July, 2017 Closed during the meeting

- See attached resolution SLS-SEA-R-2017-11-001(355.1).v1.2 (**attachment 4**)

A.I.	Actionee	Action	Deadline
SDLS0517/08	D.Fischer I.Aguilar C.Biggerstaff	Propose amendment to SDLS EP or Core to specify uniqueness of SA database for bi-directional links.	30 June, 2017 Closed during the meeting (see below)

- Uniqueness of SA database is not needed because we identify direction in SA management EP PDU (using the service group field in the PDU header).
- Uniqueness of KeyIDs (therefore of Key Database) for bi-directionnal links is needed because there is no mechanism in the protocol (SDLS EP) to identify the direction in the key management EP PDUs. Therefore, this uniqueness of the KeyIDs needs to be stated in the EP specification.
- Solved by an additional statement in §2.3.1 end of second paragraph : “The initiator and the Recipient share a common set of keys for all communication links between them.

A.I.	Actionee	Action	Deadline
SDLS0517/09	G.Moury	Issue resolution to CMC to activate SDLS EP GB project	30 June, 2017 closed

- Done. Project activated.

A.I.	Actionee	Action	Deadline
SDLS0517/10	WG members	Provide refinements to GB outline : rationale + CONOPS parts	30 Mar, 2018 open

A.I.	Actionee	Action	Deadline
SDLS0517/11	G.Moury	Organize interim telecon to solve the problem of the uniqueness of the SA database in SDLS specifications	30 August, 2017 closed

3.2.2 SDLS core protocol green book

SDLS green book was reviewed during the meeting. The resulting version (SDLS Green Book 350.5-G-0 final draft_Rev_16-11-2017.docx) is in **attachment 5** and also in CWE > SLS-SEA-DLS > CWE Private > SDLS Core Green Book.

Annex A:

- A2.3 Design of cryptographic algorithm parameters:
  - As a result of action item SDLS 0517/02, a sentence has been added after Table A-1 to justify the proposed key length of 128-bit for the baseline mode. This sentence points to a newly introduced and more recent reference [27]. Reference [25] has been modified to point to a publicly available conference paper (which was not the case of the initial ref [25] which was an internal ESA report.)
  - Quantum computing will weaken symmetric key systems in a non-foreseeable future to the point where key length will have to be increased to 256-bit

The revised version of the GB was delivered to CCSDS CTE.

The SDLS core protocol green book will be processed by CCSDS CTE before spring 2018 meeting for a CMC poll and publication hopefully before our next meeting.

3.2.3 SDLS Protocol Extension (extended procedures)

The version of the SDLS Extended Procedures book subjected to review during the meeting was red book version 1.6 (SDLS Extended Procedures Red 1v6.docx). The final version, including amendment made during the meeting, was: SDLS Extended Procedures Red 1v6 Clean 20171109.docx (**attachment 3**)

All the modifications agreed at the last meeting were introduced by Daniel Fischer in Red1 v6:

- Mandate the use of master keys for OTAR only: go back to “master keys” for OTAR instead of “session key protection keys”
- Replace static keys by master keys throughout the document
- Use of master keys for recovery operations should be mandated in the key management magenta book (§3.1.1.1.)

- §4.3.1.3 : Rekey SA: add an ARC and IV as optional field in normative part (depending on the crypto algorithm) and as a 32-bit (TC) or 96-bit (TM) ARC field in baseline mode.

- §4.2.2. : FSR specification – “Bad SA” flag has been introduced: SA verification specification in SDLS Core protocol only includes verification of SPI pointing to an SA associated with the GVCID or the GMAPID of the Transfer Frame and not the other 2 conditions we want to add, namely :

    - SPI pointing to an inactive SA
    - SPI pointing to an SA associated with an inactive key
- The specification of the "Bad SA" flag has been complemented to include the 3 above error conditions.
- Add a pre-condition of rekey SA procedure (§3.3.2.3.1) : "The new key shall be in active state".
- In general, error conditions related to EP are not specified exhaustively in the EP red book. The error conditions should be discussed in the EP GB.

- Indication of direction was introduced in the SA management PDU through the service group (§5.3.2.2.3.3)

- Challenge/response scheme for key upload verification was reintroduced in OTAR procedure

- An annex with acronyms was added.

- ReadARC procedure was moved from Monitoring & Control to SA management.

A WG resolution to submit SDLS Extended Procedures red-1 book to Agency Review has been submitted at the end of the meeting (see **attachment 4**) together with the final red-1 version amended during the meeting : SDLS Extended Procedures Red 1v6 Clean 20171109.docx (**attachment 3**).

3.2.4 SDLS Extended Procedures Intra & Interoperability testing

No further activities to report since last meeting on interoperability testing. All the amendments to the EP specifications introduced since spring meeting need to be retested to complete the interoperability testing necessary for the Blue Book publication, namely:

- OTAR
- Identification of direction in subgroup (SA management PDU)
- Key verification (challenge/response reintroduced)
- ARC field added in rekey procedure
- Enlargement of "Bad SPI" flag specification to "Bad SA" flag.

Regarding interoperability testing, the WG strongly advocates the inclusion of SDLS function in the USLP interoperability testing given the potential interaction and the tight interface between SDLS function and USLP data link protocol. A portable implementation of SDLS function would be needed to integrate SDLS into the USLP interoperability testbed.

3.2.5 Extended Procedures Green Book

The reference of the document will be : 350.11-G.
Outline v2 has been distributed after last meeting (**attachment 6**) together with resolution and concept paper for the EP GB (**attachment 7**).

The responsibility/contributions have been agreed and approved by CMC as follows:

- Editorship : Craig Biggerstaff (NASA)
- Contributors:
  - Key Management : ESA
  - SA Management : NASA
  - M&C + FSR : CNES

Craig Biggerstaff will distribute the template for the EP GB such that each contributor can provide his contribution in the right format.

A.I.	Actionee	Action	Deadline
SDLS1117/02	C.Biggerstaff	Distribute EP GB template	30 Dec, 2017

3.2.6 Discussion on bulk encryption

This topic was presented by Victor Sank (NASA GSFC) to the WG for discussion on the potential interest of bulk encryption standardization in the frame of CCSDS.

The various points discussed were the following:

- Bulk encryption protects the full frame (including frame header) both for confidentiality and authenticity

- To be practical and efficient, bulk encryption needs to be inserted (at the sending end) between data link protocol sublayer and channel coding sublayer, so that transmission errors are corrected before decryption is performed at the receiving end. The other solution (i.e. channel coding before bulk encryption at the sending end) would be completely inefficient since decryption will typically spread transmission errors and therefore saturate the channel code. Also an undue authentication error will occur for each transmission error (false security alarm).

- In bulk encryption, encrypted data stream needs to be sliced in blocks preceded by synch marker, block length info and counter (for anti-replay).

- The additional capabilities brought by bulk encryption compared to SDLS are:

  - Confidentiality of the Transfer Frame header. Bulk encryption can thus prevent traffic analysis, which is nevertheless not a required security function for civilian missions and part of the governmental missions.
  - Simplification of implementation if Channel Coding is inserted in the TC receiver. In that case, TC receiver would deliver blocks of decoded data to the Security Unit for decryption. Security Unit would deliver streams of CLTU (TC) or CADU (TM) to the transfer frames processing. Security Unit could be inserted as "black box" between receiver (including channel decoding) and frame processing.

- In the case of bulk encryption, CCSDS could specify a standard interface for bulk encryption inserted between Channel Coding and Frame processing.

- The first point is to develop use cases for bulk encryption showing that there are interoperability and/or cross-support scenarios for this technique in missions were bulk encryption would be required.

A.I.	Actionee	Action	Deadline
SDLS1117/03	V. Sank	Provide use cases for bulk encryption (missions requiring it) and associated interoperability and/or cross-support scenarios.	30 March, 2018

3.3 AOB

Next meeting: 11-12 April 2018, NIST – Gaithersburg, MD, USA.