**CCSDS Space Data Link Security WG Webconf Minutes**

January 20, 2017

# 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) |
| Daniel Fischer | ESA/ESOC | [daniel.fischer@esa.int](mailto:daniel.fischer@esa.int) |
| David Koisser | ESA/ESOC | [david.koisser@esa.int](mailto:david.koisser@esa.int) |
| John Lucas | NASA/GSFC | [john.p.lucas@ivv.nasa.gov](mailto:john.p.lucas@ivv.nasa.gov) |
| Dorothea Richter | DLR/GSOC | [dorothea.richter@dlr.de](mailto:dorothea.richter@dlr.de) |
| Charles Sheehe | NASA/GRC | [charles.j.Sheehe@nasa.gov](mailto:charles.j.Sheehe@nasa.gov) |

# Agenda :

The agenda of the webconf was the following:

SDLS WG intermediate webconf/teleconf – Jan 20, 17:00-19:00 CET

with the following agenda:

* SDLS Green Book finalization for publication
* Extended Procedures red-1 finalization for submission to CCSDS editor
* Extended Procedures interoperability testing status & associated yellow book

The list of presentations made is the following:

* + - ESA presentation on interoperability testing – D.Koisser (**attachment 7)**

The list of input documents is the following:

* Green Book Template SDLS\_21\_Dec\_2016\_Clean\_No\_Trace redline20170120.docx (**attachment 1**)
* Block cipher length bounds on cryptographic key space.pdf (**attachment 2**)
* Mail on UFER of LDPCC and necessity of frame CRC (**attachment 3**)
* NASA/JPL presentation on short LDPCC (slide 10) (**attachment 4**)
* SDLS Extended Procedures Red 1 v2 – CTB.docx (**attachment 5**)
* SDLS extended procedures interoperability test yellow book v2 (**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) > January 2017 teleconference

# Agenda points

## SDLS protocol green book finalization

SDLS green book was reviewed during the meeting. The resulting version (Green Book Template SDLS\_21\_Dec\_2016\_Clean\_No\_Trace redline20170120.docx) is in **attachment 1** and in CWE: Space Link Services Area (SLS) > Documents > SLS-SEA-DLS > CWE Private > SDLS Core Green Book.

A finalized Green Book has been generated by Ignacio Aguilar and circulated to the WG end December.

Two pending action items regarding the GB were discussed and closed:

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1016/01 | I.Aguilar | Check the validity of this assertion : GB section A2.3 – “Thus, the theoretical randomness potential of keys longer than 128 bits cannot be fully exploited” | March,  2017 |

A Technical Note (Block cipher length bounds on cryptographic key space) was produced by ESA (**attachment 2**) showing that this statement is not true. The statement was therefore removed from section A2.3.

The security analysis presented in A2.3 (Design of Crypto graphic algorithms parameters), is derived from an ESA study done in 2010. Therefore the conclusions drawn were valid until 2018 (as stated in the Green Book). More recent ESA study results could be used and potentially published by CCSDS either as yellow book (technical report) or green book (handbook).

Ignacio Aguilar will circulate among the WG the ESA Technical Note on security analysis. WG members are invited to comment. Possible CCSDS publication will be evaluated either in SDLS green book or a separate document.

Annex D :

* D.5, D.6, D.7 : Undetected Frame Error Rate (UFER) needs to be checked for LDPC Codes to verify whether the LDPCC UFER is equivalent to the RS(E=16). In that case, CRC would not be needed.

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1016/02 | G.Moury | Investigate UFER performances of LDPCC (Channel coding WG chair) | March,  2017 |

The following response was given by the Channel Coding WG chairman:

- no undetected error rate results are available for LDPCC, neither by simulation nor analysis (no useful bound could be computed)   
- for the rate 4/5 (1280, 1024) code, JPL was able to observe a few undetected errors, but never enough to be able to compute any statistically meaningful undetected error rate   
- for all the other code rate (1/2 and 2/3) and codeword lengths, no undetected error was ever observed by JPL, to date.

From that response we can probably conclude that the UFER performances of LDPCC is similar to that of RS(E=16), therefore excellent and not requiring any Frame CRC for additional frame validation against transmission errors.

This conclusion is also valid for the short LDPC codes ((128,64),(512,256)) being introduced as TC channel codes (see attached mail – **attachment 3** and NASA/JPL presentation (slide 10) – **attachment 4**)).

In consequence:

* a statement was added in D4 : “**This conclusion is also valid for the newly introduced short LDPC codes in [TC synchronization & Channel Coding] which demonstrate even lower undetected error rates than TC BCH code**”
* a statement was added in D7: “the use of a CRC is recommended whenever SDLS is applied, except when R-S (E=16) **or LDPC codes** are employed as channel coding.”

In conclusion for the SDLS Green Book, 2 AIs decided:

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0117/01 | WG members | Review final version of SDLS Green Book. Analyse ESA technical note on security analysis. | March,  2017 |

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0117/02 | G.Moury | Issue WG and Area resolution for SDLS Green Book publication. | March,  2017 |

## SDLS Protocol Extension (extended procedures)

The red book issue 1 has been produced by Daniel Fischer and completed by Craig Biggerstaff with the last inputs required for SA management procedures specification. The resulting version is:

SDLS Extended Procedures Red 1 v2 – CTB.docx (**attachment 5**) can be found in CWE ([Space Link Services Area (SLS)](http://cwe.ccsds.org/sls) > [Documents](http://cwe.ccsds.org/sls/docs/Forms/AllItems.aspx?SortField=Created&SortDir=Desc&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&SortField=Created&SortDir=Desc&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&SortField=Created&SortDir=Desc&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&SortField=Created&SortDir=Desc&View=%7b16ACDA38%2dFFA3%2d4657%2d8F27%2dB166C23C24A2%7d) > January 2017 teleconference). This version was reviewed during the telecon.

**§3.3 – SA Management Service**

All the service procedures specifications were refined to the same level of details as for the Key management and Monitoring & Control service procedures.

**§4.3 : Interface with SDLS**

Table 4-1 was added to list the status (sensitive, non sensitive) of all procedures.

**§5.3.1 : Protocol Data Units – Overview**

A note is to be added : “all fields are right justified”

Therefore, all statements in §5 and §7 mentioning that a field is right-justified, can be removed.

**§5.5.1 SA Management Procedures**

States and transitions have been numbered in a coherent way so that transition/procedure IDs corresponds to the concatenation of IDs of previous state and present state. Figure 5-9 illustrates this. Therefore, all tags of SA PDUs have been modified to match this convention.

**§6 Managed Parameters**

This chapter was added to capture all managed parameters – most of them are part of the SA data base which needs to be coherent between sending and receiving end. This chapter 6 needs to be completed with managed parameters for Key management and M&C procedures.

**Annex A : PICS**

A PICS was added for SA management, following the model of the SDLS PICS. PICS should be completed for Key Management and Monitoring & Control procedures.

Nevertheless, a complete PICS is not needed for red-1 book review. It will be needed before final review of the document.

With all those inputs, the following action is closed:

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1016/04 | C.Biggerstaff | Provide missing text and figures for §3.3 SA Management | November,  2016  closed |

**Way forward for Extended Procedures red-1:**

* Craig Biggerstaff to make final edits of its input
* Gilles Moury to provide 32-bit CRC for OTAR procedure (protection of encrypted key blocks) to close AI SDLS1016/05
* Daniel Fischer to provide mandatory security section, add a note on EP error handling & signaling and finalize document to close AI SDLS1016/06.

## Extended Procedures Interoperability testing

Interoperability testing on-going between ESA and NASA was reported by David Koisser and John Lucas:

* Intra-operability tests by ESA should cover all procedures
* Inter-operability tests between ESA and NASA will cover only SDLS and Extended Procedures baseline mode

The interoperability testing yellow book (required for blue book approval) has been initialized at the last meeting. The current version (draft) is : SDLS extended procedures interoperability test yellow book v2 (**attachment 6**). Daniel Koisser raised a number of questions regarding the extent of the testing required for Extended Procedures (see attached presentation – **attachment 7**):

* All functions already tested for SDLS Core protocol validation do not need to be retested for extended procedures, e.g.:
  + operation of COP-1not needed because interaction of COP with SDLS was already tested.
  + Injection of transmission errors or security errors on the spacelink needed only to test the correct setting and resetting of the FSR and the corresponding M&C procedures.
* Error cases which are logical errors for Extended Procedures shall be tested to check that procedure do not work if sequence or syntax or integrity check of procedure PDU is incorrect.
* FSR (Frame Security Report) shall only report SDLS Core Protocol errors. Extended Procedures error handling and Signaling is to be done at application layer through functional TM (HKTM). A note in the EP red book should be added about EP error handling & signaling.

Planning :

* FSR should be implemented on NASA side by the end of next week.
* Interoperability tests will proceed
* Test cases from the draft yellow book should be refined in detailed test cases to cover the expected intra and inter-operability test coverage.

## Overall Planning

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

SDLS core protocol:

* Green book publication: April 2017

SDLS extended procedures:

* Red book 1 (including baseline configuration) for agency review #1: April 2017

## Future Work : Physical Layer Security

A paper has been circulated by Howie Weiss on a specific technique for multiple access and physical layer security (SCMA by Hugues) (**attachment 8**).

A joint session between Sec WG, RFM WG and C&S WG should be organized during Spring 2017 meeting in San Antonio to discuss physical layer security concept paper produced before the meeting (AI SDLS1016/03). This joint meeting (1H) could be ideally schedule on Tuesday 9 May afternoon when there is already a joint RFM – C&S joint session scheduled.

## AOB

None