**October 2019 CCSDS**

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

**ESA/ESOC Darmstadium – Darmstadt, Germany**

October 23-24, 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  |
| Joost Oranje | CGI Netherland BV | joost.oranje@cgi.com |
| Dorothea Richter | DLR/GSOC | dorothea.richter@dlr.de  |
| Eric Pitts | NASA | eric.l.pitts@nasa.gov  |
| Charles Sheehe | NASA/GRC | charles.j.sheehe@nasa.gov |
| Bruno Saba | CNES | bruno.saba@cnes.fr |
| Victor Sank | NASA/GSFC | victor.j.sank@nasa.gov |
| Dai Stanton | UKSA | dstanton@keltik.co.uk |
| Paul Thompson | QinetiQ Ltd | pbthompson@quinetiq.com |
| Marcus Wallum | ESA/ESOC | marcus.wallum@esa.int |

# 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:* + CESG/CMC publication poll status
	+ Review of editorial modifications resulting from SEA AD comments
	+ ESA feedback/comments from Sentinel projects
	+ ESA testing activity (SDLS and SDLS-EP)
 |
| 3 – SDLS Extended Procedures Green Book:* Review of contributions (AI SDLS 0418/05, 1018/02, 08, 09, 10, 11, 12, 0519/01, §3.3 May MoM: redundancy handling, ISL scenarios)
* Review of document
 |
| 4 – Other topics* SDLS Core Protocol (355.0-B-1) pink sheets (5-year review update)(AI SDLS0519/06)
* Secure Key Injection through PKI (CNES)
* Missions using SDLS
* Future work
 |

The list of presentations made is the following:

* + - agenda (**attachment1)**
		- ESA Testing SDLS and SDLS-EP.pptx **(attachment 2)**
		- ESA CryptoSat study testing results - CryptoSAT-Test-results.pdf (**attachment 3**)
		- CNES presentation of secured key injection scheme using PKI - CNES SecureKeyInjSchemePKI.pptx **(attachment 4)**

The list of input/output documents is the following:

* Comments on SDLS EP from the Sentinels.msg (**attachment 5**)
* Final draft blue book for SDLS EP - 355x1Bdraft\_final\_RIDs\_implemented\_23102019.doc (**attachment 6**)
* Draft green book for SDLS EP - SDLS EP Green v1 - Darmstadt review.docx (**attachment 7**)
* Pink sheets to SDLS BB to introduce USLP, SDLS EP, extended key size, … - 355x0b1\_pink sheets for USLP insertion 24102019.doc (**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) > [October 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) > MoM

# 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,2016SupersededClosed |

* Action items superseded by event: SDLS Extended Procedures interoperability testing completed.

| **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** |
| --- | --- | --- | --- |
| SDLS0418/05 | 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. |  April2019closed |

* Closed: ARSN definition has been added in §1.6 of SDLS Extended Procedures Blue Book.

**Anti-Replay Sequence Number (ARSN)**: A counter field initialized to zero when a security association is activated between an Initiator and a Recipient, and then incremented for each transfer frame sent using that SA. This is used to provide protection against replay attacks.

| **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** |
| --- | --- | --- | --- |
| SDLS1018/08 | 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, … |  Mar2019closed |

* Closed: terminology in SDLS Extended Procedures BB has been aligned to ARSN.

| **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. |  Dec2018closed |

* Closed: text 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. |  Mar2019closed |

* Closed: text added in §3.3.5 Handling redundancy (for SAs). This text being applicable not only for SAs but being generic for handling redundancy for SDLS and SDLS EP, this section will be moved to a general section on handling redundancy.

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

* Open: partial draft text reviewed at this meeting. Complete draft text to be provided soon after this meeting.

| **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). |  Sept2019open |

| **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. |  31/05/2019closed |

* Closed: same wording for all PDUs.

| **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). |  31/05/2019closed |

* Closed: binary values removed.

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

* Closed: Key inventory procedure specification inserted in BB.

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

* Closed: text updated

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

* Open: USLP introduced in pink sheets but figure 2-6 still needs updating to include COP management and §3.2.2.5 NOTES need to be complemented to indicate clearly that for variable length USLP frames, Sec HDR and trailer do not impact the size of the frame data field (as for TC) contrary to fixed frame USLP frames for which Sec HDR and Trailer reduce the size of the transfer frame data field (as for TM and AOS).

## SDLS Extended Procedures final draft Blue Book

### CESG/CMC publication poll status

The final draft blue book, as resulting from the spring 2019 meeting, was submitted to SLS and SEA Area Directors together with an SDLS WG resolution to publish the Blue Book. We received editorial comments from SEA AD which were analyzed and resolved by a reduced set of the WG members: DF, CB, GM, HW. The resulting document is in **attachment 6.** The resulting editorial modifications were reviewed by the WG at this meeting. A few typos were spotted in the process; correction are recorded in the file in **attachment 6**. This final version coming out of this meeting has been delivered to the CCSDS CTE (Tom Gannett) for checking and starting CESG/CMC poll to approve publication.

### Review of editorial modifications resulting from SEA AD comments

§1.2: “service provider” was replaced by “service initiator” / “service recipient” as a result of PS comments. Service provider is the term used in SDLS Core Protocol. This will need alignment in the upcoming revision of the SDLS Core Protocol.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1019/01 | G. Moury | Replace “service provider” by “service initiator” and/or “service recipient” in revision of SDLS Core Protocol (pink sheets). |  31/11/2019 |

§3.2.2.1 editorial modification introduced in OTAR procedure:

b) remove “MAC”

e) **MAC of the** Protected Set of Upload Session Keys

§3.3.2.5 Create SA: SA parameters lengths are correlated with one another. For example, ARSN length is linked to key size and selected crypto algorithm. This interdependency should be emphasized in SDLS and EP Green Books.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1019/02 | C.Biggerstaff | Stress SA parameters dependency in EP GB. |  31/03/2020 |

§3.3.3.3 Rekey SA: remove “may be implicit” from all relevant SA management directives since the term implicit was ambiguous in the context.

### ESA feedback/comments from Sentinel projects

See : Comments on SDLS EP from the Sentinels.msg (**attachment 5**) reproduced hereafter with WG responses inserted in bold:

1. **Relationship between SAs and Key States**
Indeed, the link or dependency between a key state and its association to a SA is not clear from the standard. More precisely, looking at the procedures specification, I could not answer the following questions:
- does a key needs to have a given state (e.g. activated) before being associated (via the Rekey SA procedure) to a SA?

**Preconditions listed for RekeySA are listed in §3.3.3.3.2: one of the conditions is that the key is in active state. This will be clarified in EP GB by a diagram showing sequence of operations for SA and Key management (so-called swimlane diagram)**

- what happens if a key state is changed (e.g. deactivated) while being associated to a SA?

**Key should not be deactivated while associated to an active SA. This will be clarified in the Green Book (same diagram as above mentioned)**

- in general, what is the use of the key "Activated/Deactivated" states? (one could argue that a key association to a SA is de facto the activation of this key)

**Key activation is required to perform key verification. Therefore, a specific key activation procedure is needed. In an implementation, key activation and rekeySA could be combined. Same for key activation and key verification. This will be indicated in EP GB.**

1. **OTAR double authentication**
I also have a side question on the OTAR procedure: from the standard, the OTAR command PDU always contains a MAC. If transmitted over a communication channel using an 'authentication' SA, a MAC would also be present at transfer frame level. Could you confirm that my understanding is correct? Note that I don't believe this is a problem but since it looks awkward to have a 'double' authentication, I just wanted to make sure...

**Double authentication of OTAR commands is needed, especially in the case when OTAR commands are routed through the OBC back to the security processor. The second authentication guarantees the integrity of the OTAR command during its transmission/routing on-board. Section 3.2.4 of Green Book (OTAR) could include a justification of this double authentication.**

1. **Security Header and Trailer Presence**
The SDLS standard specifies that the presence or absence of e.g. the security header / trailer on a VC or a MAP shall remain constant throughout a mission (please refer to SDLS standard, clauses 4.1.1.1.1 and 4.1.2.1). However, in case a SA is stopped or deleted, it is not clear how to populate the security header and trailer (for example, in case a SA is deleted, what should be the value of the SPI on the corresponding VC or MAP?).

**The fact that when a VC is switched from secure mode (i.e. associated with an active SA) to clear mode (i.e. not associated with an active SA or associated with a clear mode SA), security header and trailer shall remain present in the data field of the transfer frames although they do not contain any meaningful data (i.e. dummy security header and trailer). This fact is not sufficiently emphasized in SDLS Core protocol BB. The following notes could be added:**

**§4.1.2 Security Trailer: reword NOTE 2 as follows: “**This field **is** present and unused where it is envisioned that the service user may switch between using authenticated SA(s) and not using them on a given Virtual Channel (e.g., if a ‘clear mode’ SA is supported). In this scenario, **the field lengths are kept constant, including Security Header, frame data field and Security Trailer** across all supported operational configurations. **The content of the Security Trailer is undefined when a VC is operating in clear mode.**”

**§4.1.1.1 Security Header: insert a NOTE 2 stating:** “**“**The Security Header **is** present and unused where it is envisioned that the service user may switch between using authenticated SA(s) and not using them on a given Virtual Channel (e.g., if a ‘clear mode’ SA is supported). In this scenario, **the field lengths are kept constant, including Security Header, frame data field and Security Trailer,** across all supported operational configurations. **The content of the Security Header is undefined when a VC is operating in clear mode.**”

The SDLS Core protocol and Extended Procedures do not cover clear mode per se. The implementation of clear mode, if a clear mode is required, is mission-specific.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1019/03 | C.Biggerstaff | Include clarifications agreed in point 1 and 2 above in EP GB. |  31/03/2020 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1019/04 | G. Moury | Insert modifications agreed above in §4.1.1.1 and §4.1.2 of SDLS Core Protocol pink sheets. |  31/03/2020 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1019/05 | G. Moury | Deliver SDLS EP final draft BB as modified during this meeting to CCSDS CTE. |  30/10/2019 |

### ESA testing activity (SDLS and SDLS-EP)

See **attachments 2 (presentation) and 3 (detailed results):** ESA/ESOC has developed a testbed to test/evaluate security protocols and techniques and integrate with real infrastructure (SCOS2000, …).

Delays on the spacelink are not simulated. Only disruption in the form of bit errors are simulated.

The testbed enabled to compare different crypto algorithms and different security protocols. SDLS demonstrated a good resilience in the presence of errors and proved more reliable than IPSec and DTLS.

The tesbed will be upgraded to include SDLS EP to validate EP and identify potential key management based threats.

One of the issue raised concerns potential desynchronization in terms of keys and/or SAs between ground (initiator) and satellite (recipient) in case a command or a reply is not received. Error conditions in the protocol operation (e.g. invalid command PDU received) should be reported in the HKTM of the Security Unit. This reporting is necessary to avoid desynchronization but it is not specified in SDLS EP blue book. This aspect should be elaborated in subsection 3.6.1 on “Failure handling” of the Green Book.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1019/06 | C. Biggerstaff | Include discussion on protocol error handling in SDLS EP GB. |  31/03/2020 |

## Extended Procedures Green Book

The reference of the document is: 350.11-G. The green book reviewed at this meeting is: SDLS EP Green v1 - Darmstadt review.docx (**attachment 7**). The following points were discussed:

* §4.1.2: Inter-Satellite Link scenarios:
	+ 2 scenarios have been developed in the green book regarding ISL. Those 2 scenarios (ground as master of masters, ground as master and inter-satellite propagation of configuration data) are not easily covered by SDLS Core protocol and Extended Procedures since SDLS and EP were designed for the “classical and simple” scenario where a Mission Control Center (Initiator) is communicating with a Satellite (Recipient).
	+ It was decided that ISL scenarios will not be developed in GB unless clear considerations can be exposed in the document on how to handle ISL and constellations with SDLS. Only 2 scenarios retained at this stage for the GB :
		- 1 MCC + 1 SAT through TC/TM links
		- 1 MCC + 1 SAT through TC + TM + Payload TM.
* §3.3.5 and 3.6.2: Handling redundancy N/R security unit and routing of EP PDUs on-board:
	+ Two diagrams have been inserted in §3.6.2.1, illustrating the cross-strapping options between the security functions/units and the receiving strings.
	+ §3.3.5 could be merged with 3.6.2 as 3.3.5 (Handling redundancy) is not specific to Security Association management
* Review of Annex A of SDLS EP GB: justification of EP baseline mode
	+ Baseline mode of extended procedures retains 6 SA Management procedures: Start SA, Stop SA, Rekey SA, Expire SA, Set ARSN, Read ARSN. Create SA, Delete SA, Set ARSN Window and SA Status Request are not selected for baseline mode for the following reasons:
		- In most missions, there is no need to create or to delete an SA in flight. All SAs needed for the mission duration are preloaded on-board. Up to 65.536 SAs can be loaded onboard before launch which is largely sufficient to cover the lifetime.
		- The ARSN Window can be selected statically for the mission. Most missions will select a window of maximum size allowing any up counting ARSN. This protects against replay while allowing for any type of gaps in the reception of frames at the recipient.
		- SA Status Request: SA status can in most cases be managed from the ground.
	+ Baseline mode of extended procedures retains 2 Monitoring & Control procedures: Ping, Alarm Flag Reset. The other procedures: Log status, Dump Log, Erase Log and Self-test are not selected for baseline mode for the following reasons:
		- In most missions, an on-board Security Log is not needed. The Frame Security Report (FSR) provides enough observability to record on the ground all security events, provided that FSR is sampled at each received TC frame.
		- Self-test is usually implemented in the Security Unit in a mission specific way for which interoperability is not needed.
* Discussion concerning Key Verification:
	+ Is it acceptable to have the Challenge (clear text) in the command PDU and the Encrypted Challenge (cipher text) in the reply PDU? Does it lead to a vulnerability linked to clear-cipher text attacks?
		- Challenge should be a random pattern to avoid this type of attacks (to be stated in GB)
		- AES-GCM (baseline mode crypto) has no known vulnerability vs clear-cipher text attacks (to be stated in GB)
	+ The MAC in the Key Verification reply PDU is the Challenge MAC and not the Encrypted Challenge MAC (to be modified in Figure D-5)

## Other topics

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

SDLS Core Protocol will be subjected to 5-year review next year (published 2015).

Pink sheets have been produced by Gilles Moury (**Attachment 8**). The following 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 and edition 2 of CCSDS Symmetric Crypto algorithms.
* 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.
* Text should be added in §2.1 or 2.2.1 to introduce the function of the Extended Procedures

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1019/07 | G. Moury | Add text in §2.1 or 2.2.1 to introduce the functions of the Extended Procedures. |  31/03/2020 |
| A.I. | Actionee | Action | Deadline |
| SDLS1019/08 | C.Biggerstaff | Provide modified Figure 2-6 showing additional input of COP Management service for USLP. |  31/03/2020 |

* Those SDLS Core Protocol pink sheets will require interoperability testing due to the addition of USLP as a possible Space Data Link Protocol supported. UKSA has a USLP simulator implementing SDLS which could be used as one of the prototype for the interoperability testing.

### Key injection using PKI

Presentation done by CNES of the results of an R&D study performed with Thales Alenia Space (see **attachment 4**) on secure key injection using Public Key Infrastructure. The use of PKI allows encrypted key injection in the satellite (either through a dedicated port or through TC link) without the need for an initial secret in the Security Processor. Only a non-confidential PKI certificate is needed on-board. This certificate can be uploaded in the satellite at any time before launch. PKI protocol is used to establish a common secret between Security Processor and key injector (either physical or remote through TC).

This technique allows the uploading of encrypted keys to constellations of spacecraft even if security has not been implemented at launch.

The scheme of Secure Key Injection through PKI could be described in the Key Management Green Book.

## AOB

**Interim telecon: to be scheduled end of January with the objective:**

* **To review progress on SDLS EP Green Book**

**Next meeting: 7-8 May 2019, NASA Huntsville, Alabama – USA.**