**April 2016 CCSDS**

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

**Hotel Westin – Cleveland, USA**

April 6-7, 2016

# Attendance:

|  |  |  |
| --- | --- | --- |
| Name | Organization | Email Address |
| Gilles Moury (Co-Chair) | CNES | [gilles.moury@cnes.fr](mailto:gilles.moury@cnes.fr) |
| Howard Weiss (Co-Chair) | NASA/SPARTA | [howard.weiss@parsons.com](mailto:howard.weiss@parsons.com) |
| Ignacio Aguilar-Sanchez | ESA/ESTEC | [ignacio.aguilar.sanchez@esa.int](mailto:ignacio.aguilar.sanchez@esa.int) |
| Brandon Bailey | NASA/GSFC | [brandon.t.bailey@nasa.gov](mailto:brandon.t.bailey@nasa.gov) |
| Craig Biggerstaff | NASA/JSC | [Craig.biggerstaff@nasa.gov](mailto:Craig.biggerstaff@nasa.gov) |
| Matthew Cosby | UKSA/QinetiQ | [mcosby@qinetiq.com](mailto:mcosby@qinetiq.com) |
| Daniel Fischer | ESA/ESOC | [daniel.fischer@esa.int](mailto:daniel.fischer@esa.int) |
| Edward Greenberg | NASA/JPL | [egreenberg@jpl.nasa.gov](mailto:egreenberg@jpl.nasa.gov) |
| Greg Kazz | NASA/JPL | [Greg.j.kazz@jpl.nasa.gov](mailto:Greg.j.kazz@jpl.nasa.gov) |
| Irina Kalininskaya | FSA | [I.kalininskaya@mail.ru](mailto:I.kalininskaya@mail.ru) |
| Dorothea Richter | DLR/GSOC | [dorothea.richter@dlr.de](mailto:dorothea.richter@dlr.de) |
| Marco Rovatti | ESA | [Marco.rovatti@esa.int](mailto:Marco.rovatti@esa.int) |
| Bruno Saba (by webex/telecon) | CNES | [Bruno.saba@cnes.fr](mailto:Bruno.saba@cnes.fr) |
| Charles Sheehe | NASA/GRC | [charles.j.Sheehe@nasa.gov](mailto:charles.j.Sheehe@nasa.gov) |
| Tomaso De Cola | DLR | [tomaso.decola@dlr.de](mailto:tomaso.decola@dlr.de) |
| Aydar Vildanov | FSA/JSC | [vildanov@iss-reshtnev.ru](mailto:vildanov@iss-reshtnev.ru) |
| Gian-Paolo Calzolari | ESA | [Gian-Paolo.Calzolari@esa.int](mailto:Gian-Paolo.Calzolari@esa.int) |

# Agenda :

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

|  |
| --- |
| **Agenda Item** |
| 1 – Action items review |
| 2 – SDLS Protocol green book :   * + Review of inputs (action items SDLS1114/06, 1111/07)   + Final review of document |
| 3 – SDLS / SLP joint session:   * Extended Procedures PDUs transmission over the spacelink * Need to further specify non protection of OID VCs |
| 4 – SDLS Protocol extension (extended procedures) :   * Review of inputs (action items 1115/03, 1115/04, 1115/05, 1115/06, 1115/07) * Finalization of White/Red Book v1   + Main text (generic specification)   + Annex E : “Baseline mode” annexenabling bit-level interoperability * Prototyping   + Status report on on-going and planned prototypes * Interoperability testing   + Objectives   + Test coverage   + Test plan |
| 5 – Dissemination : IEEE paper, journal paper |
| 6 – Action items and meeting wrap-up |

The list of presentations made is the following:

* + - Cloud testing pilot response to CESG (ESA/NASA) (**attachment 2)**
    - SDLS EP interoperability testing v2 (CNES) **(attachment 3)**
    - SDLS EP – Status of prototype and testing v2 (ESA/NASA) **(attachment 4)**
    - Transmission of EP PDUs over the spacelink (CNES) (**attachment 5**)
    - SDLS wrt OID frames and VCs (CNES) (**attachment 6**)

The list of input documents is the following:

* Update to Cloud testing (NASA/ESA) (**attachment 7**)
* SDLS Extended Proceduresv07.doc (**attachment 8**)
* SDLS Extended Proceduresv07\_CTB.doc (**attachment 9**)
* SDLS Extended Proceduresv07\_BS.doc (**attachment 10**)
* Green Book Template SDLS\_07\_Apr\_2016\_working copy\_converted\_format.doc (**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) > [Spring 2016 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 2013  open |

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

| **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,  2015  open |

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** |
| --- | --- | --- | --- |
| 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  closed |

Proposal has been made for Technical Corrigendum to AOS and TM. Several other proposals have been received. Gilles Moury has presented possible solutions at Cleveland meeting during a joint session with SLP WG. See point 3 of the agenda (Need to further specify non protection of OID VCs).

| **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  open |

Refer to slides 5 and 6 of W.Hell presentation on SDLS parameter dependencies for Functional Resources (FR):

* Authorized algorithm, key size and MAC size for cryptographic algorithms are defined in the BB for cryptographic algorithms (352.0-B-1)
* Each algorithm should be associated with a set of key lengths and **MAC lengths.**
* The list of authorized algorithms together with the allowed associated key length and MAC lengths are specified in :
  + Authentication algorithm : §4 of 352.0-B
  + Encryption algorithm : §3.1/3.2/3.3 of 352.0-B
  + Authenticated-encryption : §3.4 (only algorithm: GCM with key and MAC size 128 bits)
* Another SA service type should be added : Authenticated-encryption
* DSS is a family of algorithm, the possible algorithms are : RSA, DSA and ECDSA

G.Moury will prepare a formal response to W.Hell on this subject.

| **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  closed |

Action was closed at this meeting by CNES presentation (attachment 5) presented during the SDLS-SLP joint session (point 3 of the agenda). Decision was taken at this meeting wrt the data link transfer service to be used for Extended Procedures PDUs. See §3.3 of this MoM.

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

Open

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

Closed at this meeting:

* Various possibilities discussed at this meeting for key integrity check (MAC on a block of keys + CRC on each key, …) for the OTAR procedure. See §4 of this MoM.

| **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  closed |

**Closed :** SDLS Extended Proceduresv07.doc edited for this meeting (att8) + inputs from Craig Biggerstaff and Bruno Saba in attachments 9 and 10.

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

Closed : inputs provided in SDLS Extended Proceduresv07 CTB.doc (att9)

| **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  closed |

Closed: request was formulated. CMC was polled but no positive answer received from CMC member wrt CCSDS cloud based interoperability testing funding. See §3.4 interoperability testing of EP.

## SDLS protocol green book

SDLS green book was reviewed during the meeting. The resulting version is in **attachment 11**.

Section 3.2.5 – Authentication bit mask: new text was reviewed and amended. Subsection is now final.

Sections 3.3.2 and 3.3.3 – Protocol position in CCSDS: TM and AOS: text reviewed and approved – Figures 3 and 4 which illustrate the position/interface of the SDLS function within the TM and AOS stacks, are identical to the figures in SDLS BB.

Nota: with USLP (Unified Space Link Protocol – next generation space data link protocol under development by CCSDS), SA can be associated in all cases with one VC only since MAP sub-channeling is available for each VC.

Section 3.4.1.2 – Initialization Vector: missing reference is: RD NIST-SP-800-38D.

Section 3.5.2 – Managed parameters: text from the BB has been adapted for the GB including the table of SDLS managed parameters. In table 4 Managed parameters:

* For IV refer to the specific subsection of the GB dealing with IV §3.4.1.2
* For IV synchronization, refer to §4.3.2
* For sequence number synchronization, refer to §4.3.3

Section 3.5.3 – Signaling, monitoring & control:

* Discussion of in-band signaling vs out-of-band signaling
* In-band signaling : security header and trailer + Frame Security Report (part of data link layer)
* Out-of-band signaling: transmission of EP PDUs (monitoring & control PDUs) using an upper layer transmission service like Space Packet (see discussion in §3.3 of MoM related to EP PDUs transmission over the spacelink).
* This section needs to be revisited once a decision has been taken on the transmission service to be used for EP PDUs over the spacelink (see §3.3).

Section 3.5.7, 3.5.8: Protocol management – Telemetry, AOS

* Add indication that an SA can span over multiple VC (contrary to TC)

Section 4.2 : Generic Operation

* A figure should be added illustrating the receiving side (following the model of figure 2 for the sending side)

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0416/01 | C.Biggerstaff | Develop figure for Generic SDLS Operation – Receiving end | 15 May,  2016 |

Way forward for the Green Book:

* I.Aguilar to update the GB with all the inputs from this meeting + agreed modifications – target date : mid-June 2016
* Telecon/webex to be organized end of June (June, 24 15:00-18:00) to finalize GB and move forward to area resolution to publish.

## Joint session with SLP WG

Two topics to discuss with Space Link Protocol WG:

* Extended Procedures PDUs transmission over the SpaceLink
* Need to further specify non protection of OID frames/VCs

### EP PDUs transmission

CNES presentation (attachment 5) was used to support the discussion.

**Decisions:**

* Make EP PDUs octet aligned 🡺 modifiy reqt 5.3.2.3.1 of extended procedures WB to indicate length in octets for the EP PDU.
* For transfer of the EP PDUs on the uplink (TC or USLP data link protocols), use MAP Packet service with a dedicated MAP for EP PDUs (slide 4-Att5)
* For transfer of EP PDUs on the downlink (TM/AOS data link protocols), use VC Packet service (slide 4-Att5)
* For transfer of Frame Security Report (FSR), use VC\_OCF or MC\_OCF service. In both cases, FSR and CLCW will need to be multiplexed in the OCF (slide 5-Att5)
* Clustering EP PDUs in one single packet is a way of guaranteeing that the related PDUs are transferred and executed together and in order.

### OID frames and VCs non protection

CNES presentation (**attachment 6**) was used to support the discussion.

Objective is to guarantee that OID frames and VCs are not protected/secured by SDLS since those frames are usually completely identical (for example in AOS, there is no requirement to increment the Frame Counter – so OID frames are bit to bit identical). Encrypting/authenticating those OID frames would weaken security by facilitating cryptoanalysis.

**Present state**:

* Requirement 4.2.2.2.3 of SDLS states that: “SAs shall not be created for use with Virtual Channels carrying Only Idle Data (OID) Transfer Frames as defined in references [1] and [3])”
* For AOS, VC63 is reserved for OID frames. All OID frames have to be on VC63. Therefore, for AOS, requirement 4.2.2.2.3 of SDLS prevents any SDLS protection of OID frames.
* For TM, requirement for OID frames (4.1.4.6) is contradictory since it states: “The VCID of an OID Transfer Frame shall be one of the VCIDs used for transferring Packets.” While in the following note, it states: “OID Transfer Frames may be sent on Virtual Channels that also carry valid Packets, but it is preferred that a separate Virtual Channel be dedicated to carry OID Transfer Frames.”. Therefore, there is a possibility in TM that OID frames transmitted on VC carrying also valid packets, are SDLS protected. How to modify specification(s) to avoid this case?

**Conclusions of the discussion**:

* Message to implementers that OID frames should not be SDLS protected will be highlighted in the GB §4.4.2
* Two options have been considered and need to be further evaluated:
  + Option 1:
    - Reverse the final requirement of TM 4.1.4.6 to state: “The VCID of an OID Transfer Frame shall **not** be one of the VCIDs used for transferring Packets.”
    - This would, together with reqt 4.2.2.2.3 of SDLS, prevent any problem
    - Rationale/interpretation of TM4.1.4.6 should be further investigated prior to decide this modification

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0416/02 | G.Kazz / G.Moury | Analyse Rationale/interpretation of reqt TM4.1.4.6 and consequence of proposed modification | 15 May,  2016 |

* Option 2 :
  + Add a requirement in SDLS stating: “OID frames shall not be SDLS protected”. This will cover all cases whether OID frames are carried in an OID VCs or in a regular VC. In practice, it constraints missions to dedicate a VC for OID frames in TM (as in AOS).

## SDLS Protocol Extension (extended procedures)

### Review of inputs and White book (V07)

The document (SDLS extended procedures) that was reviewed during the meeting is version 07 with inputs from C.Biggerstaff (SA management) and B.Saba (Monitoring & Control) (**attachment 8, 9 and 10**).

The various sections/topics discussed were the following:

Key management:

**§5.4.2.1 - OTAR procedure / PDUs:**

* Can we simplify the OTAR PDU by having one MAC/IV per block of uploaded keys + one CRC per key, instead of the present solution with one IV and MAC per key ? This would greatly improve the throughput for key upload session : CRC is 4 octets while IV+MAC is 28 octets.
* This simplification can be acceptable since the transfer of keys is done on SDLS protected uplink (authenticated) and uploaded keys are encrypted and authenticated using AES-GCM.
* This subject of key upload protection scheme will be further discussed within the WG following the meeting to consider all possible alternatives while minimizing on-board complexity and transmission overhead.

**§5.4.2.2 - Key activation procedure / PDUs:**

* Remove number of session keys as managed parameters

**§5.4.2.5 - Key verification procedure / PDUs:**

* A simplified version is proposed. Instead of using a challenge-response scheme, the key verification procedure could simply verify the CRC of the key on-board. This would allow verifying the keys without using them.
* This simpler scheme is adopted.

**§5.4.2.6 - Key DB status request procedure / PDUs:**

* Not clear what this procedure is supposed to return

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0416/03 | D.Fischer | Define reply to Key DB status request | 15 May,  2016 |

A general concern was expressed during the meeting related to the sensitivity of EP commands and replies. Which EP commands and replies need confidentiality? An action is needed to identify those sensitive PDUs.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0416/04 | D.Fischer  C.Biggerstaff  B.Saba | Identify sensitive EP PDUs, i.e. those requiring authenticated encryption when transmitted over the spacelink | 15 May,  2016 |

Once those sensitive PDUs are identified, two approaches can be envisaged for the protection:

* Provide auto-protection for any sensitive EP PDUs
* Mandate authenticated-encryption of the downlink with EP.

Monitoring & Control:

**§5.6 : Monitoring & control (M&C):**

* Do we need a security log for the baseline mode ? consensus of the WG is that there is no need for a security log in the baseline mode.

**§5.6.1.2 - Log status request procedure / PDUs:**

* Would return: remaining space (as percentage) and nb of security events stored
* This reply is sensitive and should be encrypted for transmission over the spacelink

**§5.6.1.3 - Dump log procedure / PDUs:**

* The lengths of “Event message tag” and “event message length” fields are fixed and managed
* This reply is sensitive and should be encrypted for transmission over the spacelink

**§5.6.1.4 - Erase log procedure / PDUs:**

* Align erase log reply with log status reply

**§5.6.1.5 - self-test procedure / PDUs:**

* Reply not sensitive
* Reply = all zeros : OK
* Reply = 1xxxx : NOK (specific error codes are user defined)

**§5.6.1.6 - read sequence number / PDUs:**

* Reply not sensitive
* Possibility to report partly on AR counter (LSB only) – length field enables to signal the portion of the AR counter which is reported
* If SA is encryption only, reply with a length of 0

**§5.6.1.7 - Alarm flag reset procedure / PDUs:**

* No reply sensitive (effect can be seen in FSR)

SA management:

**§5.5.1.1 : Activate SA procedure / PDUs:**

* Enables to activate a given SA on a set of GVC or GMAP
* Need to add a direction flag (uplink / downlink) in the PDU or to have two different PDUs:
  + One for uplink
  + One for downlink
* More general question: should the SA have a direction flag in it ?
* **Decision:** a warning shall be put in the SDLS GB to emphasize the fact that GVCID are not unique in AOS (same GVCID can be used to designate uplink and downlink channels).

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0416/05 | I.Aguilar | Insert warning in SDLS GB on the non-uniqueness of GVCID for AOS | 15 May,  2016 |

* For Extended Procedures, one solution is to partition SPI 🡺 MSB would indicate the direction thus making non ambiguous GVCID.

**§5.5.1.2 : Deactivate SA procedure / PDUs:**

* Only SPI is needed as parameter for the PDU

**§5.5.1.3 : Rekey SA procedure / PDUs:**

* The length of the 2 key IDs need to be specified in the command
* Do we need to load the IV with key ? if yes, IV need to be part of the rekey PDU and also part of the OTAR command

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0416/06 | I.Aguilar | Check the necessity to load the IV with the key | 15 May,  2016 |

**§5.5.1.4: Expire SA procedure / PDUs:**

* Add a recommendation (should) for deactivating the key as well (to avoid using twice the same key with the same ARC or IV)

**§5.5.1.5: Create SA procedure / PDUs:**

* 4 PDUs proposed but can be concatenated in one single PDU
* Limit the authentication bit mask to the useful part (i.e. variable part) : frame header, secondary header, security header

Baseline mode for SA management:

* Activate/deactivate SA
* Rekey SA
* Expire SA
* Set ARC

Sensitivity of SA management PDUs (requiring confidentiality/encryption on the spacelink) :

* Create SA
* Set ARC
* Set ARC window

Protection (authenticated encryption) of sensitive EP PDUs:

* We should identify all the EP PDUs sensitive PDUs
* Two solutions for protecting sensitive PDUs:
  + Add a spec in normative part of EP to require authenticated encryption of sensitive commands/replies if uplink or downlink does not already provide authenticated encryption
  + Specify a generic authenticated encryption function for EP PDUs in EP recommendation.

Error conditions for EP procedures:

* Should we specify the error conditions in the EP spec ? or simply specify a generic discard report ?

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0416/07 | D.Fischer | Specification of error conditions in EP procedures : analyze need for a generic discard report | 15 May,  2016 |

### Interoperability testing

Presentation of cloud based interoperability testing: was made by Daniel Fischer and Brandon Bailey (see presentation in **attachment 4 and 2**):

* The interface between the ESA and NASA prototypes is through SLE-FCLTU and SLE-RCF protocols. This interface has been tested successfully.
* Cloud based testing:
  + The Cloud service provider selected is a swiss one : Cloud Sigma, which is one of the 3 cloud service providers authorized by ESA. NASA has an internal procedure to allow the use of non-US cloud service providers to export code. ESA and NASA purchased separately their own VM. Cost is very limited: approx.. 100$/year
  + Both VM being in the same cloud service , they can share the same WLAN, therefore avoiding any transmission between prototypes over the internet (which in our SDLS case is not so important since our PDUs are secured)
  + A presentation has been prepared by Brandon and Daniel to present the cloud based interoperability testing approach to CESG (presentation-attachment 2 and paper-attachment 7)

Demonstration of connection of the 2 prototypes over the cloud:

* The codes are developed locally at ESA and NASA and then loaded on the VMs for execution and interoperability testing. Cost of VM is therefore very limited.
* Sofar : SLE-FCLTU+SLE-RCF+TM/TC stack has been tested. EP simulators are being developed on both sides
* Demonstration of interconnection of prototypes was demonstrated.
* Security Unit integrating EP is under development at ESA:
  + Close loop testing is already implemented,
  + SA DateBase also
  + Error injection will be implemented as for SDLS Core protocol testing
  + ESA internal testing of the full EP is scheduled for end of June, thus the need for finalizing EP specifications before.

Discussion of objectives, coverage and test plan for interoperability testing:

* A presentation was made by Gilles Moury to support the discussion (see **attachment 3**):
  + Testing of EP over AOS not needed (SDLS Core already tested over AOS – no specificities of EP vs AOS)
  + Interoperability testing will be limited to baseline mode
  + Intraoperability testing internal to ESA will cover all the EP specification with a reasonable set of configurations
  + Synchronization of ground and on-board Key & SA DB will be verified manually during the interoperability testing
  + A third EP prototype will be available from CNES in 2017 but compatibility with cloud based testing need to be verified

| **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,  2016 |

Way forward on interoperability testing:

* Gilles Moury draft the Yellow Book with the test objectives, test coverage and settings
* Daniel Fischer and Brandon Bailey will complete the YB with the detailed test plan and test cases.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0416/09 | G.Moury | Draft interoperability testing Yellow Book | 15 July,  2016 |

## Overall Planning

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

SDLS core protocol:

* Green book publication: October 2016

SDLS extended procedures:

* White book V1 completed : September 2016
* Red book 1 (including baseline configuration) for agency review #1: October 2016

**Two webex/telecon have been scheduled as follows:**

* **26 May, 15:00 CEST: finalization of Extended Procedures White Book**
* **24 June, 15:00 CEST: finalization of SDLS Core protocol Green Book**

## Dissemination

* A paper has been prepared and will be presented by Daniel Fischer at the AIAA Space Forum in September in Long Beach, USA
  + Draft full paper will be circulated for comments. This paper focuses on Extended Procedures.
* Opportunity for a journal paper on SDLS+EP:
  + Potential journal candidate: International Journal of Satellite Communication & Networking
* Other opportunity: ESA TTC workshop

## AOB

SDLS WG has a draft project pending in its charter: Physical Layer Security. Decision should be taken at next meeting wrt activation or cancellation of this draft project.

Ignacio Aguilar and Charles Sheehe have agreed to produce a white paper on this subject for the next meeting to support the discussion on this topic:

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0416/10 | I.Aguilar  C.Sheehe | Draft white paper on opportunity to standardize Physical layer security in the frame of CCSDS | 15 October,  2016 |

# List of decisions and action items agreed at this meeting

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0416/01 | C.Biggerstaff | Develop figure for Generic SDLS Operation – Receiving end | 15 May,  2016 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0416/02 | G.Kazz / G.Moury | Analyse Rationale/interpretation of reqt TM4.1.4.6 and consequence of proposed modification | 15 May,  2016 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0416/03 | D.Fischer | Define reply to Key DB status request | 15 May,  2016 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0416/04 | D.Fischer  C.Biggerstaff  B.Saba | Identify sensitive EP PDUs, i.e. those requiring authenticated encryption when transmitted over the spacelink | 15 May,  2016 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0416/05 | I.Aguilar | Insert warning in SDLS GB on the non uniqueness of GVCID for AOS | 15 May,  2016 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0416/06 | I.Aguilar | Check the necessity to load the IV with the key | 15 May,  2016 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0416/07 | D.Fischer | Specification of error conditions in EP procedures : analyse need for a generic discard report | 15 May,  2016 |

| **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,  2016 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0416/09 | G.Moury | Draft interoperability testing Yellow Book | 15 July,  2016 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0416/10 | I.Aguilar  C.Sheehe | Draft white paper on opportunity to standardize Physical layer security in the frame of CCSDS | 15 October,  2016 |