**CCSDS Space Data Link Security WG**

**Minutes of Webex telecon**

June 15, 2016

# Participants:

|  |  |  |
| --- | --- | --- |
| Name | Organization | Email Address |
| Gilles Moury (Co-Chair) | CNES/DCT | [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) |
| 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) |
| Dorothea Richter | DLR/GSOC | [dorothea.richter@dlr.de](mailto:dorothea.richter@dlr.de) |
| Bruno Saba | CNES/DCT | [Bruno.saba@cnes.fr](mailto:Bruno.saba@cnes.fr) |

# Agenda :

The agenda of the meeting was the following:

* Review of the action items related to the Extended Procedures white book
* Review of the document (EP white book v10 dated 15-06-2016))
* Status of interoperability testing
* Way forward to next meeting

# Reference documents

RD1 April 2016 CCSDS SDLS WG MoM

RD2 SDLS Extended Procedures white book V10

# Agenda points

## Extended procedures action items and white book review

Review of open action items or open points from previous meeting (see RD1):

* Modify requirement 5.3.2.3.1 to indicate that PDU length is in octets (and not bits). The objective is to have EP PDU octet aligned
* Add in 3.2.3.5.2.3.4 : Verify key status
* Remove 5.4.2.6 : Key DB status request (the status of each key can be verified by the key verification procedure) (AI SDLS0416/03)
* Add a requirement in 4.3.1 to mandate the transmission of “sensitive” EP PDUs over secure channels (i.e. authenticated/encrypted) on the spacelink. A list of sensitive PDUs should be provided in the recommendation (i.e. for each PDU, it should be stated in §5 whether or not it is sensitive). A dedicated one-bit field could be added to EP PDU format to signal whether or not a PDU is sensitive or not. Note: OTAR PDU is the only sensitive EP PDU that is auto-protected.
* A requirement should be added in 4.3.1 to specify that all EP PDUs need to be transmitted over an authenticated channel over the spacelink, i.e. the SA used to transmit EP PDUs should at least be authenticated (and authenticated-encrypted if the EP PDU is sensitive).
* Add in 5.6.1.5.3.2 a partition of the self-test reply :
  + 0xxxxx OK
  + 1xxxxx NOK
  + xxxxx is left to the user to signal any self-test output it might wish to report
* 5.6.1.6 : Read sequence number reply PDU should always carry the full AR counter.
* 5.5.1.1: Start SA : a NOTE should be added to warn the user that GVCID is not unique in AOS when used both directions (since Transfer Frame Version Number (TFVN) is the same in uplink and downlink). In that case, the Start SA directive is ambiguous wrt the VC it is dealing with. The implementation should remove this ambiguity.
* 5.5.1.3: Rekey SA PDU : length of the 2 Key IDs need to be added in text (already in figure).
* AI SDLS0416/06 : Check the necessity to load the IV with the key:
  + Conclusion of the discussion : No need to upload a seed (IV) with a new key.
* 5.5.1.4: Expire SA : add a recommendation to deactivate the key as well.
* 5.5.1.5: Create SA : the format of the authentication bit mask transmitted in the PDU should be specified. It should be limited to : beginning of primary header to end of secondary header.
* 5.5.1.7: Set ARC: this PDU should be removed from the list of sensitive PDUs since ARC can be transmitted in clear on the spacelink.
* AI SDLS0416/07 : do we need to specify error conditions and corresponding error reports ?
  + Error reports should be recorded in the security log (if implemented) but not transmitted real time on the spacelink for security reasons to avoid giving information to the attacker. User should rely on security log to debug any malfunction of the SDLS EP protocol.
* In SA management, the length of the fields in PDUs are explicit but this not the case for key management and M&C. Field lengths need to be transmitted only when creating SA. Later on field lengths need not to be transmitted since both ends of the link know the lengths of the parameters (e.g. keys, key IDs) associated with a given SA.

## SDLS Extended Procedures interoperability testing

ESA EP implementation is now almost complete (only missing part of M&C procedures are not implemented).

NASA implementation status is:

* Key procedures complete
* SA procedures on-going
* M&C procedures to be done

Interoperability testing is on-going between ESA and NASA.

## Way forward to next meeting for EP white book

* Bruno Saba to provide ASAP (end of June) the missing inputs for M&C procedures/PDUs specification
* Craig Biggerstaff, Bruno Saba and Daniel Fischer to implement modifications agreed at this webex telecom.
* Daniel Fischer to provide a final version of the EP white book end of September 2016 to be reviewed at the CCSDS Fall meeting with the objective to validate it and promote it to red book Issue 1 at the fall meeting and move to agency review #1 after the meeting.