**CCSDS**

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

July 18, 2019

# Attendance:

**SDLS WG telcon:**

|  |  |  |
| --- | --- | --- |
| 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) |
| 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 |
| Joost Oranje | CGI Netherland BV | joost.oranje@cgi.com |
| Dorothea Richter | DLR/GSOC | [dorothea.richter@dlr.de](mailto:dorothea.richter@dlr.de) |

# Agenda :

The agenda of the telcon was the following:

* GVCID/GMAPID issue (see mail in **attachment 1**)
* Minor issues (see mail in **attachment 2**)
* ARSN definition (see mail in **attachment 3**)
* Review of action items from last meeting (see MoM in **attachment 4**)
* Test plan, results, report (yellow book)

The list of input/output documents is the following:

* Mail C.Biggerstaff 17/07/2019 - Re: SDLS EP GVCID Issues (**attachment 1**)
* Mail G.Moury 05/07/2019 - Re: [Sls-sea-dls] SDLS EP Minor Issues (**attachment 2**)
* Mail G.Moury – 04/07/2019 - RE: Information Security Glossary (**attachment 3**)
* SDLS WG MoM - May2019 (**attachment 4**)
* Draft blue book for SDLS EP - 355x1r1\_final\_RIDs\_implemented15062019.docx (**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) > [July 2019 telcon](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

## GVCID/GMAPID issue

See mail thread in **attachment 1**.

Conclusion of the discussion was that:

* No change needed in EP blue book related to GVCID/GMAPID definition/usage
* A note in EP GB could be added to indicate that: when activating an SA over a complete VC, all MAPIDs related to that VC need to be listed in the Start SA command.

It was noted that the SANA registry for TFVN has extended the TFVN to 4-bit for all Space Link Protocols to align with USLP which has a 4-bit TFVN in its frame primary header. The other protocols (TC, TM, AOS, Prox) have a 2-bit TFVN which has been extended to 4-bit by adding 00 as left most bits. To allow TF parsing, TFVN in SANA should rather be:

* 0000 TM/TC
* 0100 AOS
* 1000 Prox-1
* 1100 USLP

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS0719/01 | G.Moury | Contact SANA operator and SLP WG chair to modify TFVN registry | 15 Sept,  2019 |

## Minor issues

See mail thread in **attachment 2.**

* Rekey SA PDU in baseline mode (figure D-8): 2 different PDU formats are shown (one for TC, one for TM, AOS and USLP). Conclusion of the discussion is that:
* The 2 PDU can be merged following the model of set ARSN PDU (D5.6)
* The PDU field to be set as follows:
  + SPI(16-bit)
  + New Key ID (16-bit)
  + New ARSN (96-bit)
* With the following NOTES added (taken from set ARSN PDU spec):
  + NOTE – The ARSN field length needs to be 96 bits. If this affects an ARSN and not an IV, the left-most 64 bits are zeroed.
  + NOTE – Since the ARSN is identical to the IV for the SDLS baseline mode AES-GCM algorithm, executing this procedure will set the IV.
* For all PDUs related to SA management (§5.5 and §D.5), change PDU figures to show both possibilities for the Service Group (‘01’ and ‘10’) which indicates SA “direction”.
* Add SPI in Read ARSN reply PDU (figure 5-22) to make it unambiguous.
* In figure D-10 (set ARSN command PDU), remove “window” from the data field of the PDU.
* Add figures in §D5.7 to show formats of Read ARSN command & reply PDUs.
* Change the MAC length to 128 bits (instead of 32 bits) in the Key Verification Reply PDU of baseline mode (D4.2.3 and D4.3.4).

## ARSN definition

* ARSN definition (see mail thread in **attachment 3**)
* Add the following definition of ARSN in §1.6: “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”

## Action items review

Review of open action items related to EP blue book from previous meeting (May meeting – see MoM in **attachment 4**)

| **A.I.** | **Actionee** | **Action** | **Deadline** |
| --- | --- | --- | --- |
| SDLS1018/01 | H. Weiss | Add : Anti-Replay Sequence Number (ARSN) to the Security Glossary. | April  2019  closed |

ARSN definition to be added in §1.6 (see §3.3)

| **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. | Dec  2018  closed |

* Add a text at the end of §3.2.3.3.1 Overview (Key Deactivation): “The keys are not destroyed (erased) by this procedure **but can only be used to decrypt formerly encrypted data**.”

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

* Done in last version of the EP BB (**attachment 5**)

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

* Done in last version of the EP BB (**attachment 5**)

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

* Done in last version of the EP BB (**attachment 5**)

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

* Done in last version of the EP BB (**attachment 5**)

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

Interoperability testing should be completed for end July.

Objective is to have CESG/CMC poll in summer 2019.

## Extended Procedures Green Book

* Progress on the EP GB will be discussed at an interim telcon to be scheduled mid-September.

## AOB

**Next webconference: to be scheduled end of September with the objective:**

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

**Next meeting: 23-24 October 2019, ESA Darmstadt – Germany.**