IEEE P802.11
Wireless LANs

|  |
| --- |
| Proposed Changes for 4.5.4 |
| Date: 2020-08-26 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Hitoshi Morioka | SRC Software | Fukuoka, JAPAN |  | hmorioka@src-soft.com |
|  |  |  |  |  |

Abstract

This document describes proposed changes for clause 4.5.4 in D0.1.

4.5.4 Access control and data confidentiality services

*~~Change the nth paragraphs as follows:~~*

~~The current IEEE Std. 802.11 has a group temporal key security association (GTKSA) security framework for multicast that does not protect origin authenticity between devices having that GTKSA. Such protection is needed in some broadcast use cases.~~

4.5.4.6 Data origin authenticity

*Change the second paragraph as follows:*

Data origin authenticity is applicable only to individually addressed Data frames, and individually addressed robust Management frames on non-eBCS STAs. The protocols do not guarantee data origin authenticity for group addressed frames on non-eBCS STAs, as this cannot be accomplished using symmetric keys and public key methods are too computationally expensive. The enhanced broadcast service (eBCS) provides data origin authenticity for group addressed eBCS frames.