|  |  |  |
| --- | --- | --- |
| **Page** | **Section** | **Changes** |
| 238 | 6.3.2.3.8PKM identifier2nd paragraphs | The SS shall increment (modulo 256) the Identifier field whenever it issues a new PKM message. 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. In PKMv2, a PKMv2 RSA-Request, PKMv2 ECC-Request, PKMv2 SA-TEK-Challenge, or PKMv2 Key-Request message is a “new” message. For retransmissions, the Identifier field shall remain unchanged. |
| 238 | 6.3.2.3.8PKM identifier4th paragraphs | On reception of a PKM-RSP message, the SS associates the message with a particular state machine (the Authorization state machine in the case of Authorization Replies, Authorization Rejects, and Authorization Invalids for the PKMv1, PKMv2 RSA-ECC Reply, PKMv2 RSA-ECC Reject,PKMv2 EAP Transfer, PKMv2 SA-TEK-Challenge, PKMv2 SA-TEK-Response for the PKMv2; a particular TEK state machine in the case of Key Replies, Key Rejects, and TEK Invalids the PKMv1, PKMv2-Key-Reply, PKMv2-Key-Reject, PKMv2 TEK-Invalids, and PKMv2 Group-Key-Update-Command messages for the PKMv2). |
| 238 | 6.3.2.3.8PKM identifier6th paragraphs | In PKMv2, both an SS and a BS shall keep track of their latest ID. An SS shall keep track of the ID of its latest, pending PKMv2 RSA-ECC-Request. The SS shall discard PKMv2 RSA-ECC-Reply and PKMv2 RSA-ECC-Reject messages with Identifier fields not matching that of the pending PKMv2 RSA-ECC-Request. Moreover, a BS shall keep it, pending PKMv2 RSA-ECC-Reply. The BS shall discard PKMv2 RSA-ECC-Acknowledgment messages with Identifier fields not matching that of the pending PKMv2 RSA-ECC-Reply. |
| 239 | 2nd paragraph | An SS shall keep track of the ID of its latest, pending PKMv2 RSA-ECC-Request. The SS shall discard PKMv2 RSA-ECC-Reply and PKMv2 RSA-ECC-Reject messages with Identifier fields not matching that of the pending PKMv2 RSA-ECC-Request. Moreover, a BS shall keep it, pending PKMv2 RSA-ECC-Reply. The BS shall discard PKMv2 RSA-ECC-Acknowledgment messages with Identifier fields not matching that of the pending PKMv2 RSA-ECC-Reply. |
| 239 | Table 6-69 |

|  |  |
| --- | --- |
| 13 | PKMv2 RSA-ECC-Request  |
| 14 | PKMv2 RSA-ECC-Reply  |
| 15 | RSA-ECC-Reject  |
| 16 | RSA-ECC-Acknowledgment  |

 |
| 241 | 1st paragraph after table 6-71 | The SS-Certificate attribute contains an X.509 SS certificate (see 7.6) issued by the SS’s manufacturer. The SS’s X.509 certificate is a public-key certificate that binds the SS’s identifying information to its public key (RSA or ECC) in a verifiable manner. The X.509 certificate is digitally signed by the SS’s manufacturer, and that signature can be verified by a BS that knows the manufacturer’s public key. The manufacturer’s public key is placed in an X.509 certification authority (CA) certificate, which in turn is signed by a higher level CA. |
| 246 | 6.3.2.3.9.11 | **6.3.2.3.9.11 PKMv2 RSA-ECC-Request message**A client MS sends a PKMv2 RSA-ECC-Request message to the BS in order to request mutual authentication in the RSA-based or ECC-based authorization. |
| 246 | Table 6-80 | **Table 6-80— PKMv2 RSA-ECC-Request message attributes**

|  |  |
| --- | --- |
| **Attribute** | **Contents** |
| **…** | **…** |
| SigSS  | An RSA or ECC signature over all the other attributes in the message |

 |
| 246 | 2nd paragraph after table 6-80 | The SigSS attribute indicates a RSA signature or ECC signatureover all the other attributes in this message, and the MS’s private key is used to make a RSA signature or ECC signature. |
| 246 | 6.3.2.3.9.12 | **6.3.2.3.9.12 PKMv2 RSA-ECC-Reply message**Sent by the BS to a client MS in response to a PKMv2 RSA-ECC-Request message, the PKMv2 RSA-ECC-Reply message contains an encrypted pre-primary authorization key (pre-PAK), the key’s lifetime, and the key’s sequence number. The pre-PAK shall be encrypted with the MS’s public key. The MS Random number is returned from the PKMv2 RSA-ECC-Request message, along with a random number supplied by the BS, thus enabling assurance of key liveness. |
| 247 | Table 6-81 | **Table 6-81— PKMv2 RSA-ECC-Reply message attributes**

|  |  |
| --- | --- |
| **Attribute** | **Contents** |
| … | … |
| Encrypted pre-PAK | RSA-ECC-OAEP-Encrypt(PubKey(MS), pre-PAK | MS MAC Address) |
| … | … |
| SigBS | An RSA signature or ECC signature over all the other attributes in the message |

 |
| 247 | 1st paragraph after table 6-81 | The SigBS attribute indicates a RSA signature or ECC signature over all the other attributes in this message, and the BS’s private key is used to make a RSA signature or ECC signature. |
| 247 | 6.3.2.3.9.13 | **6.3.2.3.9.13 PKMv2 RSA-ECC-Reject message**The BS responds to an SS’s authorization request with a PKMv2 RSA-ECC-Reject message if the BS rejects the SS’s authorization request. When an MS receives this message, an MS may retransmit the PKMv2 RSA-ECC-Request message or quit RSA-ECC-based mutual authentication. |
| 247 | Table 6-82 | **Table 6-82—PKMv2 RSA-ECC-Reject message attributes**

|  |  |
| --- | --- |
| **Attribute** | **Contents** |
| … | … |
| SigBS | An RSA signature or ECC signature over all the other attributes in the message |

 |
| 247 | Paragraph 1-2 after Table 6-82 | The Error-Code and Display-String attributes describe to the requesting MS the reason for the RSA-ECC-based authorization failure. The SigBS attribute indicates a RSA signature or ECC signature over all the other attributes in this message, and the BS’s private key is used to make a RSA signature or ECC signature. |
| 248 | 6.3.2.3.9.14 | **6.3.2.3.9.14 PKMv2 RSA-ECC-Acknowledgment message**The MS sends the PKMv2 RSA-ECC-Acknowledgment message to BS in response to a PKMv2 RSA-ECC-Reply message. Only if the value of the Auth Result Code attribute is failure, then the Error-Code and Display-String attributes can be included in this message. |
| 248 | Table 6-83 | **Table 6-83—PKMv2 RSA-ECC-Acknowledgment message attributes**

|  |  |
| --- | --- |
| **Attribute** | **Contents** |
| … | … |
| SigBS | An RSA signature or ECC signature over all the other attributes in the message |

 |
| 248 | 1st paragraph after table 6-83 | The SigSS attribute indicates a RSA-ECC signature over all the other attributes in this message, and the SS’s private key is used to make a RSA-ECC signature. |
|  |  |  |
| 841 | f7.1 9th paragaraph | * 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-ECC-based authorization is selected as an authorization policy between an SS and a BS.
 |
| 842 | Figure 7-1 |  |
| 842 | 7.1.21st paragraph | The PKM protocol allows for both mutual authentication and unilateral authentication (e.g., where the BS authenticates SS, but not vice versa). It also supports periodic reauthentication/reauthorization and key refresh. The key management protocol uses either EAP [IETF RFC 3748] or X.509 digital certificates [IETF RFC 3280] together with RSA public-key encryption algorithm [PKCS #1 v2.2], ECC public-key encryption algorithm [FIPS 186-5] or a sequence starting with RSA-ECC authentication and followed by EAP authentication. It uses strong encryption algorithms to perform key exchanges between an SS and BS. |
| 842 | 7.1.23rd paragraph | A BS authenticates a client SS during the initial authorization exchange. Each SS presents its credentials, which shall be a unique X.509 digital certificate issued by the SS’s manufacturer (in the case of RSA-ECC authentication) or a operator-specified credential (in the case of EAP-based authentication). |
| 843 | 7.1.33rd paragraph | — RSA-ECC protocol, RSA-based [PKCS #1 v2.1 with SHA-1(FIPS 186-2)] (support is mandatory in PKMv1; support is optional in PKMv2, with RSA [PKCS#1 v2.2 with SHA-x, where x is 2 or higher (FIPS 186-5)] or ECC-based [FIPS 186-5] |
| 843 | 7.1.3.11st paragraph | The PKM RSA-ECC authentication protocol uses X.509 digital certificates [IETF RFC 3280], the RSA public key encryption algorithm [PKCS #1,v2.2] or the ECC key encryption [FIPS 186-5] that binds public RSA encryption keys to MAC addresses of SSs.  |
| 843 | 7.1.3.13rd paragraph | All SSs using RSA-ECC authentication shall have factory-installed RSA private/public key pairs or ECC private/public key pairs or provide an internal algorithm to generate such key pairs dynamically. If an SS relies on an internal algorithm to generate its public key pair, the SS shall generate the key pair prior to its first AK exchange, described in 7.2.1. All SSs with factory-installed RSA key pairs or ECC key pairs shall also have factory-installed X.509 certificates. All SSs that rely on internal algorithms to generate a public key pair shall support a mechanism for installing a manufacturer-issued X.509 certificate following key generation. |
| 844 | 7.1.6.31st par. | Similar to other MAC management messages, all the PKM messages are exchanged between MS/RS and MR-BS. For the PKM messages that are not protected by the message authentication code from the MS/RS (termed as non-authenticated PKM messages, e.g., Auth Request, Auth Reply, PKMv2 RSA-ECC-Request, PKMv2 RSA-ECC-Reply), the following procedure may be applied. For all the other cases, the access RS and the intermediate RSs just simply relay the PKM messages. |
| 861 | 7.2.2.14th par. | 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. |
| 861 | 7.2.2.16th par. | For SAs using a ciphersuite employing N bits keys, such as AES-CCM mode, the TEK in the Key Reply is AES encrypted using a N-bit key derived from the AK and a N-bit block size. |
| 862 | 7.2.2.22nd par. | Since there are two authentication schemes, one based on RSA-ECC and one based on EAP, there are two primary sources of keying material. |
| 862 | 7.2.2.23rd par. | 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-ECC-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. |
| 862 | 7.2.2.2.1 | **7.2.2.2.1 RSA-ECC-based authorization**When the RSA-ECC-based authorization is negotiated as authorization policy, the PKMv2 RSA-ECC-Request, the PKMv2 RSA-ECC-Reply, the PKMv2 RSA-ECC-Reject, and the PKMv2 RSA-ECC-Acknowledgment messages are used to share the pre-PAK. |
| 862 | 7.2.2.2.14th par. | PAK shall be used to generate the AK (see 7.2.2.2.3) if RSA-ECC authorization was used. PAK is 160 bits long. |
| 863 | 7.2.2.2.2 | If a RSA-ECC 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.The BS and the SS will share the AK which is derived from the PMK (from EAP-based authorization procedure) and/or the PAK (from RSA-ECC-based authorization procedure). Note that PAK and/or PMK can be used according to the value of Authorization Policy Support field included in the SBC-REQ/RSP messages. |
| 867 | 7.2.2.2.9.2Par. 5 | CMAC\_KEY\_GD ⇐ Dot16KDF(GKEK, “GROUP CMAC KEY”,N) (Used for broadcast MAC), N=128, 192 or 256 |
| 867 | 7.2.2.2.9.2Par. 5 | Specifically, the preprocessed value of CMAC\_PREKEY\_\* is treated as the Cipher Key of the Advanced Encryption Standard (AES) algorithm AES-N (FIPS197). The CMAC\_KEY\_COUNT is treated as the Input Block Plain Text of this algorithm. The AES-N algorithm is executed once. The Output Block Cipher Text of this algorithm is treated as the resulting CMAC\_KEY\_\*. When CMAC\_KEY\_COUNT is used as an input of AES-N algorithm, 112 zero bits are prepadded before the 16-bit CMAC\_KEY\_COUNT where the |
| 868 | 7.2.2.2.10Par. 1 | Figure 7-4 outlines the process to calculate the AK when the RSA-ECC-based authorization process has taken place, but where the EAP based authentication process has not taken place, or the EAP method used has not yielded an MSK |
| 868 | Figure 7-4 | **AK from PAK only (from RSA-ECC-based authorization)** |
| 869 | Figure 7-5 | **AK from PAK and PMK (RSA-ECC-based and EAP-based authorization)** |
| 870 | Figure 7-7 | **HMAC/CMAC/KEK derivation from AK** |
| 870 | Figure 7-8 |  |
| 875 | 7.2.2.3.1Par.3-4 | — The KEK, a N-bit key encryption key, derived from the AK.— TEK0 and TEK1, N-bit traffic encryption keys, generated within the BS and transferred from |
| 875 | 7.2.2.3.3Par 4-5 | — The MGTEK, a N-bit MBS GTEK, used indirectly to protect MBS traffic. It is updated more frequently than the MAK.— The MTK (MBS Traffic Key) a N-bit key used to protect MBS traffic, derived from the MAK and MGTEK. |
| 877 | Table 7-5 |

|  |  |  |
| --- | --- | --- |
| PMK Sequence Number | 4 | The sequence number of the PAK that this AK is derived from. If RSA-ECC authentication is not used, this value shall be set to zero |

 |
| 877 | Table 7-5 |

|  |  |  |
| --- | --- | --- |
| KEK | 256 | Used to encrypt transport keys from the BS to the SS. |

 |
| 878 | Table 7-6 |

|  |  |  |
| --- | --- | --- |
| KEK | 256 | Used to encrypt transport keys from the BS to the SS. |

 |
| 878 | 7.2.2.4.4 | The PAK context includes all parameters associated with the PAK. This context is created when RSA-ECC Authentication completes. |
| 879 | Table 7-8 |

|  |  |  |
| --- | --- | --- |
| PAK Lifetime | 32 | PAK lifetime, from when the RSA-ECC-based authorization is achieved. The value of PAK lifetime is initially set to a default value. The 3-way handshake may subsequently change this value. |
| PAK sequence number | 4 | PAK sequence number, when the RSA-ECC-based authorization is achieved and a key is generated. The 2 MSBs are the sequence counter. And the 2 LSBs set to 0. |

 |
| 880 | 7.2.2.7 | For SAs using a ciphersuite employing DES-CBC, the AK in the AK Transfer message is triple DES (3-DES) encrypted, using a two-key, 3-DES KEK derived from the Access RS AK. For SAs using a ciphersuite employing 128 bits keys, such as AES-CCM mode, the TEK in the AK Transfer message is AES encrypted using a 1N-bit key derived for the Access RS AK and a N-bit block size. |
| 899 | 7.4.2 | In PKMv1 RSA-based authentication or PKMv2 RSA-ECC-based authentication, the SS is responsible for sustaining authorization with its BS and maintaining an active AK. In PKMv2 EAP-based authentication, reauthorization can be initiated by either BS or SS to refresh the AK. An SS shall be prepared to use its two most recently obtained AKs according to the manner described in 7.4.2.1 through 7.4.2.3. |
| 899 | 7.4.2.1 | AKs have a limited lifetime and shall be periodically refreshed. 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-ECC-based authentication, the SS refreshes its AK by issuing a PKMv2 RSA-ECC-Request message. In PKMv2 EAP-based authentication, reauthorization can be initiated by either BS or SS to refresh the AK. The SS initiates reauthorization by issuing PKMv2 EAP-Start message to the BS. The BS initiates reauthorization by issuing PKMv2 EAP-Transfer message encapsulating EAP request/identity to the SS. The authorization state machine for PKMv2 EAP-based authentication is described in 7.2.2.8. |
| 906 | 7.5.1.3 | If the data encryption algorithm identifier in the cryptographic suite of an MBS GSA equals 0x80, data on connections associated with that SA shall use the CTR mode of the AES algorithm (NIST Special Publication 800-38A, FIPS 197, IETF RFC 3686) to encrypt the MAC PDU payloads. In MBS, the AES block size and cipher counter block are N bits, where N is 128, 192 or 256. |
| 907 | Par. 3 | A 32-bit nonce NONCE = n0 | n1 | n2 | n3 (n0 being the most significant byte and n3 the least significant byte) is made of ROC and 24 bits frame number in the following way: n0 = ROC and n1, n2, n3 are the byte representation of frame-number in MSB first order. NONCE shall be repeated four/six/eight times to construct the N-bit counter block required by the AES cipher. (initial counter = [N/32] x NONCE, e.g., NONCE|NONCE|NONCE|NONCE…). When incremented, this 16/24/32-byte counter shall be treated as a big endian number. |
| 907 | Par. 5 | A different N-bit counter value is used to encrypt each N-bit block within a PDU. |
| 908 | 7.5.1.4.1Par. 2 | The CBC IV is generated as the result of the AES block ciphering algorithm with the key of TEK. Its plain text for the CBC IV generation is calculated with the exclusive-or (XOR) of (1) the CBC IV parameter value included in the TEK keying information, and (2) the N-bits content which is a concatenation of the 48-bit MAC PDU header, the 32-bit PHY Synchronization value of the MAP that a data transmission occurs, and the XOR value of the 48-bit SS MAC address and the Zero Hit Counter. |
| 909 | Figure 7-22 |  |
| 910 | 7.5.2.2 | **7.5.2.2 Encryption of TEK with RSA or ECC**The RSA method of encrypting the TEK (PKCS #1 v2.2) shall be used for SAs with the TEK encryption algorithm identifier in the cryptographic suite equal to 0x02 (1024 bits RSA), 0x05 (2048 bits RSA) or 0x06 (4096 bits RSA). When the RSA algorithm is in use for TEK encryption algorithm, the TEK is encrypted with SS’s public key using the RSA algorithm. In this case, KEK is not used.The ECC method of encrypting the TEK (FIPS 186-5) shall be used for SAs with the TEK encryption algorithm identifier in the cryptographic suite equal to 0x09 (224-bits ECC) or 0x10 (256 bits ECC). When the ECC algorithm is in use for TEK encryption algorithm, the TEK is encrypted with SS’s public key using the ECC algorithm. In this case, KEK is not used. |
| 910 | 7.5.2.3 | **7.5.2.3 Encryption of TEK-N with AES**This method of encrypting the TEK-N shall be used for SAs with the TEK encryption algorithm identifier in the cryptographic suite equal to 0x03 (128 bit key length), 0x07 (192 bit key length) or 0x08 (256 bit key length). The BS encrypts the value fields of the TEK-N in the Key Reply messages it sends to client SS. This field is encrypted using N-bit AES in ECB mode.**Encryption: C = Ek1[P]****Decryption: P = Dk1[C]****P = Plaintext N-bit TEK****C = Ciphertext N-bit TEK****k1 = the N-bit KEK****E[ ] = N-bit AES ECB mode encryption**D[ ] = N-bit AES ECB decryptionWhere N is 128, 192 or 256 bit.Subclause 7.5.4 describes how the KEK is derived from the AK This method of encrypting the TEK-N shall be used for SAs with the TEK encryption algorithm identifier in the cryptographic suite equal to 0x03, 0x07 or 0x08. |
| 910 | 7.5.2.4 | **7.5.2.4 Encryption of TEK-N with AES key wrap**This method of encrypting the TEK-N shall be used for SAs with the TEK encryption algorithm identifier in the cryptographic suite equal to 0x04 (128 bit key length), 0x09 (192 bit key length) or 0x10 (256 bit key length). The BS encrypts the value fields of the TEK-N in the Key Reply messages it sends to client SS. This field is encrypted using the AES key wrap algorithm.**Encryption: C,I = Ek[P]****Decryption: P,I = Dk[C]****P = Plaintext N-bit TEK****C = Ciphertext N-bit TEK****I = Integrity Check Value****k = the N-bit KEK****Ek[ ] = AES Key Wrap encryption with key k****Dk[ ] = AES Key Wrap decryption with key k****Where N is 128, 192 or 256** |
| 911 | 7.5.3 | The calculation of the keyed hash in the HMAC Digest attribute and the HMAC Tuple shall use the HMAC (IETF RFC 2104) with the secure hash algorithm SHA-2 (FIPS 180-4). The DL authentication key HMAC\_KEY\_D shall be used for authenticating messages in the DL direction. The UL authentication key HMAC\_KEY\_U shall be used for authenticating messages in the UL direction. UL and DL message authentication keys are derived from the AK (see 7.5.4 for details). The HMAC Sequence number in the HMAC Tuple shall be equal to the AK Sequence Number of the AK from which the HMAC\_KEY\_x was derived. |
| 911 | 7.5.4 | The BS generates AKs, TEKs, and IVs. A random or pseudo-random number generator shall be used to generate AKs and TEKs. A random or pseudo-random number generator may also be used to generate IVs. Regardless of how they are generated, IVs shall be unpredictable. Recommended practices for generating random numbers for use within cryptographic systems are provided in IETF RFC 1750 [B32]. In case of using RSA-ECC algorithm, KEK is not used. |
| 912 | 7.5.4.2 | The construction of the KEK for use with TEK-N keys shall be the same as for 3-DES KEKs except that the HASH functions is SHA-256 and the full Nbits of the KEK are used directly as the N-bit AES key, instead of the KEK being split into two 64-bit DES keys. |
| 914 | 7.5.4.5.1 | The construction of the KEK for use with TEK-N keys shall be the same as for 3-DES KEKs as described in 7.5.4.2 except that the full N bits of the KEK are used directly as the N-bit AES key, instead of the KEK being split into two 64-bit DES keys. |
| 915 | 7.5.4.5.2.2 | The RSA method of encrypting the GKEK (PKCS #1 v2.2, RSA Cryptography Standard, RSA Laboratories, June 2002) shall be used for SAs with the TEK (or GTEK) encryption algorithm identifier in the cryptographic suite equal to 0x02 (1024-bit key length), 0x05 (2048-bit key length) or 0x06 (4096-bit key length).  |
| 915 | 7.5.4.5.2.3 | This method of encrypting the GKEK shall be used for SAs with the TEK (or GTEK) encryption algorithm identifier in the cryptographic suite equal to 0x03 (128 bit), 0x07 (192 bit) or 0x08 (256 bit). The BS encrypts the value fields of the GKEK in the PKMv2 Group-Key-Update-Command messages (for the GKEK update mode) it sends to client SS. This field is encrypted using 128-bit AES in ECB mode.**Encryption: C = Ek1[P]****Decryption: P = Dk1[C]****P = Plaintext N-bit GKEK****C = Ciphertext N-bit GKEK****k1 = the N-bit KEK****E [ ] = N-bit AES ECB mode encryption****D [ ] = N-bit AES ECB mode decryption****Where N=128, 192 or 256** |
| 915 | 7.5.4.5.2.4 | This method of encrypting the GKEK shall be used for SAs with the TEK (or GTEK) encryption algorithm identifier in the cryptographic suite equal to 0x04 (128 bit), 0x09 (192 bit) or 0x10 (256 bit).The BS encrypts the value fields of the GKEK in the PKMv2 Group-Key-Update-Command messages (for the GKEK update mode) it sends to client SS. This field is encrypted using N-bit AES key wrap algorithm. This N-bit AES key wrap algorithm is defined only for PKM version 2.**Encryption: C,I = Ek[P]****Decryption: P,I = Dk[C]****P = Plaintext N-bit GKEK****C = Ciphertext N-bit GKEK****k = the N-bit KEK derived from the AK****Ek[ ] = AES Key Wrap encryption with key k****Dk[ ] = AES Key Wrap decryption with key k** |
| 917 | 7.5.8 | AKs in Auth Reply messages shall be RSA public-key encrypted, using the SS’s public key. The protocol uses 65537 (0x010001) as its public exponent and a modulus length of M bits, where M is 1024, 2048 or 4096. The PKM protocol employs the RSAES-OAEP encryption scheme (PKCS #1v2.2). RSAES-OAEP requires the selection of a hash function, a mask-generation function, and an encoding parameter string. The default selections specified in PKCS #1v2.2 shall be used when encrypting the AK. These default selections are SHA-256 for the hash function, MGF1 with SHA-256 for the mask-generation function, and the empty string for the encoding parameter string. |
| 917 | 7.5.9 | The Protocol employs the RSA Signature Algorithm (PKCS #1 v2.2) with SHA-2 or SHA-3 (FIPS 186-5) for both of its certificate types.As with its RSA encryption keys, Privacy uses 65537 (0x010001) as the public exponent for its signing operation. Manufacturer CAs shall employ signature key modulus lengths of at least 1024 bits and no greater than 4096 bits. |
| 918 | 1st par after table 7-13 | All certificates described in this specification shall be signed with the RSA signature algorithm using SHA-2 or SHA-3 as the one-way hash function. The RSA signature algorithm is described in PKCS #1 v2.2; SHA-2 and SHA-3 is described in FIPS 180-4. Restrictions posed on the certificate values are described in 7.6.1.1 through 7.6.1.8. |
| 918 | 7.6.1.3 | All PKMv1 certificates described in this specification shall be signed with the RSA signature algorithm, using SHA-1 as the one-way hash function. PKMv2 certificates shall be signed with either RSA signature algorithm, using SHA-2 or SHA-3 as the one-way hash function or by the ECC signature algorithm, as described in FIPS 180-5. The ASN.1 OID used to identify the “SHA-x with RSA” signature algorithm is sha-xWithRSAEncryption OBJECT IDENTIFIER ::={ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}When the sha-xWithRSAEncryption OID appears within the ASN.1 type AlgorithmIdentifier, as is the case with both tbsCertificate.signature and signatureAlgorithm, the parameters component of that type is theASN.1 type NULL. |
| 721 | 7.6.1.8 | In all three PKM certificate types, the signatureValue contains the RSA or ECC (with SHA-2 or SHA-3) signature computed over the ASN.1 DER encoded tbsCertificate. The ASN.1 DER encoded tbsCertificate is used as input to theRSA signature function. The resulting signature value is ASN.1 encoded as a bit string and included in the Certificate’s signatureValue field. |
| 721 | 7.6.2 | Manufacturer-issued SS certificates shall be stored in SS permanent, write-once memory. SSs that have factory-installed RSA private/public key pairs or ECC private/public key pairs shall also have factory-installed SS certificates. SSs that rely on internal algorithms to generate an RSA key pair shall support a mechanism for installing a manufacturer issued SS certificate following key generation.  |
| 924 | 7.8.2 | **7.8.2 BS and SS mutual authentication** The BS mutual authentication can take place in one of three modes of operation. In one mode, only RSA-ECC mutual authentication is used. In the second mode, the RSA-ECC mutual authentication is followed by EAP authentication. In this second mode, the mutual authentication is performed only for initial network entry, and only EAP authentication is performed if authentication is needed in reentry. In the the third mode, the mutual authentication is performed with EAP-TLS, and a certificate authority authenticates both SS and BS certificates.**7.8.2.1 BS and SS RSA-ECC mutual authentication and AK exchange overview**SS RSA-ECC mutual authorization, controlled by the PKMv2 Authorization state machine, is the process of  |
| 924 | Last par. | The RSA signature or ECC signature over all the other attributes in the auth-reply message by BS, used to assure the authenticity of the above PKMv2 RSA-ECC-Reply messages. |
| 925 | 2nd par. | After successful RSA-ECC based authorization either EAP based authorization or Authenticated EAP based authorization maybe supported according to the value of Authorization policy negotiated in the SBC-REQ/RSP messages. It shall cryptographically bind RSA or ECC and further EAP authentication. |
| 925 | New par. After 2nd par. | **7.8.2.2 BS and SS EAP based mutual authentication and AK exchange overview**TBD |
| 1554 | Table 10-3 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| MS | Authorize WaitTimeout | PKMv2 RSA-ECC-Requestretransmission interval fromAuth Wait state | 2 s | 10 s | 30 s |
| MS | Reauthorize WaitTimeout | PKMv2 RSA-ECC-Requestretransmission interval fromReauth Wait state | 2 s | 10 s | 30 s |
| MS | Authorize RejectWait Timeout | Delay before resending PKMv2 RSA-ECC-Request after receiving PKMv2 RSA-ECC-Reject | 10 s | 60 s | 10 min(600 s) |

 |
|  |  |  |
| 1562 | Table 11-2 | Length: 17, 29, 33  |
| 1563 | Table 11-3 |

|  |  |  |
| --- | --- | --- |
| *Digest Length* | 4 bits | 0b0001: 224 bits0b0010: 256 bits0b0011: 384 bits0b0100: 512 bits |
| HMAC Key Sequence Number | 4 bits |  |
| HMAC Digest | N bits | HMAC with SHA-2 or SHA-3 |

 |
| 1563 | Table 11-4 | Length: 13, 17, 19, 29 or 33 |
| 1563 | Table 11-5 |

|  |  |  |
| --- | --- | --- |
| CMAC Value | N bits | CMAC with AES-N |

 |
| 1671 | 11.8.4.2 |

|  |  |  |
| --- | --- | --- |
| Type | Length | Value |
| 25.2 | 1 | Bit 0: RSA-based authorization at the initial network entryBit 1: EAP-based authorization at the initial network entryBit 2: ECC-based authorization at the initial network entryBit 3: Set to 0Bit 4: RSA-based authorization at reentryBit 5: EAP-based authorization at reentryBit 6: ECC-based authorization at reentryBit 7: *Reserved*; shall be set to 0 |

 |
| 1672 | Par 1 | The PKMv2 Auth-Request/Reply/Reject/Acknowledgment messages shall be used with RSA encryption in the RSA-based authorization procedure and with ECC encryption in the ECC-based authorization procedure. |
| 1672 | Par 3 | Bits 4–6 are only applied to the SBC-REQ message.  |
| 1683 | 11.9.2 | The AK (AUTH-Key) is a 20 byte quantity, from which a KEK, and two message authentication keys (one for UL requests, and a second for DL replies) are derived. This attribute contains a M/8 byte quantity containing the AK RSA-encrypted with the SS’s M bit RSA public key. Details of the RSA encryption procedure are given in 7.5. The ciphertext produced by the RSA algorithm shall be the length of the RSA modulus, i.e., M/8 bytes. If the AK is ECC encrypted the ciphertext produced by the ECC algorithm shall be the

|  |  |  |
| --- | --- | --- |
| Type | Length | Value |
| 7 | M | M-byte quantity representing an RSA-encrypted AK with 8M bit key length. Where M=128 (1024 bit RSA), 256 (2048 bit RSA) or 512 (4096 bit RSA).In the case of ECC-encryption, K may vary between 60 bytes (ECC 224 bit key length, with AES-128 and SHA-256) to 100 bytes (ECC 512 bit key length with AES-256) |

 |
| 1684 | 11.9.3 |

|  |  |  |
| --- | --- | --- |
| Type | Length | Value |
| 8 | 81624283240128256512 | Encrypted TEK for DESEncrypted TEK for AES-128Encrypted TEK for AES-192 or for AES-128 key wrap Encrypted TEK for ECC-224Encrypted TEK for AES-256 or for ECC-256Encrypted TEK for AES-256 key wrap Encrypted TEK for RSA-1028 or for ECC-512Encrypted TEK for RSA-2048Encrypted TEK for RSA-4096 |

 |
| 1684 |  | When the TEK encryption algorithm identifier in the SA is 0x01, the length shall be 8, and the TEK shall be encrypted with 3DES in EDE mode according to the procedure defined in 7.5.2.1.When the TEK encryption algorithm identifier in the SA is 0x03, the length shall be 16, and the TEK shall be encrypted with AES in ECB mode according to the procedure in 7.5.2.3.When the TEK encryption algorithm identifier in the SA is 0x04, the length shall be 24, and the TEK shall be encrypted with the AES key wrap algorithm according to the procedure in 7.5.2.4.Add ECC and strong TEK |
| 1684 | Table 11-41 |

|  |  |
| --- | --- |
| Value | דDescription |
| 0 | *Reserved* |
| 1 | 3-DES EDE with 128-bit key |
| 2 | RSA with 1024-bit key |
| 3 | ECB mode AES with 128-bit key |
| 4 | AES key wrap with 128-bit key |
| 5 | RSA with 2048-bit key |
| 6 | RSA with 4096-bit key |
| 7 | ECB mode AES with 192-bit key |
| 8 | ECB mode AES with 256-bit key |
| 9 | AES key wrap with 192-bit key |
| 10 | AES key wrap with 256-bit key |
| 11 | ECC with 224-bit key |
| 12 | ECC with 256-bit key |
| 11–255 | *Reserved* |

 |
|  |  |  |