**May 2017 CCSDS**

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

**SwRI – San Antonio, TX USA**

May 8-10-11-12, 2017

# 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  |
| Brandon Bailey | NASA/GSFC | brandon.t.bailey@nasa.gov  |
| Craig Biggerstaff | NASA/JSC | craig.biggerstaff@nasa.gov  |
| Gian-Paolo Calzolari | ESA/ESOC | gian-paolo.calzolari@esa.int  |
| Matthew Cosby | UKSA | matt.cosby@goonhilly.org  |
| Daniel Fischer | ESA/ESOC | daniel.fischer@esa.int  |
| Scott Reeves | NASA | scott.reeves@nasa.gov  |
| Dorothea Richter | DLR/GSOC | dorothea.richter@dlr.de  |
| Charles Sheehe | NASA/GRC | charles.j.Sheehe@nasa.gov  |

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

* Participation from RFM and C&S WG

**Joint session with Space Data Link Protocols WG:**

* Participation from SLP WG

# Agenda :

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

|  |
| --- |
| **May 08 AM, 10, 11** |
|

|  |  |  |
| --- | --- | --- |
| **Date/time** | **Room** | **Agenda Item** |
| Mon 0810H45-12H30 | CafeteriaCR 3 | 1. Joint session with RFM WG (TBC) : Physical layer security
 |
| Wed 108H15 – 16H45 | Bldg 256-CR 1A | 2 – Action items review |
| 3 – SDLS Protocol extension (extended procedures) :* Finalization of White/Red Book v1
	+ Review of SDLS Extended Procedures Red 1 v3
	+ Discussion of remaining open points (see D.Fischer mail dated 04/12):
		- SA management
		- OTAR/key verification procedures
		- Use of master keys
		- Association of ARC to key instead of SPI
		- Frame Security Report
		- Unique identification of sender and receiver VCs
		- Reserved SPI
* WG resolution for SDLS extended procedures Red-1 Agency Review
 |
| Thu 118H15-12H00 | Bldg 256-CR 1A | 4 - SDLS Protocol extension (extended procedures) (cont’d) :* Prototyping
	+ Status report on on-going prototypes
* Interoperability testing
	+ Test plan / yellow book
	+ Status/results/potential issues raised
 |
| Thu 1113H00-15H00 | CafeteriaCR 3 | 5 – Joint session with SLP WG : Unique identification of sender and receiver VCs: GVCID-S/GVCID-R  |
| Thu 1115H00-16H45 | Bldg 256-CR 1A | 6 – WG further work : SDLS Extended Procedures Green Book (SDLS GB v2)* Discussion of outline
* Key roles : editor, main contributors
 |
| 7 – Action items and meeting wrap-up |

 |

The list of presentations made is the following:

* + - agenda (**attachment1)**
		- physical layer security presentation by ESA/NASA (**attachment2**)
		- Summary of the SDLS EP Test Campaign between NASA and ESA (**attachment 7**)

The list of input/output documents is the following:

* SDLS Green book “SDLS Green Book 350.5-G-0 final draft v2.docx” (**attachment 3**)
* “CRYPTOGRAPHIC KEY INFRASTRUCTURE FOR SECURITY SERVICES PROTECTING TT&C AND PAYLOAD LINKS OF SPACE MISSIONS” ESA study report (**attachment 4**)
* SDLS Extended Procedures Red 1 v3\_no track.docx (**attachment 5)**
* Symmetric Key management (353.0-R-0) (**attachment 6**)
* Outline of SDLS EP Green Book (**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) > [May 2017 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)

# Agenda points

## Joint session with RFM/C&S WG: Physical layer security (8 May)

Presentation by Ignacio Aguilar and Charles Sheehe of the various applications and techniques of physical layer security (see presentation **in attachment 2**).

* Security exists in CCSDS at data link layer (SDLS) and network layer
* Certain threats can only be efficiently mitigated at physical layer like:
	+ Denial of service
	+ Signal interception
* Physical layer security can expand/replace security services that can be provided at other layers (authentication, confidentiality). The interest of physical layer security is that it is based purely on information theory. The channels encryption cannot be broken even when the adversary has unlimited computing power.
* Traditionally physical layer has taken care of availability (anti-jamming) and complemented confidentiality with low probability of interception/detection (LPI/LPD).
* Two main services can be provided by physical layer security:
	+ Secrecy:
		- Spread Spectrum (well known technique) but relying on cryptography and key exchange 🡺 does not bring additional performance wrt classical crypto at upper layers
		- Hybrid approach: Physical layer to agree a secret key exploiting noise in the channel, then “classical” Data link layer to cipher communications
		- Channel codes for secrecy: Two design objectives: Reliability (capacity) and Security constraint (secrecy in various metrics)
	+ Identification:
		- RF fingerprinting 🡺 uniquely identifies the transmitter protecting against spoofing.
* All those physical layer techniques have a low maturity level (apart from spread spectrum anti-jamming) wrt operational use in a space project. Therefore they are not ready for standardization yet.

**Way forward discussed and proposed:**

* Start from the “Threats to space missions” GB to identify those threats which could be advantageously mitigated by techniques at physical layer
* Identify corresponding security services which could be provided at physical layer
* If at least 2 agencies agree on providing resources, develop Green Book documenting the appropriate physical layer security techniques providing those security services.
* If at least 2 agencies agree on providing resources, develop Blue Book for those physical layer security techniques which have reached the sufficient level of maturity for standardization and which provide security services needed by space missions in an efficient manner.

I.Aguilar and C.Sheehe have agreed to continue investigating the subject following the agreed way forward. A white paper will be produced for next meeting where a joint session SDLS/SEC/RFM/C&S could be organized.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0517/01 | I.AguilarC.Sheehe | Prepare white paper on physical layer security |  30 Oct.,2017 |

Open question : is there a case for standardizing mature technique(s) for anti-jamming and protection against traffic analysis (like spread-spectrum) ? Is there a need in terms of cross-support, interoperability ?

## SDLS WG meeting (10-11 May)

### 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,2016open |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0416/10 | I.AguilarC.Sheehe | Draft white paper on opportunity to standardize Physical layer security in the frame of CCSDS |  15 October,2017open |

* Presentation given on May 8. Way forward agreed. Deadline postponed to next meeting.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1016/03 | G.Moury | Organize joint meeting between Sec WG and SLS WG on physical layer security concept paper produced by Sec WG, at the spring 2017 meeting |  March,2017closed |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0117/01 | WG members | Review final version of SDLS Green Book. Analyse ESA technical note on security analysis. |  March,2017closed |

Done. Still need to decide how to integrate results of ESA security analysis study report in SDLS Green Book – most probably as a short synthesis in A2.3 (see discussion on GB in these MoM).

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0117/02 | G.Moury | Issue WG and Area resolution for SDLS Green Book publication. |  March,2017closed |

Done. Resolution issued May 8 and sent to CESG and CTE (T.Gannett).

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1016/04 | C.Biggerstaff | Provide missing text and figures for §3.3 SA Management |  November,2016closed |

Done.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1016/05 | G.Moury | Provide a 32-bit CRC for the baseline mode OTAR procedure for Encrypted Key Block protection.  |  Dec,2016closed |

Done.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1016/06 | D.Fischer | Finalize Extended Procedures red-1.  |  January,2017closed |

Done. The version produced for the meeting is : “SDLS Extended Procedures Red 1 v3” which was reviewed during the meeting.

### SDLS protocol green book

SDLS green book was reviewed during the meeting. The resulting version (SDLS Green Book 350.5-G-0 final draft v2.docx) is in **attachment 3** and also in CWE > SLS-SEA-DLS > CWE Private > SDLS Core Green Book.

Annex A:

* A2.3 Design of cryptographic algorithm parameters:
	+ ESA has provided a detailed study report on “ CRYPTOGRAPHIC KEY INFRASTRUCTURE FOR SECURITY SERVICES PROTECTING TT&C AND PAYLOAD LINKS OF SPACE MISSIONS “ (**attachment 4**). This report provides extensive justification for Key length and MAC length. Therefore, a reference to this report is appropriate in this section together with the insertion of a synthesis of it in the text. Another complementary solution is to incorporate a synthesis of the results (+ reference) in the Key management Green Book which will be updated at the occasion of the upcoming 5-year review.
	+ Quantum computing does not change the conclusions within the 5 years to come.

AI 0117/01 is superseded and replaced by the following action item:

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0517/01 | I.Aguilar | Introduce synthesis of ESA security analysis report in SDLS GB A2.3 and reference.  |  30 June,2017 |

A resolution has been issued on May 8 to CESG and CTE (T.Gannett) to publish SDLS Core Protocol Green Book. Green Book can still be updated while the CTE is processing it.

### SDLS Protocol Extension (extended procedures)

The version of the SDLS Extended Procedures book subjected to review during the meeting was red book version 1.3 (SDLS Extended Procedures Red 1 v3\_no track.docx – **Attachment 5**)

The various sections/topics discussed were the following (see D.Fischer mail dated 12 April listing issues raised by industry):

1) SA Management service – key switching:

*Issue raised: It was pointed out that the way how keys can be changed on a running SA may not be practicable. At the moment, this requires four SA procedures to be executed. (1) Stoop SA, (2) Expire SA (3) Rekey SA (4) Start SA. However, it may be preferable to be able to change the keys "on the fly" without having to shut down the SA. This would make key changing much simpler.*

SPI was extended to 16-bit to allow for a very large number of potentially active SA and switching key “on the fly” from frame to frame by switching SPI thus pointing to different SA with different keys. In the most common scenario, SA will be activated largely in advance wrt their effective use. SAs will be keyed/activated well in advance with all the keys needed for operation of the spacelink. A section in SDLS GB Issue 2 (associated with SDLS extended procedures) should be included to describe the Concept of Operations for switching keys on the fly by switching SPI. The procedures for rekeying and SA will only be used in an offline manner.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0517/02 | 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” |  Dec,2017 |

2) OTAR / Key verification procedures:

*Issue raised: The rationale for us to introduce the CRC check was to be able to execute the Key Verification without having to start the lifetime of the key that is being checked. Industry however pointed out that (1) These kinds of checks are usually done by the spacecraft anyway on its memory and (2) That a CRC is not secure and will not guarantee that keys cannot be modified onboard the spacecraft. Instead they suggested to go back to the old Challenge/Response*

*concept but only execute that prior to activating the session key for operations anyway. In this way, the start of the key lifetime is not a problem.*

CRC check on keys before use is already done by the S/C security unit. Memory scrubbing is also done on on-board memory to protect key storage. Therefore the proposed key verification procedure is largely redundant with on-board protection mechanisms. On the contrary a challenge/response key verification procedure enables to test just before key use the integrity of the key and the correct operation of the crypto core.

**Decision: Go back to challenge/response scheme and remove CRC from OTAR procedure.**

The challenge/response directives are sensitive. They need to be protected by authenticated encryption. The response directive is the encrypted (or authenticated) version of the nonce (Number Used Once).

3) Use of Master keys:

*Issue raised: We have specified which procedures are considered sensitive. Industry pointed out that it is still not clear which procedures requires protection under a master key (so far only the OTAR specifies that directly) and in general what the master keys are being used for. Some of this is in the Symmetric Key Management Book however we should think about if we want to have other procedures especially protected under the use of a master key.*

Which procedures need to be protected by master keys ?

What are master keys and session keys used for ?

Use of master keys is specified in §3.1.1 of Magenta Book on Symmetric key management (CCSDS 353.0-R-0 – **attachment 6**). **Use of master keys for recovery operations should be added to the list of master keys purposes in §3.1.1.1 of MB.**

Section §4.3.1 Transfer of EP service PDU of the EP red book should be reworded to reflect the following **decision:**

* **Do not mandate usage of master keys for EP procedures**
* **Do not mandate use of reserved SPI either**
* **Standard should not be prescriptive on the usage of master keys apart from OTAR.**
* **Master keys should be stored in nonvolatile memory**

4) Association of ARC to Key instead of SPI:

*Issue: Industry suggested to associate the ARC to a key rather than an SPI. They argue that is is a more natural connection since a new key would also start a new ARC (TBD). I personally disagree with this but I think it’s worth discussing this in the group.*

* When you rekey an SA (stop, deactivate, rekey, start), you do not necessarily reset the ARC unless you send a separate command (setARC)
* One possibility is to add ARC as mandatory field in the rekey procedure PDU

**Decision: add an ARC as managed field in normative part and as a 64-bit ARC field in the rekey PDU for baseline mode.**

5) Frame Security Report (FSR):

*Issue: Industry appreciates the concept but has argued that the inclusion of additional error sources (and thus more flags and reduced bits from SN) should be included such as (a) bad MAC, (b) invalid Key/SA state, (c) invalid frame length. For me this makes sense.*

* (a) Bad MAC is already included in FSR
* (b) Invalid Key/SA state :
	+ **Add in §3.3.2.3.1 (Pre-conditions for Rekey SA procedure) : “The new key shall be in an active state”**
	+ This status bit would report on an SPI pointing to an SA not active or with a key in a non-active state.
	+ One solution is to enlarge the definition of “Bad SPI” flag to:
		- SPI pointing to an inactive SA
		- SPI pointing to an SA associated with an inactive key
		- SPI pointing to an SA that is associated to a VC or MAP different from the VC/MAP of the received TC frame

**Decision: update text of §4.2.2 FSR to rename the “bad SPI” flag into “Bad SA” flag and to include the 3 interpretations above.**

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0517/03 | G.Moury | Update §4.2.2 FSR according to above mentioned decision |  June,2017 |

* (c) Invalid frame length:
	+ To be clarified. If this is to report incoherent frame structure, it will be checked and reported to ground by the FARM (COP-1) and the frame will be rejected before reaching security processor.

6) Unique identification of sender and receiver VCs:

*Issue: David has raised the point once more that sender and receiver VCs can currently not be distinguished (since the GVCID is not unique for up and downlinks). A discussion with SLS should take place in the meeting to find a solution for this since it does not only touch the Extended Procedures.*

* We need to have unique identification of VC and MAP. This is not provided by GVCID/GMAPID since the Transfer Frame Version Number (TFVN) part of the GVCID/GMAPID is ambiguous – does not identify direction of the VC:
	+ 00 for TC **and** TM
	+ 01 for AOS (either uplink or downlink)
	+ 11 for Proximity
* One solution for SDLS only, would be to add to the service group in the PDU header an additional service group to identify the direction for an SA management procedure, as follows (§5.3.2.2.2.3 Service Group field):
	+ A setting of “01” shall identify a Security Association Management procedure targeting an SA that handle communication from the Initiator to the Recipient.
	+ A setting of “10” shall identify a Security Association Management procedure targeting an SA that handle communication from the Recipient to the Initiator.
* Another solution would be to partition the SPI by direction of the SA but this creates 2 problems:
	+ 2 reserved values at both ends of the range (all 0’s and all 1’s)
	+ Partitioning SPI would imply updating the SDLS Core Protocol.
* Therefore, the first solution is preferred (VC/MAP direction identification by service group in the EP PDU). See also discussion of the subject in the minutes of the joint session SDLS/SLP hereafter.

7) Additional point to discuss:

* Opportunity to add “Source SPI” in all EP PDUs to the “target SPI” to enable enforcement on-board of the rule that an SA cannot control itself.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0517/04 | D.Fischer | Circulate mail of industry on the above issue (identification of Source and Target SPI in EP PDUs). |  June,2017 |

8) Way forward on Extended Procedures red book:

The following actions have been agreed:

* **Create an annex with acronyms**
* **Move ReadARC procedure (§5.6.1.6.3) from M&C to SA management**
* **Modify §4.2.2 FSR definition**
* **Clarify “invalid frame length status” proposal for FSR with industry**
* **Circulate final draft for WG approval by end of June**
* **Issue resolution for agency review of red-1**
* **Objective is to have RIDs from AR#1 available for next meeting**

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0517/05 | D.Fischer | Circulate final draft of EP red book to the WG for approval |  30 June,2017 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0517/06 | G.Moury | Issue resolution to CESG and CTA to submit EP red-1 to Agency Review. |  30 July,2017 |

### SDLS Extended Procedures Intra & Interoperability testing

* See test presentation (**attachment 7**).
* Two types of tests were successfully performed to validate the SDLS Extended Procedures:
	+ Intra-operability tests performed between 2 ESA simulators: one for the ground segment (SCC) and one for the on-board segment (S/C simulator) both implementing SDLS Core protocol and SDLS Extended Procedures;
	+ Inter-operability tests performed between an ESA ground segment simulator and a NASA space segment simulator. Those simulators include independently developed security functions implementing SDLS Core Protocol and Extended Procedures.
* Intra-operability tests included COP-1 while inter-operability tests did not (no COP-1 on S/C side).
* Injection of SDLS protocol errors only and not of transmission errors (yellow book to be corrected)
* Master keys were used for OTAR only.
* 1 PDU per frame in TC, packets with spill-over in TM
* For M&C procedures test of baseline mode only.

Way Forward on testing:

* The following procedures need to be retested following the modifications made to the specification during this meeting:
	+ OTAR
	+ Key verification
	+ Identification of direction in subgroup (SA management)
	+ Key verification (challenge/response)
	+ ARC field added in rekey procedure
	+ ReadARC procedure moved to SA management
	+ SA direction identification
	+ Enlargement of “bad SPI” flag definition.
* Additional tests to be performed:
	+ End of May for EP specification update following this meeting
	+ End of June for completing interoperability testing.

All SDLS Extended Procedures **were successfully** tested during the intra-operability tests and the inter-operability tests.

At the occasion of these tests specification ambiguities were found which will be corrected in the final red-1 version of the SDLS EP.

Simultaneous implementation of interoperability testing and development of standard proved out to be fruitful to improve quality of specification.

## Joint session with Space Link Protocol WG:

The objective of this joint session was to discuss the opportunity to add a direction flag/indication to the GVCID and GMAPID. This would enable to identify uniquely VC/MAP operating on the forward or return link. There was a proposal to creat a new ID called: DGVCID/ DGMAPID by adding a direction bit in front of the existing GVCID/GMAPID.

The conclusion of the discussion is the following:

* The signification of a direction flag can only be interpreted locally in the context of a given link and protocol. Example:
	+ AOS is bidirectional and could be used on space-to-space links where forward and return terms are ambiguous
	+ For SDLS, since the protocol is asymmetric with an Initiator and a Recipient, a direction bit could be interpreted unambiguously. This is not the case for all SLP protocols.
* Therefore, a direction flag added to GVCID/GMAPID is ambiguous and not needed by SLP. SDLS WG will tailor its own local solution to this problem (see §3.2.3.6 of these MoM).

For SDLS protocol, the SA database needs to be unique for a bi-directional link. We need to analyse how to specify in SDLS EP and/or Core protocol the unicity of the on-board SA database. Identify statements that would prevent the uniqueness of the SA database on-board. One possibility is to add statements in Core Protocol GB.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0517/07 | D.FischerI.AguilarC.Biggerstaff | Propose amendment to SDLS EP or Core to specify uniqueness of SA database for bi-directional links. |  30 June,2017 |

## SDLS Extended Procedures Green Book

* The corresponding draft project need to be activated

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0517/08 | G.Moury | Issue resolution to CMC to activate SDLS EP GB project |  30 June,2017 |

* The objective is to develop a stand-alone GB for EP rather than an Issue 2 of the SDLS GB incorporating EP considerations.
* The outline of the GB was discussed and drafted (see **attachment 8**).
* The responsibility/contributions have been agreed as follows:
	+ Editorship : Craig Biggerstaff (NASA)
	+ Contributors:
		- Key Management : ESA
		- SA Management : NASA
		- M&C + FSR : CNES

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0517/09 | WG members | Provide refinements to GB outline : rationale + CONOPS parts |  30 Sept,2017 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0517/10 | G.Moury | Organize interim telecon to solve the problem of the uniqueness of the SA database in SDLS specifications |  30 August,2017 |

## AOB

**Next meeting: 8-9 November 2017, The Hague – Hotel Mariott.**