IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resolutions for Clause 4.5.4.6 | | | | |
| Date: 2021-01-11 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Hitoshi Morioka | Koden-TI | Fukuoka, JAPAN |  | hmorioka@src-soft.com |
|  |  |  |  |  |

Abstract

This document describes the resolutions for clause 4.5.4.6 on LB252.

# Overview of comments

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Line** | **Clause** | **Comment** | **Proposed Change** | **Resolution** |
| 1092 | 14.00 | 21 | 4.5.4.6 | The text "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."  seems a little misleading, since eBCS \*does\* in fact use "public key methods". Perhaps it would make sense to reword that. | as in comment. | Revised.  The original text “public key methods are too computationally expensive” was added 17 years ago (802.11i-2004).  Now public key methods are not too expensive.  The text is modified as in [https://mentor.ieee.org/802.11/dcn/21/11-21-0052-00-00bc-resolutions-for-clause-4-5-4-6.docx](https://mentor.ieee.org/802.11/dcn/21/11-21-0042-00-00bc-resolutions-for-clause-4-3-100.docx). |
| 1401 | 14.00 | 21 | 4.5.4.6 | The paragraph could be worded better since data origin authenticity is applicable to BCS frames | Change "Data origin authenticity is applicable only to individually addressed Data frames, and individually addressed robust Management frames on non-eBCS STAs" to "Data origin authenticity is applicable only to individually addressed Data frames, individually addressed robust Management frames, and and group addressed eBCS frames" | Reviced.  Basicaly the comment is accepted.  The text is modified as in [https://mentor.ieee.org/802.11/dcn/21/11-21-0052-00-00bc-resolutions-for-clause-4-5-4-6.docx](https://mentor.ieee.org/802.11/dcn/21/11-21-0042-00-00bc-resolutions-for-clause-4-3-100.docx). |
| 1169 | 14.00 | 22 | 4.5.4.6 | Please clarify Is the authenticity ensured for eBSC STAs when the transmitter and receiver are eBCS STAs? Currently the service description is not clear. | Please clarify | Revised.  The text is modified to clarify that EBCS frames provide origin authenticity as in [https://mentor.ieee.org/802.11/dcn/21/11-21-0052-00-00bc-resolutions-for-clause-4-5-4-6.docx](https://mentor.ieee.org/802.11/dcn/21/11-21-0042-00-00bc-resolutions-for-clause-4-3-100.docx). |
| 1252 | 14.00 | 22 | 4.5.4.6 | " on non-eBCS STAs" is not clear | Change "Data origin authenticity is applicable only to individually addressed Data frames, and individually 21 addressed robust Management frames on non-eBCS STAs. The protocols do not guarantee data origin 22 authenticity for group addressed frames on non-eBCS STAs as this cannot be accomplished using 23 symmetric keys and public key methods are too computationally expensive. The enhanced broadcast 24 service (eBCS) provides data origin authenticity for group addressed eBCS frames. " to "For non-EBCS STAs, 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 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. " | Revised.  The text is modified to clarify that EBCS frames provide origin authenticity as in [https://mentor.ieee.org/802.11/dcn/21/11-21-0052-00-00bc-resolutions-for-clause-4-5-4-6.docx](https://mentor.ieee.org/802.11/dcn/21/11-21-0042-00-00bc-resolutions-for-clause-4-3-100.docx). |
| 1633 | 14.00 | 22 | 4.5.4.6 | "The protocols do not guarantee data origin authenticity for group addressed frames" in L22 seems to contradict to "The enhanced broadcast service (eBCS) provides data origin authenticity for group addressed eBCS frames." in L24. Please clarify. | Make it clear whether data origin authenticity for group addressed eBCS frames is supported or not. | Revised.  The text is modified to clarify that EBCS frames provide origin authenticity as in [https://mentor.ieee.org/802.11/dcn/21/11-21-0052-00-00bc-resolutions-for-clause-4-5-4-6.docx](https://mentor.ieee.org/802.11/dcn/21/11-21-0042-00-00bc-resolutions-for-clause-4-3-100.docx). |
| 1234 | 14.00 | 24 | 4.5.4.6 | It would be good to explain why eBCS STAs can do data origin authenticity, to match the non-eBCS explanation. | Explain (briefly) why eBCS can use public keys or hash chains, that separates from these being "too computationally expensive" for non-eBCS. | Revised.  The original text “public key methods are too computationally expensive” was added 17 years ago (802.11i-2004).  Now public key methods are not too expensive.  The text is modified as in [https://mentor.ieee.org/802.11/dcn/21/11-21-0052-00-00bc-resolutions-for-clause-4-5-4-6.docx](https://mentor.ieee.org/802.11/dcn/21/11-21-0042-00-00bc-resolutions-for-clause-4-3-100.docx). |
| 1058 | 14.00 | 25 | 4.5.4.6 | The phrase "The enhanced broadcast service (eBCS) provides data origin authenticity for group addressed eBCS frames."should not be broadcast eBCS frames? | Change to "broadcast eBCS frames" | Reject.  “Group addressed” is correct wording. |

# Discussion of comments

# Suggested resolution

**4.5.4.6 Data origin authenticity**

Data origin authenticity is applicable only to individually addressed Data frames, ~~and~~ individually addressed robust Management frames, and group addressed EBCS frames ~~on non-eBCS STAs~~. The protocols do not guarantee data origin authenticity for group addressed non-EBCS 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.~~

**References:**