IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 11bi D1.0 12.16.8 comments | | | | |
| Date: 2025-03-28 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | Email |
| Po-Kai Huang | Intel |  |  | po-kai.huang@intel.com |

Abstract

This submission resolves the following CIDs:

273, 274, 275, 280, 281, 283, 284, 690, 696, 697,

698, 699, 700, 851, 971, 972, 701, 703, 706, 707,

708, 717

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 D1.0 Draft. This introduction is not part of the adopted material.

Editing instructions formatted like this are intended to be copied into the TGbi D1.0 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** | **Clause** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| 273 | 131.35 | 12.16.8.1 | The otherwise statement is not clear. | Please clarify when a Diffie-Hellman Parameter element is present and it is not present. | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in the latest version of 11-25/0555 under all headings that include CID 273 |
| 274 | 132.25 | 12.16.8.1 | The otherwise statement is not clear. | Please clarify when a Diffie-Hellman Parameter element is present and it is not present. | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in the latest version of 11-25/0555 under all headings that include CID 274 |
| 275 | 132.30 | 12.16.8.1 | The third bullet seems to include the first bullet of the list. | Please clarify, whether the first bullet is needed. | Rejected –  We assume the instance is on 131.49 because for other instances in 12.16.8.1, the first bullet and the third bullet are clearly on different things.  The first bullet is on verifying the existence of certain elements.  The third bullet is on verifying specific parameters in various elements. |
| 280 | 133.34 | 12.16.8.1 | Poor use of or. It is unclear whether only authenticator may support group 19. | Please change "or" to "and". | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in the latest version of 11-25/0555 under all headings that include CID 280 |
| 281 | 134.08 | 12.16.8.1 | PMKID inclusion needs shall stements. | Change to:" If a PMKSA is identified, the PMKID corresponding to PMKSA shall be in the RSNE. Otherwise, no PMKID shall be included in the RSNE. | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in the latest version of 11-25/0555 under all headings that include CID 281 |
| 283 | 134.30 | 12.16.8.1 | The otherwise statement is not clear. The otherwise is related to Authentication message 2 content, but the list talks also on the Authentication message 1 verificaiton. | Please clarify when a Diffie-Hellman Parameter element is present and it not present. | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in the latest version of 11-25/0555 under all headings that include CID 274 |
| 284 | 135.42 | 12.16.8.1 | Please clarify why RSNXE is can be different in the second authentication frame and the (re)association response frame. | Please add checks that RSNXE is identical in the second authentication frame and the (re)association response frame. | Rejected –  RSNXE is not included in the second message of FT. See Table 13-1—FT authentication elements. Client verifies RSNXE in (Re)association response against RSNXE in Beacon or Probe response. See 12.16.6. |
| 690 | 128.43 | 12.16.8.1 | "Select a finite cyclic group in the Diffie-Hellman Parameter element [...] that is at least of the security strength provided by the AKM and cipher suites." -- it is not clear how the strength of AKMs and ciphers is compared with that of FC groups. Also 130.38 | As it says in the comment | Rejected –  This is how the group is described in baseline PASN frame exchange. See citation below.  ***12.13.3.2 PASN frame construction and processing***  *Finite cyclic group from the dot11RSNAConfigDLCGroupTable that is at least of the security*  *strength provided by the (#7185)base AKMP and cipher suites.* |
| 696 | 129.36 | 12.16.8.1 | Is it clear what "the body" is, exactly? | As it says in the comment | Revised –  Agree in principle with the commenter. We change to the Frame Body field.  TGbi editor to make the changes shown in the latest version of 11-25/0555 under all headings that include CID 696 |
| 697 | 129.38 | 12.16.8.1 | "Include MIC in the FTE rather than set it to 0 as described in 13.8.3" is ambiguous as to whether 13.8.3 says to set it to 0, or says to include it in the FTE | As it says in the comment | Revised –  Agree in principle with the commenter. We just say include MIC in the FTE. Note that FTE does not include MIC in the first and second message based on 13.5.  TGbi editor to make the changes shown in the latest version of 11-25/0555 under all headings that include CID 697 |
| 698 | 129.47 | 12.16.8.1 | "If the FTO includes a Diffie-Hellman Parameter element in the first message of the FT protocol" -- this is in the past now. Ditto 131.48/59 and 131.53 | Change "includes" to "included", also at line 57, and at line 52 "does not include" to "did not include" | Revised -  Agree in principle with the commenter.  TGbi editor to make the changes shown in the latest version of 11-25/0555 under all headings that include CID 698 |
| 699 | 130.08 | 12.16.8.1 | "Have the S1KH of the FTO verify the MIC in the FTE. " -- it is not clear how the FTO makes this happen | As it says in the comment | Rejected –  Based on the FT key holder architecture, the S0KH and S1KH are part of the FTO’s SME RSNA key management. |
| 700 | 130.08 | 12.16.8.1 | "Have the S1KH of the FTO verify the MIC in the FTE. -- Discard the frame and terminate further protocol processing if the verification fails." is confusing because "the verification" is not clear | Change to "Have the S1KH of the FTO verify the MIC in the FTE, and discard the frame and terminate further protocol processing if the verification fails." | Revised -  Agree in principle with the commenter. This is addressed in 11-25/0295 CID 278.  TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 278 |
| 851 | 120.13 | 12.16.8.1 | The sentence " Upon completion of PTK generation, the shared secret, DHss, shall be irretrievably deleted" is not formed properly to be included in the bulleted list | Revise as "Irretrievably delete the ephemeral shared secret, DHss, upon completion of PTK generation." | Revised –  Agree in principle with the commenter. This is addressed in CID 276 in 11-25/0295.  TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 276 |
| 971 | 128.55 | 12.16.8.1 | Why include "For the purpose of interoperability" before "an FTO or an FTR shall support group 19"? How is this different from simply saying "An FTO or an FTR shall support group 19"? | Change "For the purpose of interoperability; an" to "An". | Rejected –  This is the language used in the baseline to explain why we have the “shall” requirement. Citations are provided below.  *For the purpose of interoperability, a STA shall support group 19, an ECC group defined over a 256-bit prime order field.*  *For the purpose of interoperability, APs that have*  *dot11ProtectedHCCATXOPNegotiationImplemented true or dot11ProtectedQLoadReportImplemented true shall implement support for group 19, an ECC group defined over a 256-bit prime order field.* |
| 972 | 130.49 | 12.16.8.2 | Why include "For the purpose of interoperability" before "an authenticator or a supplicant shall support group 19"? How is this different from simply saying "An authenticator or a supplicant shall support group 19"? | Change "For the purpose of interoperability; an" to "An" | Rejected –  This is the language used in the baseline to explain why we have the “shall” requirement. Citations are provided below.  *For the purpose of interoperability, a STA shall support group 19, an ECC group defined over a 256-bit prime order field.*  *For the purpose of interoperability, APs that have*  *dot11ProtectedHCCATXOPNegotiationImplemented true or dot11ProtectedQLoadReportImplemented true shall implement support for group 19, an ECC group defined over a 256-bit prime order field.* |
| 701 | 130.20 | 12.16.8.2 | "has the SME to act as the Supplicant," -- it's not clear what else could be a Supplicant. Similarly at line 53 | Delete the cited text | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 701 |
| 703 | 130.57 | 12.16.8.2 | "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." not clear. There is no AKM Suite Selector element (note bad case too) per line 32 | Delete from "rather" to ")" | Accepted - |
| 706 | 131.07 | 12.16.8.2 | "specified AKM" -- specified where? | As it says in the comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 706 |
| 707 | 131.07 | 12.16.8.2 | "If a PMKSA is identified, use PMKSA caching, does not process the EAPOL PDU in the first Authentication frame, and does not include EAPOL PDU in the second authentication frame. " -- grammar and meaning both unclear; also missing article | Is this trying to say "If a PMKSA is identified, the responder shall not process ... and shall not include \*\*\*\*an\*\*\* EAPOL PDU ..."? | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 707 |
| 708 | 131.22 | 12.16.8.2 | " If a PMKSA is identified" -- not clear how and by whom. Also at line 36 | As it says in the comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 708 |
| 717 | 132.34 | 12.16.8.2 | This bullet suggests you derive the PTK with just the DHss. However line 26 suggests you need the PMKSA too. Which is correct? | As it says in the comment | Rejected –  PTK derivation formula is cited as defined in 12.7.1.3 (Pairwise key hierarchy). There is a need for PMK. In the first case, PMK is from identified PMKSA. In the second case, PMK is derived from 802.1X authentication. Both refer to the formula defined in 12.7.1.3 (Pairwise key hierarchy). |

***Discussion:***

***Proposal:***

**TGbi Editor: *Instruction: Modify 12.16.8 as follows***

* Key derivation with Authentication frame exchange

This subclause defines rules to derive a temporal key (TK) through Authentication frame exchange to encrypt the Frame Body field of the (Re)Association Request/Response frame.

* FT

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

An FTO that sets the (Re)Association Frame Encryption Support field in the RSNXE to 1 and receives the RSNXE from the FTR with the (Re)Association Frame Encryption Support field set to 1 shall:

* Include a Diffie-Hellman Parameter element in the first message of the FT protocol (see 13.8 (FT authentication sequence)).
* Select a 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.
* Generate an ephemeral (random) private key with the chosen finite cyclic group, 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.(#276)

Otherwise, an FTO that sets dot11EDPReAssociationFrameEncryptionSupportActivated to false or does not receive the RSNXE from the FTR with the (Re)Association Frame Encryption Support field set to 1(#273) shall not include a Diffie-Hellman Parameter element in the first message of the FT protocol.

For the purpose of interoperability, an FTO and(#280) an FTR shall support group 19, an ECC group defined over a 256-bit prime order field.

An FTR that sets the (Re)Association Frame Encryption Support field in the RSNXE to 1 and receives the first message of the FT protocol with the (Re)Association Frame Encryption Support field 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.
* 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 if message 1 is not rejected. 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. (#276)
* Derive PTK with DHss as defined in 12.7.1.6.5 (PTK).
* Irretrievably delete the shared secret, DHss, upon completion of PTK generation.(#276)
* Include a Diffie-Hellman Parameter element 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.
* Indicate its ephemeral public key in the Diffie-Hellman Parameter element of message 2.
* 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.
* FTR's MAC address.
* RSNE sent in the Beacons transmitted by the AP with MAC address equal to A1 field of message 1.
* RSNXE sent in the Beacons transmitted by the AP with MAC address equal to A1 field of message 1.
* the Frame Body field(#696) of the second message with MIC field of the FTE set to 0.
* Include MIC in the FTE.(#697)

Otherwise, an FTR that sets dot11EDPReAssociationFrameEncryptionSupportActivated to false or does not receive the RSNXE in the first message of the FT protocol with the (Re)Association Frame Encryption Support field set to 1(#274) 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:

* Validate that there is a Diffie-Hellman Parameter element included in the second message of the FT protocol if the FTO included(#698) a Diffie-Hellman Parameter element in the first message of the FT protocol. If the validation fails, the FTO shall discard the frame and terminate further protocol processing.(#276)
* Validate that there is no Diffie-Hellman Parameter element included in the second message of the FT protocol if the FTO did(#698) not include a Diffie-Hellman Parameter element in the first message of the FT protocol. If the validation fails, the FTO shall discard the frame and terminate further protocol processing.(#276)
* 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 FTO included(#698) a Diffie-Hellman Parameter element in the first message of the FT protocol. If the validation fails, the FTO shall discard the frame and terminate further protocol processing.(#276)
* 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.
* 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, if the message 2 is not discarded.(#276)
* Derive PTK with DHss as defined in 12.7.1.6.5 (PTK).
* Irretrievably delete the shared secret, DHss, upon completion of PTK generation.
* Verify the MIC in the FTE using the S1KH of the FTO.(#277)
* Discard the frame and terminate further protocol processing if the verification fails.
* IEEE 802.1X

If an originator or a responder defined in 12.16.5 (IEEE 802.1X authentication utilizing Authentication frames) sets the (Re)Association Frame Encryption Support field in the RSNXE to 1, then the originator or the responder supports the additional rules defined in this subclause when performing IEEE 802.1X Authentication frame exchange.

An originator that sets the (Re)Association Frame Encryption Support field in the RSNXE to 1,(#701) receives the RSNXE from the responder with the (Re)Association Frame Encryption Support field set to 1, and intends to continue association after authentication shall:

* Include a Nonce element in the first Authentication frame to indicate SNonce.
* Include an RSNE in the first Authentication 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 and PMKID list set corresponding to PMKSA identifiers if exists. All other fields shall be as specified in 9.4.2.23 (RSNE) and 12.6.3 (RSNA policy selection in an infrastructure BSS).
* Not include an AKM Suite Selector element.
* Include an RSNXE in the first Authentication frame.
* Include a Diffie-Hellman Parameter element in the first Authentication frame.
* Select a 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 originator that sets dot11EDPReAssociationFrameEncryptionSupportActivated to false or does not receive the RSNXE from the responder with the (Re)Association Frame Encryption Support field set to 1(#273) shall not include a Diffie-Hellman Parameter element or an RSNE or an RSNXE or a Nonce element in the first Authentication frame for IEEE 802.1X authentication.

For the purpose of interoperability, an authenticator and(#280) a supplicant shall support group 19, an ECC group defined over a 256-bit prime order field.

A responder that sets the (Re)Association Frame Encryption Support field in the RSNXE to 1(#701) and receives the first Authentication frame with a Nonce element, RSNE, RSNXE, and a Diffie-Hellman Parameter element shall:

* Verify that the AKM indicated in the RSNE (#703)is supported. Otherwise, the 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 responder shall reject message 1 with status code set to STATUS\_INVALID\_PAIRWISE\_CIPHER.
* Validate that the finite cyclic group indicated in the Diffie-Hellman Parameter element in the first Authentication frame is supported (present in dot11RSNAConfigDLCGroupTable). Otherwise, the 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 responder shall reject the first Authentication frame with status code set to INVALID\_PUBLIC\_KEY.
* Verify that a PMKSA named via a PMKID in the RSNE exists for the specified AKM in the RSNE(#706).
* If a PMKSA is identified, the responder shall use PMKSA caching, shall not process the EAPOL PDU in the first Authentication frame, and shall not include EAPOL PDU in the second authentication frame.(#707)
* If no PMKSA is identified, continue the IEEE 802.1X authentication.
* If the first Authentication 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 originator's ephemeral public key and its own ephemeral private key to produce an ephemeral Diffie-Hellman shared secret, DHss.
* Include an RSNE in the second Authentication frame to indicate the AKM and pairwise cipher indicated in the first Authentication frame.
* If a PMKSA is identified via a PMKID in the RSNE in the first Authentication frame(#708), the responder shall(#281) include the PMKID corresponding to the PMKSA in the RSNE.
* Otherwise, the responder shall(#281) not include any PMKID in the RSNE.
* Not include an AKM Suite Selector element in the second Authentication frame.
* Include a Diffie-Hellman Parameter element in the second Authentication frame.
* Indicate chosen finite cyclic group in the Diffie-Hellman Parameter element of the second Authentication frame, which is the same as the finite cyclic group in the Diffie-Hellman Parameter element of the first Authentication frame.
* Indicate its ephemeral public key in the Diffie-Hellman Parameter element of the second Authentication frame.
* Include a Nonce element in the second Authentication frame to indicate ANonce.
* If a PMKSA is identified via a PMKID in the RSNE in the first Authentication frame(#708), use PMKSA caching and before sending the second Authentication frame, a responder shall:
* Derive PTK with the identified PMKSA and DHss as defined in 12.7.1.3 (Pairwise key hierarchy).
* Irretrievably delete the shared secret, DHss, upon completion of PTK generation.

Otherwise, a responder that sets dot11EDPReAssociationFrameEncryptionSupportActivated to false or does not receive the RSNXE in the first Authentication frame with the (Re)Association Frame Encryption Support field set to 1(#274) shall not include a Diffie-Hellman Parameter element or a Nonce element or an RSNE in the second Authentication frame for IEEE 802.1X authentication.

After receiving the second Authentication frame with the status code set to SUCCESS, an originator shall:

* If the originator included(#698) a Diffie-Hellman Parameter element in the first Authentication frame, validate that there is a Diffie-Hellman Parameter element and an RSNE included in the second Authentication frame and there is no AKM suite selector element in the second Authentication frame. If the validation fails, the originator shall discard the frame and terminate further protocol processing.
* If the originator did(#698) not include a Diffie-Hellman Parameter element in the first Authentication frame, validate that there is no Diffie-Hellman Parameter element and no RSNE included in the second Authentication frame. If the validation fails, the originator shall discard the frame and terminate further protocol processing.
* If the originator included(#698) a Diffie-Hellman Parameter element in the first Authentication frame, validate that the finite cyclic group indicated in the Diffie-Hellman Parameter element in the second Authentication frame is the same as the finite cyclic group indicated in the Diffie-Hellman Parameter element in the first Authentication frame, validate that the pairwise cipher suite and the AKM indicated in the second Authentication frame are the same as the pairwise cipher suite and the AKM indicated in the first Authentication frame. The validation of AKM is based on the AKM indication in RSNE rather than AKM suite selector element as defined 12.16.5 (IEEE 802.1X authentication utilizing Authentication frames). If the validation fails, the 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 frame as specified in 5.6.2.3 of NIST SP 800-56A R2. If verification fails, the originator shall discard the frame and terminate further protocol processing.
* If the originator includes one or more PMKID in the first Authentication frame, and the second Authentication frame includes a PMKID, validate that the Encapulation Length field is set to 0 and validate that the PMKID included in the second Authentication frame matches one of the PMKID(s) indicated in the first Authentication frame. If verification succeeds, use PMKSA caching with the PMKSA identified by the PMKID indicated in the second Authentication frame and does not continue the IEEE 802.1X Authentication frame exchange. If verification fails, the originator shall discard the frame and terminate further protocol processing.
* If the originator does not include any PMKID in the first Authentication frame, validate that there is no PMKID included in the second Authentication frame. If verification fails, the originator shall discard the frame and terminate further protocol processing.
* If the second Authentication frame is not discarded, store the indicated ANonce, perform the group's scalar-op (see 12.4.4.1 (General)) with the originator's ephemeral public key and its own ephemeral private key to produce an ephemeral Diffie-Hellman shared secret, DHss.
* If a PMKSA is identified, an originator shall:
* Derive PTK with the identified PMKSA and DHss as defined in 12.7.1.3 (Pairwise key hierarchy).
* Irretrievably delete the shared secret, DHss, upon completion of PTK generation.

If a PMKSA is not identified due to PMKSA caching, before sending the Authentication frame carrying EAP Success, a 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.

If a PMKSA is not identified due to PMKSA caching, after receiving the Authentication frame carrying EAP Success, an 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.

The originator and the responder then continue the operation as defined in 12.16.6 ((Re)Association Request/Response Frame Encryption) with the following additional rules:

* The responder shall verify that the RSNE other than the PMKID Count field and the PMKID list field in the (Re)Association Request frame is identical to the RSNE included in the first Authentication frame. Responder shall also verify that the RSNXE in the (Re)Association Request is identical to the RSNXE included in the first Authentication frame. If the validation fails, the responder shall reject the association.
* The originator shall verify that the RSNE other than the PMKID Count field and the PMKID list fieldin the (Re)Association Response frame is the same as the RSNE included in the second Authentication frame. If the validation fails, the originator shall disassociate.