

|  |
| --- |
| Space Data Link Security (SDLS) extended procedures interoperability Test report |

CCSDS Record

CCSDS 355.1-Y-draft

Yellow Book - July 2016

FOREWORD

Through the process of normal evolution, it is expected that expansion, deletion, or modification of this document may occur. This document is therefore subject to CCSDS document management and change control procedures, which are defined in the *Procedures Manual for the Consultative Committee for Space Data Systems*. Current versions of CCSDS documents are maintained at the CCSDS Web site:

http://www.ccsds.org/

Questions relating to the contents or status of this document should be addressed to the CCSDS Secretariat at the address indicated on page i.

At time of publication, the active Member and Observer Agencies of the CCSDS were:

Member Agencies

* Agenzia Spaziale Italiana (ASI)/Italy.
* British National Space Centre (BNSC)/United Kingdom.
* Canadian Space Agency (CSA)/Canada.
* Centre National d’Etudes Spatiales (CNES)/France.
* China National Space Administration (CNSA)/People’s Republic of China.
* Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)/Germany.
* European Space Agency (ESA)/Europe.
* Federal Space Agency (FSA)/Russian Federation.
* Instituto Nacional de Pesquisas Espaciais (INPE)/Brazil.
* Japan Aerospace Exploration Agency (JAXA)/Japan.
* National Aeronautics and Space Administration (NASA)/USA.

Observer Agencies

* Austrian Space Agency (ASA)/Austria.
* Belgian Federal Science Policy Office (BFSPO)/Belgium.
* Central Research Institute of Machine Building (TsNIIMash)/Russian Federation.
* Centro Tecnico Aeroespacial (CTA)/Brazil.
* Chinese Academy of Sciences (CAS)/China.
* Chinese Academy of Space Technology (CAST)/China.
* Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
* Danish National Space Center (DNSC)/Denmark.
* European Organization for the Exploitation of Meteorological Satellites (EUMETSAT)/Europe.
* European Telecommunications Satellite Organization (EUTELSAT)/Europe.
* Hellenic National Space Committee (HNSC)/Greece.
* Indian Space Research Organization (ISRO)/India.
* Institute of Space Research (IKI)/Russian Federation.
* KFKI Research Institute for Particle & Nuclear Physics (KFKI)/Hungary.
* Korea Aerospace Research Institute (KARI)/Korea.
* MIKOMTEK: CSIR (CSIR)/Republic of South Africa.
* Ministry of Communications (MOC)/Israel.
* National Institute of Information and Communications Technology (NICT)/Japan.
* National Oceanic and Atmospheric Administration (NOAA)/USA.
* National Space Organization (NSPO)/Chinese Taipei.
* Naval Center for Space Technology (NCST)/USA.
* Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
* Swedish Space Corporation (SSC)/Sweden.
* United States Geological Survey (USGS)/USA.

DOCUMENT CONTROL

|  |  |  |  |
| --- | --- | --- | --- |
| **Document** | **Title and Issue** | **Date** | **Status** |
| CCSDS 355.1-Y-draft | CCSDS Space Data Link Security extended procedures interoperability test Report, CCSDS Record | July 2016 | Preliminary draft |
|  |  |  |  |
|  |  |  |  |

CONTENTS

Section Page

[DOCUMENT CONTROL iii](#_Toc458092701)

[CONTENTS iv](#_Toc458092702)

[1 Introduction 1-1](#_Toc458092703)

[1.1 purpose 1-1](#_Toc458092704)

[1.2 Scope 1-1](#_Toc458092705)

[1.3 applicability 1-1](#_Toc458092706)

[1.4 rationale 1-1](#_Toc458092707)

[1.5 document structure 1-1](#_Toc458092708)

[1.6 References 1-2](#_Toc458092709)

[2 Acronyms 2-3](#_Toc458092710)

[3 Overview 3-4](#_Toc458092711)

[4 SDLS Extended Procedures testing OBJECTIVEs 4-6](#_Toc458092712)

[5 test settings 5-8](#_Toc458092713)

[6 Test Cases 6-11](#_Toc458092714)

[6.1 Intra-operability tests 6-11](#_Toc458092715)

[6.1.1 TEST CASE #1 : Key management service & procedures 6-11](#_Toc458092716)

[6.1.2 TEST CASE #2: SA management & procedures 6-12](#_Toc458092717)

[6.1.3 TEST CASE #3: Monitoring & Control procedures 6-13](#_Toc458092718)

[6.2 Inter-operability tests 6-14](#_Toc458092719)

[6.2.1 TEST CASE #4: Key management service & procedures (inter-operability testing – baseline mode) 6-14](#_Toc458092720)

[6.2.2 TEST CASE #5: SA management & procedures (inter-operability testing – baseline mode) 6-15](#_Toc458092721)

[6.2.3 TEST CASE #6: Monitoring & Control procedures (inter-operability testing – baseline mode) 6-16](#_Toc458092722)

[7 CONCLUSION 7-18](#_Toc458092723)

Table Page

# Introduction

## purpose

The purpose of this document is to describe the interoperability tests to be conducted for the validation of the CCSDS Space Data Link Security (SDLS) extended procedures specified in CCSDS 355.1-B-1 (reference [1]). The objective of this interoperability testing is to demonstrate that at least 2 independent implementations of the SDLS extended procedures recommendation interoperate.

## Scope

The scope of this document is to specify the test objectives, test cases and later on test results of interoperability testing of the CCSDS SDLS extended procedures which provides key management, Security Association (SA) management and Monitoring & Control of SDLS protocol for secure TC, TM and AOS data links. The complete interoperability testing of SDLS Core protocol is documented in [3].

## applicability

This interoperability test plan is proposed to validate the interoperability of at least 2 independently developed implementations of the SDLS extended procedures. It can be further used by any user of the recommendation to test its implementation against reference implementations that could be made available later by CCSDS for conformance testing.

## rationale

The CCSDS Procedures Manual states that for a draft Recommendation to become a Blue Book, the standard must be tested in an operational manner. The following requirement for an implementation exercise was excerpted from reference [2]:

“At least two independent and interoperable prototypes or implementations must have been developed and demonstrated in an operationally relevant environment, either real or simulated.”

This document outlines the Space Data Link Security Working Group’s approach to meeting this requirement for the SDLS extended procedures.

## document structure

This document describes the testing that must be accomplished to allow the CCSDS Space Data Link Security (SDLS) extended procedures to proceed forward as a Recommended Standard.

The document is split in 5 parts:

* Overview
* Test objectives
* Test settings
* Test cases
* Conclusion: test results synthesis

## References

The following documents are referenced in this document. At the time of publication, the editions indicated were valid. All documents are subject to revision, and users of this document are encouraged to investigate the possibility of applying the most recent editions of the documents indicated below. The CCSDS Secretariat maintains a register of currently valid CCSDS documents.

1. *CCSDS Space Data Link Security (SDLS) core protocol*. CCSDS 355.0-B-1. Blue Book. Issue 1, September 2015
2. *Organization and processes for the Consultative Committee for Space Data Systems*, CCSDS A02.1-Y-4. Yellow Book. Issue 4. Washington DC: CCSDS, April 2014.
3. *CCSDS SDLS Core Protocol interoperability testing*. CCSDS 355.0-Y-1. Yellow book, March 2015
4. *CCSDS Space Data Link Security (SDLS) extended procedures*. CCSDS 355.1-W-x. CCSDS white book
5. *TC Space Data Link Protocol*. CCSDS 232.0-B-3. Blue Book. Issue 3. Washington DC: CCSDS, September 2015
6. *TM Space Data Link Protocol*. CCSDS 132.0-B-2. Blue Book. Issue 2. Washington DC: CCSDS, September 2015
7. *AOS Space Data Link Protocol*. CCSDS 732.0-B-3. Blue Book. Issue 3. Washington DC: CCSDS, September 2015

# Acronyms

AES-GCM Advanced Encryption Standard – Galois Counter Mode

AR Anti-Replay

CCSDS Consultative Committee for Space Data Systems

CP Core Protocol

EP Extended Procedures

FSR Frame Security Report

IV Initialization Vector

MAC Message Authentication Code

M&C Monitoring & Control

NIS Network Interface System

OCF Operational Control Field

PDU Protocol Data Unit

SA Security Association

S/C Spacecraft

SCC Spacecraft Control Center

SCOS Spacecraft Control and Operations System

SDLS Space Data Link Security (Core Protocol)

SN Sequence Number

SPI Security Parameter Index

TC Telecommand

TM Telemetry

TMTCS Telemetry & Telecommand System

VC Virtual Channel

VM Virtual Machine

# Overview

This CCSDS Space Data Link Security (SDLS) Extended Procedures (EP) test plan describes the manner in which SDLS extended procedures tests have been accomplished. It describes the manner in which the procedures are to be implemented, configured, and data exchanged between the testing parties to determine if the procedures are performing as expected between 2 independent implementations.

The CCSDS Procedures Manual requires that testing be performed in an “operational-like” setting. This plan provides the details to test the SDLS extended procedures specification to ensure its completeness, correctness and interoperation. For the interoperability testing between 2 independent implementations, the following setting is selected:

* an independent SDLS Core Protocol (CP) and Extended Procedures (EP) implementation is used as the Spacecraft Control Center (SCC) end of the bi-directional data link (TC uplink / TM downlink)
* and another independent implementation is used as the Spacecraft (S/C) end of the bi-directional data link.

The SDLS Extended Procedures provide three different services:

* Key Management (KM) service
* Security Association (SA) management service
* SDLS Monitoring & Control (M&C) service

operating over spacelinks secured by SDLS Core protocol and using 3 types of space data link protocols: TC, TM and AOS.

SDLS Core protocol has been successfully tested for interoperability over the 3 types of space data link protocols (TC, TM, AOS) (reference [3]).

Each service is decomposed into a number of Service Procedures:

* Using service parameters
* Decomposed in procedure steps
* Associated to commands/replies PDUs

Service procedures PDUs are transmitted over the bi-directional spacelink (TC/TM or TC/AOS or AOS/AOS) using CCSDS space packet over MAP packet or VC packet service. Real-time reporting from the on-board security processor is available through the transmission in the OCF of the downlink transfer frames of the Frame Security Report (FSR).

For the SDLS Core Protocol and the SDLS Extended Procedures a so-called baseline mode has been defined:

* in annex E of SDLS Core protocol recommendation (reference [1]) for TC, TM and AOS data links
* in annex E of SDLS Extended Procedures recommendation (reference [4]) for Key management, SA management, and Monitoring & Control services

These baseline modes represent the default configurations recommended for the mainstream missions. Therefore, it is proposed to perform the interoperability testing of the SDLS EP using baseline modes setting both for Extended Procedures and the underlying SDLS Core Protocol. It is also proposed to perform this EP interoperability testing over a bi-directional space link composed of a TC uplink and a TM downlink. The other possible configurations for the bi-directional spacelink are: TC uplink / AOS downlink and AOS uplink /AOS downlink. Taking into account that:

* SDLS Core Protocol has been tested ([3]) over the 3 types of space data link : TC, TM, AOS
* Interaction of SDLS EP with space data link protocol is limited to:
	+ transfer of EP PDUs using either MAP Packet (TC) or VC Packet (TM and AOS) services
	+ Transfer of FSR in the OCF of TM or AOS transfer frames

it is proposed to limit the SDLS EP interoperability testing to the most common bi-directional spacelink configuration : TC uplink / TM downlink. This configuration covers the 2 others in terms of transfer services used (MAP Packet, VC Packet, OCF) and possible interaction (TC/COP-1).

One important objective of the testing is to validate that there is no interaction between SDLS (CP / EP) and TC/TM/AOS transmission error control procedures (in particular TC COP-1). Therefore, transmission errors and security (intentional) errors must be injected on the physical link between both ends of the SDLS secured spacelink to check the non-interaction and complementarity of SDLS and data link protocols w.r.t. error handling.

This testing will be performed over the cloud using a single Cloud service provider. The 2 independent implementations (ESA and NASA) will be uploaded on 2 Virtual Machines and communicate via a TCP/IP link. The 2 implementations will exchange SDLS secured transfer frames containing both EP PDUs, FSRs and SDLS CP Security Headers and Trailers.

# SDLS Extended Procedures testing OBJECTIVEs

SDLS extended procedures testing general objectives are the following:

* 1st phase (intra-operability testing: ESA): check completeness, correctness and non-ambiguity of SDLS EP specification for :
	+ the 3 types of services: Key management, SA management, Monitoring & Control
	+ the complete set of service procedures for each of the 3 services
	+ a bi-directional spacelink (TC+COP uplink / TM downlink) secured by SDLS Core Protocol configured in baseline mode (annex E of reference [1])
	+ In an error-free environment.
* 2nd phase (inter-operability testing: ESA/NASA): Check interoperability of at least 2 independent implementations of SDLS EP/CP for:
	+ the 3 types of services: Key management, SA management, Monitoring & Control
	+ the baseline mode of SDLS EP defined in annex E of reference [4]
	+ a bi-directional spacelink (TC+COP uplink / TM downlink) secured by SDLS Core Protocol configured in baseline mode (annex E of reference [1])
	+ The various types of errors that can be encountered on the link: transmission errors, security intentional errors.

More specifically, the detailed test coverage targeted is the following:

* Check all SDLS EP services as defined in the standard
	+ Exercising all the service procedures (for the 1st phase) , and all service procedures included in the baseline mode of SDLS EP (for the 2nd phase)
	+ With a representative subset of values for the service parameters (testing the procedures with all possible set of values for the service parameters is not feasible)
* Check resilience of service procedures to transmission and security errors affecting transmission of EP services PDUs by injecting on the link the same error patterns/configurations as the ones used for the SDLS CP validation.
* Check all SDLS EP defined PDUs (including FSR)
* Check compatibility of SDLS EP with SDLS CP and the spacelink transfer services selected for the transmission of the EP PDUs (MAP Packet, VC Packet)
* Check SDLS EP compatibility with COP-1 procedure over TC space data link
* Validate SDLS EP in a fully representative end to end bi-directional spacelink (TC uplink, TM downlink) configuration:
	+ allowing full separation / independence of ground & satellite end users
	+ allowing to simulate /configure variable transmission errors (single errors / burst errors) and intentional errors

# test settings

The following validation steps are performed in sequence first (first phase – intra-operability validation tests) with a single implementation (ESA) providing both ground segment and flight segment ends, then (second phase – interoperability tests) with 2 independent implementations providing the ground part on one side (ESA) and the on-board part on the other side (NASA).

The general end-to-end test environment is depicted below:



Transfer of TC/TM frames between the ground system simulator and the S/C simulator is done through an SLE interface using the following services:

* SLE-FCLTU: for the TC frames transfer
* SLE-RCF: for the TM frames transfer

**The test settings for the 1st phase** (intra-operability testing within ESA of the complete set of procedures) are depicted hereafter:





For the 1st phase, both ends of the link are implemented by ESA simulators operating on different Virtual Machines.

**The test settings for the 2nd phase** (inter-operability testing between ESA and NASA implementations of the baseline mode set of procedures) are depicted hereafter:



For the 2nd phase, the ground end of the bi-directional TC/TM link is implemented by ESA, while the on-board end is implemented by NASA. The interface between the 2 ends is compliant with SLE specifications (FCLTU forward, RCF return). The 2 ends/simulators are operating on different Virtual Machines hosted by the same Cloud Service Provider (CloudSigma). They communicate through a shared VLAN.

# Test Cases

For each test case, this document provides:

* Test case description & parameters
* Expected results
* Effective results obtained during the intra-operability (1st phase) and inter-operability (2nd phase) testing.

The detailed test configurations, settings and results are captured in the ESA-NASA SDLS EP interoperability test report – see annex A.

## Intra-operability tests

The objectives of the intra-operability tests are to verify completeness, correctness and non-ambiguity of SDLS EP specification for :

* + the 3 types of services: Key management, SA management, Monitoring & Control
	+ the complete set of service procedures for each of the 3 services with a representative set of service parameters
	+ a bi-directional spacelink (TC+COP uplink / TM downlink) secured by SDLS Core Protocol configured in baseline mode (annex E of reference [1]).

### TEST CASE #1 : Key management service & procedures

#### test description

The objective of this test case is to exercise the complete key lifecycle using all the SDLS EP key management procedures and to test the Over The Air Rekeying (OTAR) procedures.

The cryptographic key lifecycle is illustrated hereafter:



Test configuration:

* Bi-directional spacelink: TC uplink with COP-1, TM downlink
* SDLS Core protocol: configured in baseline mode (annex E of [1])
* FSR active (alternating with COP-1 CLCW)
* Error free environment

Test scenario:

* Uploading through OTAR procedures a set of session keys
* Verifying uploaded keys + pre-loaded keys
* Activating/deactivating uploaded keys
* Destroying uploaded keys

#### expected results

Correct operation of the various procedures

#### Intra-operability tests effective results

### TEST CASE #2: SA management & procedures

#### test description

The objective of this test case is to exercise the various states and transitions for the SAs using all the SDLS EP SA management procedures with a representative set of SA management service parameters.

The variable state model for Security Association management is illustrated hereafter:



Test configuration:

* Bi-directional spacelink: TC uplink with COP-1, TM downlink
* SDLS Core protocol: configured in baseline mode (annex E of [1])
* FSR active (alternating with COP-1 CLCW)
* Error free environment

Test scenario:

* Creating SAs
* Keying/Rekeying SAs
* Starting SAs
* Stopping SAs
* Expiring SAs
* Deleting SAs
* Setting Anti-Replay parameters (AR Counter, AR Window) for an SA
* Checking SA status

#### expected results

Correct operation of all the SA management procedures.

#### Intra-operability tests effective results

### TEST CASE #3: Monitoring & Control procedures

#### test description

The objective of this test case is to exercise the various SDLS EP M&C procedures with a representative set of M&C service parameters, checking the coherency of the Frame Security Report carried in the TM frames

Test configuration:

* Bi-directional spacelink: TC uplink with COP-1, TM downlink
* SDLS Core protocol: configured in baseline mode (annex E of [1])
* FSR active (alternating with COP-1 CLCW)
* Intentional (security) errors to be injected to test FSR content and M&C procedures (Log status, dump log, alarm flag reset, …)

Test scenario:

* Inject the various types of security errors (ARC error, MAC error, SPI error) to check FSR content
* Test the various M&C procedures:
	+ Ping
	+ Log status
	+ Dump Log
	+ Erase Log
	+ Self-test
	+ Read SN
	+ Alarm flag Reset (check through FSR)

#### expected results

Correct operation of the M&C procedures.

#### Intra-operability tests effective results

## Inter-operability tests

The objectives of the inter-operability tests are to check interoperability of 2 independent implementations (ESA/NASA) of SDLS EP/CP for:

* + the 3 types of services: Key management, SA management, Monitoring & Control
	+ the baseline mode of SDLS EP defined in annex E of reference [4]
	+ a bi-directional spacelink (TC+COP uplink / TM downlink) secured by SDLS Core Protocol configured in baseline mode (annex E of reference [1])
	+ the various types of errors that can be encountered on the link: transmission errors, security intentional errors.

### TEST CASE #4: Key management service & procedures(inter-operability testing – baseline mode)

#### test description

The objective of this test case is to exercise the key lifecycle using the SDLS EP key management procedures selected for the SDLS EP baseline mode (reference [4] annex E) and to test the Over The Air Rekeying (OTAR) procedures with the key management service parameters and PDU formats specified for the SDLS EP baseline mode (reference [4] annex E).

The cryptographic key lifecycle is illustrated hereafter:



Test configuration:

* Bi-directional spacelink: TC uplink with COP-1, TM downlink
* SDLS Core protocol: configured in baseline mode (annex E of [1])
* SDLS EP: configured in baseline mode (annex E of [4])
* FSR active (alternating with COP-1 CLCW)
* Injection of transmission and security (intentional) errors.

Test scenario:

* Uploading through OTAR procedures a set of session keys
* Verifying uploaded keys + pre-loaded keys
* Activating/deactivating uploaded keys

#### expected results

Correct operation of the various Key management procedures tested or correct detection of security errors/events.

Correct interpretation at both ends of the link of the syntax/content of all the EP Key management PDUs.

#### Intra-operability tests effective results

### TEST CASE #5: SA management & procedures(inter-operability testing – baseline mode)

#### test description

The objective of this test case is to exercise the states and transitions for the SAs using the SDLS EP SA management procedures selected in the SDLS EP baseline mode (annex E of [4]) with the SA management service parameters and PDU formats specified for the SDLS EP baseline mode (reference [4] annex E).

The variable state model for Security Association management is illustrated hereafter (SA create and SA delete procedures are not part of the SDLS EP baseline mode and therefore will not be tested in that test case):



Test configuration:

* Bi-directional spacelink: TC uplink with COP-1, TM downlink
* SDLS Core protocol: configured in baseline mode (annex E of [1])
* SDLS EP: configured in baseline mode (annex E of [4])
* FSR active (alternating with COP-1 CLCW)
* Injection of transmission and security (intentional) errors

Test scenario:

* Keying/Rekeying SAs
* Starting SAs
* Stopping SAs
* Expiring SAs
* Setting Anti-Replay parameters (AR Counter, AR Window) for an SA

#### expected results

Correct operation of the various SA management procedures tested or correct detection of security errors/events.

Correct interpretation at both ends of the link of the syntax/content of all the EP SA management PDUs.

#### Intra-operability tests effective results

### TEST CASE #6: Monitoring & Control procedures(inter-operability testing – baseline mode)

#### test description

The objective of this test case is to verify the interoperability of the SDLS EP M&C procedures selected in the SDLS EP baseline mode (annex E of [4]) with the service parameters and PDU formats specified for the SDLS EP baseline mode (reference [4] annex E).

Test configuration:

* Bi-directional spacelink: TC uplink with COP-1, TM downlink
* SDLS Core protocol: configured in baseline mode (annex E of [1])
* SDLS EP: configured in baseline mode (annex E of [4])
* FSR active (alternating with COP-1 CLCW)
* Intentional (security) errors to be injected to test FSR content and M&C procedures (alarm flag reset)

Test scenario:

* Inject the various types of security errors (ARC error, MAC error, SPI error) to check FSR content
* Test the M&C procedures selected in EP baseline mode:
	+ Ping
	+ Read SN
	+ Alarm flag Reset (check through FSR)

#### expected results

Correct operation of the M&C procedures tested or correct detection of security errors/events.

Correct interpretation at both ends of the link of the syntax/content of the EP M&C PDUs.

#### Intra-operability tests effective results

# CONCLUSION

1. SDLS Extended procedures Validation / test report

Inter-Agency Testing