**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 102)** |
| Date Submitted | 11 March, 2015 |
| Source | Don Sturek555 Broadway StreetRedwood City, CA 94063USA | Voice: +1 650 839 5306Fax: E-mail: dsturek@silverspringnet.com |
| Re: | LB98 resolution for CID 102 |
| Abstract | LB 98 resolutions to CID 102. 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 102 |
| 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 102

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Gary Stuebing | Cisco | General | A | 1 | See Cisco informative contribution "IEEE 802.15.9 for Securing Wireless Mesh Networks" ID\_TBD re: usage of 802.1X and 802.11 messaging to support device authentication, group key establishment, and node-2-node link key establishment. It may help to clarify 15.9 concepts. | Please clarify 15.9 Security Association mapping to the Cisco described message flows. Submission made to Mentor by Cisco and Silver Spring Network. Submission: DCN 15-14-0711-00-0009 |

In Section 2 add

ETSI TS 102 887-2 v1.1.1 Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices; Smart Metering Wireless Access Protocol; Part 2: Data Link Layer (MAC Sub-layer)

In Section 3.2 add

N2N Node to Node

This contribution adds a new KMP ID in Appendix A for the ETSI TS102-887-2 key exchange.

Table 19 should be updated as follows, where the TBD will be chosen during the editing process for the next version.

|  |  |
| --- | --- |
| **KMP** | **KMP ID value** |
| ETSI TS 102 887-2 | TBD |

PROPOSED CHANGES TO ANNEX A FOR ETSI TS102 887-2

*Update the second paragraph and list in A.1 as follows.*

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. Three 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. — ETSI TS 102-887-2[BXX] defines a node-to-node pairwise link key establishment protocol.
4. *Update Table 20 as follows.*
5. **Table 20 –KMP Protocols following IEEE Std. 802.1X**

|  |  |  |
| --- | --- | --- |
| **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 |
| ETSI N2N | ETSI TS 102 887-2 | ETSI TS102-887-2, Sections 7.9.4.1 through 7.9.4.4 |

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

The ETSI 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.

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



**Figure 1**

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

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 20.