2. Normative references

[Insert “IETF RFC 8446,“The Transport Layer Security (TLS) Protocol Version 1.3,” Rescorla E., and Mozilla, August 2018. (https://datatracker.ietf.org/doc/html/rfc8446)”]

4. Abbreviations and acronyms

[Remove PAK]

[Insert “TLS Transport Layer Security”]

6. MAC common part sublayer

6.3 Data/Control plane

6.3.2 MAC PDU formats

6.3.2.3 MAC management messages

6.3.2.3.9 Privacy key management (PKM) messages (PKM-REQ/PKM-RSP)

Instructions to the editor for Clause 6.3.2.3.9 are in the following text:

[Remove “In PKMv1, a “new” message is an Authorization Request or Key Request that is not a

retransmission being sent in response to a Timeout event” from 2nd paragraph under PKM Identifier parameter details]

[Remove “a PKMv2 RSA-Request” from 2nd paragraph of Table 6-68 PKM Identifier parameter details]

[Replace “The Identifier field in PKMv2 EAP-Transfer messages and Authentication Information

Messages” with “The Identifier field in PKMv2 EAP-Transfer messages and PKMv2 TLS-Transfer messages” in the third paragraph under PKM identifier parameter details]

[Remove text starting with “On reception of a PKM-RSP message…” ending with “of the pending PKMv2 RSA-Reply.”(6 paragraphs) under PKM Identifier parameter details]

[Remove entries with codes 3-16 from Table 6-69]

[Insert entry “44 PKM2 TLS-Transfer” in Table 6-69]

[Replace entry “44-255 Reserved” with [“45-255 Reserved” in Table 6-69]

6.3.2.3.9.2 Auth Request (authorization request) message

[Remove clause]

6.3.2.3.9.3 Auth Reply (authorization reply) message

[Remove clause]

6.3.2.3.9.4 Auth Reject (authorization reject) message

[Remove clause]

6.3.2.3.9.5 Key Request message

[Remove clause]

6.3.2.3.9.6 Key Reply message

[Remove clause]

6.3.2.3.9.7 Key Reject message

[Remove clause]

6.3.2.3.9.8 Authorization Invalid message

[Remove clause]

6.3.2.3.9.10 Auth Info (authentication information) message

[Remove clause]

6.3.2.3.9.11 PKMv2 RSA-Request message

[Remove clause]

6.3.2.3.9.12 PKMv2 RSA-Reply message

[Remove clause]

6.3.2.3.9.13 PKMv2 RSA-Reject message

[Remove clause]

6.3.2.3.9.14 PKMv2 RSA-Acknowledgment message

[Remove clause]

6.3.2.3.9.17 PKMv2 SA-TEK-Challenge message

[Remove “this attribute shall include only follows EAP-based authorization or EAP-based reauthorization procedures” in table 6-86]

6.3.2.3.49 MOB\_BSHO-RSP (BS HO response) message

Instructions to the editor for Clause 6.3.2.3.49 are in the following text:

[Replace “Bit 2: Reserved” with “Bit 2: 256-bit HMAC/CMAC” from Table 6-175 on p. 382]

[Replace “Bit 0: RSA authorization” to “Bit 0: TLS authorization” in Table 6-175]

[Insert the following sub section at the end of section 6.3.2.3.9]

6.3.2.3.9.?? PKMv2 TLS-Transfer message

When an MS has a TLS payload received from a TLS method for transmission to the BS or when a BS

has a TLS payload received from a TLS method for transmission to the MS, it encapsulates it in a

PKMv2 TLS-Transfer message. In the case of reauthentication, the HMAC Digest and Key

Sequence Number attributes shall be included.

Code: 44

Attributes are shown in Table 6-??.

Table 6-??:—PKMv2 TLS-Transfer message attributes

|  |  |
| --- | --- |
| Attribute | Content |
| TLS Payload | Contains the TLS data |
| Key Sequence Number | AK sequence number |
| HMAC Digest | Message digest calculated using AK |

The TLS Payload field carries data in the format described in section 4 of IETF RFC 8446.

7. Security sublayer

7.1 Architecture

Instructions to the editor for Clause 7.1 are in the following text:

[Replace “RSA-based Authentication: This stack performs the RSA-based authentication function using the SS’s X.509 digital certificate and the BS’s X.509 digital certificate, when the RSA-based authorization is selected as an authorization policy between an SS and a BS.” with “TLS-based Authentication: This stack provides the interface of TLSv1.3 authentication using the SS’s X.509 digital certificate and the BS’s X.509 digital certificate, when the TLS-based authorization is selected as an authorization policy between an SS and a BS. In the TLS-based authorization, the BS acts as an authentication server.” in Clause 7.1]

[Replace “EAP and EAP Method Protocol: These stacks are outside of the scope of this standard” with “EAP EAP-TLS and TLSv1.3 Protocols: These stacks are outside of the scope of this standard”]

[Replace in Figure 7-1 “RSA – based Authentication” with “TLS – based authentication”]

7.1.2 Key management protocol

Instructions to the editor for Clause 7.1.2 are in the following text:

[Replace “or X.509 digital certificates [IETF RFC 3280] together with RSA public-key encryption algorithm [PKCS #1] or a sequence starting with RSA authentication and followed by EAP authentication” with “or TLS-based authentication” in paragraph 1 of the clause]

[Remove: “issued by the SS’s manufacturer (in the case of RSA authentication) or a operator-specified credential (in the case of EAP-based authentication)” from paragraph 3 of the clause]

7.1.3 Authentication protocol

Instructions to the editor for Clause 7.1.3 are in the following text:

[Replace “— RSA protocol [PKCS #1 v2.1 with SHA-1(FIPS 186-2)] (support is mandatory in PKMv1; support

is optional in PKMv2)” with “-TLS v1.3 protocol” in second paragraph of cluse]

[Remove: “ (optional unless specifically required)” from clause]

7.1.3.1 PKM RSA authentication

[Remove clause]

7.1.3.2 PKM EAP authentication

[Replace “in conjunction with an operator-selected EAP Method (e.g., EAP-TLS [IETF RFC 2716]). The EAP method will use a particular kind of credential – such as an X.509 certificate in the case of EAP-TLS, or a Subscriber Identity Module in the case of EAP-SIM” with “in conjunction with TLS (EAP-TLS [IETF RFC 5216]).” In first paragraph of clause]

[Remove 2nd paragraph of clause]

[Insert new clause header after PKM EAP authentication clause: 7.1.3.3 PKM TLS authentication]

[Insert the following text after the PKM TLS authentication header: “PKM TLS Authentication uses Transfer Layer Security v1.3 Protocol [IETF RFC 8446]. During reauthentication, the TLS transfer messages are

protected with an HMAC Tuple. The BS and SS shall discard unprotected TLS transfer messages, or TLS transfer messages with invalid HMAC Digests during reauthentication”]

7.1.6.3 Protection of non-authenticated PKM messages

[Remove clause]

7.1.7 Distributed security control in a multihop relay system

7.1.7 Distributed security control in a multihop relay system 2nd paragraph.

[Remove “if PKMv2 is used” from 2nd paragraph in clause]

7.2 PKM protocol

[Remove “There are two Privacy Key Management Protocols supported in this standard: PKM version 1 and PKMv2 with more enhanced features such as new key hierarchy, AES-CMAC, AES key wraps, and MBS.” In first paragraph of clause]

7.2.1 PKM Version 1

[Remove clause]

7.2.2 PKM Version 2

[This clause header can be removed, and all other section can go up one level]

7.2.2.1 TEK exchange overview for PMP topology

Instructions to the editor for Clause 7.2.2.1 are in the following text:

[Replace paragraph 4 of Clause 7.2.2.1 with “TEK and KEKs is N bits long, where N may be either 128,

192 or 256. SAs employing any ciphersuite with a block size of N bits shall use B-bit TEKs and KEKs. The

name TEK-N is used to denote n-bit TEK. Similarly, KEK-N is used to denote a N-bit KEK.”]

[Replace “128” with “N” in the 6th paragraph of Clause 7.2.2.1]

The modified paragraph is as follows with changes highlighted in red:

TEKs and KEKs is N bits long, where N may be either 128, 192 or 256. SAs employing any

ciphersuite with a basic block size of N bits shall use B-bit TEKs and KEKs. The name TEK-N is used

to denote a n-bit TEK. Similarly, KEK-N is used to denote a N-bit KEK.

7.2.2.2 Key derivation

[Replace: “Since there are two authentication schemes, one based on RSA and one based on EAP, there are two primary sources of keying material. The keys used to protect management message integrity and transport the TEKs are derived from source key material generated by the authentication and authorization processes. The RSA-based authorization process yields the pre-Primary AK (pre-PAK) and the EAP based authentication process yields the MSK. Keys used to protect MBS traffic are derived from the MBSAK, which is supplied by means outside the scope of this specification. These keys form the roots of the key hierarchy.” with:

“Since the two authentication schemes (TLS and EAP) both use TLS, both yield the MSK”]

[Replace “the EAP inner method. The authentication part of the authorization flow (and the involvement of the generic EAP layer) is now complete.” with “the EAP-TLS or standalone TLS. The authentication part of the authorization flow is now complete.” In last paragraph of the clause]

7.2.2.2.1 RSA-based authorization

[Remove clause]

7.2.2.2.2 EAP authentication

[Replace header “EAP authentication” with header “PMK derivation”]

[Remove “If a RSA mutual authorization took place before the EAP exchange, the EAP messages may be protected. using EIK-EAP Integrity Key derived from pre-PAK (see 7.2.2.2.1). EIK is 160 bits long.” From clause]

[Replace “The product of the EAP exchange that is transferred to IEEE 802.16 layer is the Master Session Key (MSK), which is 512 bits in length. This key is known to the AAA server, to the Authenticator (transferred from

AAA server) and to the SS. The SS and the authenticator derive a PMK (Pairwise Master Key) by truncating the MSK to 160 bits” with “The product of the TLS and EAP-TLS exchange that is transferred to IEEE 802.16 layer is the Master Session Key (MSK), which is 512 bits in length. This key is known to the AAA server (in the case of EAP), to the Authenticator (BS) and to the SS. The SS and the BS derive the PMK (Pairwise Master Key) by truncating the MSK to 256 bits”]

[Replace “during first EAP method” to “during first TLS”]

[Replace “PMK ⇐ truncate (MSK, 160)” with “PMK ⇐ MSK”]

[Replace “by sending the PKMv2 EAP Start message signed by HMAC/CMAC\_KEY\_U derived from the

AK.” with ““In the case of EAP based authentication this is done by sending the PKMv2 EAP Start message signed by HMAC/CMAC\_KEY\_U derived from the AK. In the case of TLS based authentication this is done by sending TLS Keypdate message encapsulated in a PKMv2 TLS-Transfer message signed by HMAC derived from the AK” ]

7.2.2.2.3 AK derivation

[Remove “and/or the PAK (from RSA-based authorization procedure)” from first paragraph in clause]

[Replace “Note that PAK and/or PMK” with “Note that PMK” in first paragraph of clause]

[Remove “After the authorization procedure has been performed, the MS and BS will both posses the PAK” from clause]

[Remove “If both the authorization and EAP based authentication procedure were performed, the MS and the Authenticator will possess both the PAK and PMK. The derivation of the AK varies based on which keys are possessed.” From clause]

[Replace key derivation procedure:

“If (PAK and PMK)

AK ⇐Dot16KDF (PAK PMK, SS MAC Address | BSID | PAK | “AK”, 160)

Else

If (PAK)

AK ⇐ Dot16KDF (PAK, SS MAC Address | BSID | PAK | “AK”, 160)

Else // PMK only

AK ⇐ Dot16KDF(PMK, SS MAC Address | BSID | “AK”, 160);

Endif

Endif”

with the following procedure:

“AK ⇐ Dot16KDF(PMK, SS MAC Address | BSID | “AK”, N); ” Where N is the AK key length

7.2.2.2.6.1 Counter-based TEK Generation for HO

[Replace formula: “TEKi= Dot16KDF (KEK\_prime, CMAC\_KEY\_COUNT\_T | SAID | “TEKi Generation”, 128)” with “TEKi= Dot16KDF (KEK\_prime, CMAC\_KEY\_COUNT\_T | SAID | “TEKi Generation”, N), where N is the TEK key length”

7.2.2.2.8 MBS traffic key (MTK)

[Replace formula: “MTK ⇐ Dot16KDF(MAK, MGTEK | “MTK”, 128)” with “MTK ⇐ Dot16KDF(MAK, MGTEK | “MTK”, N), where N is the MTK key length”

7.2.2.2.9.2 Derivation of message authentication codes

Instructions to the editor for Clause 7.2.2.2.9.2 are in the following text:

7.2.2.2.10 Key hierarchy

[Remove first paragraph, figure 7-4, second paragraph, figure 7-5 from clause]

[Replace”160” with “N” in figure 7-6]

[Insert “Where N is the AK key length” after figure 7-6]

7.2.2.4.1 AK context

[Remove: “or PAK” in second paragraph of clause]

[Replace

“Sequence number of root keys (PAK, PMK) for the AK. The AK SN is the most significant 2 bits of the PAK SN concatenated with the least significant 2 bits of the PMK SN.

If AK = f (PAK and PMK), then AK SN = PAK SN + PMK SN

If AK = f (PAK), then AK SN = PAK SN

If AK = f (PMK), then AK SN = PMK SN”

 with

 “Sequence number of root keys (PMK) for the AK. The AK SN is the least significant 2 bits of the PMK SN.” In Table 7-5, “AK Sequence Number” entry]

[Replace

 “The time this key is valid.

If AK = f (PAK and PMK), then AK lifetime = MIN(PAK lifetime,

PMK lifetime)

If AK = f (PAK), then AK lifetime = PAK lifetime

If AK = f (PMK), then AK lifetime = PMK lifetime.

Before this expires, when AK Grace time expires, reauthentication is needed.”

 with “The time this key is valid (PMK lifetime).” in Table 7-5, “AK Lifetime entry”]

[Remove “PAK Sequence Number” entry in Table 7-5]

7.2.2.4.4 PAK context

[Remove clause, including Table 7-8]

7.2.2.9.4 Parameters

[Remove “or may be specified in Auth Reply message.” In first paragraph of clause]

[Remove “or may be specified in a configuration setting within the Auth Reply message” in 3rd bullet of clause]

7.4.1.1 AK key lifetime

[Remove “In PKMv1, the AK’s active lifetime a BS reports in an Authorization Reply message shall reflect, as accurately as an implementation permits, the remaining lifetimes of AK at the time the Authorization Reply message is sent. In PKMv2” in second paragraph of clause]

7.4.1.2 AK transition period on BS side

[Remove second and third paragraph in clause: “In PKMv1, an AK transition … activation of a new AK, and the start of a new key transition period.”

[Remove: Figure 7-14—AK management in BS and SS]

7.4.1.3 BS usage of AK

[Remove “In PKMv1, if the AK Key Sequence Number indicates the newer of the two AKs, the BS shall identify this as an implicit acknowledgment that the SS has obtained the newer of the SS’s two active AKs [see points (b) in Figure 7-14].” In paragraph 2 of clause]

[Remove “The right-hand side of Figure 7-14 illustrates the BS’s policy regarding its use of Aks in PKMv1, where the shaded portion of an AK’s lifetime indicates the time period during which that AK shall be used to derive the HMAC/CMAC\_KEY\_U, HMAC/CMAC\_KEY\_D, and KEK.” In paragraph 4 of clause]

7.4.2 SS key usage

[Remvoe “In PKMv1 or PKMv2 RSA-based authentication, the SS is responsible for sustaining authorization with its BS and maintaining an active AK. In PKMv2 EAP-based authentication,” from clause]

[Replace “reauthorization” to “Reauthorization” in clause]

7.4.2.1 SS reauthorization

[Remove: “In PKMv1, an SS refreshes its AK by reissuing an Auth Request to the BS. The Authorization state machine (7.2.1.5) manages the scheduling of Auth Requests for refreshing AKs. In PKMv2 RSA-based authentication, the SS refreshes its AK by issuing a PKMv2 RSA-Request message. In PKMv2 EAP-based authentication, reauthorization can be initiated by either BS or SS to refresh the AK.” In paragraph 1 of clause]

[Remove “In PKMv1, an SS’s Authorization state machine schedules the beginning of reauthorization a configurable duration of time, the Authorization Grace Time, [see points (x) and (y) in Figure 7-14], before the SS’s latest AK is scheduled to expire. The Authorization Grace Time is configured to provide an SS with an authorization retry period that is sufficiently long to allow for system delays and provide adequate time for the SS to successfully complete an Authorization exchange before the expiration of its most current AK.” In paragraph 2 of clause]

[Replace “In PKMv2 EAP-based authentication, reauthorization” with “Reauthorization” in paragraph 3 of clause]

7.4.2.2 SS usage of AK

[Remove “Key Reply, Key Reject, and TEK Invalid messages for PKMv1, or” from clause]

[Remove paragraph “The left-hand side of Figure 7-14 illustrates an SS’s maintenance and usage of its AKs in PKMv1, where the shaded portion of an AK’s lifetime indicates the time period during which that AK shall be used to decrypt TEKs. Even though it is not part of the message exchange, Figure 7-14 also shows the implicit acknowledgment of the reception of a new AK via the transmission of a Key Request message using the key sequence of the new AK.” From third paragraph of clause]

7.5.4 Derivation of TEKs, KEKs, and message authentication keys

7.5.4.6.1 Dot16KDF for PKMv2

[Replace all text in the clause with the following: “The Dot16KDF algorithm uses HKDF [IETF RFC 5869] as the key derivation algorithm. The following procedure is used:

Dot16KDF(key, astring, keylength)

{

Salt = SHA-256(key | astring | keylength);

PRK = HKDF(salt, key, astring, keylength);

return HMAC-keylength(PRK);

 }”]

7.5.8 Public-key encryption of AK

[Remove clause]

7.5.9 Digital signatures

[Remove clause]

7.6.1 Certificate format

[Replace “All certificates described in this specification shall be signed with the RSA signature algorithm using

SHA-1 as the one-way hash function. The RSA signature algorithm is described in PKCS #1; SHA-1 is

described in FIPS 180-1. Restrictions posed on the certificate values are described in 7.6.1.1 through 7.6.1.8” with “All certificates described in this specification shall be signed with an approved signature algorithm as described in FIPS 186-4. “ in last paragraph of clause]

7.6.1.3 tbsCertificate.signature and signatureAlgorithm

[Replace all text of the clause with “All certificates described in this specification shall be signed with an approved signature algorithm as described in FIPS 186-4. “]

7.8.2 BS and SS RSA mutual authentication and AK exchange overview

[Remove clause]

10.2 PKM parameter values

[Remove “Authorize Reject Wait Timeout” in Table 10-2—Operational ranges for privacy configuration settings, last entry]

[Remove “or PAK” from entry name “PMK or PAK prehandshake lifetime” in Table 10-3]

[Remove entry “PAK Lifetime” in Table 10-3]

[Remove entry “Authorize Wait Timeout” in Table 10-3]

[Remove entry “Authorize Reject Wait Timeout” in Table 10-3]

11. TLV encodings

11.1 Common encodings

11.1.2 Authentication tuples

11.1.2.1 HMAC Tuple

Instructions to the editor for Clause 11.1.2.1 are in the following text:

[Replace “Length: 21” with “Length: 17, 29, 33” in Table 11-2]

[Replace “Reserved” with “Digest Length” in Table 11-3, and for the same row, add the following text for

the Notes field “0b0001: 224 bits 0b0010: 256 bits 0b0011: 384 bits 0b0100: 512 bits”]

[Replace “160 bits” with “N bits” in Table 11-3, and in the same row, replace “SHA-1” in the Notes field

with “SHA-2 or SHA-3”]

The modified table is as follows with changes highlighted in red:

11.1.2.2 CMAC Tuple

Instructions to the editor for Clause 11.1.2.2 are in the following text:

[Replace “Length: 13, or 19” with “Length: 13, 17, 19, 29 or 33” in Table 11-4]

[Replace “160 bits” with “N bits” in Table 11-5]

[Replace “AES-1” with AES-N” in Table 11-5]

11.1.2.2 CMAC Tuple

Instructions to the editor for Clause 11.1.2.2 are in the following text:

[Replace “Length: 13, or 19” with “Length: 13, 17, 19, 29 or 33” in Table 11-4]

[Replace “160 bits” with “N bits” in Table 11-5]

[Replace “AES-1” with AES-N” in Table 11-5]

11.8 SBC-REQ/RSP management message encodings

11.8.4 Security negotiation parameters

11.8.4 Security negotiation parameters

11.8.4.1 PKM version support

[Replace: “Bit 0: PKM version 1” with “Bit 0: Reserved”]

11.8.4.2 Authorization policy support

Instructions to the editor for Clause 11.8.4.2 are in the following text:

[Replace “IEEE 802.16 security, constituting X.509 digital certificates and the RSA public key encryption algorithm, as authorization policy” with “EAP based authorization as authorization policy” in clause]

[Replace “Bit 0: RSA-based authorization at the initial network entry” with “Bit 0: TLS-based authorization at the initial network entry” In the table in the clause 11.8.4.2]

[Replace “Bit 4: RSA-based authorization at reentry” to “Bit 4: TLS-based authorization at reentry” In the table in the clause 11.8.4.2]

[Remove “The PKMv2 Auth-Request/Reply/Reject/Acknowledgment messages shall be used in the RSA-based authorization procedure” in the text after the table in the clause 11.8.4.2]

[Replace “Only EAP-based authorization” with “EAP-based authorization” in table following the text “The following table shows the bit representation of Bit 0–2 in Authorization Policy Support field in an SBC-RSP”]

[Replace “Only RSA-based authorization” with “TLS-based authorization” in table following the text “The following table shows the bit representation of Bit 0–2 in Authorization Policy Support field in an SBC-RSP”]

[Replace “EAP-based authorization after RSA-based authorization” to “Reserved” in table following the text “The following table shows the bit representation of Bit 0–2 in Authorization Policy Support field in an SBC-RSP”]

11.8.12 Auth Type for Single EAP

[Remove clause]

11.9

Table 11-39—PKM attribute types

[Replace entry “35: Encrypted pre-PAK” with “35 Reserved” in Table 11-39—PKM attribute types]

11.9.4 Key lifetime

[Remove: “, a PAK” from clause]

11.9.5 Key sequence number

[Remove: “a PAK” from first paragraph in clause]

[Remove: “, PAK” from the table in clause]

11.9.18 PKM Configuration Settings field

[Remove “Auth Reply, PMKv2-RSA reply,” from clause]

11.9.22 Encrypted Pre-PAK attribute

[Remove clause]

11.9.24 SigBS attribute

[Remove clause]

11.9.30 SigSS

[Remove clause]

11.9.33 Auth result code

[Remove clause]

12.1.1.4.9 PKM-REQ: Auth Info

[Remove clause]

12.1.1.4.10 PKM-REQ: Auth Request

[Remove clause]

12.1.1.4.13 PKM-RSP: Auth Reply

[Remove clause]

12.1.1.4.14 PKM-RSP: Auth Reject

[Remove clause]

14.2.2.2 RSA-based authentication procedure

]Remove clause]