Concept for CCSDS-350.x-G – Space Data Link Security Extended Procedures - Summary of Concept and Rationale

# Purpose

The proposed work is to develop a Space Data Link Security Protocol Extended Procedures Green Book containing:
- rationale and justification of the design of the protocol
- user manual of the protocol and concept of operation
This green book is associated to the SDLS Extended Procedures Blue Book (currently in development) and will cover the 3 functions of the Extended Procedures: key management, SA management, Monitoring & control.

Consistency with SDLS WG charter is detailed in Annex 1.

Project organization and planning is detailed in Annex 2.

# Key Technical Features

The outline of the SDLS Extended Procedures Green Book is the following:

# Rationale

## Key Management

Justification

Summary of capabilities

## SA Management

Justification

Summary of capabilities

## Security Unit M&C

Justification

Summary of capabilities

## FSR

Justification

Summary of capabilities

Relation to space link protocols

# Concept of Operation

## Key Management

Refer to the KM Green Book (includes key lifetime, …)

Illustrate key change scenarios (including OTAR, key verification)

Implementing key life cycle with the procedures

Contingency and off nominal scenarios

Master keys versus session keys

## SA Management

Guidelines on planning & assigning SAs

Illustrate normal procedures for SA management: getting SA ready for use, rekeying a SA, ….

Implementing SA life cycle with the EP procedures

Contingency and off nominal scenarios (recovery SA, setARC, modify window, …)

Seamless key change (from frame to frame)

How to handle redundancy (e.g. : reconfiguring redundant command chain using nominal one, logical cross-strapping, …)

## Security Unit M&C

Illustrate nominal procedures for Security Unit M&C

Contingency and off nominal scenarios (using ping, self-test, …)

Rationale, definition and usage of Security Logs

Discussion of self-test (e.g. known answer test (KAT), …)

## FSR

Operating FSR together with Space Link Protocols (alternating CLCW/FSR, …)

How to interpret the flags including the alarm flag (persistant)

Concept of operations for handling alarm flags (e.g.: discriminating transmission problems from security events/attacks, using FSR as a first stage in troubleshooting on the link, …)

## Various types of implementation

Fixed keys, OTAR, dynamic management of SA vs static

EP PDU on-board path/processing (illustrate the different types of on-board architectures, in-band vs out of band signaling, implications of routing EP PDUs in OBC, …)

# Benefits

This SDLS Extended Procedures Green Book will enable mission designers and protocol implementers to:

* Understand the purpose and usage of the SDLS EP procedures
* Select appropriate procedures and parameters for the mission
* Cover nominal and contingency scenarios w.r.t. SDLS EP
* Understand the performances and limitations of the EP procedures

# Requirements of prospective missions

SDLS Extended Procedures are needed to operate the Space Data Link Security core protocol (CCSDS-355.0) over a spacelink in a dynamic manner. They encompass well-known but however complex procedures (like Over The Air Rekeying (OTAR) procedures) which need to be documented by a Green Book detailing the concept of operations and illustrating normal and contingency scenarios. This Green Book is needed to enable mission designers and protocol implementers to make optimal use of the SDLS EP recommendation (CCSDS 355.1).

**ANNEX 1 – Consistency with Charter**

The SDLS WG charter goals include the following bullet:

* Develop a Data Link Security Protocol green book containing: rationale, justification of the design, user manual, mission profiles, discussion of performance, choice of cryptographic algorithm(s), …

This goal has led to 2 projects:

* SDLS Core Protocol Green Book (350.5) currently finalized (awaiting publication)
* SDLS Extended Procedures Green Book (350.x): present project

**ANNEX 2 – Proposed CWE Project**

**Title:** SDLS Extended Procedures Green Book

**Document Number:** 350.x

**Document Type:** Green Book

**Description of Document:** This Green Book is associated to the SDLS Extended Procedures BB (355.1) and provides justification, concept of operations and rationale for the SDLS EP.

**Applicable Patents:** None (TBC)

**Patents Comments:** None (TBC)

**Book Editor (estimated resources + Agency Volunteering):** Total resources: 4 work-months, primarily shared between NASA (2 Work-Month), ESA (1 Work-Month) and CNES (1 Work-Month). Nominal time from other Working Group members (DLR, UKSA) to review the document. Lead editor: NASA.

**Expected Contributing Agencies:** NASA (SA Management), ESA (Key Management), CNES (Monitoring & Control)

Expected Monitoring Agencies: DLR, UKSA

**Schedule**

**July 2017 – December 2019**

**Total time to complete: 31 months**

|  |  |  |
| --- | --- | --- |
| **Schedule Milestones** | **Forecast** | **Comments** |
| Project Approved | 30 June 2017 |  |
| Internal WG Review |
| - First draft circulated to WG | 15 May 2018 | At Spring 18 Meeting |
| - First draft comments due | 31 July 2018 |  |
| - Second draft circulated to WG | 15 October 2018 | At Fall 18 Meeting |
| - Second draft comments due | 31 March 2019 | Before Spring 19 Meeting |
| - Final WB Submitted to AD for further processing | 30 June 2019 | Following Spring 19 Meeting  |
| Secretariat Document Processing | 30 October 2019 |  |
| CMC Approval | 30 December 2019 | Includes CESG Poll + CMC Poll for PUBLICATION |