

|  |
| --- |
| Space Data Link Security (SDLS) protocol Test report |

DRAFT CCSDS Record

CCSDS 355.1-Y-draft

Draft Yellow Book

April 2014

FOREWORD

[Foreword text specific to this document goes here. The text below is boilerplate.]

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 (SDLS) protocol Test Report, Draft CCSDS Record | April 2014 | Current draft |
|  |  |  |  |
|  |  |  |  |

CONTENTS

Section Page

[DOCUMENT CONTROL iii](#_Toc383797298)

[CONTENTS iv](#_Toc383797299)

[1 Introduction 1-1](#_Toc383797300)

[1.1 purpose 1-1](#_Toc383797301)

[1.2 Scope 1-1](#_Toc383797302)

[1.3 applicability 1-1](#_Toc383797303)

[1.4 rationale 1-1](#_Toc383797304)

[1.5 document structure 1-1](#_Toc383797305)

[1.6 References 1-2](#_Toc383797306)

[2 Overview 2-1](#_Toc383797307)

[3 SDLS Protocol testing OBJECTIVEs 3-2](#_Toc383797308)

[4 test CASES 4-4](#_Toc383797309)

[4.1 TEST CASE #1 : SDLS protocol validation over TC link 4-5](#_Toc383797310)

[4.1.1 test description 4-5](#_Toc383797311)

[4.1.2 expected results 4-5](#_Toc383797312)

[4.2 TEST CASE #2 : SDLS protocol / Cop-1 compatibility check 4-6](#_Toc383797313)

[4.2.1 test description 4-6](#_Toc383797314)

[4.2.2 expected results 4-6](#_Toc383797315)

[4.3 TEST CASE #3 : SDLS protocol validation over TM (and/or AOS) link 4-7](#_Toc383797316)

[4.3.1 test description 4-7](#_Toc383797317)

[4.3.2 expected results 4-7](#_Toc383797318)

[4.4 TEST CASE #4 : SDLS Protocol operated concurrently over TC and TM space data links 4-8](#_Toc383797319)

[4.4.1 test description 4-8](#_Toc383797320)

[4.4.2 Expected results 4-9](#_Toc383797321)

[5 Test results 5-10](#_Toc383797322)

Table Page

# Introduction

## purpose

The purpose of this document is to describe the interoperability testing to be conducted for the CCSDS Space Data Link Security (SDLS) protocol specified in CCSDS 355.0-B-1 (reference [1]). The objective of this interoperability testing is to demonstrate that at least 2 independent implementations of the SDLS protocol recommendation interoperate.

## Scope

The scope of this document is to specify the test objectives, test cases and test results of interoperability testing of the CCSDS SDLS protocol which provides authentication, integrity, anti-replay and confidentiality to TC, TM and AOS data links. The complete interoperability testing of CCSDS recommended cryptographic algorithms (e.g. AES in various modes) (reference [3]) which are embedded in SDLS protocol, is covered by the CCSDS Cryptographic algorithms test report (reference [4]).

## applicability

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

## rationale

The CCSDS Procedures Manual states that for a Recommendation to become a Blue Book, the standard must be tested in an operational manner. The following requirement for an implementation exercise were 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.

## document structure

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

The document is split in 3 parts:

* Test objectives
* Test cases
* Test results

## 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) protocol*. CCSDS 355.0-B-1. Blue Book. Issue 1. Washington DC: CCSDS, <date>
2. *Procedures Manual for the Consultative Committee for Space Data Systems*, CCSDS A00.0-Y-9. Yellow Book. Issue 9. Washington DC: CCSDS, November 2003.
3. *CCSDS Cryptographic Algorithms*. CCSDS 352.0-B-1. Blue Book. Issue 1. Washington DC: CCSDS, November 2012
4. *CCSDS Cryptographic Algorithms test report*. CCSDS 352.1-Y-1. Yellow Book. Issue 1. Washington DC: CCSDS, November 2012

# Overview

This CCSDS Space Data Link Security Protocol test plan describes the manner in which SDLS protocol testing will be accomplished. It describes the manner in which the protocol is to be implemented, set (e.g. : keys), and data exchanged between the testing parties to determine if the protocol is performing as expected between 2 independent implementation of the SDLS recommendation.

The CCSDS Procedures Manual requires that testing be performed in an “operational-like” setting. This plan provides the details to test the SDLS protocol specification to ensure its completeness, correctness and interoperation. We propose that an independent SDLS implementation is used as the sending end of the data link and another independent implementation is used as the receiving end. This will be performed using all the recommended modes of operation (so called “baseline modes”) defined in annex E of SDLS recommendation (reference [1]) which covers TC, TM and AOS links.

Since SDLS protocol is fully embedded in TC, TM and AOS data link protocols (references [5], [6], [7]), the SDLS implementations tested will include necessarily at least TC, TM and AOS protocol simulation.

One important objective of the testing is to validate that there is no interaction between SDLS protocol and TC/TM/AOS transmission error control procedures (e.g. TC COP-1). Therefore, transmission errors and security (intentional) errors must be injected on the physical link between the SDLS sending and receiving ends to check the non-interaction and complementarity of SDLS and data link protocols w.r.t. error handling. Also TC link must be operated simultaneously with TM or AOS links so that TC protocol can be looped back to the sending end (CLCW transmission in OCF of TM or AOS transfer frames).

This testing could be performed in a single laboratory by one test bed using multiple implementations of SDLS protocol. However, optimally the testing should be conducted at multiple sites via the internet potentially using something as simple as email to send SDLS secured transfer frames between the testing parties which would then be fed into the various independent algorithm implementations. For example, Test Agent A at site X could apply SDLS to a pre defined set of transfer frames (TC, TM or AOS) using a pre-distributed set of Security Associations (SA). Test Agent A would email the SDLS secured frames as an attachment to Test Agent B at site Y. Using the pre-distributed set of SAs and a different implementation of SDLS protocol than used by Test Agent A, Test Agent B would attempt to validate received transfer frames. If the SDLS protocol receiving end is able to detect and handle correctly all errors (both security and transmission related), the test passes.

In a more elaborate testing setup, the test sites could be interconnected and a simple network application (e.g. UDP/IP) could be used to provide the test framework of generating SDLS secured transfer frames, transmitting it, and on the receiving end, validating the transfer frames.

# SDLS Protocol testing OBJECTIVEs

SDLS protocol testing general objectives are the following:

* check completeness, correctness and non ambiguity of SDLS protocol specification for :
	+ the 3 types of space data links supported by SDLS : TC, TM, AOS
	+ the 3 types of security services that can be provided by SDLS : authentication (authentication, integrity, anti-replay), encryption (confidentiality), authenticated encryption.
	+ the 3 cryptographic algorithms/modes recommended in the baseline implementation modes of SDLS (annex E of reference [1]).
	+ The various types of errors that can be encountered on the link : transmission errors, security intentional errors
* Check interoperability of at least 2 independent implementations of SDLS protocol for all settings listed above
* Check absence of interference between TC/TM/AOS protocols and SDLS protocol, in particular between TC COP and SDLS.

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

* Check all SDLS protocol procedures as defined in the standard
* Check protection (authentication and/or encryption) of all concerned TC, TM and AOS communication services as defined in relevant TC, TM and AOS SDLP recommendations and identified as services protected by SDLS protocol
* Check all parameters as defined in SDLS protocol while covering complete value range (i.e. min / max size for each concerned parameter)
* Check all SDLS functions & security services : SA management, Authentication, Encryption, Authenticated Encryption
* Check for each security service at least one algorithm (i.e. mode of operation & cryptographic primitives) among algorithms recommended by CCSDS (as defined in baseline implementation modes annex E of SDLS protocol recommendation)
* Check all SDLS defined data units
* Validate co-existence of both secure and unsecure (clear) Virtual Channels (TC & TM) / MAP channels (TC only) over a master channel
* Check compatibility of SDLS protocol with relevant TC, TM and AOS space data link protocols as defined by CCSDS
* Check SDLS protocol compatibility with COP-1 procedure over TC space data link
* Validate SDLS protocol when applied on either TC link or applied concurrently on both TC and TM (or AOS) space data link
* Check both nominal cases as non nominal / error cases
* Validate SDLS protocol in a fully representative end to end TC and TM link
	+ allowing full separation / independence of ground & satellite end users
	+ allowing to simulate /configure variable transmission delays and transmission errors (single errors / burst errors)

# test CASES

The following validation steps are performed in sequence first with a single implementation providing both sending and receiving ends, then with 2 independent implementations providing the ground part on one side and the on-board part on the other side:

* SDLS protocol validation over TC link
* SDLS protocol / COP-1 compatibility check
* SDLS protocol validation over TM and/or AOS link
* SDLS protocol operated concurrently over TC and TM (or AOS) links

Transfer of TC/TM (and/or AOS) frames between 2 independent implementations (ground simulator / space simulator) can be done through file exchange or UDP/IP local or remote connection.

## TEST CASE #1 : SDLS protocol validation over TC link

### test description

SDLS protocol over TC link will be validated in the baseline mode for TC - defined in annex E of SDLS recommendation.

Test configuration:

* Security service type : authentication only
* Cryptographic algorithm : AES-CMAC
* Key : 128 bits
* Anti-replay sequence number : 32 bits transmitted integrally in Security Header
* Total Security Header length : 6 octets
* MAC : 128 bits
* Authentication bit mask : default bit mask as defined in SDLS recommendation §4.2.2.6.2
* Anti-replay sequence number window : TBD
* Multiple VC
* Multiple MAP per VC
* Mix of secure (SDLS protected) VC/MAP and unsecure VC/MAP
* Only expedited service (no COP) : BD frames

Test scenario:

* No errors
* Replay
* Anti-replay sequence number mismatch
* MAC error (random errors, forging of frame subfields)
* Invalid SPI
* Key mismatch

### expected results

Correct detection of exceptions and ground-space configuration mismatch.

## TEST CASE #2 : SDLS protocol / Cop-1 compatibility check

### test description

SDLS protocol is in baseline mode for TC (as per annex E : authentication only + AES-CMAC). TC space link protocol over TC master channel implements COP-1. A return channel (TM or AOS) is implemented to carry CLCW and TC-SMR. This TM channel is unsecure.

Test configuration:

* TC security service type : authentication only
* Cryptographic algorithm : AES-CMAC
* Key : 128 bits
* Anti-replay sequence number : 32 bits transmitted integrally in Security Header
* Total Security Header length : 6 octets
* MAC : 128 bits
* Authentication bit mask : default bit mask as defined in SDLS recommendation §4.2.2.6.2
* Anti-replay sequence number window : TBD
* 1 single VC
* 1 single MAP per VC
* Secure VC and MAP
* Mix of AD frames and COP-1 control commands (BC frames) on TC link

Test scenario:

* No errors, no control commands
* Security exceptions/errors:
	+ Replay
	+ Anti-replay sequence number mismatch
	+ MAC error (forging of frame subfields : incorrect MAC but correct FEC)
	+ Invalid SPI
	+ Key mismatch
* Transmission errors (incorrect FEC):
	+ Single bit error
	+ Burst errors (impacting multiple frames)
	+ Errors on AD and BC frames
	+ Timeout
* COP-1 reconfiguration
	+ Set V[R]

### expected results

No interaction between SDLS and COP-1:

* SDLS should detect and handle security errors/exceptions
* COP-1 should detect and handle transmission errors

## TEST CASE #3 : SDLS protocol validation over TM (and/or AOS) link

### test description

SDLS protocol is in baseline mode for TM (as per annex E : authenticated encryption + AES-GCM). TM (and/or AOS) channel includes a mix of secure (SDLS protected) VC and unsecure VC. No forward link necessary.

Test configuration:

* TM/AOS security service type : authenticated encryption
* Cryptographic algorithm : AES-GCM
* Key : 128 bits
* Anti-replay sequence number : not needed in AES-GCM
* Total Security Header length : 14 octets
* MAC : 128 bits
* Authentication bit mask : default bit mask as defined in SDLS recommendation §4.2.2.6.2
* Anti-replay sequence number window : TBD
* Multiple VC
* Mix of secure and unsecure VCs

Test scenario:

* No error
* Security errors:
	+ Replay
	+ Anti-replay sequence number mismatch
	+ MAC error (random errors, forging of frame subfields)
	+ Invalid SPI
	+ Key mismatch
	+ IV mismatch

### expected results

Correct detection of exceptions and ground-space configuration mismatch.

## TEST CASE #4 : SDLS Protocol operated concurrently over TC and TM space data links

### test description

Aim is to validate SDLS when applied concurrently on a TC channel and a TM channel. TC channel implements a single VC with a single MAP operating COP-1. Both are SDLS protected. TM channel implements 2 secure VCs:

* One VC supporting traffic data (packet service) and CLCW
* One carrying TC-SMR

TC and TM channels are configured in their respective baseline mode.

Test configuration:

* TC channel:
* TC security service type : authentication only
* Cryptographic algorithm : AES-CMAC
* Key : 128 bits
* Anti-replay sequence number : 32 bits transmitted integrally in Security Header
* Total Security Header length : 6 octets
* MAC : 128 bits
* Authentication bit mask : default bit mask as defined in SDLS recommendation §4.2.2.6.2
* Anti-replay sequence number window : TBD
* 1 single VC
* 1 single MAP per VC
* Secure VC and MAP
* Mix of AD frames and COP-1 control commands (BC frames) on TC link
* TM channel:
* TM/AOS security service type : authenticated encryption
* Cryptographic algorithm : AES-GCM
* Key : 128 bits
* IV : 96 bits
* Anti-replay sequence number : not needed in AES-GCM
* Total Security Header length : 14 octets
* MAC : 128 bits
* Authentication bit mask : default bit mask as defined in SDLS recommendation §4.2.2.6.2
* Anti-replay sequence number window : TBD
* 2 secure VC: one for carrying traffic data (packet service), one for carrying TC-SMR.

Test scenario:

* No errors, no control commands
* Key changes both in TC and in TM
* Security exceptions/errors on both TC and TM links:
	+ Replay
	+ Anti-replay sequence number mismatch
	+ IV mismatch
	+ MAC error (forging of frame subfields : incorrect MAC but correct FEC)
	+ Invalid SPI
	+ Key mismatch
* Transmission errors (incorrect FEC) on TC link:
	+ Single bit error
	+ Burst errors (impacting multiple frames)
	+ Errors on AD and BC frames
	+ Timeout
* COP-1 reconfiguration
	+ Set V[R]

### Expected results

Correct detection/handling of exceptions/errors and ground-space configuration mismatch.

# Test results

1. [ANNEX TITLE]

[Annexes contain ancillary information. See CCSDS A20.0-Y-2, *CCSDS Publications Manual* (Yellow Book, Issue 2, June 2005) for discussion of the kinds of material contained in annexes.]