### Security Section Pictures

<table>
<thead>
<tr>
<th>Project</th>
<th>IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Security Section Pictures</td>
</tr>
<tr>
<td>Date Submitted</td>
<td>30 January, 2015</td>
</tr>
<tr>
<td>Source</td>
<td>Tero Kivinen</td>
</tr>
<tr>
<td>E-mail</td>
<td><a href="mailto:kivinen@iki.fi">kivinen@iki.fi</a></td>
</tr>
<tr>
<td>Re:</td>
<td>Security section pictures</td>
</tr>
<tr>
<td>Abstract</td>
<td>Pictures relating to the security section. These are not normative, but might help understanding security section.</td>
</tr>
<tr>
<td>Purpose</td>
<td>Security Section pictures</td>
</tr>
<tr>
<td>Notice</td>
<td>This document has been prepared to assist the IEEE P802.15. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.</td>
</tr>
<tr>
<td>Release</td>
<td>The contributor acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.15.</td>
</tr>
</tbody>
</table>
Security PIB

This picture describes security PIB tables (table 9-8 – 9-16) in graphical format. This picture shows the PIB as it is defined in the IEEE Std 802.15.4-2020:
This picture shows the PIB as it is defined in the 802.15.4y amendment:
Outgoing frame security procedure

1. Is security needed?
   - If securityLevel is non-zero, proceed.
   - If securityLevel is zero, store frame counter and exit.

2. Is security enabled?
   - If macSecurityEnabled is TRUE, proceed.
   - If macSecurityEnabled is FALSE, error: unsupported security.

3. Obtain KeyDescriptor.
   - If finding KeyDescriptor failed, error: unavailable key.

4. Check frame counter value.
   - If frame counter = 0xffffffff, error: counter error.

5. Insert Auxiliary Security Header field.

6. Secure the frame.

7. Store frame counter.

SUCCESS
Incoming frame security procedure

1. Check for Legacy security.
2. Parse security header field.
3. Obtain source address.
4. Parse auxiliary security header field.
5. Obtain KeyDescriptor.
6. Obtain DeviceDescriptor.
7. Obtain frame counter.
8. Check frame counter.
10. Store frame counter.
13. Check IE Key Usage Policy.
14. Check security level.
15. Check key usage policy.

Error messages:
- UNSUPPORTED_LEGACY
- UNSUPPORTED_SECURITY
- UNAVAILABLE_KEY
- UNAVAILABLE_DEVICE
- COUNTER_ERROR
- SECURITY_ERROR
- UNAVAILABLE_SECURITY_LEVEL
- IMPROPER_SECURITY_LEVEL
- IMPROPER_KEY_TYPE

Frame Version field is zero
Check for macSecurityEnabled.
macSecurityEnabled is FALSE
Parse Auxiliary Security Header field.
security level is zero
Obtain source address.
Obtain KeyDescriptor.
Obtain DeviceDescriptor.
Obtain frame counter.
Check frame counter.
Unsecure frame.
Store frame counter.
Obtain SecurityLevelDescriptor.
Check IE Security.
Check IE Key Usage Policy.
Check security level.
Check key usage policy.
SUCCESS
Incoming frame security procedure for security level zero frames

   - Error: `UNAVAILABLE_DEVICE`

2. Obtain source address.
3. Obtain `DeviceDescriptor`. 
   - DeviceDescriptor lookup failed

   - SecurityLevelDescriptor lookup failed
   - Error: `UNAVAILABLE_SECURITY_LEVEL`

6. Check security level.
   - Security level checking failed
   - Conditionally passed but not Exempted
   - Error: `IMPROPER_SECURITY_LEVEL`

SUCCESS