The Consultative Committee for Space Data Systems

SPACE DATA LINK SECURITY (SDLS) EXTENDED PROCEDURES INTEROPERABILITY TEST REPORT

CCSDS RECORD

CCSDS 355.1-Y-1

Yellow Book - July 2019

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.

CCSDS RECORD CONCERNING CCSDS SPACE DATA LINK SECURITY EXTENDED PROCEDURES INTEROPERABILITY TEST

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-1	CCSDS Space Data Link Security extended procedures interoperability test Report, CCSDS Record	July 2019	Final version

CONTENTS

1 INTRODUCTION

1.1 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-draft (reference [4]). The objective of this interoperability testing is to demonstrate that at least 2 independent implementations of the SDLS extended procedures recommendation interoperate.

1.2 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, AOS and USLP data links. The complete interoperability testing of SDLS Core protocol [1] is documented in [3].

1.3 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.

1.4 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.

1.5 DOCUMENT STRUCTURE

This document describes the interoperability testing that must be accomplished to allow the CCSDS Space Data Link Security (SDLS) Extended Procedures (EP) 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
- Annex A: detailed test settings and results

1.6 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-B-draft. CCSDS draft blue 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

[1] *Space Packet Protocol*. Issue 1. Recommendation for Space Data System Standards (Blue Book), CCSDS 133.0-B-1. Washington, D.C.: CCSDS, September 2003.

[2] *Unified Space Data Link Protocol (USLP).* Issue 1. Recommendation for Space Data System Standards (Blue Book), CCSDS 732.1-B-1. Washington, D.C.: CCSDS, October 2018.

2 ACRONYMS

AES-GCM	Advanced Encryption Standard – Galois Counter Mode
ARSN	Anti-Replay Sequence Number
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
SDLP	Space Data Link Protocol
SDLS	Space Data Link Security (Core Protocol)
SN	Sequence Number
SPI	Security Parameter Index
SPP	Space Packet Protocol
TC	Telecommand
TM	Telemetry
TMTCS	Telemetry & Telecommand System

USLP	Unified Space Data Link Protocol
VC	Virtual Channel
VM	Virtual Machine

3 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 4 types of Space Data Link Protocols: TC ([5]), TM ([6]), AOS ([7]) and USLP ([9]).

SDLS Core protocol has been successfully tested for interoperability over the 3 types of space data link protocols (TC, TM, AOS) (see 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 (Commands & Replies) are transmitted over the bi-directional spacelink :

- using one of the following SDLP combinations: TC/TM or TC/AOS or TC/USLP or AOS/AOS or USLP/USLP
- using CCSDS space packet over MAP packet service (for TC and USLP) or VC packet service (for TM and AOS).

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), using the OCF Service provided by TM, AOS or USLP Space Data Link Protocols.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 D 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 procedures using SDLS Core Protocol baseline mode.

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 or USLP downlink and AOS or USLP uplink /AOS or USLP downlink. Taking into account that:

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

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 others in terms of transfer services used (MAP Packet (covers TC and USLP), VC Packet (covers TM and AOS), OCF (covers TM, AOS and USLP)) and possible interaction with COP-1 (covers TC and USLP uplink).

One important objective of the testing is to validate that there is no interaction between SDLS (CP / EP) and TC/TM/AOS/USLP transmission error control procedures (in particular 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. Validating the interaction of SDLS CP/EP with COP-1 can be done either with TC or USLP since both protocols have the same interface/behavior wrt COP-1. TC uplink configuration has been used for interoperability testing.

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

4 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 complete set of SDLS EP procedures
    - 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. Testing of error cases limited to verification of correctness of FSR.

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

- Check all SDLS EP services as defined in the standard's baseline
  - Exercising all the service procedures
  - 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 correctness of FSR in presence of transmission and security errors.

- Check all SDLS EP defined PDUs (including FSR)

- Check operation of SDLS EP with SDLS Core Protocol and the spacelink transfer services selected for the transmission of the EP PDUs (MAP Packet, VC Packet)

- Check SDLS EP operation 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 intentional security events.

5 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:

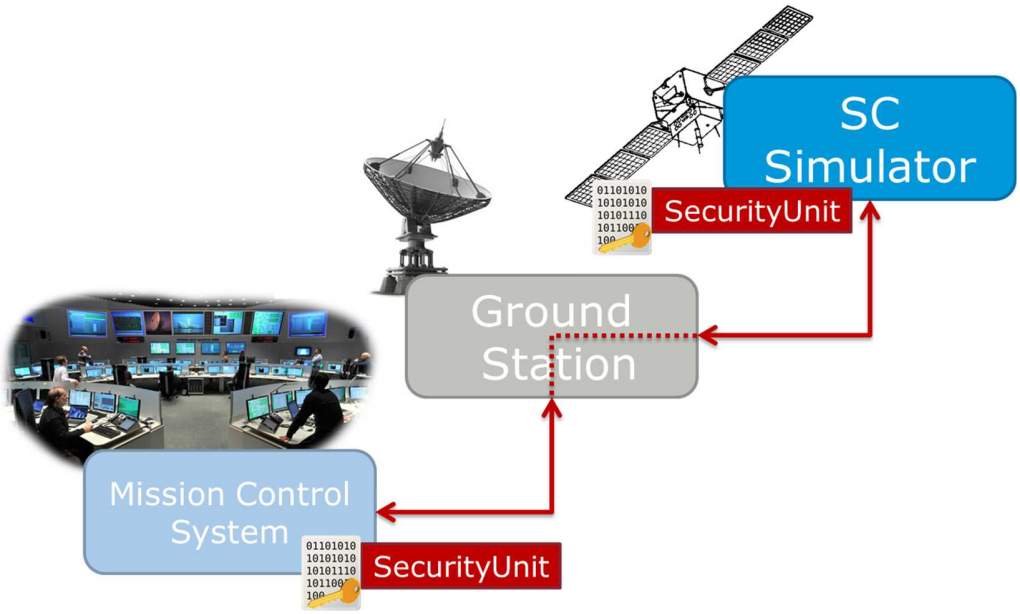


Figure 5-1: General end-to-end test environment

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:

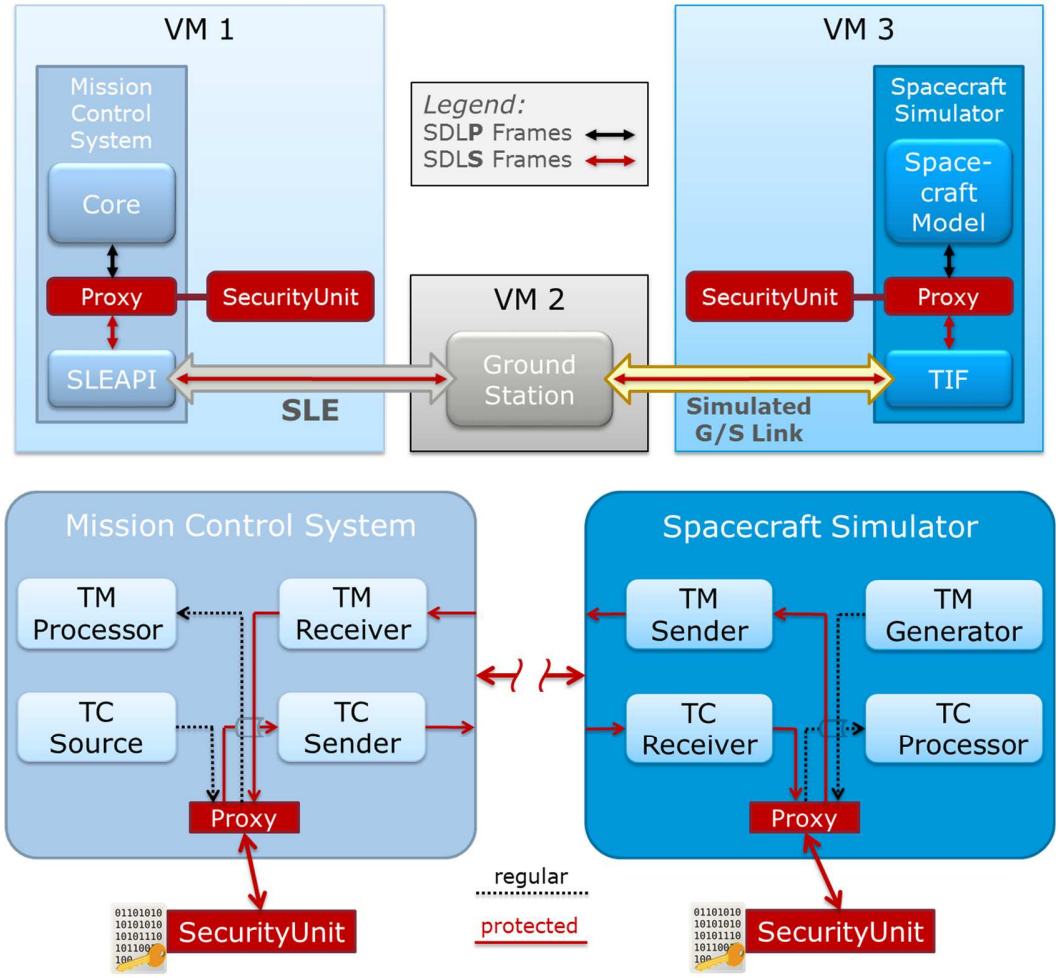


Figure 5-2 Intra-operability test configuration

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:

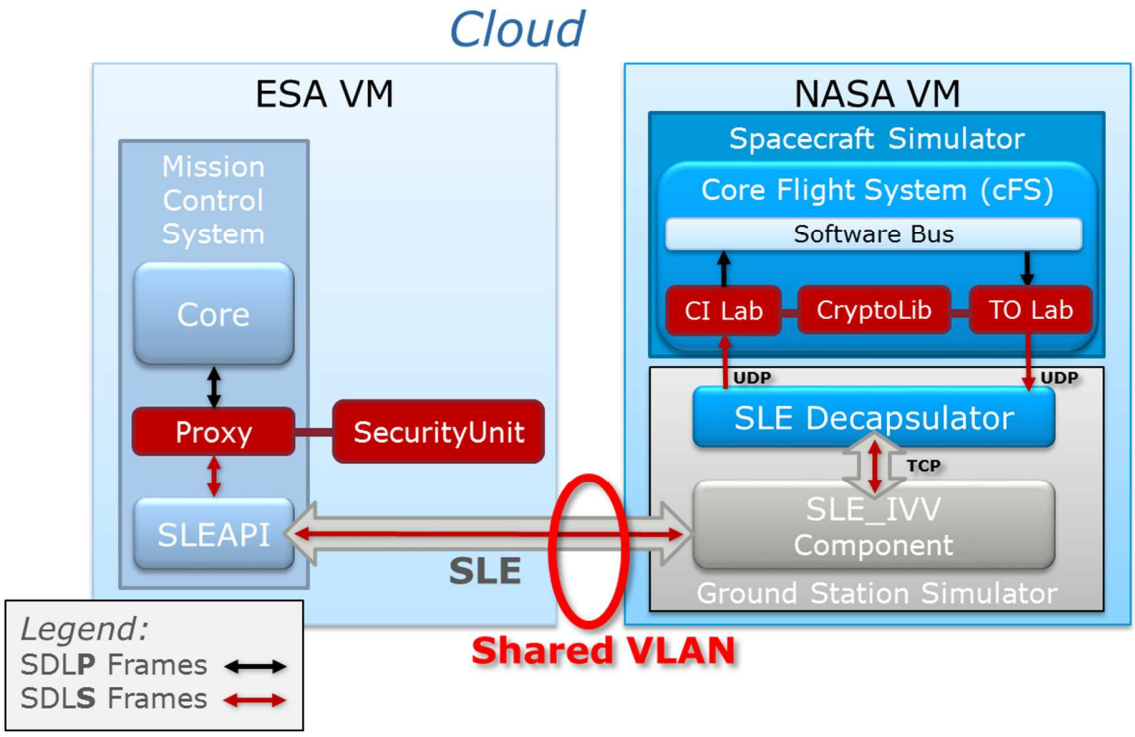


Figure 5-3: Inter-operability test configuration

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 two ends is compliant with SLE specifications (FCLTU forward, RCF return). The two ends/simulators are operating on different Virtual Machines hosted by the same Cloud Service Provider (CloudSigma). They communicate through a shared VLAN.

6 TEST CASES

For each test case, this document provides:

- Test case description & parameters
- Expected results
- Effective results obtained during:
  - intra-operability (1st phase)
  - 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.

6.1 INTRA-OPERABILITY TESTS

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

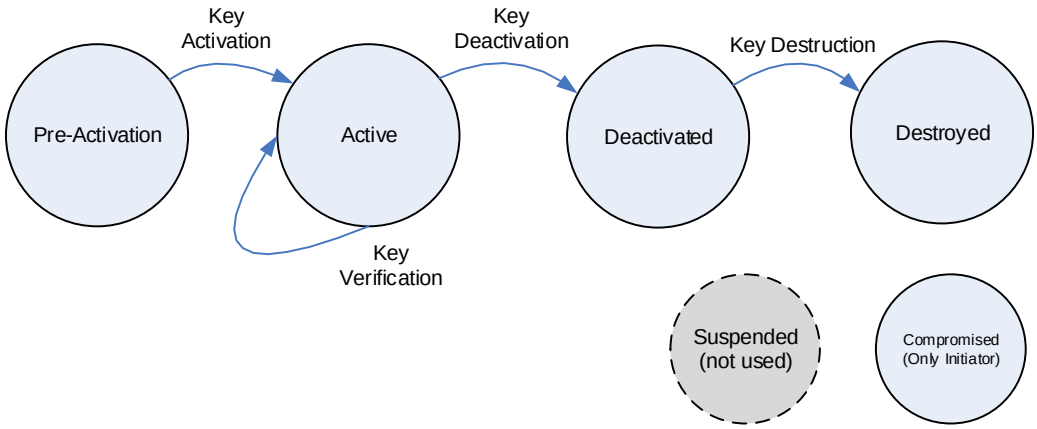
- the 3 types of services:
  - Key management, SA management, Monitoring & Control
- the complete set of service procedures for each of the 3 services with a representative set of service parameters
- a bi-directional spacelink (TC+COP uplink / TM downlink) secured by SDLS Core Protocol configured in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

6.1.1 TEST CASE #1: KEY MANAGEMENT SERVICE & PROCEDURES

6.1.1.1 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

6.1.1.2 Expected results

Correct operation of the various procedures

6.1.1.3 Intra-operability tests effective results

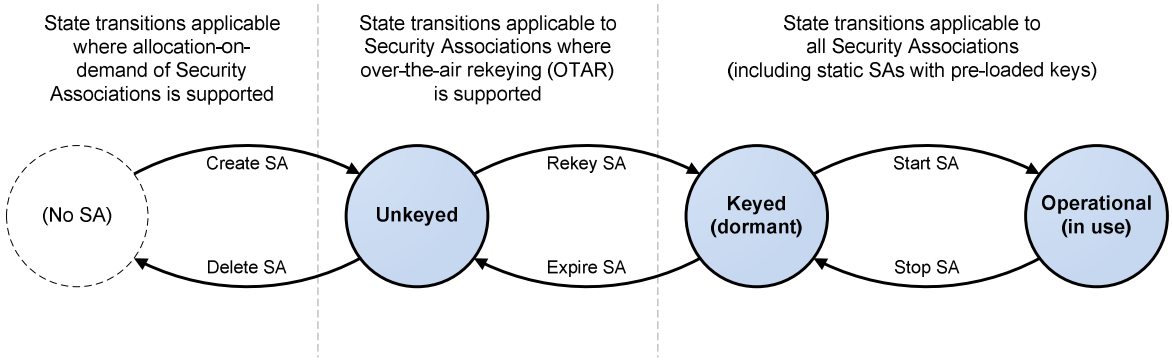
Successful – see Annex A

6.1.2 TEST CASE #2: SA MANAGEMENT & PROCEDURES

6.1.2.1 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:

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

6.1.2.2 Expected results

Correct operation of all the SA management procedures.

6.1.2.3 Intra-operability tests effective results

Successful – see Annex A

6.1.3 TEST CASE #3: MONITORING & CONTROL PROCEDURES

6.1.3.1 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 events (ARSN error, MAC error, SPI error) to check FSR content
- Test the various M&C procedures:
  - Ping
  - Alarm flag Reset (check through FSR)

6.1.3.2 Expected results

Correct operation of the M&C procedures.

6.1.3.3 Intra-operability tests effective results

Successful – see Annex A

6.2 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:

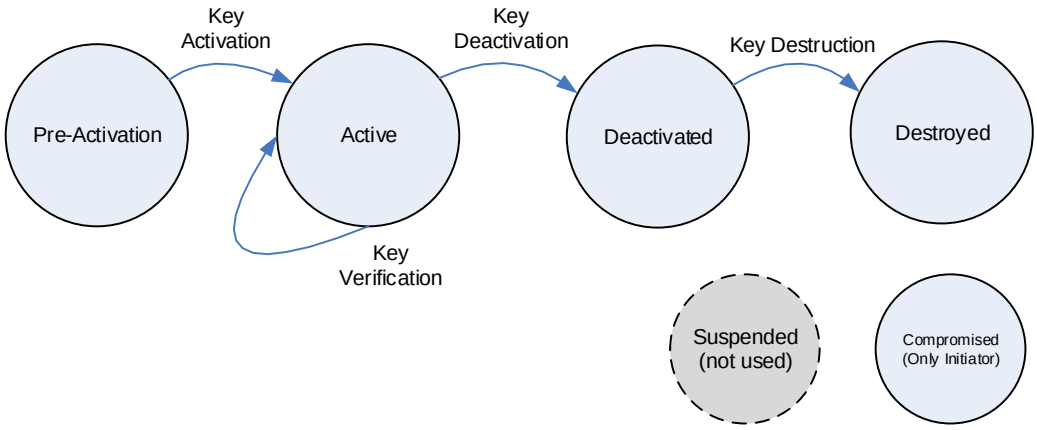
- the 3 types of services: Key management, SA management, Monitoring & Control
- the complete set of SDLS EP procedures
- a bi-directional spacelink (TC+COP uplink / TM downlink) secured by SDLS Core Protocol configured in baseline mode (annex E of reference [1])
- the various types of security events.

6.2.1 TEST CASE #4: KEY MANAGEMENT SERVICE & PROCEDURES (INTER-OPERABILITY TESTING)

6.2.1.1 Test description

The objective of this test case is to exercise the key lifecycle using the complete set of SDLS EP key management procedures including 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])
- SDLS EP: service parameters of baseline mode (annex D 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

6.2.1.2 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.

6.2.1.3 Intra-operability tests effective results

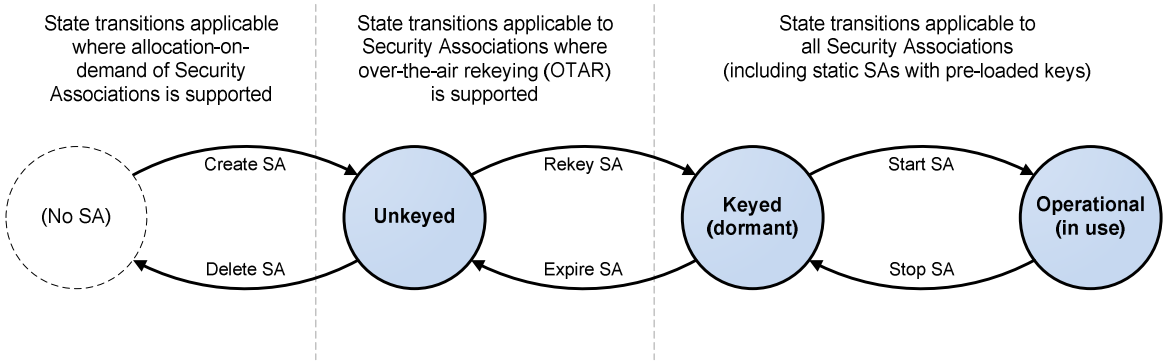
Successful – see Annex A

6.2.2 TEST CASE #5: SA MANAGEMENT & PROCEDURES (INTER-OPERABILITY TESTING)

6.2.2.1 Test description

The objective of this test case is to exercise the states and transitions for the SAs using the complete set of the SDLS EP SA management procedures.

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])
- SDLS EP: service parameters of baseline mode (annex D 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 Sequence Number and Window) for an SA

6.2.2.2 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.

6.2.2.3 Intra-operability tests effective results

Successful – see Annex A

6.2.3 TEST CASE #6: MONITORING & CONTROL PROCEDURES (INTER-OPERABILITY TESTING)

6.2.3.1 Test description

The objective of this test case is to verify the interoperability of the complete set of the SDLS EP M&C procedures.

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: service parameters of the baseline mode (annex D 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 (ARSN error, MAC error, SPI error) to check FSR content
- Test all the M&C procedures (with the service parameters of EP baseline mode):
    - Ping
    - Alarm flag Reset (check through FSR)

6.2.3.2 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.

6.2.3.3 Intra-operability tests effective results

Successful – see Annex A

7 CONCLUSION

Two types of tests were successfully performed to validate the SDLS Extended Procedures [4]:

- Intra-operability tests performed between 2 ESA simulators: one for the ground segment (SCC) and one for the on-board segment (S/C simulator) both implementing SDLS Core protocol and SDLS Extended Procedures;
- Inter-operability tests performed between an ESA ground segment simulator and a NASA space segment simulator. Those simulators include independently developed security functions implementing SDLS Core Protocol and Extended Procedures.

All SDLS Extended Procedures were successfully tested during the intra-operability tests and the inter-operability tests.

At the occasion of these tests specification ambiguities and a few errors were found which have be corrected in the final draft blue book version of the SDLS EP submitted to CESG/CMC for publication.

ANNEX A

SDLS EXTENDED PROCEDURES DETAILED TEST REPORT

Inter-Agency Testing

1 INTRODUCTION

1.1 PROJECT DESCRIPTION

The SDLS Extended Procedures (EP) Protocol [4] is a CCSDS (Consultative Committee for Space Data Systems) standard which describes the procedures needed to operate secure TC, TM, AOS or USLP spacelinks with the SDLS Core protocol [1]. The SDLS EP draft standard has been successfully submitted to Agency Review. All RIDs disposition have been implemented in the document. To finalize such a draft standard (and with that, become a “Blue Book”) it must be implemented, tested/validated through interoperability testing involving 2 independent implementations.

This annex describes the procedure of testing two individual SDLS EP Protocol implementations to validate its functionality and interoperability as described in the test cases of the present SDLS EP Protocol Test Report. One implementation is provided by ESA/ESOC, the second one is provided by NASA. Both these implementations were designed and created independently.

1.2 BIBLIOGRAPHY

See main document.

2 INTRA-OPERABILITY TEST SETUP

The intra-operability test was executed by ESA/ESOC in an end-to-end testing environment using mostly operationally used software. This allows to simulate a SDLS link from the ground segment to the space segment in a representative environment. This environment is shown in figure 1.

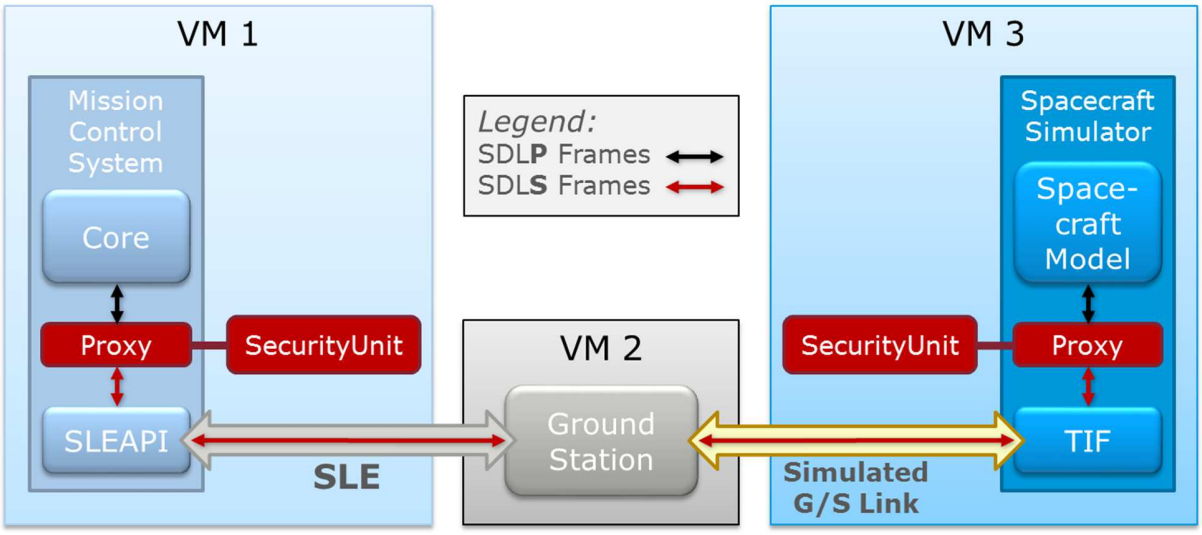


Figure A-1 – ESA/ESOCs security protocols testing environment

The environment consists of three virtual machines. The first machine contains the Mission Control System (MCS), in this case SCOS2000 the official MCS of ESOC. It is a slightly modified version for this environment, as it contains a proxy component that is capable of intercepting and re-injecting send out TC as well as received TM. After intercepting the proxy component sends it to the external SecurityUnit application responsible for the core SDLS and SDLS EP processing. After either the TC frame got secured or the TM frame security was removed, the SecurityUnit sends the regarding frame back to the proxy where it gets re-injected into the system. The MCS machine is connected to the second machine via an SLE interface. The second machine contains the ground station software called TMTCS, which is also used operationally for ESAs antennas. This software is unmodified and forwards frames via either the SLE interface or the special testing interface connecting it to the third machine. The third machine contains the generic spacecraft simulator of ESOC called GSTVi. It connects directly to the ground station via the TMTCS direct InterFace (TIF). The GSTVi simulates the technicalities of radio communication and forwards it to the spacecraft model, which emulates a generic spacecraft processing and generating frames. Similar to the MCS machine, the GSTVi was slightly modified to include a proxy component. It works analogue to its MCS counterpart of intercepting TM and TC frames, forwarding them to the SDLS processing SecurityUnit and receiving the result to re-inject it into the system.

Both sides SecurityUnit keep the security state of the keys as well as the SAs and is capable of modifying this state with received procedures of the SDLS EP. The MCS side also has a graphical interface to generate and inject the SDLS EPs in TC frames to be received on the spacecraft simulator side. In case the received SDLS EP requests a response the simulator SecurityUnit will in turn generate it and inject it into a TM frame, to be received and processed by the MCS SecurityUnit.

3 INTER-OPERABILITY TEST SETUP

To verify the SDLS EP Protocol, it is desired to test two individual independently developed implementations with each other by connecting one side MCS to the other side spacecraft simulator. To realize this NASA/IVV and ESA/ESOC each set up their respective virtual machines in a cloud environment, locally connecting both via a VLAN to ensure a closed-off and secure environment. More information regarding this cloud-based setup can be found in this yellow book section 5. The used setup is shown in figure 2.

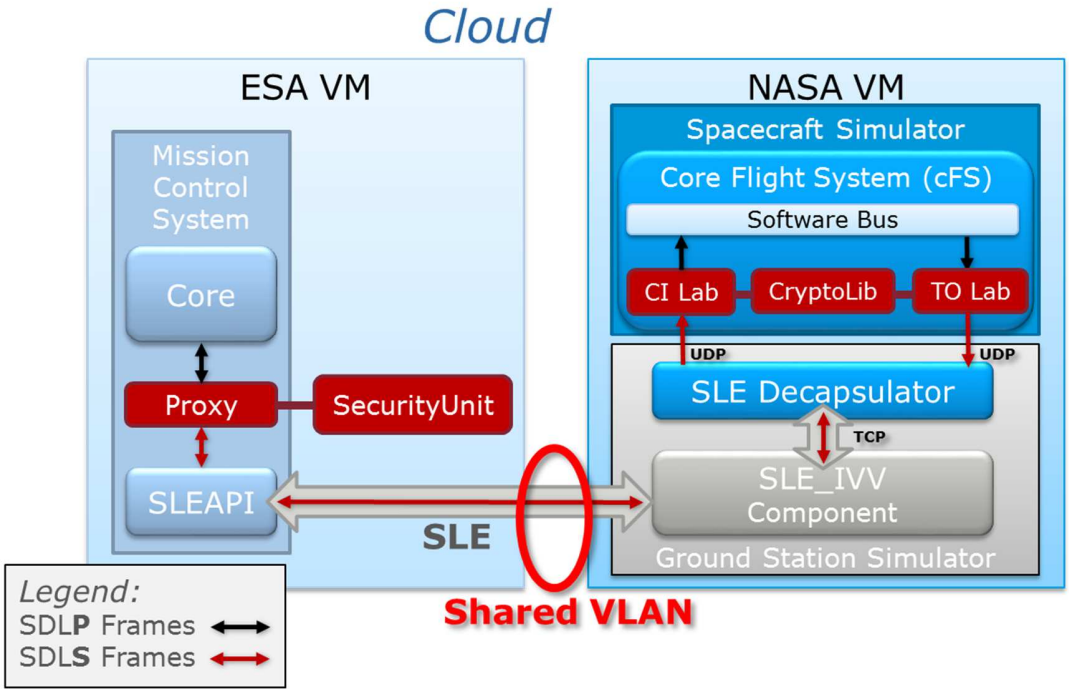


Figure A-2 – ESA/NASA security protocols interoperability testing environment

ESAs machine simply is a copy of the first virtual machine described in the preceding section 2, except for the SLE configuration. The SLE connection is configured to connect to NASAs SLE component enabling SLE communication between the two VMs. The converter then allows for closing the link to the flight software, NASA GSFC's Core Flight System (cFS), over UDP to minimize the core code changes necessary. The functionality of the SecurityUnit is contained in the Crypto Library running as part of the Command Ingest (CI) and Telemetry Output (TO) lab applications in cFS.

Upon spacecraft simulator startup, the Crypto Library loads the stored configuration and awaits for TCs to be received from the CI lab app or SDLS-EP / Space Packet Protocol packets from the TO lab app or more generally the software bus. All SDLS CP and EP functionality is contained in the Crypto Library.

4 TEST CASE #1

The first test case, described in Section 6.1.1 (main document), concentrates on exercising the complete key lifecycle using all the SDLS EP key management procedures and testing the Over The Air Rekeying (OTAR) procedures. The SLDS EP protocol is validated by using the length parameters of the baseline mode – defined in annex D of the SDLS EP recommendation [4].

4.1 TEST CONFIGURATION

The following configuration is used for the test:

Keys

We set up the keys so that the keys with ID 0 to 127 are reserved for master keys and all IDs afterwards are for session keys.

ID	Hex-String-Key	State
0	000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F	ACTIVE
1	101112131415161718191A1B1C1D1E1F101112131415161718191A1B1C1D1E1F	ACTIVE
2	202122232425262728292A2B2C2D2E2F202122232425262728292A2B2C2D2E2F	ACTIVE
128	0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF	ACTIVE
129	ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789	ACTIVE
130	FEDCBA9876543210FEDCBA9876543210FEDCBA9876543210FEDCBA9876543210	ACTIVE
131	9876543210FEDCBA9876543210FEDCBA9876543210FEDCBA9876543210FEDCBA	ACTIVE
132	0123456789ABCDEFABCDEF01234567890123456789ABCDEFABCDEF0123456789	PRE_ACTIVATION
133	ABCDEF01234567890123456789ABCDEFABCDEF01234567890123456789ABCDEF	ACTIVE
134	ABCDEF0123456789FEDCBA9876543210ABCDEF0123456789FEDCBA9876543210	DEACTIVATED

SAs

All SAs, except SPI 1, are running in authenticated encryption mode share the following parameters:

- SA_length_IV = 12 octets
- SA_length_MAC = 16 octets
- SA_encryption_algorithm = `AES-GCM`
- SA_initialization_vector = `000000000000000000000000`

SPI	SA_service_type	SA_encryption_key	State
1	Clear mode	-	ACTIVE
2	Authenticated encryption	128	KEYED
3	Authenticated encryption	129	KEYED
4	Authenticated encryption	130	KEYED
5	Authenticated encryption	131	KEYED
6	Authenticated encryption	-	UNKEYED

Mapping

All channels are mapped to SPI 1 (clear mode) for comprehensible frame output. SPI 2 is the default SA for protected TM communication, if needed. SPI 4 is the default SA for protected TC communication, if needed.

4.2 TEST PROCESS

Step	Input	Output – Expected result
1	Start all the end-to-end space communication VMs and configure SC simulator, Ground Station software, MCS and both Security Units on SC and MCS side.	All software should be running without problems. MCS receives TM flow from SC simulator and it in turn receives TCs.
2	Send SDLS EP via the Security Unit on MCS side.	Security Unit on MCS side reports successful local execution, construction and sending of SDLS EP. The state of the Security Unit has changed as expected. On an intentionally irregular SDLS EP, the Security Unit should indicate the problem, not change its state and not send the SDLS EP.
3	Check the log and state of the SC sides Security Unit for successful execution and correct resulting state of the SDLS EP.	Security Unit on SC side reports successful local execution. The state of the Security Unit has changed as expected. If the SDLS EP also includes a response, check for the construction and sending of it.
4	If the SDLS EP also includes a response, check the log of the MCS side Security Unit for the received response.	The response should reflect the state of the Security Unit on the SC side.

4.3 TEST RESULTS

TC/TM Nr.	Description	Received TC/TM	Expected Result	Actual Result

1	OTAR procedure with three new keys, sent from ground to SC. SC should add the new keys to its key repository. No report is sent back.	2003009E00FF000100001880C295008C197F0B000100840000F91E7AF8E5F9DC1036ADC4D904C804B917685CC0921A17CA90058EEBF67C56EA05F17125DF4270FB207E07C9CEE6DAB2098993577D060028603D09C76D8414EF4E6D77466876C7D39F39A4E2C617248A8552B7A9E3933294D8ED390549183E8F5E766CA0C06075C615FB395D46512E3E6F8503485DA99FBF22FD211F383A1006B5931194FFD9	OTAR - masterID: 0 keys: 141 -> 5833B73EACA3312C557E756EBEC2CF139FDBCF08C92F959901560BB2B1B7D791 140 -> 553514567BA115F39608C8985B02C85627416627D5E2D154F10F5D2844B2F8F7 142 -> 6DEA92E3C9E94946395A511090C876A60E2009CAA75B692D3E3425712E34A16C	OTAR - masterID: 0 keys: 141 -> 5833B73EACA3312C557E756EBEC2CF139FDBCF08C92F959901560BB2B1B7D791 140 -> 553514567BA115F39608C8985B02C85627416627D5E2D154F10F5D2844B2F8F7 142 -> 6DEA92E3C9E94946395A511090C876A60E2009CAA75B692D3E3425712E34A16C

2	Key Activation procedure for two keys, sent from ground to SC. SC should activate the referenced keys. No report is sent back.	2003001E00FF000100001880C296000C197F0B00020004008D008EAB05E4FC	KeyActivation - IDs: [141, 142]	KeyActivation - IDs: [141, 142]
3	Key Deactivation procedure for one key, sent from ground to SC. SC should deactivate the referenced key. No report is sent back.	2003001C00FF000100001880C297000A197F0B00030002008E578821C4	KeyDeactivation - IDs: [142]	KeyDeactivation - IDs: [142]

4	Key Verification procedure on three pre-loaded keys and two new keys, sent from ground to SC. SC should verify the referenced keys and compile a report.	2003007400FF000100001880C2980062197F0B0004005A0082EA84EAE5314487CB9E37FFDE48721A14008412C5B83075DD7BCBDA1EFF98567B360300866C049824E4561419D0E9E6405045B155008C5788A07B18148BC185B258A78BCA549E008D096628557BE61B56EA1C9CDA4120609A9CF5FACF	KeyVerification - challenges: 130 -> EA84EAE5314487CB9E37FFDE48721A14 132 -> 12C5B83075DD7BCBDA1EFF98567B3603 134 -> 6C049824E4561419D0E9E6405045B155 140 -> 5788A07B18148BC185B258A78BCA549E 141 -> 096628557BE61B56EA1C9CDA4120609A	KeyVerification - key/challenges: 130 -> EA84EAE5314487CB9E37FFDE48721A14 132 -> 12C5B83075DD7BCBDA1EFF98567B3603 134 -> 6C049824E4561419D0E9E6405045B155 140 -> 5788A07B18148BC185B258A78BCA549E 141 -> 096628557BE61B56EA1C9CDA4120609A

4.resp	Key Verification procedure response on the five referenced keys, sent from SC to ground. Ground displays the result of the verification.	00314545183800010O1A00000…0080FFFF00EA8400E600825105331A3421B53F3840B3B9CF5B697D86FC7106F73B22DC71834C359B6BF0ACD49B4F464968E994041DE4D50084B2BC8B87A1865A515D7E9048C0E8609377BD9BD2F0708278BA5CFB72C88B437869890032AFF2D9275D1AB3740086AB7996E6094C62D45E668D872121D57D8B31E98892361241F969ADE73DCA90540E4606AC844263C2D27A5021008C261D9DE52F2A35299653470E24567FBB6B73BB4221A3042F719E787E020B405A55F9645B27230AF85F7F33AA008DD95AF4AA871089019F20039A0354D10AB463309794D95534C80198E3F454614D331E13B46A07D34CC20DD5E7E8E207FF00000039…00001FC0000EF10	Key 130 was verified successfully Key 132 was verified successfully Key 134 was verified successfully Key 140 was verified successfully Key 141 was verified successfully	Key 130 was verified successfully Key 132 was verified successfully Key 134 was verified successfully Key 140 was verified successfully Key 141 was verified successfully
5	Key Activation executed on a key in DEACTIVATED state. As this an illegal operation nothing should be sent.	none	Cannot activate Key with id 134, as it is not in the PRE_ACTIVATION state!	Cannot activate Key with id 134, as it is not in the PRE_ACTIVATION state!
6	Key Deactivation executed on a key in PRE_ACTIVATION state. As this an illegal operation nothing should be sent.	none	Cannot deactivate Key with id 140, as it is not in the ACTIVE state!	Cannot deactivate Key with id 140, as it is not in the ACTIVE state!

7	OTAR procedure with five new keys, sent from ground to SC. SC should add the new keys to its key repository. No report is sent back.	200300D3007F000100001880C29900D0197F0B000100C8000214F05B1E1EEDF5D0C5C2BE692D5EFB55E37FE60C22DC9AFCDBD551EF5F647F71AB8970D3FC2C2413EB30BF021C173CAF707FA35D23711C52A9805B412A8297EDAA00D37F09CE9B9C8878117EBA0C4BDF571A4411CEBF00FDCD8C8232C453EA05BAF97030BD65608E59F5B731F8446EB98F6FCE027C36C5C1F36907B1C201E0D5015DBA68D6EA7B70BD51F1104D3AB007DBFD683100FE61313ECFA83A6B9A4BC85CC9DA735F6C36139D827930D028488E6639A7F8BD0C64B6B17043	OTAR - masterID: 2 keys: 145 -> 40B60F592B4E801ABD066F11ECF8EFE746C7C647521AAF1C90723A70C35F0984 146 -> C14626209B6B1AF42A79AEAA39FAE77B04D884C28A0F26BB7F90957F4661ED54 147 -> 0A47C0C40854DD311A54D82A611B1DA126FB291F4A72035299A52DE9223EF233 148 -> 340894776643E9A1AD63C026F6158773F7E4D7DA55352A4B4C9BA9E3E3211C64 149 -> D62C9273B73E0FF51190791B2AEF5673651EF4019B4E0E820B0DCB7A7F5A7784	OTAR - masterID: 2 keys: 145 -> 40B60F592B4E801ABD066F11ECF8EFE746C7C647521AAF1C90723A70C35F0984 146 -> C14626209B6B1AF42A79AEAA39FAE77B04D884C28A0F26BB7F90957F4661ED54 147 -> 0A47C0C40854DD311A54D82A611B1DA126FB291F4A72035299A52DE9223EF233 148 -> 340894776643E9A1AD63C026F6158773F7E4D7DA55352A4B4C9BA9E3E3211C64 149 -> D62C9273B73E0FF51190791B2AEF5673651EF4019B4E0E820B0DCB7A7F5A7784

8	Key Verification procedure on four pre-loaded keys and five new keys, sent from ground to SC. SC should verify the referenced keys and compile a report.	200300AA00FF000100001880C29A0098197F0B0004009000844366835501E843A6935696E555F3037E00857888FF070E8E9F24502D2521A00CB1750086541C892EFDB660FB77629070FD85AE870091DBC33C8456B29962648DD5AEB89C631A00926166172FA2D4410AD492D1BB29EBB23B0093F85022309A3DF6B3E382094AF276CCE400940F62F02D584C7A685DADDF551B03C1220095F9BA7636B3C4380AC13DB578EE652A704108FBFB	KeyVerification - challenges: 132 -> 4366835501E843A6935696E555F3037E 133 -> 7888FF070E8E9F24502D2521A00CB175 134 -> 541C892EFDB660FB77629070FD85AE87 145 -> DBC33C8456B29962648DD5AEB89C631A 146 -> 6166172FA2D4410AD492D1BB29EBB23B 147 -> F85022309A3DF6B3E382094AF276CCE4 148 -> 0F62F02D584C7A685DADDF551B03C122 149 -> F9BA7636B3C4380AC13DB578EE652A70	KeyVerification - challenges: 132 -> 4366835501E843A6935696E555F3037E 133 -> 7888FF070E8E9F24502D2521A00CB175 134 -> 541C892EFDB660FB77629070FD85AE87 145 -> DBC33C8456B29962648DD5AEB89C631A 146 -> 6166172FA2D4410AD492D1BB29EBB23B 147 -> F85022309A3DF6B3E382094AF276CCE4 148 -> 0F62F02D584C7A685DADDF551B03C122 149 -> F9BA7636B3C4380AC13DB578EE652A70

8.resp	Key Verification procedure response on the nine referenced keys, sent from SC to ground. Ground displays the result of the verification.	00319D9D18090001001A0000…0080FFFF017484017000845EB5AADFCB3DFD2677982655F31FD85E1F8D78DC4C1F40D5AC733481AF3ADB21A373AC94851B29EE9C97A6660085D3A8A771005D109A0D3E02E4F936B749A21806C9EAAB3267215A6EED060F116ADAA7ADD3E78EF13269B457F100865B8E64499BF10C937903372C4AD6470015742E680461A1F6ADF563462F60CD35297AE2C1CD39E127CDA9C1F200911A52841D7E9AA0536B548411F074D254F6DB9C97BA61FC9E69CEDF680A5B470B09FE699430268582DC5FEEBA0092F39062F1F02F3334B25ADC3ACF3EDA79B3FD4987A1334E2BD19A8EFBBA03C266FCDBC5CEA03835A6A96FECA50093B3057263DA33D47FC46CF089A263F28AE9F97DD0E0AB1C43258AF4C2A43A49E3B9D673FBD2C7EA105120D38D0094C38210E06B58CE29B2D64657E5104C90AD490C275777FC841CEA666B1A75C748EE6A10F5B106527E83439C350095FD3F62A2CD65364A4C80C1138554F2A7C027DB359B870706D3B169E8D02E20711B5A9357833C3BCE7AA13A4BFC7107FF00000039… 0001040201BCC3	Key 132 was verified successfully Key 133 was verified successfully Key 134 was verified successfully Key 145 was verified successfully Key 146 was verified successfully Key 147 was verified successfully Key 148 was verified successfully Key 149 was verified successfully	Key 132 was verified successfully Key 133 was verified successfully Key 134 was verified successfully Key 145 was verified successfully Key 146 was verified successfully Key 147 was verified successfully Key 148 was verified successfully Key 149 was verified successfully
9	Key Activation procedure for three keys, sent from ground to SC. SC should activate the referenced keys. No report is sent back.	2003002000FF000100001880C29B000E197F0B0002000600920093009 58DFEA61A	KeyActivation - IDs: [146, 147, 149]	KeyActivation - IDs: [146, 147, 149]
10	Key Deactivation procedure for two keys, sent from ground to SC. SC should deactivate the referenced key. No report is sent back.	2003001E00FF000100001880C29C000C197F0B0003000400930095F5F5E4FC	KeyDeactivation - IDs: [147, 149]	KeyDeactivation - IDs: [147, 149]

11	OTAR procedure with four new keys, sent from ground to SC. SC should add the new keys to its key repository. No report is sent back.	200300C000FF000100001880C29D00AE197F0B000100A6000127069A1A8B0FE0937734E289BE9D9880E8ED8EF448FCBDA732382AAAFA3B3451BBB6D290B0B0E43764A3F412B80BE4ED8DE1403C8CA63D20928401B658DF37E0AD30F9BF549980321BDE5C7F89CDB257B5D148F6B87CB80E7675EDFB733FF9B2BDA1DAC0DBCA9CEFA5F9D594759EDAB863DE13B8B3DEB4EE15F10675E9AC4A4CDE258073701D1219B3D5991B487C86EBA36183E3B30D089626BBD0C8AD8CD6BBBD73D0AA963105DE	OTAR - masterID: 1 keys: 152 -> 93466A5FEA8F9CE2F5BB76B9C28454F6EC7AD3E9217BC7C54A52A14D6E8FD892 153 -> 54EBD1D929060442C146B2E1D32368AB2E2BF3C9EECFFA765B1BE65A465B733D 150 -> AC909C73E7578FFD01F79F464E79C7D592BF197116BD29ABCE4D724F72DBC19D 151 -> AA5BED1BD9F778FC398D808C7920009569DA6E3D8F3D0BA0BA39A68531D5D78E	OTAR - masterID: 1 keys: 152 -> 93466A5FEA8F9CE2F5BB76B9C28454F6EC7AD3E9217BC7C54A52A14D6E8FD892 153 -> 54EBD1D929060442C146B2E1D32368AB2E2BF3C9EECFFA765B1BE65A465B733D 150 -> AC909C73E7578FFD01F79F464E79C7D592BF197116BD29ABCE4D724F72DBC19D 151 -> AA5BED1BD9F778FC398D808C7920009569DA6E3D8F3D0BA0BA39A68531D5D78E
12	Key Activation procedure for three keys, sent from ground to SC. SC should activate the referenced keys. No report is sent back.	2003002000FF000100001880C29E000E197F0B000200060097009800 99B722A61A	KeyActivation - IDs: [151, 152, 153]	KeyActivation - IDs: [151, 152, 153]
13	Key Deactivation procedure for two keys, sent from ground to SC. SC should deactivate the referenced key. No report is sent back.	2003001E00FF000100001880C29F000C197F0B000300040098009 9492BE4FC	KeyDeactivation - IDs: [152, 153]	KeyDeactivation - IDs: [152, 153]

14	Key Verification procedure on four new keys, sent from ground to SC. SC should verify the referenced keys and compile a report.	2003006200FF000100001880C2A00050197F0B0004004800963AFDFB471913AD8137D67AD3C5C809AE00977BC29792D163CF9ADA38BC7F6B9E1FA40098CC3A3884EF6636C23A2386764E2910590099A2E78F1CCDA428FF694837C8570D21B581429A04	KeyVerification - challenges: 150 -> 3AFDFB471913AD8137D67AD3C5C809AE 151 -> 7BC29792D163CF9ADA38BC7F6B9E1FA4 152 -> CC3A3884EF6636C23A2386764E291059 153 -> A2E78F1CCDA428FF694837C8570D21B5	KeyVerification - challenges: 150 -> 3AFDFB471913AD8137D67AD3C5C809AE 151 -> 7BC29792D163CF9ADA38BC7F6B9E1FA4 152 -> CC3A3884EF6636C23A2386764E291059 153 -> A2E78F1CCDA428FF694837C8570D21B5
14.resp	Key Verification procedure response on the four referenced keys, sent from SC to ground. Ground displays the result of the verification.	00310C0C18090001001A000…0080FFFF00BC8400B80096D64D560571B0309DA3AAD4148EB1D56131A3472BFE7B144D7D5FA3DBB264909C67A5A8E0E7D977B2DF87066700979ABE704D26D54F70A258B6015831C62DF245A1D0C1E0B6D8F71450A17A7E11D7B8237A6831F8AAB447BC397A00986E2AAADBB61EE532DCCBE3566E33A5B6965C5FB5BC8AE6945B967C4CB93481BC3D6048D1EF6476A6947B16860099B7D3DC187E7AF2320B0E75124442378FC386BFB1F08DD43291E0CD27E22DE25335774B5EB6C11B18F4E72B80DCF307FF00000039…000C0000101380E	Key 150 was verified successfully Key 151 was verified successfully Key 152 was verified successfully Key 153 was verified successfully	Key 150 was verified successfully Key 151 was verified successfully Key 152 was verified successfully Key 153 was verified successfully
-	Intentional corruption of a key on board the SC.		Corrupted Key 152 successfully.	Corrupted Key 152 successfully.

15	Key Verification procedure on four new keys, sent from ground to SC. SC should verify the referenced keys and compile a report.	2003006200FF000100001880C2A10050197F0B000400480096C784D963A3BFAB2F9991918AE5EA317100970DCC25189F4F17BB78E27A45F15A8B7B0098D18BA4B9E38BF055F9D30AD41362B9050099116E31CE6A7A1260321B3252F84753D4253F9A04	KeyVerification - challenges: 150 -> C784D963A3BFAB2F9991918AE5EA3171 151 -> 0DCC25189F4F17BB78E27A45F15A8B7B 152 -> D18BA4B9E38BF055F9D30AD41362B905 153 -> 116E31CE6A7A1260321B3252F84753D4	KeyVerification - challenges: 150 -> C784D963A3BFAB2F9991918AE5EA3171 151 -> 0DCC25189F4F17BB78E27A45F15A8B7B 152 -> D18BA4B9E38BF055F9D30AD41362B905 153 -> 116E31CE6A7A1260321B3252F84753D4
15.resp	Key Verification procedure response on the four referenced keys, sent from SC to ground. Ground displays the result of the verification. The corrupted key should be marked as such.	00312525182000001001A000…0080FFFF00BC8400B800960C5B8FD93B6BFBAE14382DB79A6834C77FEA5333C09CC9BF6823DE0F332BDA55B7BBC4F21BA02B3F917F7E680097974B3031DC81F277879910EBA892DD1652A83160905368A8AC316FF63788D418B35DBD01F968105C65231D5C0098B7DA1AF61545A314B8D6C9E0AFF7944265AEE6D95C310A8157DC3A0E830CAED33C3F58FBC13B1BDDA55418C40099B90270FFB3D70ED5A5CB06F66EC96B7AA4D23C5C713BCE68D1B82898012E64D22BD0E49544B6CD155BA4BB68893907FF00000039…000010006016CE7	Key 150 was verified successfully Key 151 was verified successfully Key 152 failed to verify! Key 153 was verified successfully	Key 150 was verified successfully Key 151 was verified successfully Key 152 failed to verify! Key 153 was verified successfully

-	Intentional corruption of four keys on board the SC.		Corrupted Key 150 successfully. Corrupted Key 151 successfully. Corrupted Key 153 successfully.	Corrupted Key 150 successfully. Corrupted Key 151 successfully. Corrupted Key 153 successfully.
16	Key Verification procedure on four new keys, sent from ground to SC. SC should verify the referenced keys and compile a report.	2003006200FF000100001880C2A30050197F0B0004004800961DAFC8383088538EB204C8710C35001300970115FB8E66A229A17CCC36F6E937CE970098D036FB7537A4847C436F3D01EE78BEBB0099D15D9AB1519D94E6C70FEAEB37AC7FB372839A04	KeyVerification - challenges: 150 -> 1DAFC8383088538EB204C8710C350013 151 -> 0115FB8E66A229A17CCC36F6E937CE97 152 -> D036FB7537A4847C436F3D01EE78BEBB 153 -> D15D9AB1519D94E6C70FEAEB37AC7FB3	KeyVerification - challenges: 150 -> 1DAFC8383088538EB204C8710C350013 151 -> 0115FB8E66A229A17CCC36F6E937CE97 152 -> D036FB7537A4847C436F3D01EE78BEBB 153 -> D15D9AB1519D94E6C70FEAEB37AC7FB3

16.resp	Key Verification procedure response on the four referenced keys, sent from SC to ground. Ground displays the result of the verification. The corrupted keys should be marked as such.	0033A20118340001001A000…0080FFFF00BC8400B800969AD637E9E4C65470FCA0B9F59BD7761C34CFC9A5D0721E092156B2347AB9EA294EB59FBFB3975095D6E589D50097EDF57785FC6798FC3E238BB273A47F72CA28AA0BE00AAD1B15121C722B82A6DEC36D9BA908677E7BBDFD547500987A6763D747311E5464AB571EC3E3DF4DDE128A338911788607B3F3DA8E6A2748A9BD558742B36B724486D833009938FFC04A6EEBEC1FDD77415BF6747B1A5670AD5147E8C04856D01CCFD566777EEF05B1AF4CB677D3C9DB005E031D07FF00000039…000C0000101E185	Key 150 failed to verify! Key 151 failed to verify! Key 152 failed to verify! Key 153 failed to verify!	Key 150 failed to verify! Key 151 failed to verify! Key 152 failed to verify! Key 153 failed to verify!

5 TEST CASE #2

The second test case, described in Section 6.1.2 (of main document), concentrates on exercising the complete SA lifecycle using all the SDLS EP SA management procedures. The SLDS EP protocol is validated by using the length parameters of the baseline mode – defined in annex D of the SDLS EP recommendation [4].

5.1 TEST CONFIGURATION

The following configuration is used for the test:

Keys

We set up the keys so that the keys with ID 0 to 127 are reserved for master keys and all IDs afterwards are for session keys.

ID	Hex-String-Key	State
0	000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F	ACTIVE
1	101112131415161718191A1B1C1D1E1F101112131415161718191A1B1C1D1E1F	ACTIVE
2	202122232425262728292A2B2C2D2E2F202122232425262728292A2B2C2D2E2F	ACTIVE
128	0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF	ACTIVE
129	ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789	ACTIVE
130	FEDCBA9876543210FEDCBA9876543210FEDCBA9876543210FEDCBA9876543210	ACTIVE
131	9876543210FEDCBA9876543210FEDCBA9876543210FEDCBA9876543210FEDCBA	ACTIVE
132	0123456789ABCDEFABCDEF01234567890123456789ABCDEFABCDEF0123456789	PRE_ACTIVATION
133	ABCDEF01234567890123456789ABCDEFABCDEF01234567890123456789ABCDEF	ACTIVE
134	ABCDEF0123456789FEDCBA9876543210ABCDEF0123456789FEDCBA9876543210	DEACTIVATED

SAs

All SAs, except SPI 1, are running in authenticated encryption mode share the following parameters:

- SA_length_IV = 12 octets
- SA_length_MAC = 16 octets
- SA_encryption_algorithm = `AES-GCM`
- SA_initialization_vector = `000000000000000000000000`

SPI	SA_service_type	SA_encryption_key	State
1	Clear mode	-	ACTIVE
2	Authenticated encryption	128	KEYED
3	Authenticated encryption	129	KEYED
4	Authenticated encryption	130	KEYED
5	Authenticated encryption	131	KEYED
6	Authenticated encryption	-	UNKEYED

Mapping

All channels are mapped to SPI 1 (clear mode) for comprehensible frame output. SPI 2 is the default SA for protected TM communication, if needed. SPI 4 is the default SA for protected TC communication, if needed.

5.2 TEST PROCESS

Step	Input	Output – Expected result
1	Start all the end-to-end space communication VMs and configure SC simulator, Ground Station software, MCS and both Security Units on SC and MCS side.	All software should be running without problems. MCS receives TM flow from SC simulator and it in turn receives TCs.
2	Send SDLS EP via the Security Unit on MCS side.	Security Unit on MCS side reports successful local execution, construction and sending of SDLS EP. The state of the Security Unit has changed as expected. On an intentionally irregular SDLS EP, the Security Unit should indicate the problem, not change its state and not send the SDLS EP.
3	Check the log and state of the SC sides Security Unit for successful execution and correct resulting state of the SDLS EP.	Security Unit on SC side reports successful local execution. The state of the Security Unit has changed as expected. If the SDLS EP also includes a response, check for the construction and sending of it.
4	If the SDLS EP also includes a response, check the log of the MCS side Security Unit for the received response.	The response should reflect the state of the Security Unit on the SC side.

5.3 TEST RESULTS

TC/TM Nr.	Description	Received TC/TM	Expected Result	Actual Result
1	Rekey SA procedure on the newly created SA with a preloaded and ACTIVE key, sent from ground to SC. SC should assign the key to the SA and set it to KEYED state. No report is sent back.	2003002A00FF000100001880C3720018197F0B0016000C000600850000000000000000000000000A9569FC8	SArekey - spi: 6 keyID: 133 IV: 0x0000000000000000	SArekey - spi: 6 keyID: 133 IV: 0x0000000000000000
2	Start SA procedure on the new SA on the VC 1 on the TC side, sent from ground to SC. SC should map the SA to the given channel and set the SA to OPERATIONAL state. No report is sent back.	2003002000FF000100001880C373000E197F0B001B00040006000003040AFBDA61A	SAstart - spi: 6 map: [GVCID: VC (1) 1]	SAstart - spi: 6 map: [GVCID: VC (1) 1]
-	Switch currently used TC channel to VC 1 to use the new SA for TCs.		Changed used VC for TC to 1	Changed used VC for TC to 1
3	Execute M&C Ping procedure to test new secure channel on new SA, sent from ground to SC. SC should be able to decrypt message and send a report back.	2003043400FF000600000000000000000000000000121E8D88F734AC14B895B514579810B13E3E4A0FF4B0373562EA25EC78F15D51701	McPingReq - was parsed!	McPingReq - was parsed!
3.resp	M&C Ping procedure response, sent from SC to ground. Ground displays the pong message.	00317B7B18040001001A000000000080FFFF0004B10000170307FF00000039…0001FC0000B301	McPingResp - received PONG	McPingResp - received PONG

4	Execute M&C Ping procedure to test new secure channel on new SA, sent from ground to SC. SC should be able to decrypt message and send a report back.	2003043400FF000600000000000000000000000002B3104C0C0B1FDB72496C8CE2037525E06DF70E1055204F5CEE10910F042121902F	McPingReq - was parsed!	McPingReq - was parsed!
4.resp	M&C Ping procedure response, sent from SC to ground. Ground displays the pong message.	00318888183400010001A000…0080FFFF0004B10000170307FF00000039…00000C0000602C8BD	McPingResp - received PONG	McPingResp - received PONG
-	Switch currently used TC channel to VC 0 to go back to clear mode.		Changed used VC for TC to 0	Changed used VC for TC to 0
5	SA Read SN procedure on the new SA to get current IV value as a reference, sent from ground to SC. SC sends back report containing the current value of the IV.	2003001C00FF000100001880C376000A197F0B001000020006F2D721C4	SaReadSN - spi: 6	SaReadSN - spi: 6
5.resp	SA Read SN procedure response, sent from SC to ground. Ground displays the expected IV value.	0031A9A9182D0001001A000…0080FFFF001290000E000600000000000000000000000002F9A807FF00000039… 00010406014EB6	SaReadSnResp - was parsed! SN is: 2	SaReadSnResp - was parsed! SN is: 2
6	Set ARSN procedure on the new SA, sent from ground to SC. SC sets the IV of the new SA to the given value. No report is sent back.	2003002800FF000100001880C3770016197F0B001A000A000600000000000000000000000000644710983E	SaSetArCounter - was parsed! SAsetARcounter - spi: 6 value: 100	SaSetArCounter - was parsed! SAsetARcounter - spi: 6 value: 100
7	SA Read SN procedure on the new SA to get current IV value as a reference, sent from ground to SC. SC sends back report containing the current value of the IV.	2003001C00FF000100001880C378000A197F0B001000020006E24121C4	SaReadSN - spi: 6	SaReadSN - spi: 6

7.resp	SA Read SN procedure response, sent from SC to ground. Ground displays the expected IV value.	0031C8C818320001001A000…0080FFFF001290000E000600000000000000000000000064F5C807FF00000039…000C00001011216	SaReadSnResp - was parsed! SN is: 100	SaReadSnResp - was parsed! SN is: 100
-	Switch currently used TC channel to VC 1 to use the new SA for TCs.		Changed used VC for TC to 1	Changed used VC for TC to 1
8	Execute M&C Ping procedure to test new secure channel on new SA, sent from ground to SC. SC should be able to decrypt message and send a report back.	2003043400FF000600000000000000000000000000656CBE840266D9015AB1F747510B36E438482AA9F6DF7812488D000A2314DE6744B1	McPingReq - was parsed!	McPingReq - was parsed!
8.resp	M&C Ping procedure response, sent from SC to ground. Ground displays the pong message.	0031DFDF18210001001A000…0080FFFF0004B10000170307FF00000039…001040001D0DE	McPingResp - received PONG	McPingResp - received PONG
9	Execute M&C Ping procedure to test new secure channel on new SA, sent from ground to SC. SC should be able to decrypt message and send a report back.	2003043400FF000600000000000000000000000000066FA1906EFE27CB4D95B5C2B5F4369FA7AFE40334DA86B10DB239299D1DA3D5D01D5	McPingReq - was parsed!	McPingReq - was parsed!
9.resp	M&C Ping procedure response, sent from SC to ground. Ground displays the pong message.	0033E60018000001001A0080FFFF0004B10000170307FF00000039…000C00006661E67	McPingResp - received PONG	McPingResp - received PONG
-	Switch currently used TC channel to VC 0 to go back to clear mode.		Changed used VC for TC to 0	Changed used VC for TC to 0
10	SA Read SN procedure on the new SA to get current IV value as a reference, sent from ground to SC. SC sends back report containing the current value of the IV.	2003001C00FF000100001880C37B000A197F0B001000020006E7DE21C4	SaReadSN - spi: 6	SaReadSN - spi: 6

10.resp	SA Read SN procedure response, sent from SC to ground. Ground displays the expected IV value.	00310C0B180A0001001A000…0080FFFF001290000E00060000000000000000000000066D58A07FF00000039…0000C00001012A4D	SaReadSnResp - was parsed! SN is: 102	SaReadSnResp - was parsed! SN is: 102
11	Stop the current SA on VC 1 on the TC side, sent from ground to SC. SC should map the SA to the given channel and set the SA to OPERATIONAL state. No report is sent back.	2003001C00FF000100001880C37C000A197F0B001E00020006203D21C4	SAstop - spi: 6	SAstop - spi: 6
12	Start SA procedure on the new SA on the VC 1 on the TC side, sent from ground to SC. SC should map the SA to the given channel and set the SA to OPERATIONAL state. No report is sent back.	2003002000FF000100001880C37D000E197F0B001B000400050000030409051A61A	SAstart - spi: 5 map: [GVCID: VC (1) 1]	SAstart - spi: 6 map: [GVCID: VC (1) 1]
-	Switch currently used TC channel to VC 1 to use the new SA for TCs.		Changed used VC for TC to 1	Changed used VC for TC to 1
13	Execute M&C Ping procedure to test new secure channel on new SA, sent from ground to SC. SC should be able to decrypt message and send a report back.	2003043400FF000500000000000000000000000001288AFA5C821B353EA9787B6AFECD239BB2F26D83C2305ECB5B33F786E900FD28C4	McPingReq - was parsed!	McPingReq - was parsed!
13.resp	M&C Ping procedure response, sent from SC to ground. Ground displays the pong message.	00313534183E0001001A0000003900…0080FFFF0004B10000170307FF00000039…001FC0000278A	McPingResp - received PONG	McPingResp - received PONG
14	Execute M&C Ping procedure to test new secure channel on new SA, sent from ground to SC. SC should be able to decrypt message and send a report back.	2003043400FF000500000000000000000000000002344E141EEE6DFA6B258A68EB11F305431AC4C4B7161BA6A07DDEF3956680BF8AC6	McPingReq - was parsed!	McPingReq - was parsed!

14.resp	M&C Ping procedure response, sent from SC to ground. Ground displays the pong message.	00313A39182D0001001A000…0080FFFF0004 B10000170307FF00000039…0C00005023AC4	McPingResp - received PONG	McPingResp - received PONG

TEST CASE #3

The third interoperability test case, described in Section 6.1.3 (main document), has the objective to execute all the Monitoring & Control procedures and their specified PDU formats as well as testing the FSR functionality. To test the FSR functionality a protected channel is set up and the SecurityUnit is capable of inducing deliberate security errors, e.g. simulating a replay attack by using the same SN twice.

5.4 TEST CONFIGURATION

The following configuration is used for the test:

Keys

We set up the keys so that the keys with ID 0 to 127 are reserved for master keys and all IDs afterwards are for session keys.

ID	Hex-String-Key	State
0	000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F	ACTIVE
1	101112131415161718191A1B1C1D1E1F101112131415161718191A1B1C1D1E1F	ACTIVE
2	202122232425262728292A2B2C2D2E2F202122232425262728292A2B2C2D2E2F	ACTIVE
128	0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF	ACTIVE
129	ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789	ACTIVE
130	FEDCBA9876543210FEDCBA9876543210FEDCBA9876543210FEDCBA9876543210	ACTIVE
131	9876543210FEDCBA9876543210FEDCBA9876543210FEDCBA9876543210FEDCBA	ACTIVE
132	0123456789ABCDEFABCDEF01234567890123456789ABCDEFABCDEF0123456789	PRE_ACTIVATION
133	ABCDEF01234567890123456789ABCDEFABCDEF01234567890123456789ABCDEF	ACTIVE
134	ABCDEF0123456789FEDCBA9876543210ABCDEF0123456789FEDCBA9876543210	DEACTIVATED

SAs

All SAs, except SPI 1, are running in authenticated encryption mode share the following parameters:

- SA_length_IV = 12 octets
- SA_length_MAC = 16 octets
- SA_encryption_algorithm = `AES-GCM`
- SA_initialization_vector = `000000000000000000000000`

SPI	SA_service_type	SA_encryption_key	State
1	Clear mode	-	ACTIVE
2	Authenticated encryption	128	KEYED
3	Authenticated encryption	129	KEYED
4	Authenticated encryption	130	KEYED
5	Authenticated encryption	131	KEYED
6	Authenticated encryption	-	UNKEYED

Mapping

All channels are mapped to SPI 1 (clear mode) for comprehensible frame output. SPI 2 is the default SA for protected TM communication, if needed. SPI 4 is the default SA for protected TC communication, if needed.

5.5 TEST PROCESS

Step	Input	Output – Expected result
1	Start both the ESA and NASA VMs and configure SC simulator, MCS and both Security Modules on NASA and ESA side.	All software should be running without problems. MCS receives TM flow from SC simulator and it in turn receives TCs.
2	Send SDLS EP via the Security Unit on ESA side.	Security Module on ESA side reports successful local execution, construction and sending of SDLS EP. The state of the Security Module has changed as expected. On an intentionally irregular SDLS EP, the Security Module should indicate the problem, not change its state and not send the SDLS EP.
3	Check the log and state of the NASA sides Security Module for successful execution and correct resulting state of the SDLS EP.	Security Module on NASA side reports successful local execution. The state of the Security Module has changed as expected. If the SDLS EP also includes a response, check for the construction and sending of it.
4	If the SDLS EP also includes a response, check the log of the ESA sides Security Module for the received response.	The response should reflect the state of the Security Module on the NASA side.

5.6 TEST RESULTS

TC/TM Nr.	Description	TC/TM	Expected Result	Actual Result
1	M&C Ping procedure, sent from ground to SC. SC sends a pong report back.	2003001A00FF000100001880C3E40008197F0B00310000B4483128	McPingReq - was parsed!	McPingReq - was parsed!
1.resp	M&C Ping procedure response, sent from SC to ground. Ground displays the pong message.	00312626181800010001A000…0080FFFF0004B10000170307FF00000039…0C00001012AF8	McPingResp - received PONG	McPingResp - received PONG
2	M&C Ping procedure, sent from ground to SC. SC sends a pong report back.	2003001A00FF000100001880C3E50008197F0B00310000DB0D3128	McPingReq - was parsed!	McPingReq - was parsed!
2.resp	M&C Ping procedure response, sent from SC to ground. Ground displays the pong message.	00332E0018000001001A0080FFFF0004B10000170307FF00000039…000C0000101CE20	McPingResp - received PONG	McPingResp - received PONG
3	Start SA procedure on preloaded SA on the VC 1 on the TC side, sent from ground to SC. SC should map the SA to the given channel and set the SA to OPERATIONAL state. No report is sent back.	2003002000FF000100001880C3E6000E197F0B001B00040004000003040E8B3A61A	SAstart - spi: 4 map: [GVCID: VC (1) 1]	SAstart - spi: 4 map: [GVCID: VC (1) 1]
-	Switch currently used TC channel to VC 1 to use a secure channel for TCs in preparation for the forced error testing.			
4	M&C Ping procedure, sent from ground to SC. SC sends a pong report back.	2003043400FF000400000000000000000000000017E1D9FC78D45CEBA17888E0CDCEB05A5A218F757D5548C91F09162E4B26F143C45	McPingReq - was parsed!	McPingReq - was parsed!

4.resp	M&C Ping procedure response, sent from SC to ground. Ground displays the pong message.	00315655183E0001001A0000003900…0080FFFF0004B10000170307FF00000039…000C00004013F19	McPingResp - received PONG	McPingResp - received PONG
5	M&C Ping procedure, sent from ground to SC. SC sends a pong report back.	2003043400FF000400000000000000000000000000219C6FEF5CD012F28EB9F38C49E73DF771D60B056895741D454C0A7C2652E3C21B3	McPingReq - was parsed!	McPingReq - was parsed!
5.resp	M&C Ping procedure response, sent from SC to ground. Ground displays the pong message.	00336201183C0001001A00390000…0080FFFF0004B10000170307FF00000039…000C00004023F85	McPingResp - received PONG	McPingResp - received PONG
-	Check FSR output in ground software read out from the idle frames coming from the SC.		Received ordinary FSR (LastSPI = 4; LastSN = 2)	Received ordinary FSR (LastSPI = 4; LastSN = 2)
-	Force a replay error on next TC frame sent from ground to SC.			
6	Erroneous M&C Ping procedure, sent from ground to SC. Frame results in processing error on the SC and it sends an alarm FSR with the regarding flags and values set. As frame is not processed no report is sent back.	2003043400FF000400000000000000000000000000219C6FEF4CD012F28EB9F38C49E1C9AAE5C92C2A3CABF9D006739B67A04B22F1678	SN is out of Bounds: Expected SN=3, window size=5, Incoming SN=2	SN is out of Bounds: Expected SN=3, window size=5, Incoming SN=2
-	Check FSR output in ground software read out from the idle frames coming from the SC.		Received Alarm FSR (BadSN = 1; BadMAC = 0; InvalidSPI = 0; LastSPI = 4; LastSN = 3)	Received Alarm FSR (BadSN = 1; BadMAC = 0; InvalidSPI = 0; LastSPI = 4; LastSN = 3)
7	M&C Reset Alarm Flag procedure, sent from ground to SC. SC resets the FSR alarm flag. No report is sent back.	2003043400FF000400000000000000000000000000035F0747B958AA0CA2EE993146A4CF3BF8E4FBF0BD51AA9EF13EFC6A2D0490760CA0	McResetAlarmFlag - FSR Alarm Flag was reset!	McResetAlarmFlag - FSR Alarm Flag was reset!

-	Check FSR output in ground software read out from the idle frames coming from the SC.		Received ordinary FSR (LastSPI = 4; LastSN = 4)	Received ordinary FSR (LastSPI = 4; LastSN = 4)
-	Force an out of bounds error on next TC frame sent from ground to SC.			
8	Erroneous M&C Ping procedure, sent from ground to SC. Frame results in processing error on the SC and it sends an alarm FSR with the regarding flags and values set. As frame is not processed no report is sent back.	2003043400FF000400000000000000000000000000009059A39B0C2DA902C63978EAF1EC2D714C189314AAABC45085F15E90714394E0BF1	SN is out of Bounds: Expected SN=4, window size=5, Incoming SN=9	SN is out of Bounds: Expected SN=4, window size=5, Incoming SN=9
-	Check FSR output in ground software read out from the idle frames coming from the SC.		Received Alarm FSR (BadSN = 1; BadMAC = 0; InvalidSPI = 0; LastSPI = 4; LastSN = 9)	Received Alarm FSR (BadSN = 1; BadMAC = 0; InvalidSPI = 0; LastSPI = 4; LastSN = 9)
9	M&C Reset Alarm Flag procedure, sent from ground to SC. SC resets the FSR alarm flag. No report is sent back.	2003043400FF000400000003000000000000000004A4E155B6B8E384A0AD0FC0FD0961AA0A0160F1BB0DA46692B90A912727606651EF	McResetAlarmFlag - FSR Alarm Flag was reset!	McResetAlarmFlag - FSR Alarm Flag was reset!
-	Check FSR output in ground software read out from the idle frames coming from the SC.		Received ordinary FSR (LastSPI = 4; LastSN = 5)	Received ordinary FSR (LastSPI = 4; LastSN = 5)
-	Force a bad MAC error on next TC frame sent from ground to SC.			
10	Erroneous M&C Ping procedure, sent from ground to SC. Frame results in processing error on the SC and it sends an alarm FSR with the regarding flags and values set. As frame is not processed no report is sent back.	2003043400FF000400000000000000000000000000005225C7EC806407BE649F7FC5B42AF1438EA523B2B8B05DDD65D9BB561EE0DD13D1C	InvalidCipherTextException: mac check in GCM failed	InvalidCipherTextException: mac check in GCM failed

-	Check FSR output in ground software read out from the idle frames coming from the SC.		Received Alarm FSR (BadSN = 0; BadMAC = 1; InvalidSPI = 0; LastSPI = 4; LastSN = 5)	Received Alarm FSR (BadSN = 0; BadMAC = 1; InvalidSPI = 0; LastSPI = 4; LastSN = 6)
11	M&C Reset Alarm Flag procedure, sent from ground to SC. SC resets the FSR alarm flag. No report is sent back.	2003043400FF00040000000000000000000000006DA4CB93630594238B9AEF9A762673C026D791603F026984C249503DDE725908FC0	McResetAlarmFlag - FSR Alarm Flag was reset!	McResetAlarmFlag - FSR Alarm Flag was reset!
-	Check FSR output in ground software read out from the idle frames coming from the SC.		Received ordinary FSR (LastSPI = 4; LastSN = 6)	Received ordinary FSR (LastSPI = 4; LastSN = 7)
-	Force an invalid SPI error on next TC frame sent from ground to SC.			
12	Erroneous M&C Ping procedure, sent from ground to SC. Frame results in processing error on the SC and it sends an alarm FSR with the regarding flags and values set. As frame is not processed no report is sent back.	2003043400FFFFFF00000000000000000000000007E9A1A6A54029EC3242B6E09128B876F44224B2C8947DEF9FDE4081128B508AF944	SA Is Null (possible reason: Invalid SPI in Security Header)	SA Is Null (possible reason: Invalid SPI in Security Header)
-	Check FSR output in ground software read out from the idle frames coming from the SC.		Received Alarm FSR (BadSN = 0; BadMAC = 0; InvalidSPI = 1; LastSPI = 65535; LastSN = 0)	Received Alarm FSR (BadSN = 0; BadMAC = 0; InvalidSPI = 1; LastSPI = 65535; LastSN = 0)
13	M&C Reset Alarm Flag procedure, sent from ground to SC. SC resets the FSR alarm flag. No report is sent back.	2003043400FF00040000000000000000000000000866CF4D19FE6E1C850C99F2DD270FE6598B566907BE83DD26000C50113938EF5F2F	McResetAlarmFlag - FSR Alarm Flag was reset!	McResetAlarmFlag - FSR Alarm Flag was reset!
-	Check FSR output in ground software read out from the idle frames coming from the SC.		Received ordinary FSR (LastSPI = 4; LastSN = 8)	Received ordinary FSR (LastSPI = 4; LastSN = 8)

6 TEST CASE #4

The fourth interoperability test case, described in Section 6.2.1 (Main document), has the objective to exercise the key lifecycle using the SDLS EP key management procedures and to test the Over The Air Rekeying (OTAR) procedures with the key management service parameters and PDU formats specified for the SDLS EP. For this interoperability test two independently implemented systems were used, ESA on the ground side including the SDLS EPs and NASA on the spacecraft side processing these procedures and returning, if applicable, SDLS EP reports.

6.1 TEST CONFIGURATION

The following configuration is used for the test:

Keys

We set up the keys so that the keys with ID 0 to 127 are reserved for master keys and all IDs afterwards are for session keys.

ID	Hex-String-Key	State
0	000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F	ACTIVE
1	101112131415161718191A1B1C1D1E1F101112131415161718191A1B1C1D1E1F	ACTIVE
2	202122232425262728292A2B2C2D2E2F202122232425262728292A2B2C2D2E2F	ACTIVE
128	0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF	ACTIVE
129	ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789	ACTIVE
130	FEDCBA9876543210FEDCBA9876543210FEDCBA9876543210FEDCBA9876543210	ACTIVE
131	9876543210FEDCBA9876543210FEDCBA9876543210FEDCBA9876543210FEDCBA	ACTIVE
132	0123456789ABCDEFABCDEF01234567890123456789ABCDEFABCDEF0123456789	PRE_ACTIVATION
133	ABCDEF01234567890123456789ABCDEFABCDEF01234567890123456789ABCDEF	ACTIVE

134	ABCDEF0123456789FEDCBA9876543210ABCDEF0123456789FEDCBA9876543210	DEACTIVATED

SAs

All SAs, except SPI 1, are running in authenticated encryption mode share the following parameters:

- SA_length_IV = 12 octets
- SA_length_MAC = 16 octets
- SA_encryption_algorithm = AES-GCM
- SA_initialization_vector = 000000000000000000000000

SPI	SA_service_type	SA_encryption_key	State
1	Clear mode	-	ACTIVE
2	Authenticated encryption	128	KEYED
3	Authenticated encryption	129	KEYED
4	Authenticated encryption	130	KEYED
5	Authenticated encryption	131	KEYED
6	Authenticated encryption	-	UNKEYED

Mapping

All channels are mapped to SPI 1 (clear mode) for comprehensible frame output. SPI 2 is the default SA for protected TM communication, if needed. SPI 4 is the default SA for protected TC communication, if needed.

6.2 TEST PROCESS

Step	Input	Output – Expected result
1	Start both the ESA and NASA VMs and configure SC simulator, MCS and both Security Modules on NASA and ESA side.	All software should be running without problems. MCS receives TM flow from SC simulator and it in turn receives TCs.
2	Send SDLS EP via the Security Unit on ESA side.	Security Module on ESA side reports successful local execution, construction and sending of SDLS EP. The state of the Security Module has changed as expected. On an intentionally irregular SDLS EP, the Security Module should indicate the problem, not change its state and not send the SDLS EP.
3	Check the log and state of the NASA sides Security Module for successful execution and correct resulting state of the SDLS EP.	Security Module on NASA side reports successful local execution. The state of the Security Module has changed as expected. If the SDLS EP also includes a response, check for the construction and sending of it.
4	If the SDLS EP also includes a response, check the log of the ESA sides Security Module for the received response.	The response should reflect the state of the Security Module on the NASA side.

6.3 TEST RESULTS

TC/TM Nr.	Description	TC/TM	Expected Result	Actual Result

1	OTAR procedure with three new keys, sent from ground to SC. SC should add the new keys to its key repository. No report is sent back.	2003009e00ff000100001880d037008c197f0b0001008400003448 92bbc54f5395297d4c37172f2a3c46f6a81c1349e9e26ac80985d8bbd55a5814c662e49fba52f99ba09558cd21cf268b8e50b2184137e80f76122034c580464e2f06d2659a50508bdfe9e9a55990ba4148af896d8a6eebe8b5d2258685d4ce217a20174fdd4f0efac62758c51b04e55710a47209c923b641d19a39001f9e986166f5ffd95555	Key OTAR Keys recieved via master key 0: 1) Key ID = 141, 0x338ed844d3d021a84533c7e7b18c1f38 2) Key ID = 140, 0xce686f50afca2d1d102cba6b4c685a47 3) Key ID = 142, 0x055d2f7d574aa92d833114c2e2e3f66c	Key OTAR: Keys recieved via master key 0: 1) Key ID = 141, 0x338ed844d3d021a84533c7e7b18c1f38 2) Key ID = 140, 0xce686f50afca2d1d102cba6b4c685a47 3) Key ID = 142, 0x055d2f7d574aa92d833114c2e2e3f66c

2	Key Activation procedure for two keys, sent from ground to SC. SC should activate the referenced keys. No report is sent back.	2003001e00ff000100001880d038000c197f0b00020004008d008e82ebe4fc55555555	Key Activate: Key ID 141 state changed to ACTIVE Key ID 142 state changed to ACTIVE	Key Activate: Key ID 141 state changed to ACTIVE Key ID 142 state changed to ACTIVE
3	Key Deactivation procedure for one key, sent from ground to SC. SC should deactivate the referenced key. No report is sent back.	2003001c00ff000100001880d039000a197f0b00030002008e1f6d21c4555555555555	Key Deactivate Key ID 142 state changed to DEACTIVATED	Key Deactivate Key ID 142 state changed to DEACTIVATED

4	Key Verification procedure on two pre-loaded keys. SC should verify the referenced keys and compile a report.	2003003e00ff000100001880d03a002c197f0b00040024008471fc3ad5b1c36ad56bd5a5432315cdab008675c06302465bc6d5091a29957eebed35c00a6ed8	Key Verify: Key ID 132, Key ID 134	Key Verify: Key ID 132, Key ID 134
4.resp	Key Verification procedure response on the two referenced keys, sent from SC to ground. Ground displays the result of the verification.	00310202180000001001a0080ffff006084005c00840000000000000000000000001d8eaa795affaa0e951bb6cf0116192e16b1977d6723e92e01123ccef548e288500860000000000000000000000000275c47f30ca26e64af30c19ebffe0b314849133e138ac65bc2806e520a90c96a8216607ff... 01000000f844	Key 132 was verified successfully and has the stateID PRE_ACTIVATION Key 134 was verified successfully and has the stateID DEACTIVATED	Key 132 was verified successfully and has the stateID PRE_ACTIVATION Key 134 was verified successfully and has the stateID DEACTIVATED
5	Key Verification procedure on two new keys, sent from ground to SC. SC should verify the referenced keys and compile a report.	2003003e00ff000100001880d03b002c197f0b00040024008c1014b4d1f1d832e90f250289a64e641f008dc43813b784f3da70b9d9b6397464b1e9ccbe6ed8	Key Verify: Key ID 140, Key ID 141	Key Verify: Key ID 140, Key ID 141

5.resp	Key Verification procedure response on the two referenced keys, sent from SC to ground. Ground displays the result of the verification.	00310303183e0001001a0000003900000000 0000000000000000000000000000000000000000 0000000000000000000000000000000000000000 0000000000000000000000000000080ffff 006084005c008c000000000000000000000000 012fcf9ec2a0c44401c749344f6519f9b914 162833e7893f32c3ca06572d4c91ac008d00 0000000000000000000020fd3ae4cd8aa79 8d5872d152fe1dd0e6a70cc17ef4e3b3a21c a7053352fda2c18d6507ff...c00001008b2 7	Key 140 was verified successfully and has the stateID PRE_ACTIVATION Key 141 was verified successfully and has the stateID ACTIVE	Key 140 was verified successfully and has the stateID PRE_ACTIVATION Key 141 was verified successfully and has the stateID ACTIVE
6	Key Activation executed on a key in DEACTIVATED state. As this an illegal operation nothing should be sent.	none	Cannot activate Key with id 134, as it is not in the PRE_ACTIVATION state!	Cannot activate Key with id 134, as it is not in the PRE_ACTIVATION state!
7	Key Deactivation executed on a key in PRE_ACTIVATION state. As this an illegal operation nothing should be sent.	none	Cannot deactivate Key with id 140, as it is not in the ACTIVE state!	Cannot deactivate Key with id 140, as it is not in the ACTIVE state!

9	OTAR procedure with five new keys, sent from ground to SC. SC should add the new keys to its key repository. No report is sent back.	200300c000ff000100001880d03c00ae197f0b000100a60001d920aeb912ed2c79690583e398e26d111d6d6de6cf13b2dedd268848d387494c834b85288a9e608a4b089d772a35ce8f7bfd4110fdcc22cd7cccf4ba45e63746f56d281d68850d6817d93d0066d6484e9a3c9e3f5e4f2aee86a035cd215ae6fe89f2f4d7855c6966952425e5e27fa3aaec98e272c1c871cdadaf5f52f9cc33d7097d564a39d75c61edf7b6ecd7dfa7b3f78e6086a49ff8321836e614667f94a4d1b5b5cdfeed05de555555	Key OTAR Keys received via master key 1: 1) Key ID = 145, 0x7aced48ae85a8438e6c1a4dbd9acf331 2) Key ID = 146, 0x6efe5ecdf68e06474811be3b7a221b77 3) Key ID = 147, 0x543f401315f14db1d64e879bd99898f2 4) Key ID = 148, 0x4d6e6d8e4575eda4bf211c41ffd750d7	Key OTAR Keys received via master key 1: 1) Key ID = 145, 0x7aced48ae85a8438e6c1a4dbd9acf331 2) Key ID = 146, 0x6efe5ecdf68e06474811be3b7a221b77 3) Key ID = 147, 0x543f401315f14db1d64e879bd99898f2 4) Key ID = 148, 0x4d6e6d8e4575eda4bf211c41ffd750d7
11	Key Activation procedure for two keys, sent from ground to SC. SC should activate the referenced keys. No report is sent back.	2003001e00ff000100001880d03d000c197f0b00020004009200 93a8e1e4fc55555555	Key Activate Keys 146 and147 changed to state ACTIVE.	Key Activate Keys 146 and147 changed to state ACTIVE.
12	Key Deactivation procedure for one key, sent from ground to SC. SC should deactivate the referenced key. No report is sent back.	2003001c00ff000100001880d03e000a197f0b000300020093d4ba21c4555555555555	Key Deactivate Keys 147 changed to state DEACTIVATED.	Key Deactivate Keys 147 changed to state DEACTIVATED.
14	Key Verification procedure on two new keys, sent from ground to SC. SC should verify the referenced keys and compile a report.	2003003e00ff000100001880d03f002c197f0b000400240091b863da1a6ad7f71291570adc1675dfa80092419319c71e0fd243374a4a5643c119308c156ed8	Key Verify Key ID 145 was verified OK and is in the PREACTIVE state. Key ID 146 was verified OK and is in the ACTIVE state.	Key Verify Key ID 145 was verified OK and is in the PREACTIVE state. Key ID 146 was verified OK and is in the ACTIVE state.

14.resp	Key Verification procedure response on the two referenced keys, sent from SC to ground. Ground displays the result of the verification.	0031040418380001001a0000000000000000 000000000000000000000000000000000000 000000000000000000000000000000000000 00000000000000000000000000080ffff0060 84005c009100000000000000000000000109 5dd36a5c4a3e92bda5b0cfa668efe8f73b4d c959f4c1b723f00099afdb6d030092000000 000000000000000002ee333ad04d4063cdf5 f7139440f001c21ba097201aeeaa580a50b9 6e88ba727244f607ff... 010000007300	Key 145 was verified successfully and has the stateID PRE_ACTIVATION Key 146 was verified successfully and has the stateID ACTIVE	Key 145 was verified successfully and has the stateID PRE_ACTIVATION Key 146 was verified successfully and has the stateID ACTIVE
15	Key Verification procedure on two new keys, sent from ground to SC. SC should verify the referenced keys and compile a report.	2003003e00ff000100001880d040002c197f 0b000400240093ada7b7137f61300912abb4 9b45d931470094253cb5cdaa4b3d044db127 37bc0f221106bb6ed8	Key Verify Key ID 147 was verified OK and is in the PREACTIVE state. Key ID 148 was verified OK and is in the ACTIVE state.	Key Verify Key ID 147 was verified OK and is in the PREACTIVE state. Key ID 148 was verified OK and is in the ACTIVE state.
15.resp	Key Verification procedure response on the two referenced keys, sent from SC to ground. Ground displays the result of the verification.	0031050518360001001a0000000000000000 000000000000000000000000000000000000 000000000000000000000000000000000000 000000000000000000000080ffff00608400 5c00930000000000000000000000001acae8f eba6b45eece52a7f1de280f56ed3a0ae6de6 3d317a387e726c0094460a00940000000000 0000000000000252927b593ab5cadcc38662 ace78dfaeb6a3df4c3472b4f2ac9a982aecf 2a0e25753907ff... c000010012fd	Key 147 was verified successfully and has the stateID PRE_ACTIVATION Key 148 was verified successfully and has the stateID ACTIVE	Key 147 was verified successfully and has the stateID PRE_ACTIVATION Key 148 was verified successfully and has the stateID ACTIVE

16	OTAR procedure with four new keys, sent from ground to SC. SC should add the new keys to its key repository. No report is sent back.	200300c000ff000100001880d04100ae197f0b000100a60002f1e37102f68dcbbba2dce280c9ac4ad7d47803d1c50573054523cdb033e4f9b3149178e8bc34bbd318ee1b82c865b40b195b833389d50a6a64485a3e3f1abf4ec824432b765ce3d82c84a62d98a699a47a3efb37fa04cd982ce0eea11bd6bfc4e5b2300d478da25246961ed4087635d9695155e3a71089d87d2f2df052202700b949d2635823a78bd50bf19145afeb875ea1f995f3d1d3a171d5a61bc92a2060a6f94f05787f05de555555	Key OTAR Keys received via master key 2: 1) Key ID = 152, 0x60d43c0555953a82258fc5801d8db4fa 2) Key ID = 153, 0xcf0e3a5e0ec0e213ef3837424fb580fc 3) Key ID = 150, 0xe8fd005dbe9cc8be447bd7203d4a5674 4) Key ID = 151, 0x66bd1d2e822a598bfc149bebcae7eaf3	Key OTAR Keys received via master key 2: 1) Key ID = 152, 0x60d43c0555953a82258fc5801d8db4fa 2) Key ID = 153, 0xcf0e3a5e0ec0e213ef3837424fb580fc 3) Key ID = 150, 0xe8fd005dbe9cc8be447bd7203d4a5674 4) Key ID = 151, 0x66bd1d2e822a598bfc149bebcae7eaf3
17	Key Activation procedure for three keys, sent from ground to SC. SC should activate the referenced keys. No report is sent back.	2003002000ff000100001880d042000e197f0b000200060097009800 99bee3a61a5555	Key Activate Keys 151, 152, and 153 changed to state ACTIVE.	Key Activate Keys 151, 152, and 153 changed to state ACTIVE.
18	Key Deactivation procedure for two keys, sent from ground to SC. SC should deactivate the referenced key. No report is sent back.	2003001e00ff000100001880d043000c197f0b0003000400980099e680e4fc55555555	Key Deactivate Keys 152, and 153 changed to state DEACTIVATED.	Key Deactivate Keys 152, and 153 changed to state DEACTIVATED.
20	Key Verification procedure on two new keys, sent from ground to SC. SC should verify the referenced keys and compile a report.	2003003e00ff000100001880d044002c197f0b000400240096a785a1801728d57ea5d7da6d4db309730097db2e5b1fb393a402d9c8b3a6edcc562d33b66ed8	Key Verify Key ID 150 was verified OK and is in the PREACTIVE state. Key ID 151 was verified OK and is in the ACTIVE state.	Key Verify Key ID 150 was verified OK and is in the PREACTIVE state. Key ID 151 was verified OK and is in the ACTIVE state.

20.resp	Key Verification procedure response on the two referenced keys, sent from SC to ground. Ground displays the result of the verification.	0031060618340001001a0000000000000000 000000000000000000000000000000000000 000000000000000000000000000000000000 00000000000000000080ffff006084005c00 960000000000000000000000000176316dbb82 60d96a20b37b57620e28915f56906a68ef8a 8cb0b1a9d9adec8168009700000000000000 00000000028eb7575fb226ad4699ab2cc3f8 2a3ee62ab5e45825ee9913df10b46abd6808 34296a07ff...010000005fdb	Key 150 was verified successfully and has the stateID PRE_ACTIVATION Key 151 was verified successfully and has the stateID ACTIVE	Key 150 was verified successfully and has the stateID PRE_ACTIVATION Key 151 was verified successfully and has the stateID ACTIVE
-	Intentional corruption of a key on board the SC.		User Modify Key Key 152 CRC invalidated!	User Modify Key Key 152 CRC invalidated!
21	Key Verification procedure on two new keys, sent from ground to SC. SC should verify the referenced keys and compile a report.	2003003e00ff000100001880d045002c197f 0b00040024009894a2b915a3154520df52ed ad8ac1acc00099dc09bd6bf7e43f1dc0d44c 08bc8b63084f526ed8	Key Verify Key ID 152 was verified NOT OK and is in the CORRUPTED state. Key ID 153 was verified OK and is in the DESTROYED state.	Key Verify Key ID 152 was verified NOT OK and is in the CORRUPTED state. Key ID 153 was verified OK and is in the DESTROYED state.
21.resp	Key Verification procedure response on the four referenced keys, sent from SC to ground. Ground displays the result of the verification.	0031070718320001001a0000000000000000 000000000000000000000000000000000000 000000000000000000000000000000000000 0000000000000080ffff006084005c009800 0000000000000000000001f637d1ea1932e9 8c1e02ecb2f17310b75552aabf78cc850778 5ff28aadc6678d0099000000000000000000 000002367f0df5816231ae79b7b7f4281ede c346410c7bc9dfed3291b96e5ba55c123d97 ff07ff... c0000100ec09	Key 152 failed to verify and has the stateID CORRUPTED Key 153 was verified successfully and has the stateID DESTROYED	Key 152 failed to verify and has the stateID CORRUPTED Key 153 was verified successfully and has the stateID DESTROYED

-	Intentional corruption of four keys on board the SC.		User Modify Key Key 150 CRC invalidated! Key 151 CRC invalidated!	User Modify Key Key 150 CRC invalidated! Key 151 CRC invalidated!
25	Key Verification procedure on four new keys, sent from ground to SC. SC should verify the referenced keys and compile a report.	2003003e00ff000100001880d047002c197f 0b0004002400969964112b3621b6b136b51b 1dc01da23b0097cdf1bb3b4d10fffcae9fac 40caefae52fee56ed8	Key Verify Key ID 150 was verified NOT OK and is in the CORRUPTED state. Key ID 151 was verified NOT OK and is in the CORRUPTED state.	Key Verify Key ID 150 was verified NOT OK and is in the CORRUPTED state. Key ID 151 was verified NOT OK and is in the CORRUPTED state.
25.resp	Key Verification procedure response on the four referenced keys, sent from SC to ground. Ground displays the result of the verification. The corrupted keys should be marked as such.	00310909182e0001001a0000000000000000 000000000000000000000000000000000000 000000000000000000000000000000000000 00000080ffff006084005c00960000000000 0000000000000119d2aff46ff28b194ddcc6 7d6c0126f794ddf80120517fad23c2040aac e7754d009700000000000000000000000028b 90f89f963b6bc79123cc54fca7772d0cbf1c 670bfadd54adbe34b268e40fd1d89c07ff.. .c00001007e98	Key 150 failed to verify and has the stateID CORRUPTED Key 151 failed to verify and has the stateID CORRUPTED	Key 150 failed to verify and has the stateID CORRUPTED Key 151 failed to verify and has the stateID CORRUPTED

7 TEST CASE #5

The fifth test case, described in Section 6.2.2 (main document), exercises the complete SA lifecycle using all the SDLS EP SA management procedures. The SLDS EP protocol is validated by using the length parameters of the baseline mode – defined in annex E of the SDLS EP recommendation [4]. For this interoperability test two independently implemented systems were used, ESA on the ground side inducing the SDLS EPs and NASA on the space side processing these procedures and returning, if applicable, SDLS EP reports.

7.1 TEST CONFIGURATION

The following configuration is used for the test:

Keys

We set up the keys so that the keys with ID 0 to 127 are reserved for master keys and all IDs afterwards are for session keys.

ID	Hex-String-Key	State
0	000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F	ACTIVE
1	101112131415161718191A1B1C1D1E1F101112131415161718191A1B1C1D1E1F	ACTIVE
2	202122232425262728292A2B2C2D2E2F202122232425262728292A2B2C2D2E2F	ACTIVE
128	0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF	ACTIVE
129	ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789	ACTIVE
130	FEDCBA9876543210FEDCBA9876543210FEDCBA9876543210FEDCBA9876543210	ACTIVE
131	9876543210FEDCBA9876543210FEDCBA9876543210FEDCBA9876543210FEDCBA	ACTIVE
132	0123456789ABCDEFABCDEF01234567890123456789ABCDEFABCDEF0123456789	PRE_ACTIVATION
133	ABCDEF012345678901234567 89ABCDEFABCDEF0123456789012345 6789ABCDEF	ACTIVE

134	ABCDEF0123456789FEDCBA9876543210ABCDEF0123456789FEDCBA9876543210	DEACTIVATED

SAs

All SAs, except SPI 1, are running in authenticated encryption mode share the following parameters:

- SA_length_IV = 12
- SA_length_MAC = 16
- SA_encryption_algorithm = AES-GCM
- SA_initialization_vector = 000000000000000000000000

SPI	SA_service_type	SA_encryption_key	State
1	Clear mode	-	ACTIVE
2	Authenticated encryption	128	KEYED
3	Authenticated encryption	129	KEYED
4	Authenticated encryption	130	KEYED
5	Authenticated encryption	131	KEYED
6	Authenticated encryption	-	UNKEYED

Mapping

All channels are mapped to SPI 1 (clear mode) for comprehensible frame output. SPI 2 is the default SA for protected TM communication, if needed. SPI 4 is the default SA for protected TC communication, if needed.

7.2 TEST PROCESS

Step	Input	Output – Expected result
1	Start all the end-to-end space communication VMs and configure SC simulator, Ground Station software, MCS and both Security Units on SC and MCS side.	All software should be running without problems. MCS receives TM flow from SC simulator and it in turn receives TCs.
2	Send SDLS EP via the Security Unit on MCS side.	Security Unit on MCS side reports successful local execution, construction and sending of SDLS EP. The state of the Security Unit has changed as expected. On an intentionally irregular SDLS EP, the Security Unit should indicate the problem, not change its state and not send the SDLS EP.
3	Check the log and state of the SC sides Security Unit for successful execution and correct resulting state of the SDLS EP.	Security Unit on SC side reports successful local execution. The state of the Security Unit has changed as expected. If the SDLS EP also includes a response, check for the construction and sending of it.
4	If the SDLS EP also includes a response, check the log of the MCS side Security Unit for the received response.	The response should reflect the state of the Security Unit on the SC side.

7.3 TEST RESULTS

TC/TM Nr.	Description	Received TC/TM	Expected Result	Actual Result
8	Rekey SA procedure on the newly created SA with a preloaded and ACTIVE key, sent from ground to SC. SC should assign the key to the SA and set it to KEYED state. No report is sent back.	2003002a00ff000100001880d0ac0018197f0b0016000c000600850000000000000000000000000da959fc8555555555555	SA Rekey SPI 6 changed to KEYED state with encrypted Key ID 133.	SA Rekey SPI 6 changed to KEYED state with encrypted Key ID 133.
9	Start SA procedure on the new SA on the VC 1 on the TC side, sent from ground to SC. SC should map the SA to the given channel and set the SA to OPERATIONAL state. No report is sent back.	2003002000ff000100001880d0ad000e197f0b001b000400060000 3040f6f7a61a5555	SA Start SPI 6 changed to OPERATIONAL state. Type TC, VCID = 0x000001	SA Start SPI 6 changed to OPERATIONAL state. Type TC, VCID = 0x000001
-	Switch currently used TC channel to VC 1 to use the new SA for TCs.		Changed used VC for TC to 1	Changed used VC for TC to 1
10	Execute M&C Ping procedure to test new secure channel on new SA, sent from ground to SC. SC should be able to decrypt message and send a report back.	2003043400ff000600000000000000000000000000121e8cb55734ac14b895b5145793ab5dd25ab112b4c5f7b99d905051102a9e132c3555555	MC Ping	MC Ping
10.resp	M&C Ping procedure response. Ground displays the pong message.	00310202180000001001a0080ffff0004b10000404307ff…010000009d6d	McPingResp - received PONG	McPingResp - received PONG
11	Execute M&C Ping procedure to test new secure channel on new SA, sent from ground to SC. SC should be able to decrypt message and send a report back.	2003043400ff000600000000000000000000000002b3105fd60b1fdb72496c8ce203ce9b2eabb8bfc4527c479319b7cad9899d15b5ed555555	MC Ping	MC Ping

11.resp	M&C Ping procedure response, sent from SC to ground. Ground displays the pong message.	0031030318220001001a0000000000000000 000000000000000000000000000000000000 00000000000000000080ffff0004b1000040 4307ff…c00006023aa7	McPingResp - received PONG	McPingResp - received PONG
-	Switch currently used TC channel to VC 0 to go back to clear mode.		Changed used VC for TC to 0	Changed used VC for TC to 0
12	SA Read SN procedure on the new SA to get current IV value as a reference, sent from ground to SC. SC sends back report containing the current value of the IV.	2003001c00ff000100001880d0b0000a197f 0b001000020006571921c4555555555555	SA Read Sequence Number spi = 6 SN = 0x0000000000000002	SA Read Sequence Number spi = 6 SN = 0x0000000000000002
12.resp	SA Read SN procedure response, sent from SC to ground. Ground displays the expected IV value.	0031040418040001001a000000000080ffff 001290000e000600000000000000000000000 021ae507ff…0100000082da	SaReadSnResp - was parsed! SN is: 2	SaReadSnResp - was parsed! SN is: 2
13	Set ARSN procedure on the new SA, sent from ground to SC. SC sets the IV of the new SA to the given value. No report is sent back.	2003002800ff000100001880d0b10016197f 0b001a000a000600000000000000000000000 6413b5983e55	SA SetARSN spi = 6 IV updated to: 0x0000000000000064	SA SetARSN spi = 6 IV updated to: 0x0000000000000064
14	SA Read SN procedure on the new SA to get current IV value as a reference, sent from ground to SC. SC sends back report containing the current value of the IV.	2003001c00ff000100001880d0b2000a197f 0b00100002000651f321c4555555555555	SA Read Sequence Number spi = 6 SN = 0x0000000000000064	SA Read Sequence Number spi = 6 SN = 0x0000000000000064

14.resp	SA Read SN procedure response, sent from SC to ground. Ground displays the expected IV value.	0031050518340001001a0000000000000000 000000000000000000000000000000000000 000000000000000000000000000000000000 00000000000000000080ffff001290000e00 060000000000000000000000064168507ff…c 0000102d685	SaReadSnResp - was parsed! SN is: 100	SaReadSnResp - was parsed! SN is: 100
-	Switch currently used TC channel to VC 1 to use the new SA for TCs.		Changed used VC for TC to 1	Changed used VC for TC to 1
15	Execute M&C Ping procedure to test new secure channel on new SA, sent from ground to SC. SC should be able to decrypt message and send a report back.	2003043400ff000600000000000000000000 00656cbe97c866d9015ab1f747510b19ccef 0376ca22becfeb3968179af7dc364f6ded55 5555	MC Ping	MC Ping
15.resp	M&C Ping procedure response. Ground displays the pong message.	0031060618240001001a0000000000000000 000000000000000000000000000000000000 000000000000000000000080ffff0004b100 00404307ff…01000000f46a	McPingResp - received PONG	McPingResp - received PONG
16	Execute M&C Ping procedure to test new secure channel on new SA, sent from ground to SC. SC should be able to decrypt message and send a report back.	2003043400ff000600000000000000000000 0066fa191521e27cb4d95b5c2b5f43ebe7a0 ee0c400f1af632186bfb26a6900bedae4a55 5555	MC Ping	MC Ping
16.resp	M&C Ping procedure response. Ground displays the pong message.	0031070718060001001a0000000000000080 ffff0004b10000404307ff…c00006669b93	McPingResp - received PONG	McPingResp - received PONG
-	Switch currently used TC channel to VC 0 to go back to clear mode.		Changed used VC for TC to 0	Changed used VC for TC to 0

17	SA Read SN procedure on the new SA to get current IV value as a reference, sent from ground to SC. SC sends back report containing the current value of the IV.	2003001c00ff000100001880d0b5000a197f0b00100002000659b821c4555555555555	SA Read Sequence Number spi = 6 SN = 0x0000000000000066	SA Read Sequence Number spi = 6 SN = 0x0000000000000066
17.resp	SA Read SN procedure response, sent from SC to ground. Ground displays the expected IV value.	00310808182800010001a0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000080ffff001290000e000600000000000000000000000006636c707ff…010000000542	SaReadSnResp - was parsed! SN is: 102	SaReadSnResp - was parsed! SN is: 102
31	Stop SA procedure on the new SA, sent from ground to SC. SC should un-map the SA on all assigned channels and set the SA to KEYED state. No report is sent back.	2003001c00ff000100001880d0b6000a197f0b001e00020006938f21c4555555555555	SA Stop SPI 15 changed to KEYED state.	SA Stop SPI 15 changed to KEYED state.
32	Expire SA procedure on the new SA, sent from ground to SC. SC should unload the key from the given SA and set the SA to UNKEYED state. No report is sent back.	2003001c00ff000100001880d0b7000a197f0b0019000200006f72e21c4555555555555	SA Expire SPI 15 changed to UNKEYED state.	SA Expire SPI 15 changed to UNKEYED state.

8 TEST CASE #6

The sixth interoperability test case, described in Section 6.2.3 (main document), has the objective to execute all the Monitoring & Control procedures and their specified PDU formats as well as testing the FSR functionality. To test the FSR functionality a protected channel is set up and the SecurityUnit is capable of inducing deliberate security errors, e.g. simulating a replay attack by using the same SN twice. For this interoperability test two independently implemented systems were used, ESA on the ground side including the SDLS EPs and NASA on the space side processing these procedures and returning, if applicable, SDLS EP reports. The space side also supplies the FSR report on every second TM frame to be read out by the ground software.

8.1 TEST CONFIGURATION

The following configuration is used for the test:

Keys

We set up the keys so that the keys with ID 0 to 127 are reserved for master keys and all IDs afterwards are for session keys.

ID	Hex-String-Key	State
0	000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F	ACTIVE
1	101112131415161718191A1B1C1D1E1F101112131415161718191A1B1C1D1E1F	ACTIVE
2	202122232425262728292A2B2C2D2E2F202122232425262728292A2B2C2D2E2F	ACTIVE
128	0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF	ACTIVE
129	ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789	ACTIVE
130	FEDCBA9876543210FEDCBA9876543210FEDCBA9876543210FEDCBA9876543210	ACTIVE
131	9876543210FEDCBA9876543210FEDCBA9876543210FEDCBA9876543210FEDCBA	ACTIVE
132	0123456789ABCDEFABCDEF01234567890123456789ABCDEFABCDEF0123456789	PRE_ACTIVATION

133	ABCDEF01234567890123456789ABCDEFABCDEF0123456789012345678 9ABCDEF	ACTIVE
134	ABCDEF0123456789FEDCBA9876543210ABCDEF0123456789FEDCBA9876543210	DEACTIVATED

SAs

All SAs, except SPI 1, are running in authenticated encryption mode share the following parameters:

- SA_length_IV = 12 octets
- SA_length_MAC = 16 octets
- SA_encryption_algorithm = AES-GCM
- SA_initialization_vector = 000000000000000000000000

SPI	SA_service_type	SA_encryption_key	State
1	Clear mode	-	ACTIVE
2	Authenticated encryption	128	KEYED
3	Authenticated encryption	129	KEYED
4	Authenticated encryption	130	KEYED
5	Authenticated encryption	131	KEYED
6	Authenticated encryption	-	UNKEYED

Mapping

All channels are mapped to SPI 1 (clear mode) for comprehensible frame output. SPI 2 is the default SA for protected TM communication, if needed. SPI 4 is the default SA for protected TC communication, if needed.

8.2 TEST PROCESS

Step	Input	Output – Expected result
1	Start both the ESA and NASA VMs and configure SC simulator, MCS and both Security Modules on NASA and ESA side.	All software should be running without problems. MCS receives TM flow from SC simulator and it in turn receives TCs.
2	Send SDLS EP via the Security Unit on ESA side.	Security Module on ESA side reports successful local execution, construction and sending of SDLS EP. The state of the Security Module has changed as expected. On an intentionally irregular SDLS EP, the Security Module should indicate the problem, not change its state and not send the SDLS EP.
3	Check the log and state of the NASA sides Security Module for successful execution and correct resulting state of the SDLS EP.	Security Module on NASA side reports successful local execution. The state of the Security Module has changed as expected. If the SDLS EP also includes a response, check for the construction and sending of it.
4	If the SDLS EP also includes a response, check the log of the ESA sides Security Module for the received response.	The response should reflect the state of the Security Module on the NASA side.

8.3 TEST RESULTS

TC/TM Nr.	Description	TC/TM	Expected Result	Actual Result
1	M&C Ping procedure, sent from ground to SC. SC sends a pong report back.	2003001a00ff000100001880d2c70008197f0b00310000b1fe312855	MC Ping	MC Ping
1.resp	M&C Ping procedure response, sent from SC to ground. Ground displays the pong message.	00310202180000001001a0080ffff0004b10000404307ff...010000009d6d	McPingResp - received PONG	McPingResp - received PONG
2	M&C Ping procedure, sent from ground to SC. SC sends a pong report back.	2003001a00ff000100001880d2c80008197f0b00310000e74f312855	MC Ping	MC Ping
2.resp	M&C Ping procedure response, sent from SC to ground. Ground displays the pong message.	00310303182200010001a0000000000000000000000000000000000000000000000000000000000000000000000000000000000080ffff0004b10000404307ff...c0000100d955	McPingResp - received PONG	McPingResp - received PONG
12	Start SA procedure on preloaded SA on the VC 1 on the TC side, sent from ground to SC. SC should map the SA to the given channel and set the SA to OPERATIONAL state. No report is sent back.	2003002000ff000100001880d2c9000e197f0b001b00040004000030040d95ea61a5555	SA Start SPI 4 changed to OPERATIONAL state. Type TC, VCID = 0x000001	SA Start SPI 4 changed to OPERATIONAL state. Type TC, VCID = 0x000001
-	Switch currently used TC channel to VC 1 to use a secure channel for TCs in preparation for the forced error testing.			
13	M&C Ping procedure, sent from ground to SC. SC sends a pong report back.	2003043400ff000400000000000000000000000017e1d8eea8d45ceba17888e0cdcd74797f2db4e6521fbbe3e8738b72bcdea797c7a555555	MC Ping	MC Ping

13.resp	M&C Ping procedure response, sent from SC to ground. Ground displays the pong message.	00310404180400010001a000000000080ffff0004b10000404307ff…01000000c435	McPingResp - received PONG	McPingResp - received PONG
14	M&C Ping procedure, sent from ground to SC. SC sends a pong report back.	2003043400ff000400000000000000000000000000219c6efd6cd012f28eb9f38c49e7669bb6af19abfb95b6627f7bafb4596a3e178a2555555	MC Ping	MC Ping
14.resp	M&C Ping procedure response, sent from SC to ground. Ground displays the pong message.	00310505182600010001a0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000080ffff0004b10000404307ff…c00004023951	McPingResp - received PONG	McPingResp - received PONG
-	Check FSR output in ground software read out from the idle frames coming from the SC.		Received ordinary FSR (LastSPI = 4; LastSN = 2)	Received ordinary FSR (LastSPI = 4; LastSN = 2)
-	Force a replay error on next TC frame sent from ground to SC.			
15	Erroneous M&C Ping procedure, sent from ground to SC. Frame results in processing error on the SC and it sends an alarm FSR with the regarding flags and values set. As frame is not processed no report is sent back.	2003043400ff000400000000000000000000000000219c6efd1cd012f28eb9f38c49e6a93c47958d3525b0aec899dd33fe1d0a7b97435555555	Error: IV not in window!	Error: IV not in window!
-	Check FSR output in ground software read out from the idle frames coming from the SC.		Received Alarm FSR (BadSN = 1; BadMAC = 0; InvalidSPI = 0; LastSPI = 4; LastSN = 2)	Received Alarm FSR (BadSN = 1; BadMAC = 0; InvalidSPI = 0; LastSPI = 4; LastSN = 2)

16	M&C Reset Alarm Flag procedure, sent from ground to SC. SC resets the FSR alarm flag. No report is sent back.	2003043400ff000400000000000000000000000035f07569e58aa0ca2ee993146a467b8e242d504a647ce56d0a3e4c0c613bdc7c588555555	MC Reset Alarm	MC Reset Alarm
-	Check FSR output in ground software read out from the idle frames coming from the SC.		Received ordinary FSR (LastSPI = 4; LastSN = 3)	Received ordinary FSR (LastSPI = 4; LastSN = 3)
-	Force an out of bounds error on next TC frame sent from ground to SC.			
17	Erroneous M&C Ping procedure, sent from ground to SC. Frame results in processing error on the SC and it sends an alarm FSR with the regarding flags and values set. As frame is not processed no report is sent back.	2003043400ff000400000000000000000000000000435d72650fa856512540e82a00668d8c68c90f418166c6693c95f3e370a1bd875ff555555	Error: IV not in window!	Error: IV not in window!
-	Check FSR output in ground software read out from the idle frames coming from the SC.		Received Alarm FSR (BadSN = 1; BadMAC = 0; InvalidSPI = 0; LastSPI = 4; LastSN = 9)	Received Alarm FSR (BadSN = 1; BadMAC = 0; InvalidSPI = 0; LastSPI = 4; LastSN = 9)
18	M&C Reset Alarm Flag procedure, sent from ground to SC. SC resets the FSR alarm flag. No report is sent back.	2003043400ff000400000000000000000000000006ba5b389a7bb28e0fca8aea45e6a74b5f2dd79d8e9bd585e53ebed302f14e6d154c555555	MC Reset Alarm	MC Reset Alarm
-	Check FSR output in ground software read out from the idle frames coming from the SC.		Received ordinary FSR (LastSPI = 4; LastSN = 4)	Received ordinary FSR (LastSPI = 4; LastSN = 4)
-	Force a bad MAC error on next TC frame sent from ground to SC.			

19	Erroneous M&C Ping procedure, sent from ground to SC. Frame results in processing error on the SC and it sends an alarm FSR with the regarding flags and values set. As frame is not processed no report is sent back.	2003043400ff000400000000000000000000000000c79ebc6ca752b40c56ecef6cda30c7ca0b1968c3bfd28b786f754b0420be7d5ef6b555555	Error: ITC_GCM128_BAD_TAG	Error: ITC_GCM128_BAD_TAG
-	Check FSR output in ground software read out from the idle frames coming from the SC.		Received Alarm FSR (BadSN = 0; BadMAC = 1; InvalidSPI = 0; LastSPI = 4; LastSN = 5)	Received Alarm FSR (BadSN = 0; BadMAC = 1; InvalidSPI = 0; LastSPI = 4; LastSN = 5)
20	M&C Reset Alarm Flag procedure, sent from ground to SC. SC resets the FSR alarm flag. No report is sent back.	2003043400ff000400000006000000000000000079776af36c8eb72afa1c53b7d19d1a486d0cf5df09b6bbad0c2f5e208e45090b13e555555	MC Reset Alarm	MC Reset Alarm
-	Check FSR output in ground software read out from the idle frames coming from the SC.		Received ordinary FSR (LastSPI = 4; LastSN = 6)	Received ordinary FSR (LastSPI = 4; LastSN = 6)
-	Force an invalid SPI error on next TC frame sent from ground to SC.			
21	Erroneous M&C Ping procedure, sent from ground to SC. Frame results in processing error on the SC and it sends an alarm FSR with the regarding flags and values set. As frame is not processed no report is sent back.	2003043400ff000400000000000000000000000000c79ebc6ca752b40c56ecef6cda30c7ca0b1968c3bfd28b786f754b0420be7d5ef6b555555	Error: SPI invalid!	Error: SPI invalid!
-	Check FSR output in ground software read out from the idle frames coming from the SC.		Received Alarm FSR (BadSN = 0; BadMAC = 0; InvalidSPI = 1; LastSPI = 65535; LastSN = 0)	Received Alarm FSR (BadSN = 0; BadMAC = 0; InvalidSPI = 1; LastSPI = 65535; LastSN = 0)

22	M&C Reset Alarm Flag procedure, sent from ground to SC. SC resets the FSR alarm flag. No report is sent back.	2003043400ff0004000000000000000000000007ba5b389a7bb28e0fca8aea45e6a74b5f2dd79d8e9bd585e53ebed302f14e6d154c555555	MC Reset Alarm	MC Reset Alarm
-	Check FSR output in ground software read out from the idle frames coming from the SC.		Received ordinary FSR (LastSPI = 4; LastSN = 9)	Received ordinary FSR (LastSPI = 4; LastSN = 9)