**May 2019 CCSDS**

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

**NASA Ames – Mountain View, CA, USA**

May 8-9, 2019

# 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  |
| Craig Biggerstaff | NASA/JSC | craig.biggerstaff@nasa.gov  |
| Matthew Cosby | UKSA | matt.cosby@goonhilly.org  |
| Daniel Fischer | ESA/ESOC | daniel.fischer@esa.int  |
| Tim Dafoe | CSA | tim.dafoe@ontario.ca |
| Joost Oranje | CGI Netherland BV | joost.oranje@cgi.com |
| Dorothea Richter | DLR/GSOC | dorothea.richter@dlr.de  |
| Charles Sheehe | NASA/GRC | charles.j.sheehe@nasa.gov |
| Bruno Saba (by teleconf only on Thursday morning) | CNES | bruno.saba@cnes.fr |
| Paul Thompson | QinetiQ Ltd | pbthompson@quinetiq.com |

* 

# Agenda :

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

|  |  |  |
| --- | --- | --- |
| **Date/time** | **Room** | **Agenda Item** |
|  |  | 1 - Action items review |
| 2 – SDLS Extended Procedures Blue Book:* Finalization of document for submission to publication poll (AI SDLS 1018/01, 03, 04, 05, 06, 07, 10)
* SDLS EP integration in AOS+TM BB (Pink sheets – AI SDLS 0418/02)
* USLP integration in SDLS EP BB
* Interoperability testing
	+ Status
	+ finalization of test report
 |
| 3 – SDLS Extended Procedures Green Book:* Review of contributions (AI SDLS 0418/05, 1018/02, 07, 08, 09, 10, 11, 12)
* Review of document
 |
| 4 – Other topics* Pink sheets for SDLS 355.0-B-1 to introduce USLP
* Missions using SDLS
* Future work
 |

The list of presentations made is the following:

* + - agenda (**attachment1)**
		- Presentation of SDLS Core protocol - Presentation SDLS CB.pptx **(attachment 2)**
		- Presentation of SDLS Extended Procedures - Presentation SDLS EP CB.pptx **(attachment 3)**

The list of input/output documents is the following:

* Pink sheets for TM Space Data Link introducing FSR and SDLS EP - 132x0b2\_final modif 4.1.5 insertion FSR v3.doc (**attachment 4**)
* Pink sheets for AOS Space Data Link introducing FSR and SDLS EP - 732x0b3\_final modif 4.1.5 insertion FSR v3.doc (**attachment 5**)
* Draft blue book for SDLS EP - 355x1r1\_final\_RIDs\_implemented + reviewed20190508+DF.doc (**attachment 6**)
* Draft green book for SDLS EP - SDLS Extended Procedures Green v1 - California review.docx (**attachment 7**)
* Pink sheets to SDLS BB to introduce USLP - 355x0b1\_final PS for USLP insertion.doc (**attachment 8**)
* CNES RID for the addition of Key Inventory procedure - 355x1r1.CNES\_RID\_BS (**attachment 9**)
* ESA slide on KM-Synch issue - SDLS\_KM-Sync issue.pdf (**attachment 10**)
* Key Inventory PDUs figures - 355x1r1\_final\_RIDs\_implemented - Key Inventory drawing.vsd (**attachment 11**)

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 2019 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

## 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 |

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

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1117/01 | G.Moury | Initiate agency poll at CMC level to determine potential interest in physical layer security (protection against jamming/interference) |  30 Dec.,2017open |

* Open: security WG considers developing a Green Book on physical layer security including potential user requirements and solutions (see §3.5).

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0418/02 | G.Moury | Submit input to TM and AOS SDLP BB upcoming pink sheets to introduce reference to FSR in §4.1.5 of those BB. |  July,2018closed |

* Pink sheets generated impacting §3.6.1 and 4.1.5 of those 2 books (**attachments 4 & 5**).

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0418/05 | C.BiggerstaffIgnacio Aguilar | Develop scenarios including ISL and constellations in §4.2 scenarios of EP GB |  Sept2018open |

* Open : see discussion on EP GB (§3.3)

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1018/01 | H. Weiss | Add : Anti-Replay Sequence Number (ARSN) to the Security Glossary. |  April2019open |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1018/02 | C. Biggerstaff | Add a text discussing EP PDU protection over the spacelink in EP GB . |  April2019open |

* Open: see discussion on EP GB (§3.3)

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1018/03 | D. Fischer | Replace all terms related to on-board security function by : Recipient Security Function. |  April2019closed |

* Closed: implemented (see last version of EP draft BB in **attachment 6**)

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1018/04 | D. Fischer | Change key length to 256 bit for AES in baseline mode of EP. |  Jan2019closed |

* Closed: implemented (see last version of EP draft BB in **attachment 6**). Key length change to 256 bits needs to be reflected also in baseline mode of SDLS BB (Pink Sheets for the document to be produced for 5-year review introducing: USLP, 256-bit key length for AES baseline mode, SDLS EP, …). Pink sheets introducing USLP in SDLS BB have been produced (**attachment 8**). See §3.4

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1018/05 | D. Fischer | Insert all RIDs dispositions in EP red book master file. Produce EP Blue Book draft for transmission to CTE when interoperability testing will be completed. |  Jan2019closed |

* Closed: implemented (see last version of EP draft BB in **attachment 6**). Final draft BB still to be prepared inserting all modifications agreed at this meeting (see § 3.2)

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1018/06 | G.Moury | Return all RIDs dispositions to initiators for potential feedback. |  Nov2018closed |

* Closed: done – all RIDs initiators have accepted the proposed dispositions

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1018/07 | C. BiggerstaffD.Fischer | Add USLP to the list of compatible/supported Space Data Link Protocols in respectively the EP GB and the EP BB. |  Dec2018closed |

* Closed: implemented (see last version of EP draft BB in **attachment 6** and last version of EP draft GB in **attachment 7**)

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1018/08 | C. Biggerstaff | Add a justification in EP GB why key derivation (scheme 3) is not included in EP. |  Mar2019open |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1018/09 | C. Biggerstaff | Align terminology to Anti-Replay Sequence Number (ARSN) to replace : ARC, SN, … |  Mar2019open |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1018/10 | D. Fischer | Propose wording for Deactivated state to be reflected in Key management MB, EP BB, EP GB to clarify the fact that deactivated keys can only be used to decrypt formerly encrypted data but not to encrypt/authenticate new data. |  Dec2018open |

* Open : text to be inserted in Key Management Magenta Book and EP BB. Both document should be submitted simultaneously for publication.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1018/11 | C.Biggerstaff | Complement sections 3.3.6 and 3.6.2 to reflect various routing options to address N/R Security Unit and on-board routing of EP directives. |  Mar2019open |

* Open : discussed during the meeting (see §3.3). Already some text inserted in section 3.6.2. To be complemented following meeting conclusion.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1018/12 | G. Moury | Develop Annex A Baseline mode to justify Baseline Mode settings. |  Mar2019open |

## SDLS Extended Procedures draft Blue Book

A draft Blue Book has been prepared by Daniel Fischer incorporating all RIDs disposition from the Agency Review. This draft has been reviewed in detail during the meeting. The updated draft with the modification made during the meeting is in **Attachment 6**. The following points have been discussed:

* SDLS EP is a unidirectional protocol for which in the most common scenario, the initiator is on the ground (Satellite Control Center) and the recipient is the satellite. Based on this main scenario, the link between the initiator and the recipient is an uplink potentially using the COP-1 retransmission protocol. Therefore, it was decided to allow only the following Space Data Link protocols for the forward link (Initiator to Recipient) and return link (Recipient to Initiator):
	+ Forward link : TC, AOS, USLP (rationale : TM cannot be used for uplink with COP)
	+ Return link : TM, AOS, USLP (rationale : TC transfer frames do not have OCF to transmit FSR and therefore cannot be used for downlink)
	+ In §4.2.2 FSR and the rest of the document, it was agreed that the term uplink and downlink would be avoided to allow for scenarios were SDLS will be deployed on space-to-space links. The neutral term “link” will be used instead, the direction being indicated wrt Initiator and Recipient.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0519/01 | G. Moury | Justify in EP GB the set of Space Data Link protocols allowed for forward and return links (as specified in §4.2.2). |  Sept2019 |

* The wording for the specification of the fields of all the PDU which include N-iteration in the data field, has been improved to clarify the fact that fields lengths and number of iteration (N) are managed parameters.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0519/02 | D. Fischer | Use wording agreed for Key Verification PDU specification (5.4.2.5.2.2) for all PDUs. |  31/05/2019 |

* The length field in the PDU header indicates the length of the PDU data field in bits (as specified in 5.3.2.3). The binary value indicated in some of the figures of PDUs are erroneous since they indicate length in octets. It was agreed to remove all the binary value from the PDU figures.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0519/03 | D. Fischer | Remove binary values in length fields from PDU figures in §5 (as in 5.5.1.11). |  31/05/2019 |

* In the frame of SDLS EP implementation studies performed separately by CNES and ESA, it was identified a need for an additional procedure: Key Inventory. The rationale for this addition can be found in:
	+ CNES RID (**Attachment 9** - 355x1r1.CNES\_RID\_BS.docx)
	+ ESA slide on issue of reception confirmation in key exchange (**Attachment 10** - SDLS\_KM-Sync issue.pdf)

As defined, the Extended Procedures do not allow for downloading any information on on-board keys such as key-ID and key status. From a ground point of view, it would be very useful if a “Key Inventory” procedure could be added. This procedure would allow the ground segment to know exactly how many keys are present in the on-board security processor, their ID, and their state (“pre-activated”, “activated”, “deactivated”). If a key is activated, knowing to which SA(s) it is bound to, would also be useful. Key inventory procedure allows also to have confirmation of the reception of keys and state of keys as a verification for all the key management procedures. It enables easy check of key synchronisation between both ends of the link.

Regarding Key Inventory procedure, the following was agreed:

* + Specify the range of Key ID to be inventoried in the command PDU. This to avoid reply PDU of unlimited size
	+ Return in the reply PDU only (Key ID, Key state) (avoid transmitting as well associated SA)
	+ C. Biggerstaff drafted the diagram for the corresponding PDUs (in **Attachment 11** - 355x1r1\_final\_RIDs\_implemented - Key Inventory drawing.vsd)
	+ Key Inventory will not be part of baseline mode

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0519/04 | B. Saba | Draft text for Key Inventory procedure (§3 service definition and §5 PDUs specification) |  31/05/2019 |

* Baseline mode:
	+ The Rekey SA PDU figure needs to be duplicated to show the 2 different cases:
		- TC with only an authentication key and ARSN
		- TM, AOS and USLP with potentially all fields: authentication key, encryption key, ARSN, IV.
	+ USLP should be added to the baseline mode on top of TM, TC and AOS

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0519/05 | D. Fischer | Update text for baseline mode : Rekey SA PDU, USLP addition |  31/05/2019 |

Resolution to submit EP BB to CESG/CMC poll for publication will be issued as soon as:

* Final draft BB available and circulated to WG for approval
* Interoperability testing completed between ESA and NASA
* Interoperability test report (yellow book) finalized

Interoperability testing should be completed within 2 weeks after baseline mode specification is finalized.

Objective is to have CESG/CMC poll in summer 2019.

## Extended Procedures Green Book

The reference of the document is: 350.11-G. The green book resulting from the review/modifications made during the meeting is: SDLS Extended Procedures Green v1 - California review.docx (**attachment 7**). The following points were discussed:

* §3.3.5 and 3.6.2: Handling redundancy N/R security unit and routing of EP PDUs on-board:
	+ Two scenarios are detailed for the routing of EP PDU to the appropriate Security Unit (N or R):
		- Scenario 1: use different VCs to address nominal vs redundant receiving string and its corresponding security unit. Use dedicated VC/MAP for addressing specifically the security unit of a given string.
		- Scenario 2 : In the case where the same set of VCs are used for normal traffic through nominal and redundant strings, use separate/dedicated VCs/MAPs to route to specific Security Processor (N or R)
	+ SPI space (i.e. SAs) could be portioned between Nominal and Redundant strings to guarantee uniqueness across strings, which is a necessity since SA states are a priori not shared across strings.
	+ Two diagrams have been inserted in §3.6.2.1, illustrating the cross-strapping options between the security functions/units and the receiving strings.
	+ A discussion of the possible hardware architectures where security unit is implemented in series vs. implemented as a branch, should be added in §3.6 Various types of implementation.
* §4.2: Inter-Satellite Link scenario:
	+ The SDLS EP being essentially a master-slave protocol where the Initiator is the master and the Recipient the slave, in an inter-satellite link it is necessary either to introduce a hierarchy for each link, or if peer-to-peer is necessary a master should be placed in the constellation or on the ground to control all those slave nodes through the transmission of EP commands. The 2 scenarios have been discussed and will be developed in green book:
		- Scenario 1: master-slave. A full hierarchy is defined across the constellation where for each possible ISL there is a master and a slave.
		- Scenario 2: peer-to-peer: a central master to configure all satellite nodes of the constellation. In this latter case, EP commands of the master need to be transmitted to the each of the slave possibly through ISLinks as well as through ground to space links. In that case, since there is no hierarchy between satellite nodes, the space data link protocol should be bi-directional (i.e. AOS or USLP configured as AOS).
	+ The Lunar Gateway could be taken as an example to illustrate one or both scenarios.
* Two presentations have been prepared by Craig Biggerstaff to introduce SDLS and SDLS EP to projects (**attachment 2 & 3**). Those 2 presentations contain diagrams that can be used to illustrate the discussions of the green book. It is also very valuable as a presentation of SDLS functions and usage to projects.

## Pink Sheets to SDLS core protocol (355.0-B-1) to introduce USLP

For coherency with SDLS EP, USLP need to be introduced in SDLS core protocol as a fourth compatible Space Data Link Protocol. Pink sheets have been produced by Gilles Moury (**Attachment 8**). Additional edits need to be introduced at the occasion of the 5-year review of the document due in 2020:

* AES key length change to 256 bits needs to be reflected also in baseline mode of SDLS BB to be coherent with SDLS EP BB
* SDLS EP needs to be properly referenced in SDLS BB.
* §2.2.6: figure 2-6: add an additional entry for COP management service for USLP
* §3.2.2.5: NOTES: USLP ApplySecurity Payload: USLP is compatible with variable or fixed frame length. For SDLS over TC, Transfer Frame are variable length and SDLS will increase the size of the submitted frame by the size of Security Header + Trailer. For SDLS over TM/AOS, the frame length is fixed and SDLS will reduce the size of the available frame data field by the size of the security header and trailer so that the overall frame length is kept constant. For USLP, since the two cases are possible, it is decided that the length of the fixed-length frames will be kept constant as for AOS and TM, meaning that the frame data field will be reduced by the size of the Sec Header and Trailer. This is to reflected in the 3.2.2.5 NOTES.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0519/06 | G. Moury | Update pink sheets to SDLS BB to introduce USLP and the above mentioned edits. |  31/07/2019 |

## Future Work

* Physical layer security was discussed in the Security WG meeting. Different solutions were listed that could be proposed for standardization:
	+ Anti-jamming through the use of Direct Sequence – Spread Spectrum (DS-CDMA as proposed by Dan Olsen (Aerospace Corp.))
	+ AES based DS-CDMA as proposed by ETSI as an option to ETSI uplink standard for GEO satellites (EN 321 926)
	+ Spread spectrum CDMA solutions developed for Multiple Satellite per Aperture scenarios
	+ RF transport (e;g; RF over IP)
* Sec WG will continue this analysis of requirements and possible solutions for physical layer security (potential green book).

## AOB

**Next webconference: to be scheduled end of June with the objective:**

* **To finalize SDLS EP Blue Book + interoperability test report**
* **To review progress on SDLS EP Green Book**

**Next meeting: 23-24 October 2019, ESA Darmstadt – Germany.**