Leon S. Scaldeferri
Office of Information Security Research

NSA, R22
9800 Savage Rd.
Ft. Meade MD 20755-6000

(301) - 688 - 0293 /0289[fax]
em: lsscald@afterlife.ncsc.mil

1. Opinions expressed in this paper are those of the author and do not represent the opinions or position of the FWUF or NSA.
SDE PDU Structure

SDE uses a single PDU type.

SDE PDU may contain up to five elements.

1. Clear Header
2. Protected Header
3. Data (SDE SDU)
4. PAD
5. Integrity Check Value (ICV)

All these elements are optional except Data.

Protected Header, Data, and PAD may be transformed by the Integrity algorithm.

Protected Header, Data, PAD and ICV shall be transformed when the confidentiality algorithm is applied.
Construction of the SDE PDU

SDE Security Associations

Initial Exchange

Security Associations

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Confid.</th>
<th>Integ.</th>
<th>Alg. ID</th>
<th>Alt. ID</th>
<th>MDF</th>
<th>SMIB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Ass. #1</td>
<td>Y</td>
<td>Y</td>
<td>1</td>
<td>2</td>
<td>8ADBC7</td>
<td></td>
</tr>
<tr>
<td>Security Ass. #2</td>
<td>N</td>
<td>Y</td>
<td>1</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Ass. #3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Ass. #n</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SMIB
Station Objects

- Station_Clear_Hdr: Boolean
- Station_MDF: Boolean

Security Association Objects

- Local_SAID: Octetstring
- Remote_SAID: Octetstring
- Assoc_MDF: Boolean
- Confid: Boolean
- Confid_Alg_ID: Octetstring
- Integ: Boolean
- Integ_Alg_ID: Octetstring
- Padding_pres: Boolean
- ID_pres: Boolean
- SDE_SAP: Octetstring
- Remote_SDE: Boolean
- Outgoing_Source_MAC_Address: Octetstring
- Outgoing_Destination_MAC_Address: Octetstring
- Incoming_Source_MAC_Address: Octetstring
- Incoming_Destination_MAC_Address: Octetstring
SDE TYPES

Case 1. Single SDE used by STA1 & STA2

Case 2. Two Options;
   a. Single SDE used by STA1 & STA3, API passes
      SDE unmodified, may still check validity.
   b. Two SDE's used one for STA1 to API and
      another for API to STA3, API removes SDE
      from one path and insert new SDE other path.

Case 3. STA1 to API SDE may be same or different from
        AP2 to STA4 SDE.

Case 4. STA1 SDE is passed unmodified through API
        and AP2 to STA4, may check for validity, other
        combinations possible.

Case 5. API removes SDE for transport of SDU to WS1,
        (no knowledge on WS1).

Case 6. API leaves SDE intact with knowledge that WS1
        is an SDE entity, may check for validity.
   • In cases 2b, 3, and 5 Access Point treats all SDE's alike,
     applies SDE on wireless portion of path only.
   • In cases 2a, 4, and 6 AP determines final destination and
     either passes SDE unmodified or replaces it with new
     SDE. SDE's treatment is dependent on knowledge resi-
     dent in AP data base.

Station Security Associations

1. STA1 ← SDE → STA2
2. STA1 ← SDE₁ → API ← SDE₃ → STA3
3. STA1 ← SDE₁ → API ← CLR → AP2 ← SDE₄ → STA4
4. STA1 ← SDE₁ → API ← SDE → AP2 ← SDE₄ → STA4
5. STA1 ← SDE₁ → API ← CLR → PT ← CLR → WS₁
6. STA1 ← SDE₁ ← SDE₂ ← PT ← SDE₃ ← WSI (SDE)