|  |  |
| --- | --- |
| Project | **IEEE 802.21d**  **Multicast Group Management****<**[**http://www.ieee802.org/21/**](http://www.ieee802.org/21/)**>** |
| Title | **Ciphersuites of IEEE 802.21d** |
| DCN | **21-15-0033-00-MuGM** |
| Date Submitted | **March 12, 2015** |
| Source(s) | Yoshikazu Hanatani (Toshiba)  |
| Re: | IEEE 802.21 Session #67 in Berlin, Germany |
| Abstract | This document provides explanation texts of the use cases of IEEE 802.21d described in DCN 21-12-0157-MuGM for IEEE 802.21.1 Draft standard. |
| Purpose | To inform ciphersuites of IEEE 802.21d to IEEE 802.24. |
| Notice | This document has been prepared to assist the IEEE 802.21 Working Group. 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 grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE’s name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE’s sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that IEEE 802.21 may make this contribution public. |
| Patent Policy | The contributor is familiar with IEEE patent policy, as stated in [Section 6 of the IEEE-SA Standards Board bylaws](http://standards.ieee.org/guides/opman/sect6.html#6.3) <[http://standards.ieee.org/guides/bylaws/sect6-7.html#6](http://127.0.0.1:4664/cache?event_id=757737&schema_id=1&s=5X0vID10lu_E6yrIkWkNd4Wz2H8&q=hancock)> and in *Understanding Patent Issues During IEEE Standards Development* <http://standards.ieee.org/board/pat/faq.pdf> |

1. **Introduction**

IEEE 802.21d standardizes a mechanism for distributing a symmetric key to group members, securely and efficiently.



**Figure 1. Group Key Distribution**

1. A PoS (Point of Service) with group manager selects group members and generates GroupKeyData for the group members.
2. The PoS with group manager distributes GroupKeyData using a multicast transport.
3. Recipients receive GroupKeyData.
	1. If the recipient is a group member, the recipient can derive a symmetric key from GroupKeyData.
	2. If the recipient is not a group member, the recipient cannot derive the symmetric key from GroupKeyData.
4. **Payload Protection**

Payload is protected by a symmetric key encryption and a digital signature. The symmetric key is shared by the group members.

The ciphersuites used for securing group addressed messages are defined in Table below

 **Table 1 --- Group ciphersuites**



In Table 1, AES-CCM is an AES mode of operations specified in NIST SP 800-38C. AES-CCM provides confidentiality and data integrity. In Table 1, ECDSA-256 uses curve P-256 and hash function SHA-256. Notice that in IEEE 802.21d AES-CCM uses the group key for authenticated encryption of a payload. This scheme only provides data integrity but does not guarantee data origin authentication because the symmetric key is shared among a group of recipients. On the other hand, the data origin authentication is provided using a digital signature ECDSA.

1. **Group key distribution**
Symmetric keys used for payload protection is distributed by Complete Subtree method which is one of the broadcast encryption schemes proposed in the literature [1]. The Complete Subtree method allows minimizing the number of encryptions for a given group key. The protection of group key in IEEE 802.21d uses the following ciphersuites in Table below.

 **Table 2 --- Group key distribution Ciphersuites**



In Table 1, AES\_Key\_Wrapping is an AES mode of operations specified in NIST SP 800-38F. Note that ECB mode is not recommended to protect a key, because it cannot provide proper security level for the key. In particular, the same plaintext will be encrypted to the same ciphertext, since no random IV (Initialization Vector) is used for each encryption. On the other hand, if transmitting IVs will increase the size of GroupKeyData to an unacceptable point for the transport protocol, then ECB mode may be used, assuming that the same key will be retransmitted with a very small probability. The signature is applied to provide authentication and integrity.

References

[1] Dalit Naor, Moni Naor, Jeffery Lotspiech:

Revocation and Tracing Schemes for Stateless Receivers. CRYPTO 2001: 41-62

1. 1.
	2.
	3.
	4.