

Report Concerning Space Data System Standards

|  |
| --- |
| SDLS Extended Procedures –  concept and rationale |

Draft Informational Report

Draft Green Book

AUTHORITY

|  |  |  |  |
| --- | --- | --- | --- |
|  | | | |
|  | Issue: |  |  |
|  | Date: |  |  |
|  | Location: | Not Applicable |  |
|  | | | |

**(WHEN THIS INFORMATIONAL REPORT IS FINALIZED, IT WILL CONTAIN THE FOLLOWING STATEMENT OF AUTHORITY:)**

This document has been approved for publication by the Management Council of the Consultative Committee for Space Data Systems (CCSDS) and reflects the consensus of technical panel experts from CCSDS Member Agencies. The procedure for review and authorization of CCSDS Reports is detailed in *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-4).

This document is published and maintained by:

CCSDS Secretariat

Space Communications and Navigation Office, 7L70

Space Operations Mission Directorate

NASA Headquarters

Washington, DC 20546-0001, USA

FOREWORD

This document is a CCSDS Report, which contains background, rationale and a concept of operation to support the CCSDS Recommended Standard on the Space Data Link Security Protocol (reference [1]).

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 *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-4). Current versions of CCSDS documents are maintained at the CCSDS Web site:

http://www.ccsds.org/

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

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

Member Agencies

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

Observer Agencies

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

DOCUMENT CONTROL

|  |  |  |  |
| --- | --- | --- | --- |
| **Document** | **Title and Issue** | **Date** | **Status** |
|  | Space Data Link Security (SDLS) Extended Procedures –  Concept and Rationale,  , |  | First draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

CONTENTS

Section Page

[DOCUMENT CONTROL iii](#_Toc509932636)

[CONTENTS v](#_Toc509932637)

[1 Introduction 1-1](#_Toc509932638)

[1.1 purpose 1-1](#_Toc509932639)

[1.2 scope 1-1](#_Toc509932640)

[1.3 organization of this report 1-2](#_Toc509932641)

[1.4 conventions and definitions 1-2](#_Toc509932642)

[1.5 References 1-2](#_Toc509932643)

[2 Overview and Rationale 2-4](#_Toc509932644)

[2.1 SDLS and Extended Procedures 2-4](#_Toc509932645)

[2.2 design goals and constraints 2-4](#_Toc509932646)

[2.2.1 compatibility with sdl services 2-4](#_Toc509932647)

[2.2.2 requirements 2-4](#_Toc509932648)

[2.3 Key Management 2-5](#_Toc509932649)

[2.3.1 Justification 2-5](#_Toc509932650)

[2.3.2 Summary of capabilities 2-5](#_Toc509932651)

[2.4 Security Association (SA) Management 2-5](#_Toc509932652)

[2.4.1 Justification 2-5](#_Toc509932653)

[2.4.2 Summary of capabilities 2-7](#_Toc509932654)

[2.5 Security Unit Monitoring & Control 2-8](#_Toc509932655)

[2.5.1 Justification 2-8](#_Toc509932656)

[2.5.2 Summary of capabilities 2-8](#_Toc509932657)

[2.6 Frame Security Report (FSR) 2-8](#_Toc509932658)

[2.6.1 Justification 2-8](#_Toc509932659)

[2.6.2 Summary of capabilities 2-8](#_Toc509932660)

[2.6.3 Relation to space link protocols 2-8](#_Toc509932661)

[3 Concept of Operation 3-9](#_Toc509932662)

[3.1 Key Management 3-9](#_Toc509932663)

[3.1.1 Refer to the KM Green Book (includes key lifetime, …) 3-9](#_Toc509932664)

[3.1.2 Illustrate key change scenarios (including OTAR, key verification, key change ‘on the fly’ from frame to frame) 3-9](#_Toc509932665)

[3.1.3 Contingency and off nominal scenarios 3-9](#_Toc509932666)

[3.1.4 Master keys versus session keys 3-9](#_Toc509932667)

[3.2 Security Association Management 3-9](#_Toc509932668)

[3.2.1 Guidelines on planning & assigning Security Associations 3-9](#_Toc509932669)

[3.2.2 Normal procedures for SA management 3-9](#_Toc509932670)

[3.2.3 Implementing SA life cycle with the EP procedures 3-10](#_Toc509932671)

[3.2.4 Contingency and off-nominal scenarios 3-10](#_Toc509932672)

[3.2.5 Seamless key change (from frame to frame) 3-10](#_Toc509932673)

[3.2.6 How to handle redundancy (e.g. : reconfiguring redundant command chain using nominal one, logical cross-strapping, …) 3-10](#_Toc509932674)

[3.3 Security Unit Monitoring & Control 3-10](#_Toc509932675)

[3.3.1 Illustrate nominal procedures for Security Unit M&C 3-10](#_Toc509932676)

[3.3.2 Contingency and off nominal scenarios (using ping, self-test, …) 3-10](#_Toc509932677)

[3.3.3 Rationale, definition and usage of Security Logs 3-10](#_Toc509932678)

[3.3.4 Discussion of self-test (e.g. known answer test (KAT), …) 3-10](#_Toc509932679)

[3.4 Frame Security Report (FSR) 3-11](#_Toc509932680)

[3.4.1 Operating FSR together with Space Link Protocols (alternating CLCW/FSR, …) 3-11](#_Toc509932681)

[3.4.2 How to interpret the flags including the alarm flag (persistant) 3-11](#_Toc509932682)

[3.4.3 Concept of operations for handling alarm flags (e.g.: discriminating transmission problems from security events/attacks, using FSR as a first stage in troubleshooting on the link, …) 3-11](#_Toc509932683)

[3.5 Various types of implementation 3-11](#_Toc509932684)

[3.5.1 Fixed keys, OTAR, dynamic management of SA vs static 3-11](#_Toc509932685)

[3.5.2 EP PDU on-board path/processing (illustrate the different types of on-board architectures, in-band vs out of band signaling, implications of routing EP PDUs in OBC, …) 3-11](#_Toc509932686)

[4 design concepts 4-12](#_Toc509932687)

[4.1 security services selection 4-12](#_Toc509932688)

[4.1.1 threat analysis 4-12](#_Toc509932689)

[4.1.2 baseline security services 4-12](#_Toc509932690)

[4.2 protocol data structures, fields and functions 4-12](#_Toc509932691)

[4.2.1 security header 4-12](#_Toc509932692)

[4.3 protocol management 4-12](#_Toc509932693)

[4.3.1 security association 4-12](#_Toc509932694)

[4.3.2 signaling, monitoring and control 4-12](#_Toc509932695)

[4.3.3 redundancy 4-14](#_Toc509932696)

[4.3.4 cryptographic keys 4-15](#_Toc509932697)

[5 concept of operation 5-16](#_Toc509932698)

[5.1 security association 5-16](#_Toc509932699)

[5.2 generic operation 5-16](#_Toc509932700)

[5.3 synchronization 5-17](#_Toc509932701)

[5.3.1 cryptographic key synchronization 5-17](#_Toc509932702)

[5.3.2 sequence count synchronization 5-18](#_Toc509932703)

[5.4 scenarios 5-18](#_Toc509932704)

# Introduction

## purpose

This Report has been developed to present the concept and rationale of the CCSDS Recommended Standard on the Space Data Link Security Protocol Extended Procedures []. This Green Book will enable mission designers and protocol implementers to:

1. Understand the purpose and usage of the SDLS Extended Procedures;
2. Select appropriate procedures and parameters for the mission;
3. Cover nominal and contingency scenarios;
4. Understand the performance and limitations of the Extended Procedures.

The Space Data Link Security (SDLS) Protocol [1] is a security protocol that implements user-selected Security Services to the data transported by the Space Data Link (SDL) protocol in space-to-ground and ground-to-space links. The SDLS protects the Service Data Units transported by the SDL protocol and, in addition, selected SDL protocol data structures taking into account compatibility constraints with SDL and Space Link Extension services.

The Recommended Standard for SDLS Extended Procedures [2] extends the core SDLS protocol with services for managing the security parameters of the space link. The purpose of SDLS Extended Procedures (EP) is to provide a standardized set of auxiliary services for managing an implementation of the SDLS protocol. These EP services are categorized into Key Management, Security Association (SA) Management, and SDLS Monitoring & Control. Further, [2] specifies service interfaces and data structures for transport of EP service messages within the Space Data Link (SDL) protocols along with a security unit status reporting mechanism.

SDLS Extended Procedures encompass well-known but however complex procedures (like Over-The-Air Rekeying (OTAR) procedures) which need to be documented by a Green Book detailing the concept of operations and illustrating normal and contingency scenarios. This Green Book is needed to enable mission designers and protocol implementers to make optimal use of the SDLS EP recommendation [2].

## scope

The information contained in this Report is not part of the CCSDS Recommended Standards on the Space Data Link Security Protocol [1] and [2]. In the event of any conflict between the Recommended Standard and the material presented herein, the Recommended Standard shall prevail.

## organization of this report

Section 2 presents an overview of the Extended Procedures, the rationale for their development, and the major design goals and constraints;

Section 3 provides a detailed description and discussion of the key design concepts of the protocol; in particular the selection of security services, the position of the protocol in CCSDS stacks, and its data structures, fields and functions are given;

Section 4 presents the operation of the protocol in detail;

Annex A elaborates on the baseline implementations;

Annex C includes the latest version of the User Requirements Document (URD);

Annex E provides a list of acronyms and abbreviations.

## conventions and definitions

Generic definitions for the security terminology applicable to this and other CCSDS documents are provided in [3].

## References

The following documents are referenced in this Report. At the time of publication, the editions indicated were valid. All documents are subject to revision, and users of this Report 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] | *Space Data Link Security Protocol*. Recommendation for Space Data System Standards, CCSDS 355.0-B-1. Blue Book. Issue 1. Washington, D.C.: CCSDS, September 2015. |
| [2] | *Space Data Link Security Extended Procedures*. Recommendation for Space Data System Standards, CCSDS 355.1-R-1. Red Book. Issue 1. Washington, D.C.: CCSDS, forthcoming. |
| [3] | *Information Security Glossary of Terms*. Report Concerning Space Data Systems Standards, CCSDS 350.8-G-1. Green Book, Issue 1. Washington, D.C.: CCSDS, November 2012. |
| [4] | *TM Space Data Link Protocol*. Recommendation for Space Data System Standards, CCSDS 132.0-B-2. Blue Book. Issue 2. Washington, D.C.: CCSDS, September 2015. |
| [5] | *TC Space Data Link Protocol*. Recommendation for Space Data System Standards, CCSDS 232.0-B-3. Blue Book. Issue 3. Washington, D.C.: CCSDS, September 2015. |
| [6]  [7] | *AOS Space Data Link Protocol*. Recommendation for Space Data System Standards, CCSDS 732.0-B-3. Blue Book. Issue 3. Washington, D.C.: CCSDS, September 2015.  *Communications Operation Procedure-1.* Recommendation for Space Data System Standards, CCSDS 232.1-B-2.Blue Book. Issue 2. September 2010. |
| [10] | *CCSDS Cryptographic Algorithms*. Recommendation for Space Data System Standards, CCSDS 352.0-B-1. Blue Book. Issue 1. Washington, D.C.: November 2012. |
| [11] | *Space Missions Key Management Concept*, Report Concerning Space Data Systems Standards, CCSDS 350.6-G-1, Green Book, November 2011. |
| [13] | *The Application of CCSDS Protocols to Secure Systems*. Report Concerning Space Data System Standards, CCSDS 350.0-G-2. Green Book. Issue 2. Washington, D.C.: CCSDS, January 2006. |
| [20] | *Packet Telecommand Standard.* ESA PSS-04-107. Issue 2. European Space Agency, Paris, France. April 1992. |

# Overview and Rationale

## SDLS and Extended Procedures

The Space Data Link Security (SDLS) Protocol [1] is a security protocol that implements user-selected Security Services to the data transported by the Space Data Link (SDL) protocol in space-to-ground and ground-to-space links. The SDLS protects the Service Data Units transported by the SDL protocol and, in addition, selected SDL protocol data structures taking into account compatibility constraints with SDL and Space Link Extension services.

The Recommended Standard for SDLS Extended Procedures [2] extends the core SDLS protocol [1] with services for managing the security parameters of the space link. The purpose of SDLS Extended Procedures (EP) is to provide a standardized set of auxiliary services for managing an implementation of the SDLS protocol. These EP services are categorized into Key Management, Security Association (SA) Management, and SDLS Monitoring & Control. The SDLS EP specification also includes service interfaces and data structures for transport of EP service messages within the Space Data Link (SDL) protocols and a security unit status reporting mechanism.

## Design goals and constraints

### compatibility with sdl services

The SDLS standard has been developed for use with existing CCSDS TC, TM, and AOS Space Data Link Protocols.

### requirements

## Key Management

### Justification

The detailed specification of a cryptographic key management concept supporting the SDLS security services has been identified as part of the extended services of the protocol [2]. The first release of the SDLS protocol is specified to accommodate the required level of flexibility. The SDLS protocol shall be compatible with the following schemes for key management:

* Scheme 1: all session keys are pre-loaded on satellite before launch and cover the whole mission lifetime;
* Scheme 2: a subset of keys (master keys/key encryption keys (KEKs) and session/traffic protection keys) are pre-loaded on satellite before launch; session keys are uploaded encrypted during satellite operation (Over The Air Rekeying, OTAR);
* Scheme 3: a subset of keys (master keys/KEKs and session keys) are pre-loaded on satellite before launch; session keys are generated on-board from master keys and an uploaded non secret seed.

CCSDS has produced general documentation on key management [11]. In addition, it has been decided to undertake the specification of such concept on a companion document as part of the future extended services.

### Summary of capabilities

## Security Association (SA) Management

The SDLS protocol provides encryption, authentication, or authenticated encryption for data link layer services of the TC, TM, and AOS protocols. Central to the operation of this protocol is the Security Association (SA), a data schema used at both sending and receiving ends of a space link for managing the session state of cryptographic parameters.

### Justification

The Security Association Management Service for the SDLS protocol is designed to carry out the most basic functions of Security Association setup, activation, status, and control necessary to command the configurable Security Association parameters of a remote system’s SDLS implementation into a state suitable for operations.

The SA Management Service is designed to support an operational state model that may be simple or complex as mission needs indicate. Many missions of ordinary duration and lower data rates can be satisfied with support for statically-defined Security Associations and pre-loaded cryptographic keys and algorithms. For these, it is sufficient to choose which SA to use on a particular virtual channel along with all of its pre-loaded attributes.

It is anticipated that future complex or long-duration missions may need the capability to reuse and/or reconfigure Security Associations as the SAs and keys loaded into the system prior to the mission are used up over time. For this reason, the SA Management Service state model includes optional directives supporting over-the-air rekeying, or even instantiation on demand of Security Associations.

Figure 2‑2 illustrates the state model for Security Associations.



Figure 2‑2: Variable State Model for Security Association Management

### Summary of capabilities

#### Switching between SAs on a channel

As depicted in Figure 2‑2, the most basic operation to perform upon Security Associations is to change which SA is used on a channel (thus, which cryptographic operations are to be performed, using which key, and so on).

This is carried out through the two EP directives Stop SA and Start SA. The Stop SA directive transitions the current (‘old’) SA from its Operational (in use) state into the Keyed (dormant) state. The Start SA directive transitions the ‘new’ SA from the Keyed state to the Operational state.

#### Changing cryptographic keys associated with a SA

If a mission needs the capability to generate or upload new cryptographic keys (or sets of keys) during the mission lifetime (as in the case of Over-The-Air Rekey (OTAR)), it also needs the capability to change individual Security Associations’ parameters to use new keys instead of any keys originally pre-loaded prior to the start of the mission.

As depicted in Figure 2‑2, to associate a new key with a Security Association, the two EP directives Expire SA and Rekey SA are employed. The SA’s existing key (presumably not to be used anymore) is removed from the SA via the Expire SA directive, which transitions the SA from Keyed state into Unkeyed state. The new key is associated with the SA via the Rekey SA directive, which transitions the SA from Unkeyed state to Keyed state.

#### Creating Security Associations

Although it is not expected to be common, some long-duration missions may desire the capability to replace existing Security Associations altogether. For example, this could be used in conjunction with re-programmable cryptographic systems (and ample system redundancy!) in order to retire obsolete algorithms and carefully transition to use newer ones.

As depicted in Figure 2‑2, to replace a Security Association, the two EP directives Delete SA and Create SA are needed. The Delete SA directive erases all existing parameters of the SA and its state information, so that the specified Security Parameter Index no longer references any defined SA at all. The Create SA directive instantiates a new SA in the Unkeyed state containing the initial parameters and context supplied in the directive.

#### Query and modify SA parameters

Certain EP directives are provided to allow mission operations staff to adjust SA parameters in response to observed performance or unexpected behavior on the RF space link. The SA Status Request directive is used to query the receiving end to report the current state of a specified SA.

The Set Anti-Replay Counter (ARC) and Set Anti-Replay Window directives are used to adjust the ARC and ARC window respectively. SDLS SAs including Authentication protect against “replay attacks” – the potential for an unauthorized party to record and retransmit previously transmitted frames, esp. commands to a spacecraft – by making use of a transmitted sequence counter and a managed “window” indicating how close a sequence number has to be to its expected value to be accepted as valid.

## Security Unit Monitoring & Control

### Justification

### Summary of capabilities

## Frame Security Report (FSR)

The SDLS Extended Procedures specify a Frame Security Report (FSR) that contains a brief report on the status of the on-board security unit. It is reported as an Operational Control Field (OCF) within TM and AOS frames. This FSR, which is the protocol data unit transmitted from the Recipient to the Initiator of an SDLS secured TC or AOS uplink, provides the systematic, real-time mechanism by which the SDLS function at the receiving end reports the status of uplink TC or AOS frame acceptance to the sending end.

The FSR is similar to the Command Link Control Word (CLCW) [7] which provides real-time reporting of the status of uplink TC or AOS frame acceptance by the COP function to the sending end.

The FSR is not the only reporting mechanism for the SDLS protocol. Several on-demand or on-event reporting mechanisms and corresponding messages are specified in the Extended Procedures. They provide non real-time or non-systematic reporting of the frame acceptance status at the receiving end of the SDLS secured TC or AOS uplink. They enable further investigation of security events occurring on-board.

### Justification

When operating a SDLS secured uplink, the sending end (Mission Operation Center - MOC) needs to detect as promptly as possible major security events, occurring on-board the spacecraft at the receiving end, resulting in TC or AOS uplink frames rejection due to SDLS security checks violation. Uplink frame rejections, either due to uncorrectable transmission errors or due to security violations, have a major impact on uplink operations. While transmission errors will be dealt with by the COP [7] and trigger automatic retransmission of rejected frames, frames rejection by on-board SDLS function will need to be swiftly detected and analyzed by MOC to decide a course of action and potential retransmission of SDLS rejected frames in order to avoid, if appropriate, partial or complete loss of uplink session. The FSR provides a real-time synthetic report of SDLS function receiving end status and operation, enabling to inform MOC of uplink frame rejections as soon as they occur. MOC can then investigate further the related security event(s) by using the EP Monitoring and Control directives (e.g. Dump Log, Self-Test, Read Sequence Number).

### Summary of capabilities

The Frame Security Report (FSR) specifies a new type of telemetry frame Operational Control Field (OCF), for reporting of link security status events, fully compatible with the existing SDL protocols (TM and AOS) [4,6]. FSR content is updated each time an uplink frame is processed by the on-board SDLS function.

The reporting capabilities of the FSR are the following:

* a persistent Alarm flag that will signal any uplink frame rejection by SDLS on-board function. This flag can be reset by the user once the rejection has been taken into account by the MOC,
* non persistent Security Event Flags which enable to characterize security violation detected on the last received uplink frame: invalid Sequence Number, invalid MAC (failed authentication), invalid SA
* SPI of the last received uplink frame
* Sequence Number (SN) of the last received uplink frame

The Alarm flag enables the systematic detection on the ground of any uplink frame rejection by SDLS. The latency of this detection is made as low as feasible by the transmission of the FSR in the OCF field which is carried in every downlink frame.

The Security Event Flags and the associated SPI/SN information enable the characterization of major security events occurring on any uplink frame, providing that the FSR is transmitted to ground at least for each uplink frame received (see next section for discussion of FSR transmission rate).

### Relation to space link protocols

FSR are transmitted in the Operational Control Field (OCF) of downlink TM or AOS frames. Since a TM or AOS frame cannot contain two OCFs at the same time, the FSR insertion is multiplexed with the insertion of CLCW. The multiplexing scheme is mission-specific. Nevertheless, if the downlink frame rate is significantly higher than the uplink frame rate, it can be assumed that the FSR can be transmitted to ground at a higher rate than the uplink frame rate, therefore providing real-time security reporting on the validation of every uplink frame. If this is not the case, on-board security log (if implemented) will need to be dumped to ground to relate security event(s) to individual frame(s).

# Concept of Operation

## Key Management

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

### Illustrate key change scenarios (including OTAR, key verification, key change ‘on the fly’ from frame to frame)

### Contingency and off nominal scenarios

### Master keys versus session keys

## Security Association Management

### Guidelines on planning & assigning Security Associations

#### SAs for nominal traffic

The Security Parameter Index is a 2-byte field of the Security Header, so the number of available SAs per Master Channel has an upper bound of 216 (65536). The actual number of SAs that an implementation needs to assign and prepare for use is notionally equivalent to the number of keys that the spacecraft’s security unit is capable of storing simultaneously.

Specific ranges of SPI values are sometimes assigned for operational convenience to mission-specific operational use cases, where there are use cases whose traffic protection requirements are not interchangeable (e.g. subdivision into SAs used for spacecraft housekeeping and SAs used for private payload data, or SAs used for testing in ‘clear mode’).

#### SAs for SDLS EP traffic and other special uses

In the SDLS core protocol specification [1], two values were reserved for future use; these values (0 and 65535) were reserved intentionally so that they would remain available for use by the Extended Procedures [2] for special SDLS management use cases.

SDLS EP traffic can be carried over the same SAs used by nominal traffic, and routed by normal VC or MAP packet processing to the correct remote security unit for PDU processing. It is critical, however, that SDLS EP directives never modify the same SA currently being used to transmit their own EP PDUs!

Alternatively, SDLS EP traffic can be carried over different SAs not used by nominal traffic, or over one of the reserved SPI values (0 and 65535). In any case, VC or MAP packet processing is still necessary for routing EP traffic to the security unit for PDU processing.

A SA can only cover a single VC on Telecommand. However, SDLS does not exclude the duplication of SAs over a given Telecommand VC. Experience acquired with previous ad-hoc implementations of security functions for the protection of Telecommand [20] has shown that the existence of a redundant SA, only to be called as a last resource, could be very beneficial. When the ‘nominal’ SA has failed and possibly left the spacecraft telecommanding unavailable, this ‘redundant’ SA will allow to restore telecommanding without jeopardizing security. This special SA is labelled *Recovery SA*.

Special care should be taken to store and segregate the context of this SA at both ends of the space link. This Recovery SA should not be used for regular operations. Preferably the on-board keys associated with this Recovery SA should be neither erasable nor reloadable nor revocable, in order to maximize operational safety.

### Normal procedures for SA management

#### Preparing SA for first use

Many SA service parameters are managed. Each SA must specify the values of these parameters, whether implicitly via pre-loaded static definition or explicitly via EP directive. This information is collectively known as the SA database, although that term does not imply a RDBMS-type implementation.

SA parameters which are fixed at the time of creation and do not change thereafter:

a) Security parameter index (SPI);

b) SA Service Type;

c) The field lengths for Security Header and Security Trailer fields;

e) Encryption cipher suite length and identifier;

f) Initialization vector (IV) length;

g) Authentication cipher suite length and identifier;

h) Authentication bit mask length and value;

i) Anti-replay counter (ARC) length; and

j) Anti-replay counter window length.

SA parameters which change during use, but must be provided with initial values:

f) Initialization vector (IV) initial value;

i) Anti-replay counter (ARC) initial value; and

j) Anti-replay counter window value.

Static pre-loading commonly initializes all of the above managed parameters; if implemented, the Create SA directive can accomplish the same function. The Create SA directive instantiates a new SA in the Unkeyed state containing the initial parameters and context supplied in the directive.

Static pre-loading also commonly initializes associates cryptographic keys with SAs. Since the Create SA directive (if used) does not associate cryptographic keys with the SA, the Create SA directive for an SA should be followed by the Rekey SA directive to transition from Unkeyed to Keyed state, so that the SA is ready for later activation via the Start SA directive.

#### Changing cryptographic keys associated with a SA

If a mission needs the capability to generate or upload new cryptographic keys (or sets of keys) during the mission lifetime (as in the case of Over-The-Air Rekey (OTAR)), it also needs the capability to change individual Security Associations’ parameters to use new keys in place of keys originally pre-loaded prior to the start of the mission.

As depicted in Figure 2‑2, to associate a new key with a Security Association, the two EP directives Expire SA and Rekey SA are employed. The SA’s existing key (presumably not to be used anymore) is removed from the SA via the Expire SA directive, which transitions the SA from Keyed state into Unkeyed state. The new key is associated with the SA via the Rekey SA directive, which transitions the SA from Unkeyed state to Keyed state.

#### Switching between SAs on a channel

As depicted in Figure 2‑2, the most basic operation to perform upon Security Associations is to change which SA is used on a channel (thus, which cryptographic operations are to be performed, using which key, and so on).

This is carried out through the two EP directives Stop SA and Start SA. The Stop SA directive transitions the current (‘old’) SA from its Operational (in use) state into the Keyed (dormant) state. The Start SA directive transitions the ‘new’ SA from the Keyed state to the Operational state.

### Implementing SA life cycle with the EP procedures

### Contingency and off-nominal scenarios

#### (recovery SA, set ARC, modify window, …)

Certain EP directives are provided to allow mission operations staff to adjust SA parameters in response to observed performance or unexpected behavior on the RF space link. The SA Status Request directive is used to query the receiving end to report the current state of a specified SA.

The Set Anti-Replay Counter (ARC) and Set Anti-Replay Window directives are used to adjust the ARC and ARC window respectively. SDLS SAs including Authentication protect against “replay attacks” – the potential for an unauthorized party to record and retransmit previously transmitted frames, esp. commands to a spacecraft – by making use of a transmitted sequence counter and a managed “window” indicating how close a sequence number has to be to its expected value to be accepted as valid.

### Seamless key change (from frame to frame)

Depending on the capabilities of the security units at sending and receiving ends, it is possible for the sending end to change which SA is used on a channel (and which key is in effect) from one frame to the next, without the receiving end dropping frames during the transition.

If frame-upon-frame key change is to be supported, both the sending end’s and receiving end’s security units should be capable of handling more than one active cryptographic session and key simultaneously. The receiving end’s security unit should be capable of supporting more than one SA in the Operational state on a given VC or MAP, so that when newly arrived frames indicate SAs different from previous frames, the security unit can correctly process without delay in transition.

### Handling redundancy

Most spacecraft implementing SDLS will also have redundancy of frame processing and associated security units. It is possible to manage security units through the SDLS Extended Procedures such that secure communications is maintained while the security unit is actively being managed. Two implementation scenarios are discussed below.

#### Reconfiguring redundant command chain using nominal one

Scenario 1: Redundancy provided where each communications ‘string’ (i.e. each side of a redundant prime/backup pair) has its own independent virtual channel(s) so that RF traffic is directed explicitly to use a specific string (‘Side A’ vs. ‘Side B’).

In Scenario 1, each security unit is addressed using the virtual channels and SAs which belong to that string. Nominal RF traffic may continue along one string ‘Side A’ using Side A’s virtual channels at the same time SDLS EP directives are addressed to the other string ‘Side B’ using Side B’s virtual channels. There is no ambiguity about which security unit can be addressed by a specific SDLS EP directive.

#### Logical cross-strapping

Scenario 2: Redundancy provided where both communications strings of a redundant pair share the same virtual channel(s), processing traffic in parallel so that RF traffic is supplied as output by whichever specific string currently acts as prime.

In Scenario 2, even though nominal RF traffic may continue along the virtual channel(s) shared by both strings, it is necessary that each string’s security unit be addressable using virtual channels and/or SAs which belong to it alone. It is further necessary that, in addition to each communications string being able to route SDLS EP directives to its own security unit, that it also be able to route SDLS EP directives to the security unit belonging to the other string.

In this case, assignment of separate virtual channels (not used by nominal traffic) and/or SAs for each side’s security unit will prevent ambiguity about which security unit is addressed by a specific SDLS EP directive. Use of the two reserved SPI values (0 and 65535) to address separate security units is one possible method of accomplishing this.

## Security Unit Monitoring & Control

### Illustrate nominal procedures for Security Unit M&C

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

### Rationale, definition and usage of Security Logs

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

## Frame Security Report (FSR)

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

Frame Security Report (FSR) is a real-time report of the on-board SDLS function at the receiving end of a TC or AOS uplink. FSR is transmitted on the TM or AOS downlink in the Operational Control Field (OCF) of transfer frames using the MC\_OCF or VC\_OCF services as defined in [4] and [6]. Since a TM or AOS frame cannot contain two OCFs at the same time, the FSR insertion has to be multiplexed with the insertion of CLCW (report word from the Communications Operation Procedure - COP [7]) whenever COP is used on the uplink. The multiplexing scheme is mission-specific. Nevertheless, the following considerations need to be taken into account:

- since all fields of the FSR, apart from the Alarm flag, are non persistent and updated at each uplink frame received by the on-board SDLS function, it is desirable that the transmission rate of the FSR on the downlink is equal to or higher than the uplink frame rate. This would guarantee that any security event detected by the on-board SDLS function is reported real-time to ground and that each security event can be associated unambiguously with the uplink frame that caused it. This would enable direct investigation of security events by Mission Operation Center (MOC) without the need for dumping and analysis of on-board security log (if implemented) or usage of appropriate Extended Procedures directives. This constraint on FSR transmission rate can only be met if the downlink frame rate is significantly higher that the uplink frame rate since some downlink frames OCF will be reserved for CLCW. Although it is not necessary that the CLCW reporting rate (from the receiving end to the sending end) match the Transfer Frame transfer rate (from the sending end to the receiving end), some minimum CLCW sampling rate is necessary for the proper operation of the COP.

– in case the above mentioned constraint on the FSR transmission rate cannot be met, FSR contains a persistent Alarm flag which will in all cases inform the MOC that a security event has occurred on an uplink frame since last FSR was transmitted. Determination of the type of security event(s) and of the uplink frame(s) involved will require sending appropriate SDLS Extended Procedures (EP) directives (see Monitoring & Control and SA management sections).

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

The purpose of the FSR being real-time reporting of the on-board SDLS function at the receiving end of a TC or AOS uplink, all fields but one (the Alarm Flag) are non-persistent and updated at each uplink frame processed by the SDLS function.

The various information carried by the FSR can be interpreted as follows:

* Alarm flag (persistent): indicate that at least one TC Transfer Frame has been rejected by the on-board SDLS function since the last reset of the Alarm Flag. This flag can be reset from the ground by sending the Alarm Flag Reset Command PDU. This flag being persistent guarantees that no security event detected on-board will go unnoticed at the MOC, whichever the FSR transmission rate.
* Security event flags (non persistent): indicate the type of security event triggered by the last received uplink frame by the on-board SDLS function. They are updated at each TC Transfer Frame processed by the SDLS on-board function. Three generic types are reported : invalid SN, invalid MAC, invalid SA. Their significance are detailed hereafter. The uplink frame to which those flags relate is identified by the SPI and SN values transmitted in the last part of the FSR:
  + Invalid SN: indicate that the SN carried by the last received TC Transfer Frame by the on-board SDLS function is invalid (i.e. outside the SN window)
  + Invalid MAC: indicate that the MAC carried by the last received TC Transfer Frame by the on-board SDLS function is invalid (i.e. does not match the MAC computed over the received Transfer Frame). This flag signals an integrity or authentication error on the related frame.Invalid SA: indicate whether the last TC Transfer Frame received by the SDLS on-board function failed SA verification or carried an SPI pointing to an inactive SA or to an active SA associated with an inactive key. SA verification consists in checking that the SPI carried by the received uplink frame is pointing to an SA that is associated with the GVCID/GMAPID of that frame.
* Last SPI used (non-persistent): indicates the SPI carried in the last received TC Transfer Frame by the on-board SDLS function. This information combined with the Sequence Number (SN) information enables to identify unambiguously the last received TC transfer frame to which above mentioned Security Event Flags relate.
* Sequence Number (SN) value: contains the 8 Least Significant Bits (LSB) of the Sequence Number (SN) carried in the last received TC Transfer Frame by the on-board SDLS function. This SN is related to the Security Association that is pointed to by the SPI. SN combined with SPI unambiguously identify the last received TC transfer frame.

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

While operating a secured uplink to a spacecraft with limited contact time, it is of utmost importance to detect as promptly as possible any link disruption and be able to discriminate between the 2 main causes of disruption, namely:

* Transmission problems causing outage or frame rejection due to transmission errors
* Security events/attacks causing frame rejection by the on-board SDLS function

At the uplink receiving end, two Frame Acceptance and Reporting Mechanism (FARM) operate in sequence:

* the FARM of the Communications Operation Procedure (COP-1) specified in [7]. This mechanism checks the validity of the TC transfer frame based on:
  + the results of the decoding of the TC channel code (presence of uncorrectable errors)
  + the results of the check of the frame CRC (FEC)
  + the result of the check of structure of the frame and validity of its header fields
* the FARM of the on-board SDLS function specified in [1]. This mechanism checks the validity of the TC transfer frame based on:
  + validity of the MAC which guarantees if valid the integrity and authenticity of the frame
  + validity of the SN which guarantees if valid that the frame is not a reply from a previously sent frame
  + validity of the SPI which guarantees if valid that appropriate active key and SA have been used to protect the frame

The COP FARM and the SDLS FARM will reject/discard any frame that fails their respective checks. Both FARMs have their real-time reporting message that will enable the MOC to detect and discriminate between transmission errors and security events/attacks:

* Command Link Control Word (CLCW) for the COP
* Frame Security Report (FSR) for SDLS

Both types of report messages (CLCW and FSR) will be multiplexed in the Operational Control Field of downlink TM or AOS frames. In most cases, downlink frame rate being significantly higher than uplink frame rate, at least one CLCW and one FSR can be transmitted for each uplink frame received enabling full real-time reporting of any communication (COP) or security (SDLS) related discarding of an uplink frame.

## Various types of implementation

### Fixed keys, OTAR, dynamic management of SA vs static

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

# design concepts

#### Recovery SA in Telecommand

A SA can only cover a single VC on Telecommand. However, SDLS does not exclude the duplication of SAs over a given Telecommand VC. Experience acquired with previous ad-hoc implementations of security functions for the protection of Telecommand [20] has shown that the existence of a redundant SA, only to be called as a last resource, could be very beneficial. When the ‘nominal’ SA has failed and possibly left the spacecraft telecommanding unavailable, this ‘redundant’ SA will allow to restore telecommanding without jeopardizing security. This special SA is labelled *Recovery SA*.

Special care should be taken to store and segregate the context of this SA at both ends of the space link. This Recovery SA should not be used for regular operations. Preferably the on-board keys associated with this Recovery SA should be neither erasable nor reloadable nor revocable, in order to maximize operational safety.

### sequence count synchronization

Authentication requires the verification of proper sequence of the received frame to be able to reject replay attacks. The mechanism used in SDLS is based on sequence counters for every Security Association. These counters are both managed at sending and receiving ends.

In order to maintain a reliable data flow, it is essential that counters at the sending and receiving end are sufficiently synchronized. Ideally, if all the frames are received in sequence at the receiving end, the counters would be naturally synchronized.

Such synchronization could be forced with space link protocols like TC with the request of a sequence-controlled service. However, this is not possible for TM, AOS and even for TC when expedited service is used. For this reason, provision shall be made for the allowance of missing frames (gaps) without blocking the flow of frames at receiving end.

The provision of a sequence counter ‘window’ allows for a certain extent of desynchronization between the counters at both ends due to time of flight and/or lost frames. The verification and acceptance of a subsequent frame will recover the counter synchronization. Furthermore, the SDLS Extended Procedures will allow to monitor and control the on-board counter synchronization.

## scenarios

This subsection elaborates on the need for so-called recovery SA(s) in order to cope with emergency situations where the use of operational SAs is no longer possible.

Some emergency situations impacting SDLS operation and likely to be encountered can be listed as follows (not limitative):

* Spacecraft tumbling or TM sub-system failure on-board, resulting in the TM downlink being interrupted. This forces the use of blind commanding meaning no reporting from the on-board SDLS function is available. In that configuration, it is impossible to guarantee that secured TC frames, sent with operational SA, will be accepted on-board by the SDLS function. Moreover, a mismatch in anti-replay counter between the ground sending end and the on-board receiving end is likely. Telecommands need to be sent to the spacecraft in a secure manner to restore the TM link (e.g., by switching to the redundant TM transmitter) or the attitude control of the spacecraft.
* Content of the programmable keys storage has been corrupted by the environment or a malfunction (i.e. programmable keys are not known anymore). New value for operational keys needs to be uploaded in a secure manner by telecommand.
* Synchronization on the anti-replay counter of operational SA in use has been lost between SDLS ground sending end and on-board receiving end. Re-initialization of anti-replay counter (i.e. re-initialization of the SA context) on-board is needed.

In all those emergency situations, there is a need to re-establish a secure TC channel. The usual way to achieve that is to define so-called Recovery SA(s), only to be called at last resource. When the ‘nominal’ SA has failed and possibly left the spacecraft telecommanding unavailable, this Recovery SA will allow to restore telecommanding without jeopardizing security. Special care should be taken to store and segregate the context of this SA at both ends of the space link. This Recovery SA *should never be used for regular operations*. The context of this(these) Recovery SA(s), including the on-board keys associated with it, *should be kept in non-erasable, non-volatile memory* so as to survive on-board transient power loss and operational errors.

1. BASELINE MODES
   1. Introduction
2. Acronyms and Abbreviations

This annex lists the acronyms and abbreviations used in this Report.

AAD Additional Authenticated Data

AES Advanced Encryption Standard

AOS Advanced Orbiting Systems

CCSDS Consultative Committee for Space Data Systems

COP-1 Communications Operation Procedure-1

CRC Cyclic Redundancy Check

CTR Counter Mode

FSP Forward Space Packet

HMAC Hash-based Message Authentication Code

HPC High Priority Command

IEC International Electrotechnical Commission

IP Internet Protocol

ISO International Standards Organization

IV Initialization Vector

KEK Key Encryption Key

MAC Message Authentication Code

MAP Multiplexer Access Point

MC Master Channel

MCID Master Channel Identifier

N/A Not Applicable

OCF Operational Control Field

OID Only Idle Data

OSI Open Systems Interconnection

OTAR Over-the-air Rekeying

PDU Protocol Data Unit

PVN Packet Version Number

RS Reed-Solomon

SA Security Association

SCID Spacecraft Identifier

SDL Space Data Link

SDLS Space Data Link Security Protocol

SDU Service Data Unit

SLP Space Link Protocol

SPI Security Parameter Index

TC Telecommand

TM Telemetry

URD User Requirements Document

VC Virtual Channel

VCA Virtual Channel Access

VCID Virtual Channel Identifier