**Fall 2015 CCSDS**

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

**Darmstadium – Darmstadt, Germany**

November 11-12, 2015

# Attendance:

|  |  |  |
| --- | --- | --- |
| 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  |
| Jian Chen | CNSA | chenjiach@gmail.com  |
| Matthew Cosby | UKSA/QinetiQ | mcosby@qinetiq.com  |
| Daniel Fischer | ESA/ESOC | daniel.fischer@esa.int  |
| Edward Greenberg | NASA/JPL | egreenberg@jpl.nasa.gov  |
| Greg Kazz | NASA/JPL | Greg.j.kazz@jpl.nasa.gov  |
| David Koisser | ESA | David.koisser@esa.int  |
| Dorothea Richter | DLR/GSOC | dorothea.richter@dlr.de  |
| Marco Rovatti | ESA | Marco.rovatti@esa.int  |
| Bruno Saba | CNES | Bruno.saba@cnes.fr  |
| Charles Sheehe | NASA/GRC | charles.j.Sheehe@nasa.gov  |
| Stefan Veit | DLR | Stefan.veit@dlr.de  |
| Aydar Vildanov | FSA/JSC | vildanov@iss-reshtnev.ru  |

# Agenda :

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

|  |
| --- |
| **Agenda Item** |
| 1 – Action items review |
| 2 – SDLS Protocol green book :* Review of contributions (AI 1114/01&06, 1111/07)
* Completing missing sections
	+ Objective : publication post fall 2015 meeting
 |
| 3 – SDLS Protocol extension (extended procedures) :* Review of inputs (action items 1114/08, 1114/09, 0315/04, 0315/05, 0315/06, 0315/07)
* Finalization of White Book v1
	+ Main text (generic specification)
	+ Annex E : “Baseline mode” annexenabling bit-level interoperability
* Demonstration of extended procedures prototype (ESA)
* Joint session with CSTS and SLP WGs to discuss SDLS managed parameters for cross-support services
 |
| 4 – SDLS Protocol extension (extended procedures) (cont’d) :* + Finalization of white book v1 (cont’d)
	+ Interoperability testing (action item 0315/01)
 |
| 5 – Action items and meeting wrap-up |

The list of presentations made is the following:

* + - W.Hell presentation: Space Data Link Security Protocol FR parameters (**attachment 2)**

The list of input documents is the following:

* CCSDS cloud testing summary – Brandon Bailey (**attachment 3**)
* SDLS Extended Proceduresv05.doc (**attachment 4**)
* SDLS Green Book 12 Nov 2015.doc (**attachment 5**)

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) > [November 2015 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** |
| --- | --- | --- | --- |
| SDLS1111/07(supersedes SDLS0511/12) | I.Aguilar, C.Biggerstaff, G.Moury, B.Saba | Provide missing subsections of the green book taking into account miscellaneous points listed in section 6. |  oct 2013open |

Open: on-going - see point 2 of the agenda : SDLS green book

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1114/01 | I.Aguilar | Emphasize in Green Book the fact that BC frames are not protected and therefore do not carry Security Header nor Trailer. |  April 30,2015closed |

Closed: BC frames not protected already specified in §5.2 of Blue Book. Precision added in §2.3.3.3 Excluded services – to clarify the fact that BC frames (COP management directives) are not protected. Table 2 Summary of services – makes clear that COP management service is not protected. §3.1.1.4 Residual Risks – discuss in detail the justification for not protecting BC frames.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1114/06 | I.Aguilar | Add short summary text in annex D of GB for SDLS potential interaction with TM performances. |  March 30,2015open |

Open: §2.3.6 Decoupling of SDL and SDLS data integrity performance – last paragraph indicates that undetected error rate depends on channel code used, pointing to Annex D for further details. At the moment Annex D deals only with TC SDLP with SDLS. A section on interaction with TM/AOS needs to be added to discuss the undetected error rates for the various TM channel codes with and without transfer frame CRC. ESA study results available on R-S undetected error performances – to be inserted in that section.

The requirements/recommendations for transfer frame CRC usage are the following according to channel code used:

* LDPC : optional
* R-S : optional but recommended for E=8
* Convolutional Code : compulsory unless concatenated with R-S (E=16) code
* Turbo Codes : mandatory.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1114/08 | B.Saba | Provide specification for Monitoring & Control services (services, directives, procedures, SCD/SMD definition) – text for §3.4 and 5.6 |  March 30,2015closed |

Closed: text provided for section 3.4 and 5.6- monitoring & control directives and corresponding PDUs – see point 3 of the agenda and attachment 4.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1114/09 | D.Fischer | Introduce the TLV format as agreed at this meeting for the SCD/SMD format (extended procedures PDU spec) |  March 30,2015closed |

Closed: TLV format specified in section 5.3.1.1 of extended procedures book – see point 3 of the agenda

## SDLS protocol green book

SDLS green book was reviewed during the meeting. The resulting version is in **attachment 5**.

Section 2.3.5.2 : text has been added to warn users against encryption only mode: text similar to annex B- §1.3 was inserted.

Section 3.1: security service selection – justification for the non protection of OID (Only Idle Data) frames and corresponding VCs. A requirement in TM Space Data Link Protocol (6.4.6.2) clearly stipulates that VCs carrying OID frames should not be SDLS protected. A similar requirement is missing for AOS (section 6.4.4 or 6.4.5) where VC #63 (“all ones”) is reserved for OID frames and should not be SDLS protected.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1115/01 | G. Moury | Propose Technical Corrigendum to AOS SDLP (732.0) to add requirement for non protection of OID VC (i.e. VC63) |  15 March,2016 |

Section 3.3 – figure 1: for better understanding, it would be preferable to align the separation line between channel coding and data link sublayers for CCSDS and SDLS.

Section 3.5.6 – Telecommand : text was added to make explicit that in TC there is a limitation of one VC max per SA to remain compatible with COP which operates before SDLS at the receiving end and is operating VC per VC.

SDLS Green book needs to be completed before it can be submitted to CESG/CMC for publication. Intermediate telecon should enable progress.

## Joint session with CSTS and SLP WGs to discuss managed parameters for cross support services

CSTS WG is working on so-called Functional Resources (FR) parameters for each CCSDS protocol/function. They have analysed SDLS managed parameters list and came up with a list of parameters with dependencies. This list is in **attachment 2.** This should be cross-checked by SDLS WG.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1115/02 | SDLS WG | Cross-check list of SDLS parameters dependencies and report to CSTS WG (W.Hell – ESA) |  15 March,2016 |

There is no interest for introducing SDLS in FSP (Forward Space Packet) SLE service since FSP does not correspond to SDLS use case where SDLS is only used end-to-end between the Satellite Control Center (SCC) and the satellite. Forward Space Packet SLE service would require implementing SDLS in the ground station which is not envisioned for security reasons.

## SDLS Protocol Extension (extended procedures)

### Review of inputs and document (V05)

The document (SDLS extended procedures) that was reviewed during the meeting is version 05 (**attachment 4**).

The various sections discussed were the following:

**§5.3.1.1 - Tag, Length, Value (TLV):**

* The need for “nested” TLV is not clear but possibility should be left open in the recommendation for a user to create its own nested TLV if needed for project specific directives/reports
* Baseline mode will use only simple non-nested TLV for directives/reports

**§5.3.2.1.2 – Extended procedures PDU**

* Tag length can be limited to 8-bit. Partitioning of this tag can be introduced:
	+ MSB to identify Command/Reply
	+ Specific prefix for each of the 3 services
	+ Specific partitions for :
		- CCSDS defined
		- CCSDS reserved
		- User defined
* Table 5-1 (recap of all tags) should be transferred in section 2 (non normative). Controlling specification for tags will be in section 5.4/5.5/5.6
* Length field should be kept at 16-bit

**§4.2.1 – Transfer of EP services PDU over the spacelink**

* It is left open in the core text (normative part) of the recommendation provided that the transfer service used is protectable by SDLS. SDLS protecting only TC, TM or AOS transfer frames, transfer service used should use TC, TM or AOS as data link layer. Space packet is one of those transfer services and could be selected for baseline mode.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1115/03 | M.Cosby/G.Moury | Propose a generic bi-directional service for transmitting EP PDUs (commands/reports) |  15 March,2016 |

**§4.2.2 – Frame Security Report (FSR)**

* Baseline mode shall integrate FSR
* Transmission of FSR:
	+ Proposal to make it optional to use or not the OCF to transmit FSR
	+ Change “shall” in “should” in 4.2.2.1.2 to make optional (recommendation but not a requirement) the use of OCF to transmit FSR. Space packet could also be used if regular access to the link can be guaranteed.

**§4.3.1 –** **usage of SA for securing transfer of EP services PDU over the spacelink**

* SPI “all 0’s” and “all 1’s” are reserved in SDLS core protocol. Those 2 SA’s could be active permanently and used to transmit EP Monitoring & Command PDUs.
* For the baseline mode of the EP, those 2 reserved SPI’s could be our master SAs using master key, active before launch, used for loading, configuring and activating all other SAs.
* SA used to configure a given SA has to be different from that SA.
* Interoperability tests of EP should not be limited to baseline mode.

**Annex E – Baseline mode:**

* Key management :
	+ Will include:
	+ OTAR
	+ Key activation
	+ Key deactivation
	+ Key verification
	+ Key destruction is not needed since key deactivation is not reversible.
	+ Master SA/key can be deactivated
	+ Master key/SA can be used to deactivate themselves but only themselves.
* SA management:
	+ Activate SA
	+ Deactivate SA
	+ Load SA (strictly for key loading) and Modify SA (strictly for key modification) to be collapsed in one directive : rekey SA
	+ Set AR counter
	+ Set AR window
	+ SA status request (summary of the current status of an SA is to be specified in normative part of the EP blue book)
* Management & Control:
	+ Ping
	+ No directive related to security logs because security log is not necessarily implemented in simple configurations/missions
	+ Self-test implementation is mission specific and not retained for baseline mode.
	+ Read sequence number
	+ Reset alarm flag (“alarm flg” to be renamed “security event flag”)
	+ FSR implemented in baseline mode

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1115/04 | I.Aguilar/ D.Fischer | Investigate usual practices in terms of Security Logs  |  15 March,2016 |

**§ E2.1.1 – algorithm for OTAR:**

* End to end integrity check of the uploaded keys is needed and provided by authentication of the key. Key separate authentication is necessary.
* Add E2.1.1c) IV (needed to decrypt the key)
* Requirement should point to NIST GCM and GMAC standards (SP-800-38D)

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1115/05 | I.Aguilar | Analyse truncation necessary/possible for the MAC used for key integrity check.  |  15 March,2016 |

**§E2.2.1 – OTAR:**

* 128 Master Keys are enough
* 1 key = 128-bit key + 128-bit MAC + 96-bit IV = 44 octets
* All EP PDUs should fit into one single TC frame (to avoid segmentation)

**§E2.2.6 – Key DB status request**

* Not needed

**§E4.1.2, 4.1.3, 4.1.4** : to be removed 🡺 security log not recommended for simple missions. Only classified missions will typically require security logs.

**§E4.1.5** : self-test to be removed

**§E4.1.6: read sequence number**

* 32-bit in TC
* 96-bit in TM/AOS

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1115/06 | D.Fischer | Update Extended Procedures white book taking into account all modifications/inputs agreed during the meeting  |  15 Jan,2016 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1115/07 | C.Biggerstaff | Provide missing section on SA management for EP white book  |  15 Jan,2016 |

Objective : final white book by next meeting (April 2016). Intermediate telecom will be organized to make progress.

### Interoperability testing

Presentation of cloud based interoperability testing was made by Brandon Bailey (see paper in **attachment 3**):

* One single cloud provider is the preferred configuration (Cloud Sigma)
* In case it is not possible for the various agencies involved to converge on a single provider, different servers/providers can be used
* Only binaries would be uploaded on servers
* Each virtual machine is owned by an agency with the appropriate privacy/confidentiality/security clauses
* Cost : roughly 500$ for 6 months

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1115/08 | G.Moury | Formulate request to CMC for possible funding of this cloud service for SDLS EP interoperability testing  |  15 Jan,2016 |

SDLS EP prototyping plan :

* ESA : full closed loop TC/TM implementation
* NASA : full closed loop TC/TM implementation
* CNES : full closed loop TC/TM implementation

### ESA/ESOC SDLS prototype demonstration

ESA/ESOC has developed a closed loop simulator for SDLS that is being upgraded to include Extended Procedures. This simulator is based on 3 Virtual Machines each implementing part of the space link:

* VM1 : emulates Spacecraft Control Center and is based on SCOS2000
* VM2 : TMTCS emulates ground station. Communications between SCC and G/S is based on SLE
* VM3: SIMSAT/GSTVI emulates spacecraft

An error injection module enables to inject both transmission and security errors.

The operation of the 3 VMs in closed loop was demonstrated successfully.

## Overall Planning

The target planning (which will be put on the CWE framework for the SDLS project) is:

SDLS core protocol:

* Green book publication: June 2016

 SDLS extended procedures:

* White book V1 completed : February 2016
* Red book 1 (including baseline configuration): June 2016

## AOB

Two possible communication opportunities need to be investigated:

* A paper to be submitted at AIAA Space in September 2016
* A long paper in an IEEE journal

# List of decisions and action items agreed at this meeting

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1115/01 | G. Moury | Propose Technical Corrigendum to AOS SDLP (732.0) to add requirement for non protection of OID VC (i.e. VC63) |  15 March,2016 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1115/02 | SDLS WG | Cross-check list of SDLS parameters dependencies and report to CSTS WG (W.Hell – ESA) |  15 March,2016 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1115/03 | M.Cosby/G.Moury | Propose a generic bi-directional service for transmitting EP PDUs (commands/reports) |  15 March,2016 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1115/04 | I.Aguilar/ D.Fischer | Investigate usual practices in terms of Security Logs  |  15 March,2016 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1115/05 | I.Aguilar | Analyse truncation necessary/possible for the MAC used for key integrity check.  |  15 March,2016 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1115/06 | D.Fischer | Update Extended Procedures white book taking into account all modifications/inputs agreed during the meeting  |  15 Jan,2016 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1115/07 | C.Biggerstaff | Provide missing section on SA management for EP white book  |  15 Jan,2016 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1115/08 | G.Moury | Formulate request to CMC for possible funding of this cloud service for SDLS EP interoperability testing  |  15 Jan,2016 |