**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | TG9 IEEE Std. 802.1X/802.11 Keying as a KMP |
| Date Submitted | Nov. 6, 2014 |
| Source | Brian Weis |
| Re: | IEEE 802.15.9 |
| Abstract | Describes the use of IEEE 802.1X/802.11i as a KMP |
| Purpose | All the use of IEEE 802.11 key management as a KMP method. |
| Notice | This document has been prepared to assist IEEE P802.15 coexistence. 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. |

Introduction

The Draft Recommended Practice for transport of key management protocol (KMP) datagrams (P802.15.9) includes a set of key management protocols that than be transported. Appendix A includes a description specifying how IEEE Std. 802.1X-2010 and the MACsec Key Agreement (MKA) protocol can be used as a KMP with the framework.

This document proposes descriptive text for a new Appendix, which describes the use of IEEE Std. 802.1X-2010 and the 4-Way Handshake defined in IEEE Std. 802.11i-2004 for generating session keys. This process is most recently documented in Clause 4.10.3 of IEEE Std. 802.11-2012. It should be noted that certain protocol elements might need additional definitions before this vision can be fully achieved.

1. KMP Specifics - 802.1X/KEY
	1. Description

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. 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. 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.

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 802.1X.

The 802.1X/KEY KMP makes use of these two protocols, as described in the following clauses.

* + 1. Device Authentication

When a Wireless Personal Area Network (WPAN) network includes a network Access Point (AP) controlling access to devices on a secured network behind the AP, the AP can act as an Authenticator. The Authenticator facilitates authentication and authorization of each Supplicant (i.e., WPAN device) desiring to communicate to the secured network behind it, and discards data frames prior to the completion of the authentication process. An Authenticator PAE relies upon an Authentication Server (AS) to perform Supplicant PAE authentication and authorization. The AS may be either co-located with the Authenticator or the Authenticator may access the AS remotely via a network to which the Authenticator has access.

The Supplicant PAE and AS use EAP (Extensible Authentication Protocol) “Extensible Authentication Protocol (EAP)”, RFC 3748. transported in EAPOL (EAP over LAN) messages. The Supplicant PAE and AS share credentials appropriate for the EAP method used for authentication. Credentials can be passwords or device identifiers (e.g., digital certificates).

* + 1. Device Authentication and Cryptographic Key Agreement

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 the 4-Way Handshake is to be initiated, 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.

* 1. Use Cases

The 802.1X/KEY KMP can be used in any use case where private security association is required between two devices. Its specification and operation is identical to the authentication and key management method defined in IEEE 802.11.

* 1. 802.15 Specifics
		1. EAPOL Message Framing

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 (TBD) in the first KMP Fragment.

* + 1. EAPOL-KEY

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: TBD

Note: A new Cipher Suite Selector needs to be defined for CCM\*. It need not be under the OUI used by IEEE 802.11 (“00-0F-AC”).

# Normative References

The following normative reference is added to P802.15.9/D01.

[B9] IEEE Std 802.11-2012. “IEEE Standard for Information technology — Telecommunications and information exchange between systems Local and metropolitan area networks — Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.”