IEEE P802.11
Wireless LANs

|  |
| --- |
| 11bi D0.4 CR for 12.14.7 |
| Date: 2024-07-10 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Po-Kai Huang | Intel |  |  | po-kai.huang@intel.com |
|  |  |  |  |  |

Abstract

This submission proposes resolutions for the following CIDs:

1032, 1033, 1150, 1474, 1475, 1476, 1477, 1478, 1479, 1480,

1481, 1482, 1483, 1034, 1124, 1151, 1152, 1153, 1484, 1486,

1402, 1485, 1147, 1154

Revisions:

* Rev 0: Initial version of the document.

Interpretation of a Motion to Adopt

A motion to approve this submission means that the editing instructions and any changed or added material are actioned in the TGbi D0.4 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbi D0.4 Draft. (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents). TGbi Editor: Editing instructions preceded by “TGbi Editor” are instructions to the TGbi editor to modify existing material in the TGbi draft. As a result of adopting the changes, the TGbi editor will execute the instructions rather than copy them to the TGbi Draft.***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Clause** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| 1032 | Chaoming Luo | 12.14.7.1 | 80.25 | Diffie-Hellman Parameter element is defined in 802.11 but not RFC 8110. | Remove "as defined in IETF RFC 8110" | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1171r0 under all headings that include CID 1032 |
| 1033 | Chaoming Luo | 12.14.7.1 | 81.02 | Diffie-Hellman Parameter element is defined in 802.11 but not RFC 8110. | Remove "as defined in IETF RFC 8110" | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1171r0 under all headings that include CID 1032 |
| 1150 | Po-Kai Huang | 12.14.7.1 | 80.62 | Use the same style of describe locaton of DHss in PTKSA derivaition like P83 L58 | As in comment | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1171r0 under all headings that include CID 1150 |
| 1474 | Mark RISON | 12.14.7.1 | 80.22 | "sees" is not how we normally describe things. Also next subclause | Refer to receving an X frame with they Y field set to Z | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1128r0 under all headings that include CID 1474 |
| 1475 | Mark RISON | 12.14.7.1 | 80.25 | "Include a Diffie-Hellman Parameter element as defined in IETF RFC 8110" -- elements are defined in Clause 9, not an RFC, no? | As it says in the comment | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1128r0 under all headings that include CID 1032 |
| 1476 | Mark RISON | 12.14.7.1 | 80.27 | "Choose indicated finite cyclic group in the Diffie-Hellman Parameter element from the dot11RSNA-ConfigDLCGroupTable that is at least of the security strength provided by the AKM and cipher suites." should start "Select a group in" but the second half is unclear too: is it the table that is of security strength or the group? And how do you measure security strength ayway? | As it says in the comment | Revised – We have the following existing texts in the baseline. “Finite cyclic group from the dot11RSNAConfigDLCGroupTable that is at least of the securitystrength provided by the (#7185)base AKMP and cipher suites.”TGbi editor to make the changes shown in 11-24/1128r0 under all headings that include CID 1476 |
| 1477 | Mark RISON | 12.14.7.1 | 80.40 | "For the purpose of interoperability, a" -- justification not required. Ditto next subclause | Change to "A" | Rejected – "For the purpose of interoperability, a…" has been used in the baseline for similar purpose.  |
| 1478 | Mark RISON | 12.14.7.1 | 80.45 | "receives the first message" -- the first message of what? | Clarify | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1128r0 under all headings that include CID 1478 |
| 1479 | Mark RISON | 12.14.7.1 | 0.00 | "that finite cyclic group indicated" missing article | As it says in the comment | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1128r0 under all headings that include CID 1479 |
| 1480 | Mark RISON | 12.14.7.1 | 0.00 | " end of context " missing article | As it says in the comment | Revised – Agree in principle with the commenter. We now directly refer to 12.7.1.6.5TGbi editor to make the changes shown in 11-24/1171r0 under all headings that include CID 1150 |
| 1481 | Mark RISON | 12.14.7.1 | 0.00 | Some of the bullets end with a full stop, some not | Be consistent | Revised – Agree in principle with the commenter. We examine all the bullets to add full stop. TGbi editor to make the changes shown in 11-24/1171r0 under all headings that include CID 1481 |
| 1482 | Mark RISON | 12.14.7.1 | 0.00 | Should any of the discarding be silent? | Clarify | Rjected –We follow the sylte in 12.13, which just use “shall discard” |
| 1483 | Mark RISON | 12.14.7.1 | 81.01 | "Upon completion of PTK generation, the shared secret, DHss, shall be irretrievably deleted." is inconsistent with the other bullets. Ditto below and in next subclause | Change to "Shall irretrievably delete the shared secret, DHss, upon completion of PTK generation." | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1171r0 under all headings that include CID 1483 |
| 1034 | Chaoming Luo | 12.14.7.2 | 82.17 | For 802.1X, it's not necessary to include the Nonce element in the authentication frames because the Diffie-Hellman Parameter element provides the same but better functionality by generating a DHss. The existing PASH has done it with DHss instead of Nonces, see 12.13.7 PTKSA derivation with PASN authentication. | Remove P82L17 and P83L16, and change P69L59 to:PTK = PRF-Length(PMK, "Pairwise key expansion", Min(AA,SPA) || Max(AA,SPA) || DHss) if key derivation with Authentication frame exchange for 802.1X is used as defined in 12.14.7.2 (802.1X). | Rejected – We still keep the nonce element to minimize the change to the existing implementations that utilizes SNonce and ANonce. |
| 1124 | Po-Kai Huang | 12.14.7.2 | 82.20 | "a AKM Selector element" should be "an AKM Suite Selector element" | As in comment | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1171r0 under all headings that include CID 1124 |
| 1151 | Po-Kai Huang | 12.14.7.2 | 82.22 | RSNXE will always be included because Encrypted of the Frame body field capability bit will always set to 1. Remove the "if" description | As in comment | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1171r0 under all headings that include CID 1151 |
| 1152 | Po-Kai Huang | 12.14.7.2 | 83.01 | should be "authentication originator" rather than "authenticator originator" | As in comment | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1171r0 under all headings that include CID 1152 |
| 1153 | Po-Kai Huang | 12.14.7.2 | 84.08 | RSNXE should be always there because Encrypted of the Frame body field capability bit will always set to 1. Remove the "if present" | As in comment | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1171r0 under all headings that include CID 1153 |
| 1484 | Mark RISON | 12.14.7.2 | 82.12 | "has the corresponding SME to act as the Sup-plicant," -- not clear. All STAs have a single SME | As it says in the comment | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1171r0 under all headings that include CID 1484 |
| 1486 | Mark RISON | 12.14.7.2 | 0.00 | "Include RSNE" missing article. Ditto RSNXE. Ditto "Choose indicated finite cyclic group" | As it says in the comment | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1171r0 under all headings that include CID 1486 |
| 1402 | Mark RISON | 12.7.1.3 | 69.60 | Where is DHss defined? Also should have spaces around || | As it says in the comment | Revised – DHss is defined in “Perform the group's scalar-op (see 12.4.4.1 (General)) with the authenticatior originator's ephemeral public key and its own ephemeral private key to produce an ephemeral Diffie-Hellman shared secret, DHss. ”We do the editorial change. TGbi editor to make the changes shown in 11-24/1171r0 under all headings that include CID 1402 |
| 1485 | Mark RISON |   | 0.00 | " authentication frame" should be " Authentication frame" | As it says in the comment | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1171r0 under all headings that include CID 1485 |
| 1147 | Po-Kai Huang | 12.14.7.2 | 84.05 | Suggest to move these rules to 12.14.5. These rules seem to be required anyway in general for SAE, 802.1X, and PMKSA caching except FT, which already has the rules. | As in comment | Rejected – It seems that the description for the rules will be different. In EPDKE for SAE, the AKM is indicated in a wrapped place. PMKSA caching is not defined yet and if defined will have rules to described how to verify the fields. |
| 1154 | Po-Kai Huang | 12.14.7.2 | 84.05 | Clarify specifically what "the same" means. It likely means the whole content is the same, but we then need to specify how RSNE is indicated in authentication message 1. Similar to FT, it can just follows the definition in RSNE clause. | As in comment | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1171r0 under all headings that include CID 1154 |

**Discussion:**

**Proposal:**

*TGbi editor: Modify Clause 12.14.7.1 as follows (track change on):*

* FT(#150r5)

If an FTO or FTR (see 13 (Fast BSS transition)) sets the Encryption of the Frame Body Field of the (Re)Association Request/Response Frame Support subfield in the RSNXE to 1, then FTO or FTR supports the additional rules defined in this subclause.

An FTO that sets the Encryption of the Frame Body Field of the (Re)Association Request/Response Frame Support subfield in the RSNXE to 1 and receives the RSNXE from the FTR with the Encryption of the Frame Body Field of the (Re)Association Request/Response Frame Support subfield (#1474)set to 1 shall:

* Include a Diffie-Hellman Parameter element (#1032)in the first message of the FT protocol (see 13.8 (FT authentication sequence)).
* Select a(#1476) finite cyclic group in the Diffie-Hellman Parameter element from the dot11RSNAConfigDLCGroupTable that is at least of the security strength provided by the AKM and cipher suites.
* With the chosen finite cyclic group, generate an ephemeral (random) private key, use the selected group's scalar operation (see 12.4.4.1 (General)) with the private key to generate its ephemeral public key, and indicate the ephemeral public key in the Diffie-Hellman Parameter element.

Otherwise, an FTO shall not include a Diffie-Hellman Parameter element in the first message of the FT protocol.

For the purpose of interoperability, an FTO or an FTR shall support group 19, an ECC group defined over a 256-bit prime order field.

An FTR that sets the Encryption of the Frame Body Field of the (Re)Association Request/Response Frame Support subfield in the RSNXE to 1 and receives the first message of the FT protocol(#1478) with the Encryption of the Frame Body Field of the (Re)Association Request/Response Frame Support subfield in the RSNXE set to 1 shall:

* Validate that finite cyclic group indicated in the Diffie-Hellman Parameter element in message 1 is supported (present in dot11RSNAConfigDLCGroupTable). Otherwise, the FTR shall reject message 1 with status code set to UNSUPPORTED\_FINITE\_CYCLIC\_GROUP.
* Verify the public key indicated in the Diffie-Hellman Parameter element in message 1 as specified in 5.6.2.3 of NIST SP 800-56A R2. If verification fails, the FTR shall reject message 1 with status code set to INVALID\_PUBLIC\_KEY.
* If the message 1 is not rejected, generate an ephemeral (random) private key with the chosen finite cyclic group and use the selected group's scalar operation with the private key to generate its ephemeral public key. Perform the group's scalar-op (see 12.4.4.1 (General)) with the FTO's ephemeral public key and its own ephemeral private key to produce an ephemeral Diffie-Hellman shared secret, DHss.
* (#1150)Derive PTK with DHss (#1150)as defined in 12.7.1.6.5 (PTK) .(#1481)
* Upon completion of PTK generation, the shared secret, DHss, shall be irretrievably deleted.
* Include a Diffie-Hellman Parameter element (#1032)in the second message of the FT protocol (see 13.8 (FT authentication sequence)).
* Indicate chosen finite cyclic group in the Diffie-Hellman Parameter element of message 2, which is the same as the finite cyclic group in the Diffie-Hellman Parameter element of message 1.(#1481)
* Indicate its ephemeral public key in the Diffie-Hellman Parameter element of message 2.(#1481)
* Calculate MIC in the FTE as follows:
* Use the key, the algorithm, and the MIC size as defined in 13.8.5 (FT authentication sequence: contents of fourth message)
* On the concatenation of the following data, in the order given here as the input:
* FTO's MAC address.(#1481)
* FTR's MAC address.(#1481)
* RSNE sent in the Beacons transmitted by the AP with MAC address equal to A1 field of message 1.(#1481)
* RSNXE sent in the Beacons transmitted by the AP with MAC address equal to A1 field of message 1.(#1481)
* the body of the second message with MIC field of the FTE set to 0.(#1481)
* Include MIC in the FTE rather than set it to 0 as described in 13.8.3 (FT authentication sequence: contents of second message) .(#1481)

Otherwise, an FTR shall not include a Diffie-Hellman Parameter element in the second message of the FT protocol.

After receiving the second message of the FT protocol with the status code set to SUCCESS, an FTO shall:

* If the FTO includes a Diffie-Hellman Parameter element in the first message of the FT protocol, validate that there is a Diffie-Hellman Parameter element included in the second message of the FT protocol. If the validation fails, the FTO shall discard the frame and terminate further protocol processing.
* If the FTO does not include a Diffie-Hellman Parameter element in the first message of the FT protocol, validate that there is no Diffie-Hellman Parameter element included in the second message of the FT protocol. If the validation fails, the FTO shall discard the frame and terminate further protocol processing.
* If the FTO includes a Diffie-Hellman Parameter element in the first message of the FT protocol, validate that the finite cyclic group indicated in the Diffie-Hellman Parameter element in message 2 is the same as the finite cyclic group indicated in the Diffie-Hellman Parameter element in message 1. If the validation fails, the FTO shall discard the frame and terminate further protocol processing.
* Verify the public key indicated in the Diffie-Hellman Parameter element in message 2 as specified in 5.6.2.3 of NIST SP 800-56A R2. If verification fails, the FTO shall discard the frame and terminate further protocol processing.
* If the message 2 is not discarded, perform the group's scalar-op (see 12.4.4.1 (General)) with the FTR's ephemeral public key and its own ephemeral private key to produce an ephemeral Diffie-Hellman shared secret, DHss.
* (#1150)Derive PTK with DHss(#1150) as defined in 12.7.1.6.5 (PTK).(#1481)
* Irretrievably delete the shared secret, DHss, upon completion of PTK generation, .(#1483)
* Have the S1KH of the FTO verify the MIC in the FTE.(#1481)
* Discard the frame and terminate further protocol processing if the verification fails.(#1483)

*TGbi editor: Modify Clause 12.14.7.2 as follows (track change on):*

* 802.1X(#762r2)

If an authentication originator or an authentication responder defined in 12.14.4 (IEEE 802.1X authentication utilizing Authentication frames) sets the Encryption of the Frame Body Field of the (Re)Association Request/Response Frame Support subfield in the RSNXE to 1, then the authentication originator or the authentication responder supports the additional rules defined in this subclause when performing 802.1X Authentication frame exchange.

An authentication originator that sets the Encryption of the Frame Body Field of the (Re)Association Request/Response Frame Support subfield in the RSNXE to 1, has the (#1484)SME to act as the Supplicant, receives the RSNXE from the authentication responder with the Encryption of the Frame Body Field of the (Re)Association Request/Response Frame Support subfield (#1474)set to 1, and intends to continue association after authentication shall:

* Include a Nonce element in the first Authentication(#1485) frame to indicate SNonce.
* Include a(#1486) RSNE in the first Authentication(#1485) frame to indicate AKM and pairwise cipher suite. Version field shall be set to 1. Pairwise Cipher Suite Count field shall be set to 1. AKM Suite Count field shall be set to 1. PMKID Count field, if present, shall be set to 0. All other fields shall be as specified in 9.4.2.23 (RSNE) and 12.6.3 (RSNA policy selection in an infrastructure BSS).(#1154)
* Not include an(#1124) AKM Suite Selector element.
* Include a(#1486) RSNXE in the first Authentication(#1485) frame.(#1151)
* Include a Diffie-Hellman Parameter element in the first Authentication(#1485) frame.
* Select a(#1486) finite cyclic group in the Diffie-Hellman Parameter element from the dot11RSNAConfigDLCGroupTable that is at least of the security strength provided by the AKM and cipher suites.
* With the chosen finite cyclic group, generate an ephemeral (random) private key, use the selected group's scalar operation (see 12.4.4.1 (General)) with the private key to generate its ephemeral public key, and indicate the ephemeral public key in the Diffie-Hellman Parameter element.

Otherwise, an authentication originator shall not include a Diffie-Hellman Parameter element or a RSNE or a RSNXE or a Nonce element in the first Authentication(#1485) frame for 802.1X authentication.

For the purpose of interoperability, an authenticator or a supplicant shall support group 19, an ECC group defined over a 256-bit prime order field.

An authentication responder that sets the Encryption of the Frame Body Field of the (Re)Association Request/Response Frame Support subfield in the RSNXE to 1, has the (#1484)SME to act as the Authenticator, and receives the first Authentication(#1485) frame with a Nonce element, RSNE, RSNXE, and a Diffie-Hellman Parameter element shall:

* Verify that the AKM indicated in the RSNE rather than AKM suite selector element as defined in 12.4.4 (IEEE 802.1X authentication utilizing Authentication frames) is supported. Otherwise, the authentication responder shall reject message 1 with status code set to STATUS\_INVALID\_AKMP.
* Verify that the pairwise cipher indicated in the RSNE is supported. Otherwise, the authentication responder shall reject message 1 with status code set to STATUS\_INVALID\_PAIRWISE\_CIPHER.
* Validate that the(#1479) finite cyclic group indicated in the Diffie-Hellman Parameter element in the first Authentication(#1485) frame is supported (present in dot11RSNAConfigDLCGroupTable). Otherwise, the authentication responder shall reject message 1 with status code set to UNSUPPORTED\_FINITE\_CYCLIC\_GROUP.
* Verify the public key indicated in the Diffie-Hellman Parameter element in message 1 as specified in 5.6.2.3 of NIST SP 800-56A R2. If verification fails, the authentication responder shall reject the first Authentication(#1485) frame with status code set to INVALID\_PUBLIC\_KEY.
* If the first Authentication(#1485) frame is not rejected, store the indicated SNonce and generate an ephemeral (random) private key with the chosen finite cyclic group and use the selected group's scalar operation with the private key to generate its ephemeral public key. Perform the group's scalar-op (see 12.4.4.1 (General)) with the authentication(#1152) originator's ephemeral public key and its own ephemeral private key to produce an ephemeral Diffie-Hellman shared secret, DHss.
* Include a RSNE in the second Authentication(#1485) frame to indicate the AKM and pairwise cipher indicated in the first Authentication(#1485) frame.
* Not include an(#1124) AKM Suite Selector element in the second Authentication(#1485) frame.
* Include a Diffie-Hellman Parameter element in the second Authentication(#1485) frame.
* Indicate chosen finite cyclic group in the Diffie-Hellman Parameter element of the second Authentication(#1485) frame, which is the same as the finite cyclic group in the Diffie-Hellman Parameter element of the first Authentication(#1485) frame.
* Indicate its ephemeral public key in the Diffie-Hellman Parameter element of the second Authentication(#1485) frame.
* Include a Nonce element in the second Authentication(#1485) frame to indicate ANonce.

Otherwise, an authentication responder shall not include a Diffie-Hellman Parameter element or a Nonce element or a RSNE in the second Authentication(#1485) frame for 802.1X authentication.

After receiving the second Authentication(#1485) frame with the status code set to SUCCESS, an authentication originator shall:

* If the authentication originator includes a Diffie-Hellman Parameter element in the first Authentication(#1485) frame, validate that there is a Diffie-Hellman Parameter element and a RSNE included in the second Authentication(#1485) frame and there is no AKM suite selector element in the second Authentication(#1485) frame. If the validation fails, the authentication originator shall discard the frame and terminate further protocol processing.
* If the authentication originator does not include a Diffie-Hellman Parameter element in the first Authentication(#1485) frame, validate that there is no Diffie-Hellman Parameter element and no RSNE included in the second Authentication(#1485) frame. If the validation fails, the authentication originator shall discard the frame and terminate further protocol processing.
* If the authentication originator includes a Diffie-Hellman Parameter element in the first Authentication(#1485) frame, validate that the finite cyclic group indicated in the Diffie-Hellman Parameter element in the second Authentication(#1485) frame is the same as the finite cyclic group indicated in the Diffie-Hellman Parameter element in the first Authentication(#1485) frame, validate that the pairwise cipher suite and the AKM indicated in the second Authentication(#1485) frame are the same as the pairwise cipher suite and the AKM indicated in the first Authentication(#1485) frame. The validation of AKM is based on the AKM indication in RSNE rather than AKM suite selector element as defined 12.14.4 (IEEE 802.1X authentication utilizing Authentication frames). If the validation fails, the authentication originator shall discard the frame and terminate further protocol processing.
* Verify the public key indicated in the Diffie-Hellman Parameter element in the second Authentication(#1485) frame as specified in 5.6.2.3 of NIST SP 800-56A R2. If verification fails, the authentication originator shall discard the frame and terminate further protocol processing.
* If the second Authentication(#1485) frame is not discarded, store the indicated ANonce, perform the group's scalar-op (see 12.4.4.1 (General)) with the authentication originator's ephemeral public key and its own ephemeral private key to produce an ephemeral Diffie-Hellman shared secret, DHss.

Before sending the Authentication(#1485) frame carrying EAP Success, an authentication responder shall:

* Derive PTK with DHss as defined in 12.7.1.3 (Pairwise key hierarchy).
* Irretrievably delete the shared secret, DHss, upon completion of PTK generation.(#1483)

After receiving the Authentication(#1485) frame carrying EAP Success, an authentication originator shall:

* Derive PTK with DHss as defined in 12.7.1.3 (Pairwise key hierarchy).
* Irretrievably delete the shared secret, DHss, upon completion of PTK generation.(#1483)

The authentication originator and the authentication responder then continue the operation as defined in 12.14.5 (Encryption of the Frame Body Field of the (Re)Association Request/Response Frame) with the following additional rules:

* Authentication responder shall verify that the RSNE in the (Re)Association Request frame is identical to(#1143) the RSNE included in the first Authentication(#1485) frame. Authentication responder shall also verify that the RSNXE (#1153)in the (Re)Association Request is identical to(#1143) the RSNXE included in the first Authentication(#1485) frame. If the validation fails, the authentication responder shall reject the association.
* Authentication originator shall verify that the RSNE in the (Re)Association Response frame is the same as the RSNE included in the second Authentication(#1485) frame. If the validation fails, the authentication originator shall disassociate.

*TGbi editor: Modify Clause 12.7.1.6.5 as follows (track change on):*

* PTK

The third-level key in the FT key hierarchy is the PTK. When FILS authentication is used to establish the FT key hierarchy, PTK for the initial mobility domain association is derived as part of the FILS authentication as defined in 12.11.2.5.3 (PTKSA Key derivation with FILS authentication). Otherwise, this key is mutually derived by the S1KH and the R1KH used by the target AP, with the key length being a function of the negotiated cipher suite as defined by Table 12-8 (Cipher suite key lengths(#1083)(#3532)) in 12.7.2 (EAPOL-Key frames).

Using the KDF defined in 12.7.1.6.2 (Key derivation function (KDF)), the PTK derivation is as follows:

PTK = KDF-Hash-Length(PMK-R1, “FT-PTK”, SNonce || ANonce || BSSID || STA-ADDR || DHss) if key derivation with Authentication frame exchange for FT is used as defined in 12.14.7.2 (FT). (#1150)

(#478)Otherwise,(#1150) PTK = KDF-*Hash*-*Length*(PMK-R1, “FT-PTK”, SNonce || ANonce || BSSID || STA-ADDR)

where

(#478)KDF-*Hash*-*Length* is the key derivation function as defined in 12.7.1.6.2 (Key derivation function (KDF)) using the hash algorithm identified by the AKM suite selector (see Table 9-190 (AKM suite selectors))

PMK-R1 is the key that is shared between the S1KH and the R1KH

SNonce is a 256-bit random bit string contributed by the S1KH

ANonce is a 256-bit random bit string contributed by the R1KH

STA-ADDR is the non-AP STA’s MAC address

BSSID is the BSSID of the target AP’s BSS

*Length*(#3686) is the total number of bits to derive, i.e., number of bits of the PTK. The length is dependent on the negotiated cipher suites and (#3266)AKMP as defined by Table 12-8 (Cipher suite key lengths(#1083)(#3532)) in 12.7.2 (EAPOL-Key frames) and Table 12-11 (Integrity and key wrap algorithms(#3244)) in 12.7.3 (EAPOL-Key PDU construction and processing)(11ba), and whether a KDK is derived. A KDK shall be derived if any of the following are true:(11az)(#7220)

* WUR frame protection is negotiated(11az)
* dot11SecureLTFImplemented is true and the peer STA has advertised secure HE-LTF support capability in its RSNXE (see 9.4.2.240 (RSNXE(#1776)))(11az)

Otherwise, it shall not be derived.(#7220)

*TGbi editor: Modify Clause 12.7.1.3 as follows (track change on):*

* Pairwise key hierarchy(#762r2)

***Change the seventh paragraph (not all shown) as follows:***

The following apply when not using FILS authentication:

* SNonce is a random or pseudorandom value contributed by the Supplicant; its value is taken when a PTK is instantiated and is sent to the PTK Authenticator.
* ANonce is a random or pseudorandom value contributed by the Authenticator.
* The PTK shall be derived from the PMK by

PTK = PRF-Length(PMK, "Pairwise key expansion", Min(AA,SPA) || Max(AA,SPA) || Min(ANonce,SNonce) || Max(ANonce,SNonce) || (#1402)DHss) if key derivation with Authentication frame exchange for 802.1X is used as defined in 12.14.7.2 (802.1X).

Otherwise, PTK = PRF-Length(PMK, "Pairwise key expansion", Min(AA,SPA) || Max(AA,SPA) || Min(ANonce,SNonce) || Max(ANonce,SNonce))