**October 2018 CCSDS**

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

**DIN – Berlin, Germany**

October 17-18, 2018

# 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  |
| David Koisser | ESA/TUD | david.koisser@esa.int |
| Robert Pitts | NASA/MSFC | robert.l.pitts@nasa.gov |
| Anthony Scott Reeves | NASA/MSFC | scott.reeves@nasa.gov  |
| Charles Sheehe | NASA/GRC | charles.j.sheehe@nasa.gov |
| Dorothea Richter | DLR/GSOC | dorothea.richter@dlr.de  |
| Bruno Saba | CNES | bruno.saba@cnes.fr |
| Scott Reeves | NASA/MSFC | scott.reeves@nasa.gov  |
| Marcus Wallum | ESA | marcus.wallum@esa.int |

# Agenda :

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

|  |  |  |
| --- | --- | --- |
| **Date/time** | **Room** | **Agenda Item** |
|  | R183 | 1 - Action items review |
| 2 – SDLS Protocol extension (extended procedures):* Agency Review #1:
	+ RIDs disposition
* USLP integration in SDLS BB
* SDLS EP integration in AOS+TM BB
* Interoperability testing
	+ Plan for completing
 |
| 3 – SDLS Extended Procedures Green Book:* Review of contributions (AI SDLS 0418/03, 04, 05)
* Review of document
 |
| 4 – Security at CLTU level:* Presentation/proposal by NASA/GSFC

5 - Meeting conclusions* Missions using SDLS
* Future work
 |

The list of presentations made is the following:

* + - agenda (**attachment1)**
		- Security at CLTU level – presentation by V.Sank**:**CCSDS DRAFT S-X Cmd CLTU w bulk security 10-16-18.ppt **(attachment 2)**

The list of input/output documents is the following:

* SDLS EP RIDs disposition.7z (**attachment 3**)
* SDLS Extended Procedures Red 1version submitted to Agency Review – 355x1r1\_final.pdf (**attachment 4**)
* SDLS Extended Procedures Green v1 - Berlin review.docx (**attachment 5**)
* SDLS EP interoperability test report v3 (**attachment 6**)

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) > [october 2018 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: will be submitted to CESG. ETSI TM/TC standard and CCSDS 415.1-B (Data Transmission and PN Ranging for 2 GHz CDMA Link via Data Relay Satellite) provides spread spectrum CDMA physical link although not meant for anti-jamming protection.

| **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,2018closed |

* Closed : Presentation made at this meeting discussing security at CLTU level – see point 4 of the agenda.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0418/01 | G.Moury | Generate RID for SDLS EP red book agency review to introduce editorial modification made to §4.1 during meeting (see **attachment 3**) |  July,2018closed |

* Closed : RID CNES GM1

| **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,2018open |

* Open : pink sheets to be generated impacting §3.6.1 and 4.1.5 of those books. Update of the documents for 5-year review in 2020.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0418/03 | G.Moury | Issue RID against EP red-1 to add a definition of Security Unit. |  July2018closed |

* Closed : CNES RID GM3

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0418/04 | G.Moury | Provide text for §3.5.1 Failure handling |  Sept2018closed |

* Closed : input provided by mail.

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

* Open : see discussion on EP GB §3

## SDLS extended procedures red book 1 agency review RIDs

33 RIDs were received and processed:

* 23 ESA
* 5 CSA
* 2 NASA
* 3 CNES

All dispositions have been recorded in: SDLS EP RIDs disposition.7z (**attachment 3**). The document submitted to review is EP red-1 (**attachment 4**).

The following point have been discussed:

ESA-MW-01 : key suspended state optional in Key Management Magenta Book and useful only for ground. Compromised state only useful for the initiator (master) i.e. ground in the case of EP. Two NOTES will be added in the EP red book to explain why those 2 states are not used in EP.

ESA-MW-06 : terminology has to unified for ARC and Sequence Number. Terminology will be unified in EP with the term : Anti-Replay Sequence Number (ARSN). This term will be added to Security Glossary.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1018/01 | H. Weiss | Add : Anti-Replay Sequence Number (ARSN) to the Security Glossary. |  April2019 |

ESA-MW-16: table 4-1 specifying sensitive directives and requirement 4.3.1.1. requiring protection by authentication-encryption of those directives were decide to be removed and replaced by NOTES indicating that protection of EP directives beyond authentication is mission specific and driven by risk analysis. A specific subsection should be added to EP GB on this subject:

“SDLS EP directives PDUs are protected as a minimum with authentication. As an option, authenticated encryption could be applied if risk analysis requires it.”

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1018/02 | C. Biggerstaff | Add a text discussing EP PDU protection over the spacelink in EP GB . |  April2019 |

Various denominations exist for the on-board security function:

* On-board security unit
* On-board security processor
* On-board security function
* SDLS on-board function

It is agreed to replace all those different terms by: Recipient Security Function.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1018/03 | D. Fischer | Replace all terms related to on-board security function by : Recipient Security Function. |  April2019 |

For coherency with update of cryptographic algorithm blue book, it is needed to upgrade key length to 256 bits in baseline mode of EP for AES.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1018/04 | D. Fischer | Change key length to 256 bit for AES in baseline mode of EP. |  Jan2019 |

**Conclusion of the EP red-1 agency Review:**

All the RIDs have been dispositioned. No significant technical changes have been introduced as a result of RIDs disposition. The vast majority of RIDs were editorial and improved the quality of the document. As a result, a second agency review is not needed.

All RIDs dispositions will be inserted in EP red book master file by the editor (D. Fischer) by the end of the year. All RIDs dispositions will be sent back to the initiators by the review coordinator (G.Moury).

| **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. |  Jan2019 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1018/06 | G.Moury | Return all RIDs dispositions to initiators for potential feedback. |  Nov2018 |

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

Objective is to have CESG/CMC poll before spring 2019 meeting.

## SDLS Extended Procedures Interoperability testing

ESA/ESOC (David Koisser) and NASA/IVV (John Lucas) have reactivated the EP test bed and will resume and complete interoperability testing of Extended Procedures based on the final draft Blue Book. This last round of interoperability testing will take into account all the modifications to the specification introduced in the last 2 meeting cycles. The test report will be updated (**attachment 6**).

In the test configuration, ESA simulates the Initiator and NASA the Recipent. Code modifications need to be done on both sides.

In terms of planning, interoperability testing could be finished January 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 - Berlin review.docx (**attachment 5**).

Since the USLP BB will be published before the EP BB, it is agreed to add USLP in the list of Space Data Link Protocols compatible with SDLS EP.

| **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. |  Dec2018 |

Figure 2-1 will depict the SDLS EP interfaces.

§2.3.2: scheme 3 for key generation (key derivation) is mentioned in SDLS Core protocol GB but not covered by SDLS EP BB. After discussion it was decided not to add it in EP BB since OTAR already provides the ability for mission to upload new keys. As a consequence, EP GB should explain why this scheme 3 (key derivation) is not included in Extended Procedures.

| **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. |  Mar2019 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1018/09 | C. Biggerstaff | Align terminology to Anti-Replay Sequence Number (ARSN) to replace : ARC, SN, … |  Mar2019 |

§3.2.3.2 : Key deactivation:

| **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. |  Dec2018 |

§3.3.6. : Handling redundancy:

Discussion should be added on: how to address from the ground Nominal String vs Redundant String Security Unit. The 3 routing mechanisms are through: VC, MAP or APID to address unambiguously N or R Security Unit.

It should be made clear that each Security Unit has its own Key DB and SA DB. There is no need to partition SPI and Key ID between the 2 Security Units.

As a consequence, 2 subsections need to be reworded/complemented:

* 3.3.6 Handling Redundancy
* 3.6.2 EP PDU on-board path

| **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. |  Mar2019 |

Section 4.1 needs to be developed to illustrate how EP can be used in Space to Space Links or constellation scenarios for which the role of Initiator and Recipient on a link cannot be assigned in a straightforward manner. AI SDLS0418/05 covers this point.

Annex A needs to be developed to justify the baseline mode of EP and the parameters chosen.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1018/12 | G. Moury | Develop Annex A Baseline mode to justify Baseline Mode settings. |  Mar2019 |

## Security at CLTU level

Presentation made by V.Sank (NASA/GSFC) **in attachment 2**.

Proposal (see slide 2 of presentation) is to encapsulate complete CLTU between Security Header and Trailer (Security Hdr and Trailer being SDLS compliant) with the following rationale:

* Prevent any corrupted CLTU/frame to enter C&DH computer
* Avoid any modification in the C&DH computer which does not have to incorporate any security function.
* Inserting security (encryption) at CLTU level avoid traffic analysis.

This type of solution has been used in various agencies as an interim solution to insert security on TC links without impacting C&DH computer. Nevertheless, this type of solution is not felt by the WG as a viable solution for standardization for the following reasons:

* It would be a competing standard wrt SDLS since it provides the same service although at a different layer. The only plus being traffic analysis protection (partial).
* It compromises compatibility with SLE services (F-CLTU, F-frame, …) since frame headers would not be in clear.
* Decryption and authentication at the recipient would be done before channel decoding therefore preventing any discrimination between channel errors and security attacks.

## AOB

**Next meeting: 8-9 May 2019, NASA/Ames Research Center – Montain View, CA, USA.**