SDLS Extended Procedures red-1 Agency Review

Compilation of RIDs dispositions

Synthesis:
Reviewed document: 355.1-R-1 SDLS Extended Procedures
42 RIDs submitted by ESA, CNES, CSA, NASA
34 accepted – 8 rejected

ESA RIDs:

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER: ESA-MW-01
SUBMITTING ORGANIZATION (Agency, Center): ESA , ESOC

REVIEWER'S NAME: Marcus Wallum
CODE: OPS-GES
E-MAIL ADDRESS: marcus.wallum@esa.int
TELEPHONE: +49 6151 90 3506

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 2-2 PARAGRAPH NUMBER: 2.3.1
RID SHORT TITLE: Use of Suspended and Compromised States

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

From:
NOTE - The Suspended and Compromised Sates as specified in reference [2] are not used in the SDLS Extended Procedures Recommended Standard. They are shown in grey in figure 2-1.

To:
NOTE - The Suspended and Compromised Sates as specified in reference [2] are not used in the SDLS Extended Procedures Recommended Standard. They are shown in grey in figure 2-1. This is due to [INSERT EXPLANATION]

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended _X__ Editorial ___
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.

EDITORIAL: Typographical or other factual error needing correction.
(This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:
Reference [2] Symmetric Key Management, section 3.2.1.1 identifies c) Suspended state (optional). Here the inserted explanation might be simply for reasons of reduced complexity. Note that this means lost capabilities e.g. Suspension during investigation into possible corruption.

Reference [2] Symmetric Key Management, section 3.2.1.1 identifies f) Compromised state (note: NOT optional) as a state which “shall be present in the lifecycle for all cryptographic keys”. It is not clear if SDLSP/SDLSP-EP will NOT support compromised key states, how possible key corruption and associated state transitions are to be managed.

For both cases, adding a brief explanation would clarify the reasoning for exclusion and would align with Reference [2].

DISPOSITION: Compromised state should be adopted for the initiator but not for the recipient. No directives associated with compromised state.

- Add following text in the §2.3.1 NOTE: The Suspended State as specified in reference [2] is not used in the SDLS Extended Procedures Recommended Standard. It is shown in grey in figure 2.1. The Compromised state is only applicable to the Initiator. There are no procedures associated with that state. Change figure 2-1 accordingly.
- Add NOTE in § 5.4.1.2: The Suspended State as specified in reference [2] is not used in the SDLS Extended Procedures Recommended Standard. The Compromised state is only applicable to the Initiator. There are no procedures associated with that state.

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER: ESA-MW-02
SUBMITTING ORGANIZATION (Agency, Center): ESA , ESOC

REVIEWER'S NAME: Marcus Wallum
CODE: OPS-GES
E-MAIL ADDRESS: marcus.wallum@esa.int
TELEPHONE: +49 6151 90 3506

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 3-5 PARAGRAPH NUMBER: 3.2.3.1.3.4
RID SHORT TITLE: Output for processing of upload session keys

---

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

From:
c) have the following output: none;

To:
c) have the following output: Decrypted Set of Upload Session Keys stored in Pre-Active state

---

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended ___ Editorial _X__
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:
Whilst there is no new output in the sense of a newly created entity in the system, there is an output of this procedural step which is meaningful for the Recipient and which should be noted.

DISPOSITION: accepted

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER: ESA-MW-03
SUBMITTING ORGANIZATION (Agency, Center): ESA , ESOC

REVIEWER'S NAME: Marcus Wallum
CODE: OPS-GES
E-MAIL ADDRESS: marcus.wallum@esa.int
TELEPHONE: +49 6151 90 3506

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 3-11 PARAGRAPH NUMBER: 3.2.3.5.1
RID SHORT TITLE: Implied transition after key verification

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

From:
It should be noted that if this procedure is executed for session or master keys associated with pre-activation state this would imply a transition to active state.

To:
It should be noted that if this procedure is executed for session or master keys associated with pre-activation state this would imply that the keys are verified for subsequent activation.

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended _X__ Editorial ___
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:
Reference [2] Symmetric Key Management, section 3.2.2.1.5 states “Key Verification as per 4.3.4 can be executed on keys in Pre-activation state without triggering their transition to Active state”. Therefore a state transition is not necessarily implied after key verification and would still require subsequent key activation.

DISPOSITION:

- modify text for §3.2.3.5.1 as follows: The Key Verification procedure allows the verification of a set of active ~~session~~ keys at the Recipient. This gives confirmation to the Initiator that the keys are not corrupted or modified and fully operational. ~~It should be~~

~~noted that if this procedure is executed for session ormaster keys associated with pre-activation state this would imply a transition to active state~~.

- Modify §3.2.3.5.2: Both entities shall have an identical set of ~~session~~ keys in ~~Pre-Activation or~~ Active State.

- Add Key Verification directive as a looping back arrow from Active to Active state in figure 2-1.

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER: ESA-MW-04
SUBMITTING ORGANIZATION (Agency, Center): ESA , ESOC

REVIEWER'S NAME: Marcus Wallum
CODE: OPS-GES
E-MAIL ADDRESS: marcus.wallum@esa.int
TELEPHONE: +49 6151 90 3506

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 3-11 PARAGRAPH NUMBER: 3.2.3.5.3.2
RID SHORT TITLE: Reference algorithms for Challenges

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

From:
NOTE – The specification of the algorithm for the creation of the Challenges is outside the scope of this Recommended Standard.

To:
NOTE – The specification of the algorithm for the creation of the Challenges is outside the scope of this Recommended Standard, however associated authentication algorithms shall be compliant with those approved in reference [7].

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended _X__ Editorial ___
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:
Associated authentication algorithms for computation of challenges, responses and responses verification shall be in sync with the Cryptographic Algorithms Blue Book published by CCSDS

DISPOSITION: accepted.

- Note in 3.2.3.5.3.2 to be changed according to RID.
- Subsection to be added in annex D (baseline mode) §D4.2.3 Algorithm for key verification:
  - The baseline implementation to be used for Key verification is:

- For the authenticated encryption of the challenge: AES-GCM as defined in reference **Erreur ! Source du renvoi introuvable.**;
- The keys are 256 bits in total length;
- The IV is 96 bits in total length;
- The output MAC for the authentication is 32 bit in length.

- Modify in annex D key length for AES-GCM to 256 bits.
- Modify D4.2.2 Algorithm for OTAR accordingly:
  The baseline implementation to be used for OTAR operation is:
  - For **the authenticated encryption** of the key block: AES-GCM as defined in reference **Erreur ! Source du renvoi introuvable.**;
  - The keys are **256** bits in total length;

- `Modify title of Figure D-5 to: Key Verification Reply PDU`
- `Modify title of Figure D-6 to: Start SA Command PDU`

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER: ESA-MW-05
SUBMITTING ORGANIZATION (Agency, Center): ESA , ESOC

REVIEWER'S NAME: Marcus Wallum
CODE: OPS-GES
E-MAIL ADDRESS: marcus.wallum@esa.int
TELEPHONE: +49 6151 90 3506

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 3-13 PARAGRAPH NUMBER: 3.2.3.5.3.6
RID SHORT TITLE: Output for challenge response verification

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

From:
c) have the following output: none;

To:
c) have the following output: Verification results associated with each key in the Set of Key IDs

---

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended ___ Editorial _X__
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:
Whilst there is no new output in the sense of a newly created entity in the system, there is an output of this procedural step which is meaningful for the Initiator and which should be noted.

DISPOSITION: accepted.

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER: ESA-MW-06
SUBMITTING ORGANIZATION (Agency, Center): ESA , ESOC

REVIEWER'S NAME: Marcus Wallum
CODE: OPS-GES
E-MAIL ADDRESS: marcus.wallum@esa.int
TELEPHONE: +49 6151 90 3506

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 3-15 PARAGRAPH NUMBER: 3.3.2.5
RID SHORT TITLE: ARC and SN differentiation

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

From:
i) ARC length and initial value; and
j) Anti-replay counter window length and value.

To:
i) ARC length and initial Anti-replay counter value; and
j) Anti-replay sequence number window length and value.

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended _X__ Editorial ___
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:

It is not clear the difference between the ARC Window and the SN Window.

There is some inconsistency with reference to ARC and SN throughout the document which could cause misunderstandings, for example:
- 5.5.1.11.2 refers to ARC Command PDU and then 5.5.1.11.2.1 refers to SN Command PDU
- 3.3.3.7 refers to both ARC value and anti-replay sequence number
- 5.3.2.2.2.4.2 and Table 5-1 assigns a PDU Header value only for a Read Sequence Number procedure, not Read ARC
The same applies for the window, for example:
- 4.2.2.5.2.3 and also reference [1] refer only to a SN window whereas 3.3.2.5 refers to ARC window

It is therefore recommended that the terminology and usage of ARC, SN and Window values are checked and aligned throughout. Note all PDU fields, descriptions etc. and Table 5-1 should then be aligned accordingly.

DISPOSITION:

- Change Anti-Replay Counter, ARC, Sequence Number to : “anti-replay sequence number” everywhere in the document.
- Add definition of “anti-replay sequence number” in security glossary for consistency.

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER: ESA-MW-07
SUBMITTING ORGANIZATION (Agency, Center): ESA , ESOC

REVIEWER'S NAME: Marcus Wallum
CODE: OPS-GES
E-MAIL ADDRESS: marcus.wallum@esa.int
TELEPHONE: +49 6151 90 3506

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 3-13 PARAGRAPH NUMBER: 3.3.1
RID SHORT TITLE: Add Expire SA and Read ARC procedures to Overview

---

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

From:
The following service procedures are specified:
– Start SA;
– Stop SA;
– Rekey SA;
– Create SA;
– Delete SA;
– Set Anti-Replay Counter;
– Set Anti-Replay Window; and
– SA Status Request.

To:
The following service procedures are specified:
– Start SA;
– Stop SA;
– Rekey SA;
- Expire SA
– Create SA;
– Delete SA;
– Set Anti-Replay Counter;
– Set Anti-Replay Window;
– SA Status Request; and
- Read Anti-Replay Counter

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended ___ Editorial _X__
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:
Expire SA and Read ARC procedures are missing from the Overview.

DISPOSITION: accepted.

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER: ESA-MW-08
SUBMITTING ORGANIZATION (Agency, Center): ESA , ESOC

REVIEWER'S NAME: Marcus Wallum
CODE: OPS-GES
E-MAIL ADDRESS: marcus.wallum@esa.int
TELEPHONE: +49 6151 90 3506

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 3-24 PARAGRAPH NUMBER: 3.3.3.5.3.3
RID SHORT TITLE: Create SA PDU section reference

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

From:
d) execute the following: a Create SA PDU as defined in 5.5.1.2 shall be created and transmitted to the Recipient using the interface specified in section 4.
To:
d) execute the following: a Create SA PDU as defined in 5.5.1.6 shall be created and transmitted to the Recipient using the interface specified in section 4.

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended ___ Editorial _X__
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:
Create SA PDU is specified in section 5.5.1.6, not 5.5.1.2

DISPOSITION: accepted.

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER: ESA-MW-09
SUBMITTING ORGANIZATION (Agency, Center): ESA , ESOC

REVIEWER'S NAME: Marcus Wallum
CODE: OPS-GES
E-MAIL ADDRESS: marcus.wallum@esa.int
TELEPHONE: +49 6151 90 3506

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 3-27 PARAGRAPH NUMBER: 3.3.3.7.3.2
RID SHORT TITLE: Output for execution of Set ARC

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

From:
c) have the following output: none;.

To:
c) have the following output: Security Association with new anti-replay sequence number

---

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended ___ Editorial _X__
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:
Whilst there is no new output in the sense of a newly created entity in the system, there is an output of this procedural step which is meaningful for the Initiator and which should be noted.

DISPOSITION: accepted. Change procedure name to Set anti-replay sequence number.

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER: ESA-MW-10
SUBMITTING ORGANIZATION (Agency, Center): ESA , ESOC

REVIEWER'S NAME: Marcus Wallum
CODE: OPS-GES
E-MAIL ADDRESS: marcus.wallum@esa.int
TELEPHONE: +49 6151 90 3506

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 3-27 PARAGRAPH NUMBER: 3.3.3.7.3.4
RID SHORT TITLE: Output for execution of Set ARC

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

From:
c) have the following output: none;.

To:
c) have the following output: Security Association with new anti-replay sequence number

---

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended ___ Editorial _X__
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:
Whilst there is no new output in the sense of a newly created entity in the system, there is an output of this procedural step which is meaningful for the Recipient and which should be noted.

DISPOSITION: accepted.

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER: ESA-MW-11
SUBMITTING ORGANIZATION (Agency, Center): ESA , ESOC

REVIEWER'S NAME: Marcus Wallum
CODE: OPS-GES
E-MAIL ADDRESS: marcus.wallum@esa.int
TELEPHONE: +49 6151 90 3506

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 3-30 PARAGRAPH NUMBER: 3.3.3.9.3.2
RID SHORT TITLE: Output for Signalling of SA Status Request

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

From:
c) have the following output: SA Status Request Command PDU;

To:
c) have the following output: SA Status Request transmitted to the Recipient;

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended ___ Editorial _X__
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:
Alignment of output description with all other signalling procedure steps

---

DISPOSITION: accepted.

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER: ESA-MW-12
SUBMITTING ORGANIZATION (Agency, Center): ESA , ESOC

REVIEWER'S NAME: Marcus Wallum
CODE: OPS-GES
E-MAIL ADDRESS: marcus.wallum@esa.int
TELEPHONE: +49 6151 90 3506

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 3-32 PARAGRAPH NUMBER: 3.4.1
RID SHORT TITLE: Remove Read Sequence Number from Overview

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)
From:
The following service procedures are specified:
– Ping;
– Log Status;
– Dump Log;
– Erase Log;
– Self-Test;
– Read Sequence Number; and
– Alarm Flag Reset.

To:
The following service procedures are specified:
– Ping;
– Log Status;
– Dump Log;
– Erase Log;
– Self-Test; and
– Alarm Flag Reset.

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended ___ Editorial _X__
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:
Read Sequence Number (or Read ARC) is a procedure currently belonging to the SA Management Service (3.3.3.10) – it does not appear in the M&C Service sections 3.4.2 or 3.4.3.

DISPOSITION: accepted.

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER: ESA-MW-13
SUBMITTING ORGANIZATION (Agency, Center): ESA , ESOC

REVIEWER'S NAME: Marcus Wallum
CODE: OPS-GES
E-MAIL ADDRESS: marcus.wallum@esa.int
TELEPHONE: +49 6151 90 3506

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 3-33 PARAGRAPH NUMBER: 3.4.2.3
RID SHORT TITLE: Add TLV format reference

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

From:
NOTE – The content of each security message is implementation specific and not specified by this recommended standard. However, each security message has to comply with the TLV format.

To:
NOTE – The content of each security message is implementation specific and not specified by this recommended standard. However, each security message has to comply with the TLV format (see 5.3.1.2).

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended ___ Editorial _X__
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:
First time mention of TLV, reference can guide the reader.

DISPOSITION: modify NOTE as follows: The content of each security message is implementation specific and not specified by this recommended standard. ~~However, each security message has to comply with the TLV format.~~

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER: ESA-MW-14
SUBMITTING ORGANIZATION (Agency, Center): ESA , ESOC

REVIEWER'S NAME: Marcus Wallum
CODE: OPS-GES
E-MAIL ADDRESS: marcus.wallum@esa.int
TELEPHONE: +49 6151 90 3506

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 3-36 PARAGRAPH NUMBER: 3.4.3.2.3.4
RID SHORT TITLE: Output for Signalling of the Log Status Response

---

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

From:
c) have the following output: none

To:
c) have the following output: The Log status reply transmitted to the Initiator

---

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended ___ Editorial _X__
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:
Whilst there is no new output in the sense of a newly created entity in the system, there is an output of this procedural step which is meaningful for the Recipient and Initiator and which should be noted. It is also an alignment with 3.4.3.2.3.2.

DISPOSITION: accepted.

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER: ESA-MW-15
SUBMITTING ORGANIZATION (Agency, Center): ESA , ESOC

REVIEWER'S NAME: Marcus Wallum
CODE: OPS-GES
E-MAIL ADDRESS: marcus.wallum@esa.int
TELEPHONE: +49 6151 90 3506

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 4-1 PARAGRAPH NUMBER: 4.1
RID SHORT TITLE: Reference for SDLS EP Concept of Operations

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

From:
The SDLS Extended Procedures Concept of Operations describes various options to implement the interface.

To:
The SDLS Extended Procedures Concept of Operations [ADD APPROPRIATE REFERENCE] describes various options to implement the interface.

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended ___ Editorial _X__
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:
Appropriate reference should also be added in the informative reference Annex C.

DISPOSITION: accepted. Add reference to SDLS EP Green Book (350.11-G) in Annex C.

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER: ESA-MW-16
SUBMITTING ORGANIZATION (Agency, Center): ESA , ESOC

REVIEWER'S NAME: Marcus Wallum
CODE: OPS-GES
E-MAIL ADDRESS: marcus.wallum@esa.int
TELEPHONE: +49 6151 90 3506

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 4-5 PARAGRAPH NUMBER: 4.3.1.1
RID SHORT TITLE: Extended Procedures Sensitivity as recommendation

---

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)
From:
Sensitive EP Service PDUs shall only be communicated over a SDLS channel protected by authenticated encryption. Table 4-1 shows the sensitivity attributes for each procedure.
To:
Sensitive EP Service PDUs shall only be communicated over a SDLS channel protected by authenticated encryption. Table 4-1 shows the recommended sensitivity attributes for each procedure.
NOTE – Sensitivity values may change according to mission-specific implementations and security risk profiles

---

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended __X_ Editorial ___
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:
Some missions with very low security risk tolerance may choose to also protect some of the SA / Rest Alarm Flag procedures. This addition provides this flexibility.

DISPOSITION:

- Delete requirement 4.3.1.1
- Add note to requirement 4.3.1.2 with the following text:
  - NOTE : the choice between authentication-only and authenticated-encryption for the transmission of EP service PDUs is driven by mission risk analysis.
- Delete Table 4-1.
- AI: Add text discussing the EP PDUs protection in EP GB.

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER: ESA-MW-17
SUBMITTING ORGANIZATION (Agency, Center): ESA , ESOC

REVIEWER'S NAME: Marcus Wallum
CODE: OPS-GES
E-MAIL ADDRESS: marcus.wallum@esa.int
TELEPHONE: +49 6151 90 3506

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 3-12 PARAGRAPH NUMBER: 3.2.3.5.3.5
RID SHORT TITLE: Key Verification Response PDU should be Reply

---

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

From:
d) execute the following: a Key Verification Response PDU as defined in 5.4.2.5 shall be created and transmitted to the Initiator using the interface specified in section 4.
To:
d) execute the following: a Key Verification Reply PDU as defined in 5.4.2.5 shall be created and transmitted to the Initiator using the interface specified in section 4.

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended ___ Editorial __X_
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:
Align terminology

DISPOSITION: accepted.

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER: ESA-MW-18
SUBMITTING ORGANIZATION (Agency, Center): ESA , ESOC

REVIEWER'S NAME: Marcus Wallum
CODE: OPS-GES
E-MAIL ADDRESS: marcus.wallum@esa.int
TELEPHONE: +49 6151 90 3506

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 6-1 PARAGRAPH NUMBER: Table 6-1
RID SHORT TITLE: Remove OTAR IV length reference

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

From:

Managed Parameter	Allowed Values	Defined in Reference
OTAR IV length		[1]

To:

Managed Parameter	Allowed Values	Defined in Reference
OTAR IV length		

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended ___ Editorial __X_
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:
Could not find any reference to the OTAR IV length parameter in reference [1]

DISPOSITION: remove ref [1] from the table for OTAR IV length.

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER: ESA-MW-19
SUBMITTING ORGANIZATION (Agency, Center): ESA , ESOC

REVIEWER'S NAME: Marcus Wallum
CODE: OPS-GES
E-MAIL ADDRESS: marcus.wallum@esa.int
TELEPHONE: +49 6151 90 3506

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: D-2 PARAGRAPH NUMBER: D4.2.2
RID SHORT TITLE: Baseline mode key lengths

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

From:
b) The keys are 128 bits in total length;
To:
b) The keys are 256 bits in total length;

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended _X__ Editorial ___
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:
Key lengths in reference [7] are proposed to be increased (see CCSDS 352.0-P-1.1). SDLS EP Baseline Mode should be aligned accordingly. This should also be updated on page D-3, paragraph D4.3.1 C) 2) the Session Key fields (128 bits) -> (256 bits).

DISPOSITION: Change throughout document 128 bit keys by 256 bit keys for all AES authentication and/or encryption.

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER: ESA-MW-20
SUBMITTING ORGANIZATION (Agency, Center): ESA , ESOC

REVIEWER'S NAME: Marcus Wallum
CODE: OPS-GES
E-MAIL ADDRESS: marcus.wallum@esa.int
TELEPHONE: +49 6151 90 3506

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 4-4 PARAGRAPH NUMBER: 4.2.2.5.4.2
RID SHORT TITLE: SA and key status terminology

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

From:
The Bad SA Flag shall 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.
To:
The Bad SA Flag shall indicate whether the last TC Transfer Frame received by the SDLS on-board function failed SA verification or carried an SPI pointing to a non-Operational SA or to an Operational SA associated with a non-Active key.

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended ___ Editorial _X__
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:
SA and Key states are well defined and the terminology to describe them should be consistent (not just ‘inactive’).

DISPOSITION: accepted with modification as follows:
The Bad SA Flag shall indicate whether the last TC Transfer Frame received by the SDLS on-board function:

- failed SA verification, or
- carried an SPI pointing **to a SA that is not in Operational state,** or
- carried an SPI pointing to an Operational SA associated with **a key that is not in Active state**.

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER: ESA-MW-21
SUBMITTING ORGANIZATION (Agency, Center): ESA , ESOC

REVIEWER'S NAME: Marcus Wallum
CODE: OPS-GES
E-MAIL ADDRESS: marcus.wallum@esa.int
TELEPHONE: +49 6151 90 3506

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 5-10 PARAGRAPH NUMBER: 5.4.2.5.3.2
RID SHORT TITLE: Key Verification Reply PDU description

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

From:
The Key Verification Reply PDU shall consist of a managed number of contiguously positioned mandatory fields:
(Key ID Field, Response Field) pairs fields (managed length; mandatory).

To:
The Key Verification Reply PDU shall consist of a managed number of contiguously positioned mandatory fields:
(Key ID Field, IV Field, Encrypted Challenge Field, Challenge MAC Field) pairs fields (managed length; mandatory).

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended ___ Editorial _X__
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:
PDU description (5.4.2.5.3.2) is not aligned with PDU depiction (Figure 5-8)

DISPOSITION: accepted.

SUBMITTING ORGANIZATION	CODE	DOCUMENT NUMBER	PARAGRAPH NUMBER	RID SHORT TITLE	DESCRIPTION OF REQUESTED CHANGE	CATEGORY OF REQUESTED CHANGE	SUPPORTING ANALYSIS	DISPOSITION
ESA	MR-03	355x1r1		Compliance with 354x0r1	354x0r1 uses ambiguous language for specifiying the minimum services for key management. It is not clear if 355 shall or may implement the zeroing service.	Recommended		Modify § 3.2.1 as follows : The following **SDLS-specific** service procedures are defined:
ESA	MR-01	355x1r1	4.3.1	Sidechannel elimination	It appears as if for a full implementation, a secure channel with authenticated encryption is required for at least a subset of service commands. Another set of service commands can be communiated in clear, provided that the channel is authenticated. To eliminate side channel information, I propose to recommend the use of authenticated encryption for all service commands. This eliminates some side channels that adversaries have available today. For instance, if they want to provide a rekeying, they	Technical Fact	The use of authenticated encryption is protecting us from ciphertext malleability and therefore from Bleichenbacher-type attacks. Still, at a higher protocol level, side channels may become a problem as soon as the observable system behaviour is a function of adversary actions. In fact, such side channel attacks are typically what breaks cryptographic systems, be it information leakage through timing, message length, or error messages.	see disposition of ESA-MW-16: no requirement for authenticated encryption of EP PDUs. Subject to be discussed in EP GB.

					can determine if they are successful. Similarly, the values set during Set Anti Replay Counter may give rise to refined replay attacks.			
ESA	MR-02	355x1r1	4.2.2	Protection of FSR	Frame Security Reports may contain sensitive information in the sense that they provide feedback to adversaries about their actions. I recommend specifying a protection mechanism for the FSR itself	Recommended		Rejected: FSR are needed at all times to enable TC link operation. An encrypted FSR could be an operational risk: e.g. encryption keys out of synch. Transmission of FSR in the clear is an acceptable risk.

CNES RIDs:

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER: CNES-GM-01
SUBMITTING ORGANIZATION (Agency, Center): CNES Toulouse

REVIEWER'S NAME: Gilles Moury
CODE: DSO/AVI
E-MAIL ADDRESS: gilles.moury@cnes.fr
TELEPHONE: +33 561 273 790

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 4-1 PARAGRAPH NUMBER: 4.1
RID SHORT TITLE: Security Association for transporting EP PDUs

---

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

From:
The interfaces however are generally on the Initiator and Recipient side, and not directly on protocol level. However, a Security Association should be allocated to the Secure Channel (see reference **Erreur ! Source du renvoi introuvable.**) used to transport Extended Procedures PDUs over the space link.

To:
The interfaces however are generally on the Initiator and Recipient side, and not directly on **SDLS** protocol level. **However, at least one Security Association should be allocated for transporting Extended Procedures PDUs over the space link.**

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended _X__ Editorial ___
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:
Modification agreed at the spring 2018 meeting. Avoids referring to the notion of Secure Channel and implying that one Secure Channel should be dedicated to EP PDUs transport.

DISPOSITION: accepted.

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER: CNES-GM-02
SUBMITTING ORGANIZATION (Agency, Center): CNES Toulouse

REVIEWER'S NAME: Gilles Moury
CODE: DSO/AVI
E-MAIL ADDRESS: gilles.moury@cnes.fr
TELEPHONE: +33 561 273 790

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 4-1 PARAGRAPH NUMBER: 4.1
RID SHORT TITLE: Adding reference to upcoming EP green book

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

From:
The SDLS Extended Procedures Concept of Operations describes various options to implement the interface.

To:
The SDLS Extended Procedures Concept of Operations **([C13])** describes various options to implement the interface.

+ add reference [C13] SDLS EP green book 350.11-G in Annex C Informative references

---

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended _X__ Editorial ___
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:
Modification agreed at the spring 2018 meeting. Pointing to the upcoming EP green book in the EP blue book will help implementers.

DISPOSITION: accepted.

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER: CNES-GM-03
SUBMITTING ORGANIZATION (Agency, Center): CNES Toulouse

REVIEWER'S NAME: Gilles Moury
CODE: DSO/AVI
E-MAIL ADDRESS: gilles.moury@cnes.fr
TELEPHONE: +33 561 273 790

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 1-3 PARAGRAPH NUMBER: 1.6
RID SHORT TITLE: Adding definition of Security Unit

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

From:

To:
Add the following definition of Security Unit in §1.6:

On-board electronic unit implementing the recipient part of the SDLS Core and Extended Procedures protocols.

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended _X__ Editorial ___
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:
Security Unit is mentioned in several paragraphs of this standard (1.1, 2.2, 2.4) but not defined. Definition is needed to clarify specification. Modification agreed at spring 2018 meeting but not implemented in final version submitted to CTE.

DISPOSITION: rejected. The following terms should be replaced by “Recipient Security Function”:

- On-board security unit
- On-board security processor
- On-board SDLS function
- SDLS on-board function.

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER: CNES-BS-01
SUBMITTING ORGANIZATION (Agency, Center): CNES Toulouse

REVIEWER'S NAME: Bruno Saba
CODE: DSO/TB/ET
E-MAIL ADDRESS: Bruno.saba@cnes.fr
TELEPHONE: +33 561 282 876

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: - PARAGRAPH NUMBER: -
RID SHORT TITLE: Missing “Key Inventory” procedure

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

From:
-

To:
-

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended _X_ Editorial ___
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:
As defined, the Extended Procedures do not allow for downloading any information on on-board keys such as key-ID and key status.
From a ground point of view, it would be very useful if a “Key Inventory” procedure could be added. This procedure would allow the ground segment to know exactly how many keys are present in the on-board security processor, their ID, and their state (“pre-activated”, “activated”, “deactivated”). If a key is activated, knowing to which SA(s) it is bound to would also be useful.

DISPOSITION: accepted.

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER: CNES-BS-02
SUBMITTING ORGANIZATION (Agency, Center): CNES Toulouse

REVIEWER'S NAME: Bruno Saba
CODE: DSO/TB/ET
E-MAIL ADDRESS: Bruno.saba@cnes.fr
TELEPHONE: +33 561 282 876

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 3-13 PARAGRAPH NUMBER: 3.3.1
RID SHORT TITLE: Missing “Read Anti-Replay Counter” in list

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)
From:
§3.3.1
...
The following service procedures are specified:
– Start SA;
– Stop SA;
– Rekey SA;
– Create SA;
– Delete SA;
– Set Anti-Replay Counter;
– Set Anti-Replay Window; and
– SA Status Request.

To:
§3.3.1
...
The following service procedures are specified:
– Start SA;
– Stop SA;
– Rekey SA;
– Create SA;
– Delete SA;
– Set Anti-Replay Counter;
– Set Anti-Replay Window;
– SA Status Request; and
– Read Anti-Replay Counter.

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended ___ Editorial _X_
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.

EDITORIAL: Typographical or other factual error needing correction.
 (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:
The “Read Anti-Replay Counter” procedure is not in the list in §3.3.1.
Reordering the list (and the related paragraphs...) to put this procedure
immediately after “Set Anti-Replay Counter” may add to readability.

DISPOSITION: accepted

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER: CNES-BS-03
SUBMITTING ORGANIZATION (Agency, Center): CNES Toulouse

REVIEWER'S NAME: Bruno Saba
CODE: DSO/TB/ET
E-MAIL ADDRESS: Bruno.saba@cnes.fr
TELEPHONE: +33 561 282 876

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 3-32 PARAGRAPH NUMBER: 3.4.1
RID SHORT TITLE: “Read Sequence Number” procedure in the list

---

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)
From:
The following service procedures are specified:
– Ping;
– Log Status;
– Dump Log;
– Erase Log;
– Self-Test;
– Read Sequence Number; and
– Alarm Flag Reset.

To:
The following service procedures are specified:
– Ping;
– Log Status;
– Dump Log;
– Erase Log;
– Self-Test; and
– Alarm Flag Reset.

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended ___ Editorial _X_
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:
The Read Sequence Number procedure has been replaced by Read Anti-Replay Counter procedure, now defined in section 3.3.1

DISPOSITION: accepted

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER: CNES-BS-04
SUBMITTING ORGANIZATION (Agency, Center): CNES Toulouse

REVIEWER'S NAME: Bruno Saba
CODE: DSO/TB/ET
E-MAIL ADDRESS: Bruno.saba@cnes.fr
TELEPHONE: +33 561 282 876

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 4-6 PARAGRAPH NUMBER: Table 4.1
RID SHORT TITLE: Read Sequence Number / Read Anti-Replay Counter in list

---

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

From:

-

To:

-

Suppress “Read Sequence Number” from the list.
Add “Read Anti-Replay Counter” after “Set Anti-Replay Counter”

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended ___ Editorial _X_
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:
The Read Sequence Number procedure has been replaced by Read Anti-Replay Counter procedure, now defined in section 3.3.1

DISPOSITION: accepted

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER: CNES-BS-05
SUBMITTING ORGANIZATION (Agency, Center): CNES Toulouse

REVIEWER'S NAME: Bruno Saba
CODE: DSO/TB/ET
E-MAIL ADDRESS: Bruno.saba@cnes.fr
TELEPHONE: +33 561 282 876

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 5-22 PARAGRAPH NUMBER: Figure 5.20
RID SHORT TITLE: Read Sequence Number / Read Anti-Replay Counter (1)

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

From:

Figure 5-20: Read Sequence Number Command PDU

To:

Figure 5-20: Read Anti-Replay Counter Command PDU

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended ___ Editorial _X_
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:
The Read Sequence Number procedure has been replaced by Read Anti-Replay Counter procedure.

DISPOSITION: accepted

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER: CNES-BS-06
SUBMITTING ORGANIZATION (Agency, Center): CNES Toulouse

REVIEWER'S NAME: Bruno Saba
CODE: DSO/TB/ET
E-MAIL ADDRESS: Bruno.saba@cnes.fr
TELEPHONE: +33 561 282 876

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 5-23 PARAGRAPH NUMBER: Figure 5.21
RID SHORT TITLE: Read Sequence Number / Read Anti-Replay Counter (2)

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

From:

Figure 5-21: Read Sequence Number Reply PDU

To:

Figure 5-21: Read Anti-Replay Counter Reply PDU

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended ___ Editorial _X_
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:
The Read Sequence Number procedure has been replaced by Read Anti-Replay Counter procedure.

DISPOSITION: accepted

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER: CNES-BS-07
SUBMITTING ORGANIZATION (Agency, Center): CNES Toulouse

REVIEWER'S NAME: Bruno Saba
CODE: DSO/TB/ET
E-MAIL ADDRESS: Bruno.saba@cnes.fr
TELEPHONE: +33 561 282 876

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: General PARAGRAPH NUMBER: General
RID SHORT TITLE: Read Sequence Number / Read Anti-Replay Counter (3)

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

From:

-

To:

-

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended _X_ Editorial ___
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:
In SDLS core protocol, there is no reference to any “Anti-Replay Counter”. “Anti-Replay Sequence Number” is used throughout the whole document. It might add to readability to align the EP on this terminology.

DISPOSITION: accepted

CSA RIDs:

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER:
SUBMITTING ORGANIZATION (Agency, Center): Government of Ontario, Cyber Security Division

---

REVIEWER'S NAME: Tim Dafoe
CODE:
E-MAIL ADDRESS: tim.dafoe@ontario.ca
TELEPHONE: +1 (416) 327 1260

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 4 PARAGRAPH NUMBER: 2
RID SHORT TITLE: Zeroize Optional

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

Recommend review of decision to render "Zeroize" an optional extended procedure. If adopted would change From: "Zeroize" being included in the second paragraph bullets To: being included instead in the first paragraph bullets.

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended _X_ Editorial ___
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:
Recommend review of decision to render "Zeroize" an optional extended procedure. In contrast to the per-Key-ID revoke and erase support within the extended procedures, FIPS or ISO/IEC zeroize applies to both all keys and all internal critical/sensitive cryptographic and security parameters, including but not limited to seed values, state, and KM credentials. If no mission need exists, please disregard - but if there are reasonable scenarios where a zeroize would be a more expedient and complete measure than revoke and erase of individual keys, with plausible need for such, would recommend revisiting the optional status of "Zeroize'. Another consideration here would be implementation difficulty relative to any relevant/current KM designs or deployments.

DISPOSITION: no requirement for zeroize directive in space system we consider for this standard.

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER:
SUBMITTING ORGANIZATION (Agency, Center): Government of Ontario, Cyber Security Division

---

REVIEWER'S NAME: Tim Dafoe
CODE:
E-MAIL ADDRESS: tim.dafoe@ontario.ca
TELEPHONE: +1 (416) 327 1260

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 12 PARAGRAPH NUMBER: 7
RID SHORT TITLE: "Key OD" in error

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

Revise From: "(Key OD, enc_i)" To: "(Key ID, enc_i)".

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended ___ Editorial _X_
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:

"Key OD" does not appear in the document otherwise, appears to be "Key ID" in error.

DISPOSITION: rejected : unable to find Key OD in the document !

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER:
SUBMITTING ORGANIZATION (Agency, Center): Government of Ontario, Cyber Security Division

---

REVIEWER'S NAME: Tim Dafoe
CODE:
E-MAIL ADDRESS: tim.dafoe@ontario.ca
TELEPHONE: +1 (416) 327 1260

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 6 PARAGRAPH NUMBER: 1 (and throughout)
RID SHORT TITLE: Simplify step wording throughout

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

First line of pg. 6 and wording throughout document reads to the effect of "The step 1" - suggest general change throughout to "Step 1" and omit "The".

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended ___ Editorial _X_
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:

Current wording is awkward, and steps are conveyed even if a leading "The" is removed throughout from the wording of individual steps.

DISPOSITION: rejected : could not find Step 1 in document.

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER:
SUBMITTING ORGANIZATION (Agency, Center): Government of Ontario, Cyber Security Division

---

REVIEWER'S NAME: Tim Dafoe
CODE:
E-MAIL ADDRESS: tim.dafoe@ontario.ca
TELEPHONE: +1 (416) 327 1260

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 17 & 18 PARAGRAPH NUMBER: 2 and 3 (respectively)
RID SHORT TITLE: Confirm outcome of key revocation processing

---

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

Amend the requirement that "a destruction confirmation shall be produced" and to in fact indicate that the true required outcome of step 1 amd step 4 processing is fulsome destruction of the key, not merely status transition, or a confirmation message.

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended _X_ Editorial ___
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:

The current wording of desired/required step 1 and step 4 processing for key revocation is limited to the key status change and production of a key destruction message - suggested that some mention of processing re: actually performing the destruction be included (e.g., one or both of these steps be revised and more clearly indicate such).

DISPOSITION: rejected : no key revocation directive in document.

REVIEW ITEM DISPOSITION (RID):
RED BOOK RID INITIATION FORM

AGENCY RID NUMBER:
SUBMITTING ORGANIZATION (Agency, Center): Government of Ontario, Cyber Security Division

---

REVIEWER'S NAME: Tim Dafoe
CODE:
E-MAIL ADDRESS: tim.dafoe@ontario.ca
TELEPHONE: +1 (416) 327 1260

DOCUMENT NUMBER: CCSDS 355.1-R-1 Red Book, Issue 1
DOCUMENT NAME: SDLS Protocol--Extended Procedures
DATE ISSUED: June 2018
PAGE NUMBER: 1 and 19 PARAGRAPH NUMBER: 3 and 2 (respectively)
RID SHORT TITLE: Amend two uses of "concrete"

DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)

Amend first use of "concrete" on pg. 1, and the sole use of "concrete" on pg. 19. to read "In particular" in the former instance, and "To be more clear" in the latter instance.

CATEGORY OF REQUESTED CHANGE:
Technical Fact ___ Recommended ___ Editorial _X_
NOTES:
TECHNICAL FACT: Major technical change of sufficient magnitude as to render the Recommendation inaccurate and unacceptable if not corrected. (Supporting analysis/rationale is essential.)
RECOMMENDED: Change of a nature that would, if incorporated, produce a marked improvement in document quality and acceptance.
EDITORIAL: Typographical or other factual error needing correction. (This type of change will be made without feedback to submitter.)

SUPPORTING ANALYSIS:

The current wording is awkward and could be seen as imprecise, this is an attempt to tighten both pg. 1 and pg. 19 paragraphs.

DISPOSITION: rejected. No concrete in the document. RID apparently related to some other other unknown document or older version.

NASA RIDs:

REVIEWER 'S NAME	CATEGORY OF REQUESTED CHANGE	DESCRIPTION OF REQUESTED CHANGE: (Use From: "..." To "..." format)	SUPPORTING ANALYSIS	Item Type	Path	DISPOSITION
Craig Biggers taff	technical	Figure 5-20, and 5-21 : Service group and procedure identifiers need to be changed to reflect SA management procedure	Read anti-replay sequence number procedure has been transfered from Monitoring & Control to SA management.			Accepted: Craig will provide correct ID.
Craig Biggers taff	Editorial	From: "c) SDLS Management & Control Service." to: "c) SDLS Monitoring & Control Service."	Use consistent terminology throughout the document.	Item	Lists/ CCSDS 3551R1	Accepted. One occurrence to be corrected in § 2.3.3.
Craig Biggers taff	Editorial	From: "[2] Symmetric Key Management. Proposed Recommendation for Space Data System Practices. Forthcoming." to: "[2]Symmetric Key Management. Issue 1. Draft Recommendation for Space Data System Practices (Red Book), CCSDS 354.0-R-1. Washington, D.C.: CCSDS, June 2018."		Item	Lists/ CCSDS 3551R1	Accepted.