IEEE P802.11
Wireless LANs

|  |
| --- |
| LB249-Some-DMG-CIDs-Part-III |
| Date: 2020-09-30 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Assaf Kasher | Qualcomm |  |  | assaf.kasher@gmail.com |
|  |  |  |  |  |

Abstract

This document proposes resolutions to CIDs: 3204, 3639, 3937, 3534, 3170, 3534, 3635, 3773, 3368, 3870, 3905, 3209

Editor instruction based on D2.4

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 3204 | 65.00 | 26 | 9.4.2.167 | "The Number of Random Sequences" this field is not reference anywhere in the draft, therefore it should be removed with the whole ranging operation parameters field | Remove Rangin Operation Paramters field and related text | **Revise**: TGaz Editor make the changes as in 11-20-1687r2 (accept in principle) |

***TGaz Editor: Remove the Ranging Operation Parameter filed from figure 9-619c***

***TGaz Editor: Remove lines 19-26in page 66 (including figure 9-619d)***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 3639 | 124.00 | 32 | 11.22.6.3.5 | "A STA that supports secure ToF measurement as described in 11.22.6.4.8 (Secure EDMG 32Measurement Exchange Protocol) shall set the Secure ToF Supported field in the EDMG 33capabilities element to 1." is duplicated at 125.41 | Delete the cited text | **Revise:** TGaz Editor make the changes as in 11-20-1687r2 |
| 3937 | 124.00 | 32 | 11.22.6.3.5 | "11.22.6.4.8 (Secure EDMG Measurement Exchange Protocol)" wrong reference | replace by "11.22.6.4.2.1.6 Secure measurement exchange for EDMG STAs" |  **Revise:** TGaz Editor make the changes as in 11-20-1687r2 |

Discussion: There is some mixed up of DMG capabilities in wrong subclauses.

***TGaz Editor: Add the following text before 11.21.6.3.5***

 ***11.21.6.3.5 Capability Negotiation for EDCA based Ranging with the Format and Bandwidth Field set to 31-43***

A STA that supports first Path Beamforming Training shall set the First Path Beamforming Training Supported field of the Beamforming Capability subelement in the RSNXE (#**3940**) to 1. Otherwise it shall set the First Path Beamforming Training Supported field to 0.

A STA that supports secure RTT measurement as described in 11.21.6.4.2.1.6 (Secure EDMG Measurement Exchange Protocol) shall set the Secure RTT Supported field of the Beamforming Capability subelement in the RSNXE (#**3940**) to 1. Otherwise it shall set the Secure RTT Supported field to 0. A STA shall not set the Secure RTT Supported field of the Beamforming Capability subelement in the RSNXE to 1 if it has not also set the First Path Beamforming Training Supported field of the Beamforming Capability subelement in the RSNXE to 1.

A STA that supports EDMG SC Ranging shall set the EDMG SC Ranging Supported field of the Beamforming Capability subelement in the RSNXE (#**3940**) to 1. Otherwise it shall set the EDMG SC Ranging Supported field to 0. A STA shall not set the Secure RTT Supported field if it has not also set to 1the First Path Beamformign Training Supported field of the Beamforming Capability subelement in the RSNXE (#**3940**).

A STA that supports EDMG OFDM Ranging shall set the EDMG OFDM Ranging Supported field of the Beamforming Capability subelement in the RSNXE (#**3940**) to 1. Otherwise, it shall set the EDMG OFDM Ranging Supported field to 0.

***TGaz Editor: Renumber headings following 11.21.6.3.5 to reflect a new subclause 11.21.6.3.5.***

***TGaz Editor: Remove the text in P 131L20-36 as follows:***

***TGaz Editor: Remove the text in P130L19-23 as follows:***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 3534 | 108.00 | 1 | 11.10.10.3 | " DMG location supporting APs information field" -- no such field | Change to "DMG/ location supportingAPs in the area field" (sic) | Accept. |

***Note to editor: in D2.4 the location is P112L27***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 3170 | 125.00 | 3 | 11.22.6.3.5 | "The ISTA shall generate a 32 octet random Secret Key and include it in the Secure Ranging Operation Parameters" - it shall also generate a 32 octet Salt. | Repalce with "The ISTA shall generate a 32 octet random Secret Key and 32 octet Salt and include it in the Secure Ranging Operation Parameters" |  **Reject –** the salt isis the PMKID corresponding to the security association between the ISTA and RSTA |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 3634 | 125.00 | 3 | 11.22.6.3.5 | " The ISTA" is confusing because the previous sentence was about an ISTA that does not use secure ranging | Change to " An ISTA that sets the Secure ToF Measurement subfield to 1" and in the previous sentence add " to 1" after "subfield" |  Accept |

***Note to editor: in D2.4 in P130L28***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 3635 | 125.00 | 6 | 11.22.6.3.5 | " An RSTA that supports Secure ToF 6measurement shall acknowledge a request for Secure ToF measurement by setting the Secure ToF 7Measurement subfield in the Measurement Parameters field in the initial (#1449) Protected Dual 8of the Fine Timing Measurement frame. " -- why? The ISTA won't make the request unless the RSTA supports it (above in same para), so the ISTA knows it will be used | Delete the cited sentence |  Accept |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 3773 | 159.00 | 46 | 11.22.6.4.6.2 | I don't think three PHY-RXLTFSEQUENCE.request primitive are issued | Reword as "shall issue a PHY-RXLTFSEQUENCE.request primitive with: a) a LTFVECTOR parameter LTF\_OFFSET that" etc. |  **Revise:** TGaz Editor make the changes as in 11-20-1687r2 |

***TGaz Editor: change the text in P161L5-15 as follows:***

When an ISTA receives a Ranging NDP Announcement frame from an RSTA in which the AID11/RSID11 subfield in the STA Info field contains the 11 least significant bits of the AID or RSID of the ISTA, the ISTA shall Issue a PHY-RXLTFSEQUENCE.request primitive with the following LTFVECOR parameter values:

1. LTF\_OFFSET that is set to the Offset subfield value in the STA Info field;
2. LTF\_N\_STS that is set to the R2I N\_STS subfield value in the STA Info field;
3. LTF\_REP that is set to the R2I Rep subfield value in the STA Info field;

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3368 | 156.00 | 11.22.6.4.6.1 | Figure 11-36n refer to LTF\_GEN\_INFO 1,2,3. the terminology of LTF\_GEN\_INFO was update to Secure-LTF-Counter. The figure needs updating and same goes to figures 11-36o, 11-36p, 11-36q, | Update figures from LTF\_GEN\_INFO to show Secure-LTF-Counter 1,2,3... |  **Revise:** This is already resolved in D2.4, “LTF\_GEN\_INFO” is replace by “SEC\_LTF\_CTR”. TGaz Editor, no further changes needed. |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 3870 | 66.00 | 7 | 9.4.2.167 | Figure 9-169e Secure Ranging Operation Parameters field format includes salt which is not used in the construction of TRN sequences. It should be removed | Remove it from the field and adjust the description accordingly |  **Revise:** TGaz Editor make the changes as in 11-20-1687r2 |

***TGaz Editor: Remove the Saltf field from figure 9-626e (Secure Ranging Operation Parameters field format)***

***TGaz Editor: change the text in P67L4-6 as follows:***

The Secret Key subfield is used to carry the secret key which is used along with Salt value (based on the PMKID), to generate the random sequence(s) as described in Subclause 12.2.11 (EDMG Secure Ranging Sequences).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 3905 | 128.00 | 30 | 11.22.6.4.2 | "When a Secure Fine Timing Measurement Session is established as described in 11.22.6.3.1, the31 Fine Timing Measurement frames transmitted during the execution of Measurement Exchange32 shall be Protected Dual of Public Action frames (See Cl. 9.6.10 Protected Dual of Public Action33 frames)." What is a "secure Fine Timing Measurement session" precisely? Using PMF to protect the negotiation frames without employing secure LTF also provides some level of security, is it considered a secure Fine Timing Measurement session? Or, does the highlighted text mean "a FTM session using secure LTF"? | Please clarify the meaning of a secure Fine Timing Measurement session, and modify the text accordingly throughout the 11az spec wherever appropriate. |  **Reject:** the Secure Fine Timing Measurement Session is defined in 11.22.6.3.1, no clarifications are needed. |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 3209 | 28.00 | 9 | 216 | Replace "PDMG secure ranging" with "EDMG secure ranging" throughout clause 28. | as in comment |  Accept |

***Note to Editor: PDMG appear once in the heading of 28.9.3 and references thereof***

**References:**