Updated PICS

Tuesday, January 30, 2024 3:14 PM

Protocol Implementation Conformance Statement (PICS)

- **SDLS - Annex A**
    - □ A4 - Supported Space Data Link Protocols
        - ▪ A4/1 - TM Space Data Link Protocol, O.1
        - ▪ A4/2 - TC Space Data link Protocol, O.1
        - ▪ A4/3 - AOS Space Data Link Protocol, O.1
        - ▪ A4/4 - Unified Space Data Link Protocol, O.1
        - ▪ A, O.1 - Support for at least one of A4/1, A4/2, A4/3, A4/4 is M
    - □ A5 - Supported Security Services
        - ▪ A5/1 - Encryption, 4.2.2.4, O.2
            - □ *4.2.2.4 - Every SA shall specify one and only one of the following cryptographic functions to perform: authentication, encryption, or authenticated encryption.*
            - □ *4.2.2.4 NOTE - It is possible to create a 'clear mode' SA using one of the defined service types by specifying the algorithms as a `no-op` function. Such an SA might be used during development. For security reasons, the use of such an SA is not recommended in normal operation.*
        - ▪ A5/2 - Authentication, 4.2.2.4, O.2
            - □ *4.2.2.4 - ^^*
        - ▪ A5/3 - Authenticated Encryption, 4.2.2.4, O.2
            - □ *4.2.2.4 - ^^*
        - ▪ A5, O.2 - Support for at least one of A5/1, A5/2, A5/3 is M
    - □ A6 - Security Association Management Data
        - ▪ A6/1 - GVCID, 3.4.2.2.1 and 4.2.2.2.1, M
            - □ *3.4.2.2.1 - The GVCID parameter shall contain the ID of the Global Virtual Channel(s) applicable to the SA.*
            - □ *3.4.2.2.1 NOTE - The GVCID consists of a Master Channel ID and a Virtual Channel ID. If the TC Space Data Link Protocol is used on the physical channel, a single Global Virtual Channel is applicable to the SA (see requirement 5.2 c).*
            - □ *4.2.2.2.1 - Every SA shall specify one of more Global Virtual Channels or GMAP_IDs (TC and USLP only) with which the SA is the used.*
            - □ *4.2.2.2.1 NOTE 1 - The GVCID consists of a Master Channel ID and a Virtual Channel ID.*
            - □ *4.2.2.2.1 NOTE 2 - The GMAP_ID parameter is applicable only if USLP is used on the physical channel, or if the TC Space Data Link Protocol is used on the physical channel and Segment Headers are used on the TC Virtual Channel. In all other cases it is invalid.*
        - ▪ A6/2 - GMAP_ID, 3.4.2.2.2 and 4.2.2.2.1, C.1
            - □ *3.4.2.2.2 - The GMAP_ID parameter shall contain the ID of the GMAP(s) applicable to the SA.*
            - □ *4.2.2.2.1 - ^^*
        - ▪ A6/3 - SPI, 3.4.2.2.3 and 4.2.2.3, M
            - □ *3.4.2.2.3 - The Security Parameter Index parameter shall contain an index identifying the SA applicable to a frame.*
            - □ *3.4.2.2.3 Note - Each SA on a physical channel is identified by a unique SPI.*
            - □ *4.2.2.3 - SAs shall not be crated for use with Virtual Channels carrying Only Idle Data (OID) Transfer Frames*

- A6/4 - SA_service_type, 3.4.2.2.4 and 4.2.2.4, M
    - *3.4.2.2.4* - The SA_service_type parameter shall indicate the cryptographic function(s) specified for the *SA: one of authentication, encryption, or authenticated encryption.*
    - *4.2.2.4 - ^^*
- A6/5 - SA_length_SN, 3.4.2.2.5 and 4.2.2.5C, M
    - *3.4.2.2.5 - The SA_length_SN parameter shall indicate the length of the Sequence Number field in the Security Header.*
    - *4.2.2.5C - Every SA shall specify the following: c) length of Sequence Number field in Security Header;*
- A6/6 - SA_length_IV, 3.4.2.2.6 and 4.2.2.5B, M
    - *3.4.2.2.6 - The SA_length_IV parameter shall indicate the length of the Initialization Vector field in the Security Header*
    - *4.2.2.5B - Every SA shall specify the following: b) length of Initialization Vector field in Security Header;*
- A6/7 - SA_length_PL, 3.4.2.2.7 and 4.2.2.5D, M
    - *3.4.2.2.7 - The SA_length_PL parameter shall indicate the length of the Pad Length field in the Security Header.*
    - *4.2.2.5D - Every SA shall specify the following: d) length of Pad Length field in Security Header;*
- A6/8 - SA_length_MAC, 3.4.2.2.8 and 4.2.2.5E, M
    - *3.4.2.2.8 - The SA_length_MAC parameter shall indicate the length of the MAC field in the Security Trailer.*
    - *4.2.2.5E - Every SA shall specify the following: e) length of MAC field in Security Trailer.*
- A6/9 - SA_authentication_algorithm, 3.4.2.3.1 and 4.2.2.6.1A, C.2
    - *3.4.2.3.1 - The SA_authentication_algorithm parameter shall indicate the applicable authentication algorithm and mode of operation.*
    - *4.2.2.6.1A - Every SA providing authentication shall specify the following: a) authentication algorithm and mode of operation;*
- A6/10 - SA_authentication_key, 3.4.2.3.2, C.2
    - *3.4.2.3.2 - The SA_authentication_key parameter shall indicate the value of a provided authentication key, or of an index that refers to the actual key.*
- A6/11 - SA_authentication_mask, 3.4.2.3.3 and 4.2.2.6.1B and 4.2.2.6.2, C.2
    - *3.4.2.3.3 - The SA_authentication_mask parameter shall indicate the value of a provided bit mask that is applied against the Transfer Frame in a bitwise-AND operation to generate an Authentication Payload.*
    - *4.2.2.6.1B - Every SA providing authentication shall specify the following: b) authentication bit mask;*
    - *4.2.2.6.2 - Every SA providing authentication shall initialize its authentication bit mask as follows:*
        - *a) the mask to be applied shall be greater or equal in length to the data extending from the first octet of the Transfer Frame Primary Header to the last octet of the Transfer Frame Data Field immediately preceding the MAC field in the Security Trailer;*
        - *NOTE – For variable-length TC or USLP Transfer Frames, accounting for the largest expected frame data field will result in a mask suitable for all Transfer Frames.*
        - *b) the mask bits corresponding to the Virtual Channel ID field of the Transfer Frame Primary Header shall contain 'all ones';*
        - *c) (USLP only) the mask bits corresponding to the MAP ID field of the Transfer Frame Primary Header shall contain 'all ones';*
        - *d) (TM only) the mask bits corresponding to the Master Channel Frame Count*

        field of the Transfer Frame Primary Header shall contain 'all zeros' (i.e., the field shall be excluded from the authenticated data);
        - *e) (AOS only) the mask bits corresponding to the optional Frame Header Error Control field shall contain 'all zeros' (i.e., the field shall be excluded from the authenticated data);*
        - *f) (TC only) the mask bits corresponding to the Segment Header shall contain 'all ones';*
        - *g) (AOS and USLP only) the mask bits corresponding to the Insert Zone shall contain 'all zeros' (i.e., the field shall be excluded from the authenticated data);*
        - *h) the mask bits corresponding to the Security Header, except for the mask bits corresponding to the Initialization Vector field, shall contain 'all ones';*
        - *i) the mask bits corresponding to the Frame Data Field shall contain 'all ones';*
        - *j) the mask bits corresponding to all other Transfer Frame header fields should contain 'all zeros', unless otherwise specified according to mission requirements.*
        - *Note 1 - Missions desiring to authenticate other fields (e.g., Spacecraft ID, TM Frame Secondary Header) can include them among the authenticated data merely by selecting an authentication mask that overrides the defaults listed in paragraph j) above. Possible security concerns affecting the selection of an authentication mask are discussed in reference [D3].*
        - *Note 2 - If the Master (not Virtual) Channel Frame Secondary Header Service (TM only) is used, the TM Frame Secondary Header is excluded from the authenticated data.*
- A6/12 - SA_sequence_number, 3.4.2.3.4 and 4.2.2.6.1C, C.2
    - *3.4.2.3.4 - The SA_sequence_number parameter shall indicate the present value of a managed antireplay sequence number.*
    - *4.2.2.6.1C - Every SA providing authentication shall specify the following: c) managed anti-replay sequence number;*
- A6/13 - SA_sequence_windows, 3.4.2.3.5 and 4.2.2.6.1D, C.3
    - *3.4.2.3.5 - The SA_sequence_window parameter shall indicate the amount of deviation the receiving end will accept between the expected anti-replay sequence number and the sequence number in the received frame.*
    - *4.2.2.6.1D - Every SA providing authentication shall specify the following: d) managed sequence number window.*
- A6/14 - SA_encryption_algorithm, 3.4.2.4 and 4.2.2.7A, C.3
    - *3.4.2.4*
        - *Note - The parameters under this subsection are applicable only if the SA_service_type parameter is Encryption or Authenticated Encryption.*
        - *3.4.2.4.1 - The SA_encryption_algorithm parameter shall indicate the applicable encryption algorithm and mode of operation.*
        - *3.4.2.4.2 - The SA_encryption_key parameter shall indicate the value of a provided encryption key, or of an index that refers to the actual key.*
        - *3.4.2.4.3 - The SA_initialization_vector parameter shall indicate the present value of a managed initialization vector.*
    - *4.2.2.7A - Every SA providing encryption shall specify the following: a) encryption algorithm and mode of operation;*
        - *NOTE – The chosen algorithm and mode also imply other attributes, such as the required block size and the corresponding need to pad undersized data blocks.*
- A6/15 - SA_encryption_key, 3.4.2.4.2, C.3
    - *3.4.2.4.2 - ^^*
- A6/16 - SA_initialization_vector, 3.4.2.4.3 and 4.2.2.7B, C.4

- - - *3.4.2.4.3 - ^^*
      - *4.2.2.7B - Every SA providing encryption shall specify the following: b) managed initialization vector.*
    - A6, C.1 if A4/2 is supported then M, else n/a
    - A6, C.2 if A5/2 or A5/3 is supported then M, else n/a
    - A6, C.3 if A5/1 or A5/3 is supported then M, else n/a
    - A6, C.4 if A5/1 or A5/3 is supported then M, else O
- A7 - Service Primitives
    - A7/1 - ApplySecurity, 3.2.1, Sender M, Receiver n/a
        - *3.2.1 - Overview*
            - *The ApplySecurity Function is defined for the sending end of a physical channel. The function processes a Transfer Frame to apply security features to the frame. The Transfer Frame is a protocol (TM, TC, AOS, or USLP) data structure that is in use on the physical channel.*
            - *The input parameters of the function include the ApplySecurity Payload, containing the partially formatted frame, and the identifiers of the Virtual Channel and the MAP channel (for TC and USLP only). When the function is called, the Security Protocol applies encryption and/or authentication to the data supplied in the ApplySecurity Payload. In any given call to the ApplySecurity Function, the processing depends on the settings for the Security Association of the applicable Virtual Channel or MAP.*
            - *When the ApplySecurity Function has completed the processing, it returns the resulting data to the caller in the return parameter, the ApplySecurity Return.*
    - A7/2 - ProcessSecurity, 3.3.1, Sender n/a, Receiver M
        - *3.3.1 - Overview*
            - *The ProcessSecurity Function is defined for the receiving end of a physical channel. The function provides the receiving end security processing for a Transfer Frame belonging to the underlying protocol (TM, TC, AOS, or USLP) that is in use on the physical channel.*
            - *The input parameters include the ProcessSecurity Payload, containing the frame, and the identifiers of the Virtual Channel and the MAP channel (TC and USLP only). When the function is called, the Security Protocol always applies verification and may apply decryption to the data supplied in the ProcessSecurity Payload. In any given call to the ProcessSecurity Function, the processing depends on the settings for the Security Association of the applicable Virtual Channel or MAP.*
            - *When the ProcessSecurity Function has completed the processing, it returns the results to the caller in the return parameters, which include status indicators and the ProcessSecurity Return.*
- A7.1.1.1 - Apply Security (Sending)
    - A7.1.1/1 - TM ApplySecurity Payload, 3.2.2.2, C.5
        - *3.2.2.2 - The TM ApplySecurity Payload shall consist of the portion of the TM Transfer Frame (see reference [1]) from the first octet of the Transfer Frame Primary Header to the last octet of the Transfer Frame Data Field.*
        - *NOTE 1 - The TM Transfer Frame is the fixed-length protocol data unit of the TM Space Data Link Protocol. The length of any Transfer Frame transferred on a physical channel is constant, and is established by management.*
        - *NOTE 2 - The portion of the TM Transfer Frame contained in the TM ApplySecurity Payload parameter includes the Security Header field. When the ApplySecurity Function is called, the Security Header field is empty; that is, the caller has not set any values in the Security Header.*
    - A7.1.1/2 - TC ApplySecurity Payload, 3.2.2.3, C.1
        - *3.2.2.3 - The TC ApplySecurity Payload shall consist of the portion of the TC Transfer*

Frame (see reference [2]) from the first octet of the Transfer Frame Primary Header to the last octet of the Transfer Frame Data Field.

  - *NOTE 1 - The TC Transfer Frame is the variable-length protocol data unit of the TC Space Data Link Protocol.*
  - *NOTE 2 - The portion of the TC Transfer Frame contained in the TC ApplySecurity Payload parameter includes the Security Header field. When the ApplySecurity Function is called, the Security Header field is empty; that is, the caller has not set any values in the Security Header.*
- A7.1.1/3 - AOS ApplySecurity Payload, 3.2.2.4, C.6
  - *3.2.2.4 - The AOS ApplySecurity Payload shall consist of the portion of the AOS Transfer Frame (see reference [3]) from the first octet of the Transfer Frame Primary Header to the last octet of the Transfer Frame Data Field.*
  - *NOTE 1 - The AOS Transfer Frame is the fixed-length protocol data unit of the AOS Space Data Link Protocol. The length of any Transfer Frame transferred on a physical channel is constant, and is established by management.*
  - *NOTE 2 - The portion of the AOS Transfer Frame contained in the AOS ApplySecurity Payload parameter includes the Security Header field. When the ApplySecurity Function is called, the Security Header field is empty; that is, the caller has not set any values in the Security Header.*
- A7.1.1/4 - USLP ApplySecurity Payload, 3.2.2.5, C.7
  - *3.2.2.5 - The USLP ApplySecurity Payload shall consist of the portion of the USLP Transfer Frame (see reference [5]) from the first octet of the Transfer Frame Primary Header to the last octet of the Transfer Frame Data Field.*
  - *NOTE 1 - The USLP Transfer Frame is the fixed-length or variable-length protocol data unit of USLP. The length of a fixed-length USLP Transfer Frame transferred on a physical channel is established by management.*
  - *NOTE 2 - The portion of the USLP Transfer Frame contained in the USLP ApplySecurity Payload parameter includes the Security Header field. When the ApplySecurity Function is called, the Security Header field is empty, that is, the caller has not set any values in the Security Header.*
- A7.1.1/5 - GVCID, 3.2.2.5, M
  - ***3.2.2.6*** *- The Global Virtual Channel Identifier (GVCID) parameter shall contain the ID of the Global Virtual Channel (see references [1], [2], [3], and [5]) of the partially formatted Transfer Frame contained in the ApplySecurity Payload.*
  - *NOTE - The GVCID consists of a Master Channel ID and a Virtual Channel ID.*
- A7.1.1/6 - GMAP_ID, 3.2.2.7, C.1
  - *3.2.2.7 - The GMAP Identifier (GMAP_ID) parameter shall contain the ID of the GMAP (see references [2] and [5]) of the partially formatted TC or USLP Transfer Frame contained in the TC or USLP ApplySecurity Payload.*
  - *NOTE 1 - The GMAP_ID consists of a GVCID and a TC or USLP MAP ID that indicates a MAP Channel within the Virtual Channel specified by GVCID.*
  - *NOTE 2 - The GMAP_ID is applicable only if the ApplySecurity Payload is a TC or USLP ApplySecurity Payload and the Virtual Channel specified by the GVCID is using Segment Headers (applicable only to TC).*
- A7.1.1/7 - AEAD algorithms' plaintext, 4.2.3.2.2.3.A.1, C.8
  - *4.2.3.2.2.3.A.1 - When the Security Type is authenticated encryption: a) If the cryptographic algorithm requires both plaintext and Additional Authenticated Data (AAD) as separate inputs, then: 1) the plaintext shall be the Transfer Frame Data Field*
- A7.1.1/8 - AEAD algorithms' AAD, 4.2.3.2.2.3.A.2, C.8
  - *4.2.3.2.2.3.A.2 - When the Security Type is authenticated encryption: If the cryptographic algorithm requires both plaintext and Additional Authenticated Data (AAD) as separate inputs, then: 2) the AAD shall be the portion from the first octet*

of the Authentication Payload to the octet immediately preceding the Transfer Frame Data Field;

- *NOTE – This definitional distinction is common to a class of cryptographic algorithms known as 'Authenticated Encryption with Associated Data' (AEAD) algorithms.*

- A7.1.1/9 - Encrypt frame data, 4.2.3.3A, C.3
  - *4.2.3.3A - If encryption is selected for an SA, then for each transmitted frame belonging to that SA, the sender shall: a) encrypt the Transfer Frame Data Field*
- A7.1.1/10 - Put length of pad in header, 4.2.3.3B, O
  - *4.2.3.3B - If encryption is selected for an SA, then for each transmitted frame belonging to that SA, the sender shall: b) if the algorithm and mode selected for the SA require the use of fill padding, place the number of fill bytes used into the Pad Length field of the Security Header.*
- A7.1.1/11 - Increment SN, 4.2.3.4A, C.2
  - *4.2.3.4A - If authentication is selected for an SA, then for each transmitted frame belonging to that SA, the sender shall: a) increment the SA's managed sequence number by one;*
- A7.1.1/12 - Put SN in header, 4.2.3.4B, C.2
  - *4.2.3.4B - If authentication is selected for an SA, then for each transmitted frame belonging to that SA, the sender shall: b) place the managed sequence number in the Sequence Number field of the Security Header, unless that SA specifies use of the Initialization Vector field of the Security Header instead;*
  - *NOTE – The interpretation of a sequence number rollover (to zero) is mission specific. Possible interpretations and problems linked with this rollover are discussed in reference [D3].*
- A7.1.1/13 - Get Authentication Payload data, 4.2.3.4C, C.2
  - *4.2.3.4C - If authentication is selected for an SA, then for each transmitted frame belonging to that SA, the sender shall: c) complete the Security Header as specified in 4.1.1;*
- A7.1.1/14 - Apply mask, 4.2.3.4D, C.2
  - *4.2.3.4D - If authentication is selected for an SA, then for each transmitted frame belonging to that SA, the sender shall: d) apply the SA's authentication bit mask in a bitwise-AND operation against the partial frame, thus resulting in the Authentication Payload;*
  - *NOTE – The partial frame supplied in the ApplySecurity Payload consists of the portion from the start of the Transfer Frame Primary Header to the end of the Transfer Frame Data Field. The result is used for the masking operation.*
- A7.1.1/15 - Compute MAC, 4.2.3.4E, C.2
  - *4.2.3.4E - If authentication is selected for an SA, then for each transmitted frame belonging to that SA, the sender shall: e) compute a MAC over the Authentication Payload;*
- A7.1.1/16 - Truncate MAC, 4.2.3.4F, O
  - *4.2.3.4F -If authentication is selected for an SA, then for each transmitted frame belonging to that SA, the sender shall: f) (if necessary) truncate the least-significant bits of the computed MAC, such that the result is of identical length to the MAC field in the Security Trailer;*
- A7.1.1/17 - Put MAC in trailer, 4.2.3.4G, C.2
  - *4.2.3.4G - If authentication is selected for an SA, then for each transmitted frame belonging to that SA, the sender shall: g) place the computed MAC in the Security Trailer;*
- A7.1.1/18 - Return status to caller, 3.2.3, M
  - *3.2.3 - The ApplySecurity Return shall consist of the portion of the Transfer Frame starting at the first octet of the Security Header and ending at the last octet of the*

        Security Trailer, if present, or the last octet of the Transfer Frame Data Field, if the Security Trailer is not present.
    - *NOTE - When the ApplySecurity function has completed the processing for the frame that was input in the ApplySecurity Payload parameter, it returns part of the processed frame in the ApplySecurity Return parameter*
  - A7.1.1, C.1 if A4/2 is supported them M, else n/a
  - A7.1.1, C.2 if A5/2 or A5/3 is supported then M, else n/a
  - A7.1.1, C.3 if A5/1 or A5/3 is supported then M, else n/a
  - A7.1.1, C.5 if A4/1 is supported then M, else n/a
  - A7.1.1, C.6 if A4/3 is supported then M, else n/a
  - A7.1.1, C.7 if A4/4 is supported then M, else n/a
  - A7.1.1, C.8 if A5/3 is supported then M, else n/a
- A7.1.2 - Process Security (Receiving)
  - A7.1.2/1 - TM ProcessSecurity Payload, 3.3.2.2, C.5
    - 3.3.2.2 - The TM ProcessSecurity Payload shall consist of the portion of the TM Transfer Frame (see reference [1]) from the first octet of the Transfer Frame Primary Header to the last octet of the Security Trailer, if present, or the last octet of the Transfer Frame Data Field, if the Security Trailer is not present.
    - NOTE - The TM Transfer Frame is the fixed-length protocol data unit of the TM Space Data Link Protocol. The length is constrained by the TM Synchronization and Channel Coding Blue Book (reference [D5]). The length of any Transfer Frame transferred on a physical channel is constant, and is established by management.
  - A7.1.2/2 - TC ProcessSecurity Payload, 3.3.2.3, C.1
    - 3.3.2.3 - The TC ProcessSecurity Payload shall consist of the portion of the TC Transfer Frame (see reference [2]) from the first octet of the Transfer Frame Primary Header to the last octet of the Security Trailer, if present, or the last octet of the Transfer Frame Data Field, if the Security Trailer is not present.
    - NOTE - The TC Transfer Frame is the variable-length protocol data unit of the TC Space Data Link Protocol.
  - A7.1.2/3 - AOS ProcessSecurity Payload, 3.3.2.4, C.6
    - 3.3.2.4 - The AOS ProcessSecurity Payload shall consist of the portion of the AOS Transfer Frame (see reference [3]) from the first octet of the Transfer Frame Primary Header to the last octet of the Security Trailer, if present, or the last octet of the Transfer Frame Data Field, if the Security Trailer is not present.
    - NOTE - The AOS Transfer Frame is the fixed-length protocol data unit of the AOS Space Data Link Protocol. The length is constrained by the TM Synchronization and Channel Coding Blue Book (reference [D5]). The length of any Transfer Frame transferred on a physical channel is constant, and is established by management.
  - A7.1.2/4 - USLP ProcessSecurity Payload, 3.3.2.5, C.7
    - 3.3.2.5 - The USLP ProcessSecurity Payload shall consist of the portion of the USLP Transfer Frame (see reference [5]) from the first octet of the Transfer Frame Primary Header to the last octet of the Security Trailer, if present, or the last octet of the Transfer Frame Data Field, if the Security Trailer is not present.
    - NOTE - The USLP Transfer Frame is the variable- or fixed-length protocol data unit of USLP
  - A7.1.2/5 - GVCID, 3.3.2.5, C.7
    - ***3.3.2.6*** *- The GVCID parameter shall contain the ID of the Global Virtual Channel (see references [1], [2], [3], and [5]) of the partial Transfer Frame contained in the ProcessSecurity Payload.*
    - *NOTE - The GVCID consists of a Master Channel ID and a Virtual Channel ID.*
  - A7.1.2/6 - GMAP_ID, 3.3.2.7, C.1
    - *3.3.2.7 - The GMAP_ID parameter shall contain the ID of the GMAP (see references [2] and [5]) of the partial TC or USLP Transfer Frame contained in the TC or USLP*

ProcessSecurity Payload.

- *NOTE 1 - The GMAP_ID consists of a GVCID and a TC or USLP MAP ID that indicates a MAP Channel within the Virtual Channel specified by GVCID.*
- *NOTE 2 - The GMAP_ID is applicable only if the ProcessSecurity Payload is a TC or USLP ProcessSecurity Payload and the Virtual Channel specified by the GVCID is using Segment Headers (applicable only to TC).*

- A7.1.2/7 - Discard frames with wrong SA and report exceptions, 4.2.4.3, M
    - *4.2.4.3 - If encryption is selected for an SA, then for each transmitted frame belonging to that SA, the sender shall:*
        - *a) encrypt the Transfer Frame Data Field;*
        - *b) if the algorithm and mode selected for the SA require the use of fill padding, place the number of fill bytes used into the Pad Length field of the Security Header.*
- A7.1.2/8 - AEAD algorithms' plaintext, 4.2.4.2.3.2.A.1, C.8
    - *4.2.4.2.3.2.A.1 - When the Security Type is authenticated encryption: a) If the cryptographic algorithm requires both plaintext and AAD as separate inputs, then: 1) the plaintext shall be the Transfer Frame Data Field,*
- A7.1.2/9 - AEAD algorithms' AAD, 4.2.4.2.3.2.A.2, C.8
    - *4.2.4.2.3.2.A.2 - When the Security Type is authenticated encryption: a) If the cryptographic algorithm requires both plaintext and AAD as separate inputs, then: 2) the AAD shall be the portion from the first octet of the Authentication Payload to the octet immediately preceding the Transfer Frame Data Field; NOTE – This definitional distinction is common to a class of cryptographic algorithms known as AEAD algorithms.*
- A7.1.2/10 - Get Authentication Payload data, 4.2.4.4A, C.2
    - *4.2.4.4A - If authentication is selected for an SA, then for each received frame belonging to that SA, the receiver shall: a) apply the SA's authentication bit mask in a bitwise-AND operation against the portion of the partial Transfer Frame in the ProcessSecurity Payload parameter, extending from the first octet of the Transfer Frame Primary Header to the last octet of the Transfer Frame Data Field immediately preceding the MAC field in the Security Trailer, thus resulting in the Authentication Payload;*
- A7.1.2/11 - Apply mask, 4.2.4.4A, C.2
    - *4.2.4.4A - ^^*
- A7.1.2/12 - Compute MAC, 4.2.4.4B, C.2
    - *4.2.4.4B - If authentication is selected for an SA, then for each received frame belonging to that SA, the receiver shall: b) compute a MAC over the Authentication Payload;*
- A7.1.2/13 - Truncate computed MAC, 4.2.4.4B, C.2
    - *4.2.4.4B - ^^*
- A7.1.2/14 - Compare to received MAC, 4.2.4.4D, C.2
    - *4.2.4.4D - If authentication is selected for an SA, then for each received frame belonging to that SA, the receiver shall: d) verify that the computed MAC matches the MAC received in the Security Trailer;*
- A7.1.2/15 - Report MAC exceptions, 4.2.4.4E, C.2
    - *4.2.4.4E - If authentication is selected for an SA, then for each received frame belonging to that SA, the receiver shall: e) report an exception to the service user for frames in which the received frame fails MAC verification and discard those frames;*
- A7.1.2/16 - Discard frames with bad MAC, 4.2.4.4E, C.2
    - *4.2.4.4E - ^^*
- A7.1.2/17 - Archive rejected-MAC frames, 4.2.4.4E, O
    - *4.2.4.4E - ^^*
- A7.1.2/18 - Read received SN, 4.2.4.4F, C.2

- *4.2.4.4F - If authentication is selected for an SA, then for each received frame belonging to that SA, the receiver shall: f) extract the received sequence number from either the Sequence Number field or the Initialization Vector field of the Security Header, according to the options specified for that SA;*
  - A7.1.2/19 - Compare to managed SN, 4.2.4.4G, C.2
    - *4.2.4.4G - If authentication is selected for an SA, then for each received frame belonging to that SA, the receiver shall: g) compare the received sequence number to the managed sequence number;*
  - A7.1.2/20 - Report SN exceptions, 4.2.4.4I, C.2
    - *4.2.4.4I - If authentication is selected for an SA, then for each received frame belonging to that SA, the receiver shall: i) report an exception to the service user for frames in which the received sequence number is larger than the managed sequence number by a value greater than the window defined for that SA, and discard those frames;*
    - *NOTE – Discarded frames can be archived for forensic investigation if desired.*
  - A7.1.2/21 - Discard frames with bad SN, 4.2.4.4I, C.2
    - *4.2.4.4I - ^^*
  - A7.1.2/22 - Archive rejected-SN frames, 4.2.4.4I, O
    - *4.2.4.4I - ^^*
  - A7.1.2/23 - Update managed SN, 4.2.4.4J, C.2
    - *4.2.4.4J - If authentication is selected for an SA, then for each received frame belonging to that SA, the receiver shall: j) only upon receipt of frames that pass the verification operations a)–i) above, replace the managed sequence number with the received sequence number;*
    - *NOTE – The interpretation of a sequence number rollover (to zero) is mission specific. Possible interpretations and problems linked with this rollover are discussed in reference [D3].*
  - A7.1.2/24 - Removed trailer, 4.2.4.4, C.2
    - *4.2.4.4 - ^^*
  - A7.1.2/25 - Decrypt frame data, 4.2.4.5A, C.3
    - *4.2.4.5A - If encryption is selected for an SA, then for each received frame belonging to that SA, the receiver shall: a) decrypt the Transfer Frame Data Field;*
  - A7.1.2/26 - Remove header, 4.2.4.5B, M
    - *4.2.4.5B - If encryption is selected for an SA, then for each received frame belonging to that SA, the receiver shall: b) (optionally) if specified for that SA, extract the count of fill bytes used from the Pad Length field of the Security Header, and remove those fill bytes from the Frame Data Field to be returned.*
  - A7.1.2/27 - Return status to caller, -, M
  - A7.1.2, C.1 if A4/2 is supported them M, else n/a
  - A7.1.2, C.2 if A5/2 or A5/3 is supported then M, else n/a
  - A7.1.2, C.3 if A5/1 or A5/3 is supported then M, else n/a
  - A7.1.2, C.5 if A4/1 is supported then M, else n/a
  - A7.1.2, C.6 if A4/3 is supported then M, else n/a
  - A7.1.2, C.7 if A4/4 is supported then M, else n/a
  - A7.1.2, C.8 if A5/3 is supported then M, else n/a
- A8.1 - Security Header
  - A8.1/1 - SPI, 4.1.1.1.3A and 4.1.1.2, M
    - *4.1.1.1.3A - The Security Header shall consist of one mandatory field and three optional fields, positioned contiguously, in the following sequence: a) Security Parameter Index (16 bits; mandatory);*
    - *4.1.1.2*
      - *4.1.1.2.1 - Bits 0-15 of the Security Header shall contain the SPI.*
      - *4.1.1.2.2 - The SPI shall be used as an index to identify an SA.*

        - *4.1.1.2.3 - The values of 'all zeros' (0) and 'all ones' (65535) for this field are reserved by CCSDS for future use.*
    - A8.1/2 - IV, 4.1.1.1.3B and 4.1.1.3, C.4
      - *4.1.1.1.3B - The Security Header shall consist of one mandatory field and three optional fields, positioned contiguously, in the following sequence: b) Initialization Vector (octet-aligned, fixed-length for the duration of the SA; optional);*
      - *4.1.1.3*
        - *4.1.1.3.1 - The Initialization Vector field shall follow the Security Parameter Index field, without gap.*
        - *4.1.1.3.2 - The Initialization Vector field shall contain the initialization vector, or an agreed upon portion of it, consisting of an integral number of octets.*
        - *4.1.1.3.3 - The Initialization Vector field length is managed and is fixed for the duration of the SA.*
        - *4.1.1.3.4 - If an initialization vector is not required for an SA, the Initialization Vector field shall be zero octets in length.*
    - A8.1/3 - SN, 4.1.1.1.3C and 4.1.1.4, C.2
      - *4.1.1.1.3C - The Security Header shall consist of one mandatory field and three optional fields, positioned contiguously, in the following sequence: c) Sequence Number (octet-aligned, fixed-length for the duration of the SA; optional);*
      - *4.1.1.4*
        - *4.1.1.4.1 - The Sequence Number field shall follow the Initialization Vector field, without gap.*
        - *4.1.1.4.2 - The Sequence Number field, if authentication or authenticated encryption is selected for an SA, shall contain the anti-replay sequence number, consisting of an integral number of octets.*
        - *NOTE - For systems that implement authenticated encryption using a simple incrementing counter as an initialization vector (i.e., as in counter-mode cryptographic algorithms), the Initialization Vector field of the Security Header may serve also as the Sequence Number. In this case, the Sequence Number field in the Security Header is zero octets in length.*
        - *4.1.1.4.3 - The Sequence Number field length is managed and is fixed for the duration of the SA.*
        - *4.1.1.4.4 - If authentication or authenticated encryption is not selected for an SA, the Sequence Number field shall be zero octets in length.*
    - A8.1/4 - PL, 4.1.1.1.3D and 4.1.1.5, C.3
      - *4.1.1.1.3D - The Security Header shall consist of one mandatory field and three optional fields, positioned contiguously, in the following sequence: d) Pad Length (octet-aligned, fixed-length for the duration of the SA; optional).*
      - *4.1.1.5 - If authentication or authenticated encryption is not selected for an SA, the Sequence Number field shall be zero octets in length.*
    - A8.1/5 - Max length, 4.1.1.4, M
      - *4.1.1.1.4 - ^^*
    - A8.1, C.2 if A5/2 or A5/3 is supported then M, else n/a
    - A8.1, C.3 if A5/1 or A5/3 is supported then M, else n/a
    - A8.1, C.4 if A5/1 or A5/3 is supported then M, else O
  - A8.2 - Security Trailer
    - A8.2/1 - MAC, 4.1.2.1, C.9
      - *4.1.2.1 - The presence or absence of a Security Trailer on a Virtual Channel or MAP shall remain constant throughout a mission.*
    - A8.2, C.9 if A5/2 or A5/3 is supported then M, else O

- **SDLS-EP - Annex A**
  - A4 - Supported Security Services

    - A4/1 - Key Management, -, O.1
    - A4/2 - SA Management, -, O.1
    - A4/3 - Monitoring & Control, -, O.1
    - A4, O.1 Support for at least one of A4/1, A4/2, or A4/3 is M
- A5.1 - Key Management Service Primitives
    - A5.1/1 - OTAR, -, M
    - A5.1/2 - Key Activation -, M
    - A5.1/3 - Key Deactivation, -, M
    - A5.1/4 - Key Destruction, -, O
    - A5.1/5 - Key Verification, 0, M
    - A5.1/6 - Key Inventory, -, M
- A5.2 - SA Management Service Primitives
    - A5.2/1 - Start SA, -, M
    - A5.2/2 - Stop SA, -, M
    - A5.2/3 - Rekey SA, -, O
    - A5.2/4 - Expire SA, -, C.2
    - A5.2/5 - Create SA, -, O
    - A5.2/6 - Delete SA, -, C.3
    - A5.2/7 - Set ARSN, -, O
    - A5.2/8 - Set ARSNW, -, O
    - A5.2/9 - SA Status Request, -,O
    - A5.2/10 - Read Sequence Number, -, M
    - A5.2, C.2 if A5.2/3 is supported then M, else O
    - A5.2, C.3 if A5.2/5 is supported then M, else n/a
- A5.3 - Monitoring & Control Service Primitives
    - A5.3/1 - Ping, -, M
    - A5.3/2 - Log Status, -, C.1
    - A5.3/3 - Dump Log, -, C.1
    - A5.3/4 - Erase Log, -, C.1
    - A5.3/5 - Self-test, -, M
    - A5.3/6 - Alarm Flag Reset, -, M
    - A5.3, C.1 if Security Log implemented then Items 2, 3, and 4 mandatory
- A6.1 - PDU Header
    - A6.1/1 - Procedure Type, -, M
    - A6.1/2 - User Flag, -, M
    - A6.1/3 - Service Group, -, M
    - A6.1/4 - Procedure Identification, -, M
    - A6.1/5 - Length, -, M
    - A6.1/6 - PDU Data Field, -, O
- A6.2 - OTAR Command PDU Data Field
    - A6.2/1 - Master Key ID, -, M
    - A6.2/2 - Initialization Vector, -, O
    - A6.2/3 - Encrypted Key ID, -, M
    - A6.2/4 - Encrypted Key, -, M
- A6.3 - Key Activation Command PDU Data Field
    - A6.3/1 - Key ID, -, M
- A6.4 - Key Deactivation Command PDU Data Field
    - A6.4/1 - Key ID, -, M
- A6.5 - Key Destruction Command PDU Data Field
    - A6.5/1 - Key ID, -, M
- A6.6 - Key Verification PDU Data Field
    - A6.6/1 - Set of Key IDs, -, M
    - A6.6/2 - Set of Challenges, -, M

  - A6.6/3 - Set of Challenge Responses, -, M
- A6.7 - Key Inventory PDU Data Field
  - A6.7/1 - Range of Key IDs, -, M
  - A6.7/2 - Set of (Key ID, Key States), -, M
- A6.8 - Start SA PDU Data Field
  - A6.8/1 - SPI, -, M
  - A6.8/2 - GVCID/GMAP ID, -, M
- A6.9 - Stop SA PDU Data Field
  - A6.9/1 - SPI, -, M
- A6.10 - Rekey SA PDU Data Field
  - A6.10/1 - SPI, -, M
  - A6.10/2 - ARSN, -, M
  - A6.10/3 - Encryption Key ID, - O.1
  - A6.10/4 - Authentication Key ID, -, O.1
  - A6.10, O.1 Support for at least one of A4/3 or A4/4 is M
- A6.11 - Expire SA PDU Data Field
  - A6.11/1 - SPI, -, M
- A6.12 - Create SA PDU Data Field
  - A6.12/1 - SPI, -, M
  - A6.12/2 - Encryption Key ID, -, M
  - A6.12/3 - Authentication Key ID, -, M
  - A6.12/4 - SH IV Length, -, M
  - A6.12/5 - SH SN Length, -, M
  - A6.12/6 - SH PL Length, -, M
  - A6.12/7 - ST MAC Length, -, M
  - A6.12/8 - Encr. Cipher Suite Length, -, M
  - A6.12/9 - Encryption Cipher Suite, -, M
  - A6.12/10 - IV Length, -, M
  - A6.12/11 - IV, -, M
  - A6.12/12 - Auth. Cipher Suite Length, -, M
  - A6.12/13 - Authentication Cipher Suite, -, M
  - A6.12/14 - Auth. Bit Mask Length, -, M
  - A6.12/15 - Authentication Bit Mask, -, M
  - A6.12/16 - ARSN Length, -, M
  - A6.12/17 - ARSN, -, M
  - A6.12/18 - ARSNW Length, -, M
  - A6.12/19 - ARSNW, -, M
- A6.13 - Delete SA PDU Data Field
  - A6.13/1 - SPI, -, M
- A6.14 - Set ARSN PDU Data Field
  - A6.14/1 - SPI, -, M
  - A6.14/2 - ARSN, -, M
- A6.15 - Set ARSNW PDU Data Field
  - A6.15/1 - SPI, -, M
  - A6.15/2 - ARSNW, -, M
- A6.16 - SA Status Request PDU Data Field
  - A6.16/1 - SPI, -, M
- A6.17 - Read Sequence Number Reply PDU Data Field
  - A6.17/1 - Anti-Replay Sequence Number Value, -, M
- A6.18 - SA Status Request Reply PDU Data Field
  - A6.18/1 - SPI, -, M
  - A6.18/2 - Last State Transition, -, M
- A6.19 - Ping Command PDU Data Field

    - None
- A6.20 - Ping Reply PDU Data Field
    - None
- A6.21 - Log Status Command PDU Data Field
    - None
- A6.22 - Log Status Reply PDU Data Field
    - A6.22/1 - Event Message Tag, -, M
    - A6.22/2 - Event Message Length, -, M
    - A6.22/3 - Event Message Value, -, M
- A6.23 - Erase Log Command PDU Data Field
    - None
- A6.24 - Log Status Reply PDU Data Field
    - A6.24/1 - Number of events, -, M
    - A6.24/2 - Remaining Space, -, M
- A6.25 - Self-Test Command PDU Data Field
    - None
- A6.26 - Self-Test Reply PDU Data Field
    - A6.26/1 - Self-Test Result, -, M
- A6.27 - Alarm-Flag Reset Command PDU Data Field
    - None