**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title | **ETSI TS 102 887-2 addition for 15-9 doc (CID 234 and 157)** | |
| Date Submitted | 11 March, 2015 | |
| Source | Don Sturek  555 Broadway Street  Redwood City, CA 94063  USA | Voice: +1 650 839 4329 Fax:  E-mail: dsturek@silverspringnet.com |
| Re: | LB98 resolution for CID 234 and 157 | |
| Abstract | LB 98 resolutions to CID 234 and 157. This document amends document 15-15-0127-01-0009-lb98-resolutions-weis (after 15-15-0127-01 is included). This submission in based on the Node to Node (N2N) section of 15-14-0711-00-0009. | |
| Purpose | LB98 resolution for CID 234 | |
| Notice | 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. | |
| Release | The contributor acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.15. | |

# CID 157

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Kunal Shah/ Don Sturek | Silver Spring | 45 | A | 1 | For the 802.1x/KEY section (used by Wi-SUN), we really need 4 distinct Multiplex ID's (Protocol IDs): 802.1x/EAPOL, 802.11-4WayHandshake,, 802.11GTK and Node2Node (which will look a little like TLS session negotiation) | Expand the 802.1x section to cover 4 distinct Multiplex IDs and explain the pre-requisites on the use of each. | AIP |

This amendment to 15-14-0127-00 adds in a new KMP ID for the ETSI TS102-887-2 key exchange.

Table 18 should be updated as follows, where the TBD will be chosen during the editing process for the next version.

|  |  |
| --- | --- |
| **KMP** | **KMP ID value** |
| 802.X/EAP | 1 |
| 802.1X/MKA | TBD |
| 802.11/4WH | TBD |
| 802.11/GKH | TBD |
| ETSI TS 102 887-2 | TBD |











PROPOSED NEW ANNEX A with additions for ETSI TS102 887-2

**Annex A**

**A.1 Description**

*Replace the text of A.1 as follows, incorporating text from the old A.1 and F.1.*

IEEE 802.1X,IEEE Std 802.1X-2010, “IEEE Standard for Local and Metropolitan Area Networks: Port- based Network Access Control” defines a port-based network access control for IEEE 802 networks. It allows network administrators to restrict the use of IEEE 802 LAN service access points (ports) to secure communication with authenticated and authorized systems. Before a device is granted access to a network it is authenticated. EAP (Extensible Authentication Protocol) “Extensible Authentication Protocol (EAP)”, RFC 3748, is transported between a Supplicant PAE (Port Access Entity, see Clause 6.3 of IEEE Std 802.1X-2010, “IEEE Standard for Local and Metropolitan Area Networks: Port-based Network Access Control”) and an Authenticator PAE.

Device Authentication does not itself provide for any protection of frames between WPAN devices themselves. Successful authentication can be accompanied by the secure delivery, to both PAEs, of a secret key that can be used to prove mutual authentication and to distribute or agree further secret keys. These secret keys are then used to provide security services (e.g., confidentiality, integrity, and replay protection) for WPAN frames. Two such key agreement protocols to agree upon the secret keys are:

1. —  IEEE Std. 802.1X-2010 (Clause 9) specifies the MACsec Key Agreement (MKA) protocol, where the secret key derived from EAP is the Connectivity Association Key (CAK). The CAK is used to discover other PAEs attached to the same LAN, to confirm mutual possession of a CAK and hence prove a past mutual authentication, and to agree the secret keys used by a datagram security services. The CAK can either be derived from an EAP exchange, or pre-shared between a set of stations that are authorized to communicate between themselves.
2. —  IEEE Std. 802.11-2012 [B9] describes the use of IEEE Std. 802.1X, where the secret key derived from EAP is the Master Session Key (MSK). The MSK is used as the basis to protect 4-Way Handshake and Group Key Handshake protocols, which are encapsulated in EAPOL-KEY message types defined in IEEE Std. 802.1X-2010.
3. In addition to support for group keys based on IEEE Std. 802.11-2012, ETSI TS 102-887-2 node-to-node pairwise link key establishment is defined.
4. **A.1.1 Device Authentication**
5. *No change to the text of A.1.1 is proposed.*
6. **A.1.2 Device Authentication and Cryptographic Key Agreement**
7. *Replace the text of A.1.2 as follows, incorporating text from the old A.1.2 and F.1.2.*
8. Device Authentication does not itself provide for any protection of frames between WPAN devices themselves. However, when AS policy includes the use of an EAP method that produces a shared secret (e.g., EAP-TLS) “The EAP-TLS Authentication Protocol”, RFC 5216, and the Authenticator and Supplicant policy indicates that a key agreement protocol, then it is possible for the devices to agree upon keys and policy to provide security services (e.g., confidentiality, integrity, and replay protection) for WPAN frames.

Several key agreement protocols are available to use the EAP shared secret. They are described in the following sections, summarized in Table X.

1. **Table X – IEEE Std. 802.1X and IEEE Std. 802.11 KMP Protocols**

|  |  |  |
| --- | --- | --- |
| **KMP** | **PDU Format** | **Reference** |
| 802.1X/EAP | EAPOL-EAP | IEEE Std. 802.1X-2010 Clause 8 |
| 802.1X/MKA | EAPOL-MKA | IEEE Std. 802.1X-2010 Clause 9 |
| 802.11/4WH | EAPOL-KEY | IEEE Std. 802.11-2012 Clause 11.6.6 |
| 802.11/GKH | EAPOL-KEY | IEEE Std. 802.11-2012 Clause 11.6.7 |

1. **A.1.2.1 802.1X/MKA**
2. *Add clause A.1.2.1, incorporating text from the old clause A.1.2.*

As defined in IEEE Std. 802.1X-2010, MKA provides agreement of MACsec policy and keying material. MKA can also be used as a WPAN KMP key agreement method. An additional definition defining the CCM\* cipher has been defined for WPAN use.

The scope of MKA can be pairwise (i.e., between the Authenticator and a single Supplicant), effectively extending the pair-wise security obtained during device authentication to WPAN frames. Alternatively, an MKA session can be shared between a set of devices, effectively providing for shared secure communications including broadcast and multicast frames.

While other uses of MKA allow MKA to autonomously generate replacement keys, when MKA is used as a WPAN KMP service it shall only create keys as the result of a new key exchange created by a KMP-CREATE.request. This restriction is required because the Higher Layer protocols manage keys and their properties (see Annex X [Editor: this is Tero’s new Annex G, which may be renamed due to the removal of Annex F as part of this action]). MKA can continue to exchange messages following the successful installation of a new key, but it shall only install subsequent keys as indicated by the Higher Layer, and will ignore indications sent within MKA (e.g., the delivery of PendingPNExhaustion, or discovery of a new live peer). MKA should deliver a notification to the Higher Layer when it receives these events.

Figure Y shows the protocol exchanges between the Higher Layers of two PAN devices using 802.1X/MKA. As shown, the first KMP-CREATE.request results in the 802.1X/EAP protocol followed by the 802.1X/MKA protocol, because authentication is required before MKA can agree upon a 15.9 Security Association. Higher layer protocols can make additional KMP-CREATE.requests using the same IEEE 802.1X/MKA instance (shown as the second KMP-CREATE.request in the figure).

When KMP-FINISHED.indication is returned to the Higher Layer, one WPAN Security Association can be installed by the Higher Layer.

Appendix-A-drawing-1-01

**Figure Y – 802.1X/EAP and 802.1X/MKA as a PAN KMP**

**A.1.2.1.1 Cryptographic Key Agreement with Pre-shared CAK**

1. *Add clause A.1.2.1.1, incorporating text from the old clause A.1.3.*

Some use cases will require key agreement without WPAN devices having previously executed Supplicant PAE or Authenticator PAE state machines. This is possible by pre-installing a CAK on each of the WPAN devices, and setting a policy on each device requiring that no WPAN data frames be transmitted and received WPAN data frames are discarded until MKA has obtained and installed WPAN cipher keys. When a pre-shared CAK is used, the 802.1X/EAP protocol shown in Figure Y is omitted.

The use of a pre-shared CAK is most expedient for resource-constrained WPAN devices, however a secure method of installing and refreshing CAKs to the WPAN devices would be critical to maintaining strong security.

1. **A.1.2.2 802.11/4WH and 802.11/GKH**

*Add clause A.1.2.2.*

The IEEE 802.11 4-Way Handshake (4WH) and Group Key Handshake (GKH) protocols can also be used as WPAN KMP key agreement methods. The protocols are inherently pair-wise protocols between two peers but the scope of the agreed upon keys differs: The result of an 802.11/4WH is a pairwise key, and the result of an 802.11/GKH is a group key that may be shared with multiple WPAN devices.

Each invocation of 802.11/4WH and 802.11/GKH is independent and the exchanges can be delivered in any order, according to the policy of the Higher Layer. Figure Z shows an example protocol flow where the 802.11/4WH exchange is followed by an 802.11/GKH. Because 802.1X/4WH was the first protocol between the two KMP elements, 802.1X/EAP precedes 802.1X/4WH.

Only one WPA Security Association can be returned to the Higher Layer, so the KMP-FINISHED.indication is restricted to returning just one Security Association. The optional distribution of a GTK in the 802.1X/4WH cannot be used. When an GTK is needed, it should be distributed using an 802.11/GTK KMP.

Appendix-A-drawing-2-01

**Figure Z - 802.1X/EAP, 802.1X/4WH and 802.1X/GKH as a PAN KMP**

1. **A.1.2.3 ETSI TS102 887-2 Node to Node (N2N) Link Key Establishment**

*Add clause A.1.2.3.*

The N2N key establishment is used to establish session keys between pairs of communicating one-hop neighbor nodes in the mesh. A unique session key is established between each pair of one-hop neighbor nodes. ETSI TS102-887-2, section 7.9.3 serves as the reference for this exchange. Section 7.9.4 details the message exchange between *source* and *destination* one-hop neighbors. The *source* device is simply the first to send the New Session Create message to the one-hop *destination*. In practice, either of the devices in the pairwise key establishment exchange can serve as *source* or *destination* for New Session establishment (although, once the New Session exchange begins, the devices remain in the role of *source* or *destination* until the New Session is created). Communication between the devices using the session SA can originate on either device once secured communication begins.

The N2N SA supports 4 message constructs as shown in Table X.

1. **Table X – ETSI TS102 887-2 KMP Protocol**

|  |  |  |
| --- | --- | --- |
| **KMP** | **PDU Format** | **Reference** |
| ETSI TS 102 887-2 | New Session Create | ETSI TS102-887-2, Section 7.9.4.1 |
| ETSI TS 102 887-2 | New Session Created | ETSI TS102-887-2, Section 7.9.4.2 |
| ETSI TS 102 887-2 | New Session Acknowledgement | ETSI TS102-887-2, Section 7.9.4.3 |
| ETSI TS 102 887-2 | New Session Destruction | ETSI TS102-887-2, Section 7.9.4.4 |

Figure 1 shows the PDU exchange for N2N link key establishment. Note that the link key establishment re-uses the 802.1X/EAP KMP for authentication.



**Figure 1**

**A.2 Use Cases**

*Replace the text of A.1 as follows.*

1. The flexibility of Device Authentication makes 802.1X/EAP suitable for a variety of use cases. The following sections describe optimal uses for each key agreement protocol used with 802.1X/EAP.

**A.2.1 Isolated Enclave**

*Replace the text of A.2.1 as follows.*

1. 802.1X/MKA was designed to provide Cryptographic Key Agreement services to a group (i.e., two or more) of devices that need to communicate together. An isolated enclave of WPAN devices that need to communicate amongst themselves with a mix of unicast, broadcast, and/or multicast frames could benefit from MKA’s shared security model. If needed, strong authentication of group members can be first obtained using Device Authentication, when one device acts as both an Authenticator and AS. Alternatively, if strong device authentication is not required the WPAN devices can use a pre-shared CAK to establish group authorization.
2. 802.11/GTK could also be used to distribute a shared key to a group of devices in an isolated enclave of WPAN devices.
3. ETSI TS102 887-2 can further be used to establish pair-wise link keys to one-hop neighbors in an isolated enclave of WPAN devices.
4. **A.2.2 Star Topology**
5. *Replace the text of A.2.2 as follows.*

A network topology where a set of WPAN devices communicate privately with a PAN Coordinator would benefit from pair-wise key agreement services. A PAN Coordinator could use either 802.1X/MKA or 802.11/4WH to create pairwise keys between itself and each PAN participant.

The Controller may use Device Authentication to strongly authenticate the WPAN devices, or in the case of 802.1X/MKA may depend on a pre-shared pair-wise CAK in order to guarantee keying material is shared only with the expected WPAN device.

1. **A.2.3 Mesh**
2. *No change to the text of A.2.3 is proposed.*
3. **A.3 802.15 Specifics**
4. *No change to the text of A.3 is proposed.*
5. **A.3.1 EAPOL Message Framing**
6. *Replace the text of A.3.1 as follows. The only change is removing “(1)” following “KMP ID value”.*
7. IEEE 802.1X-2010 messages are specified as being carried in EAPOL PDUs. When carried in a KMP Information Element, the EAPOL PDU (beginning with the Protocol Version field) follows the KMP ID value in the first KMP Fragment.
8. **A.3.2 EAPOL-MKA**
9. *No change to the text of A.3.2 is proposed.*
10. **A.3.3 EAPOL-KEY**
11. *Add clause A.3.3, incorporating text from the old clause F.3.2.*

EAPOL-KEY messages are framed according Clause 11.9 of IEEE 802.1X and used as specified in Clause 11.6 of IEEE 802.11. Minor modifications are necessary.

Clause 6.3.19 of IEEE 802.11 describes a SetKeyDescriptor, which describes the interface whereby the key management algorithm describes the material generated for the use of the 4-Way Handshake and Group Key Handshake protocol. The following fields of the SetKeyDescriptor will require re-interpretation when used with IEEE 802.15.9.

* Key ID: maps to the 802.15.4 Key Index field
* Cipher Suite Selector: The first three octets are the IEEE 802.15 Company ID (value TBD) appended with a one-octet Suite Type value from Table Y.

**Table Y – IEEE 802.15 Cipher Suite Selectors**

|  |  |
| --- | --- |
| **Suite Type** | **Meaning** |
| 0 | Reserved |
| 1 | CCM\* |
| 2-255 | Reserved |

1. **A.3.4** ETSI TS 102 887-2
2. *Add clause A.3.4, as follows:*

The ETSI TS 102 887-2 SA messages are framed as described in ETSI TS 102 887-2 Section 7.9.4. The specific frames used in this specification are included in Table X.