ANEXO D. CARACTERISTICAS DE SEGURIDAD DEL ESTANDAR 802.16.

La seguridad del estándar 802.16 tiene dos metas, una es proveer privacidad a través de la red inalámbrica, y la otra es dar control de acceso para poder acceder en forma segura a la red. La privacidad se lleva a cabo cifrando la conexiones entre EB y ES. La EB protege contra acceso no autorizado haciendo cifrar el flujo de datos a través de la red. Un protocolo de privacidad y otro de gestión de claves PKM son usados para que la EB controle la distribución de información protegida hacia las ES permitiendo que estas entidades sincronicen su información en forma segura [1] [2].

ASOCIACIONES DE SEGURIDAD (SA)

Una SA es el conjunto de reglas de información de seguridad que una o mas ESs comparten para soportar comunicaciones seguras a través de la red WiMAX, El estándar utiliza dos diferentes tipos de SA. Datos y Autorización. La figura D.1 resume la información usada en las SAs.

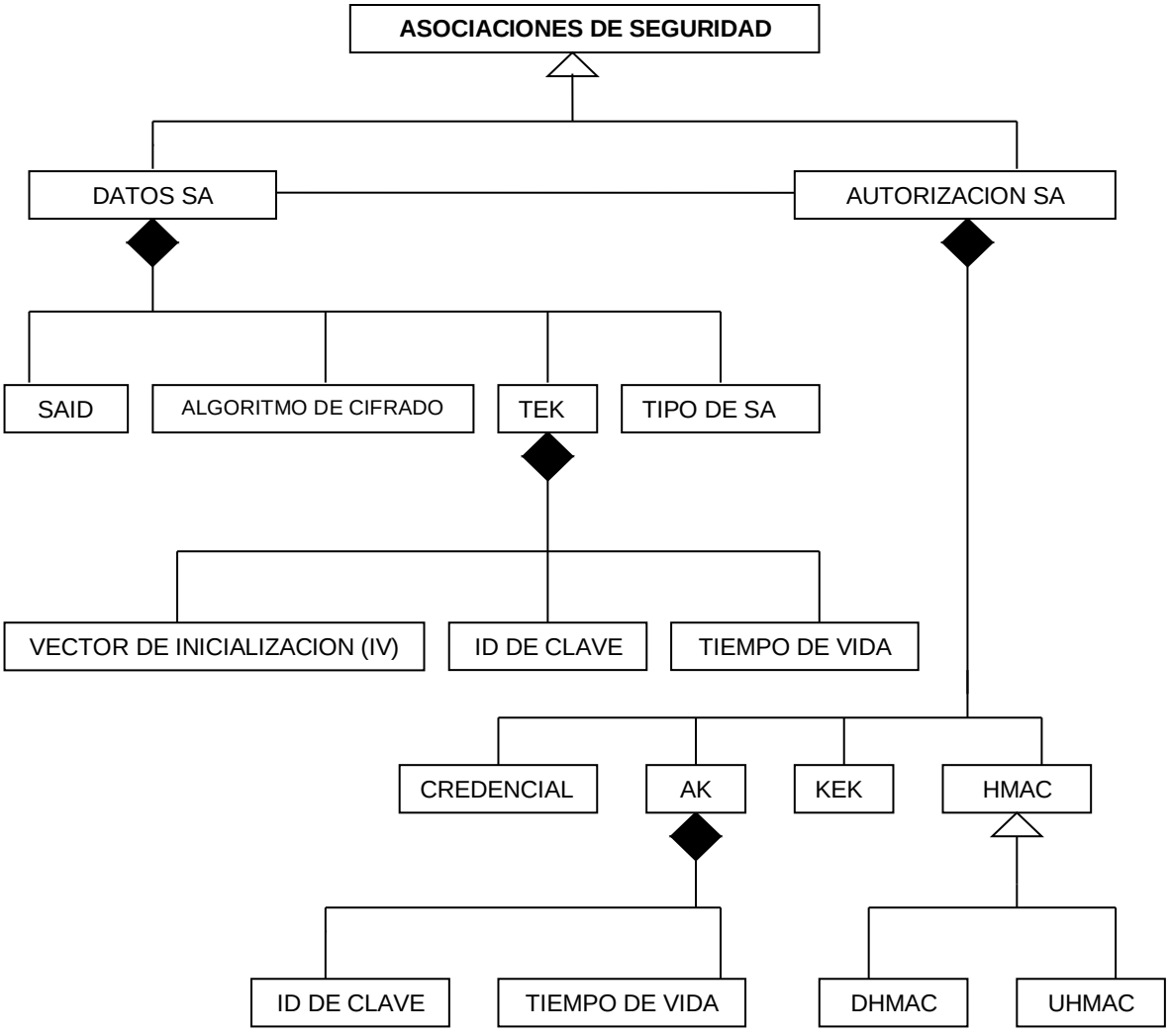
Hay tres diferentes tipos de SA de datos, primaria, estática y dinámica. Las SA primarias son establecidas por la ES durante su proceso de inicialización, la EB provee las SA estáticas, las SA dinámicas son establecidas y descartadas necesario esto para el intercambio de información. Las SA dinámicas y estáticas pueden ser repartidas entre múltiples ES.

El identificador de SA (SAID) es usado únicamente para identificar la SA de datos. El mensaje cifrado define que método de cifrado de datos fue utilizado inicialmente, el estándar define el uso del algoritmo de cifrado de datos DES en modo CBC.

Las claves de cifrado de trafico (TEKs) son usadas para cifrar la transmisión de datos entre la EB y la ES. La SA define dos TEK, una para operaciones corrientes y la otra es usada cuando la TEK de uso corriente expira. Los dos identificadores de TEK están

incluidas, uno en cada clave. Un TEK con un tiempo de vida también se incluye para indicar cuando el TEK expira. El tiempo de vida por defecto es de 12 horas a un día, pero este puede variar desde 30 minutos a 7 días.

Figura D.1 Diagrama de clases de una SA.



El algoritmo DES en modo CBC requiere un vector de inicialización (IV) para su operación, uno para cada TEK el cual es incluido en los datos de la SA. Los dos vectores de inicialización son de 64 bits de longitud para alojar el bloque de 64 bits utilizado en el cifrado del DES. Los tipos de datos de la SA son también incluidos indicando cual es primario, estático o dinámico [2].

La SA de datos protege la conexión del transporte entre una o más ESs y una EB. Una ES generalmente tiene una SA para la gestión del canal secundario y una SA cualquiera para el transporte de conexión de subida y bajada en forma separada. Para múltiples conexiones cada grupo requiere una SA que estará entre estas entidades, de este modo, el estándar maneja muchos identificadores de conexiones los cuales son parte de una SA particular. Las SA de autorización forman parte de las EB y las ES, estas son usadas por la EB para configurar las SA de datos por la ES.

En la tabla D.1 se muestra el contenido de una SA de autorización, un certificado X.509 se incluye para permitir que la EB identifique la ES, la clave de autorización (AK) de 160 bits es incluida para permitir que la EB y la ES se autentiquen mediante el intercambio de claves TEK. Una AK identificadora de 4 bits es usada para diferenciarse entre diferentes AKs. El tiempo de vida de una AK se incluye también para indicar cuando la AK expira, este tiempo de vida es de 7 días, pero este puede ir desde 1 a 70 días [2].

Las claves de cifrado de llaves (KEKs) se usan para cifrar las TEKs durante el intercambio de estas. Dos KEKs son requeridas para este proceso de cifrado derivándose de las AK. Las KEKs son calculadas en la primera concatenación del valor Hexadecimal 0x53 repitiéndole 64 veces junto con las AK. Luego las funciones hash SHA-1 de estos valores son calculadas con una salida de datos de 160 bits. Finalmente, los primeros 128 bits de esta salida son tomados y divididos en dos TEKs de 64 bits los cuales son incluidos en la SA.

Tabla D.1 Contenidos de Asociaciones de Seguridad de Autorización

Certificado X.509 que identifica la EB
Clave de autorización de 160 bits
Identificador de clave de autorización de 4 bits
Tiempo de vida de la clave de autorización, mínimo de 1 día, máximo 70, 7 días por defecto
Llave de cifrado de claves (KEK) para distribución de TEKs
Clave de código de autenticación de mensaje de función hash de subida (HMAC)
Clave HMAC de bajada
Lista de autorización de SA de datos

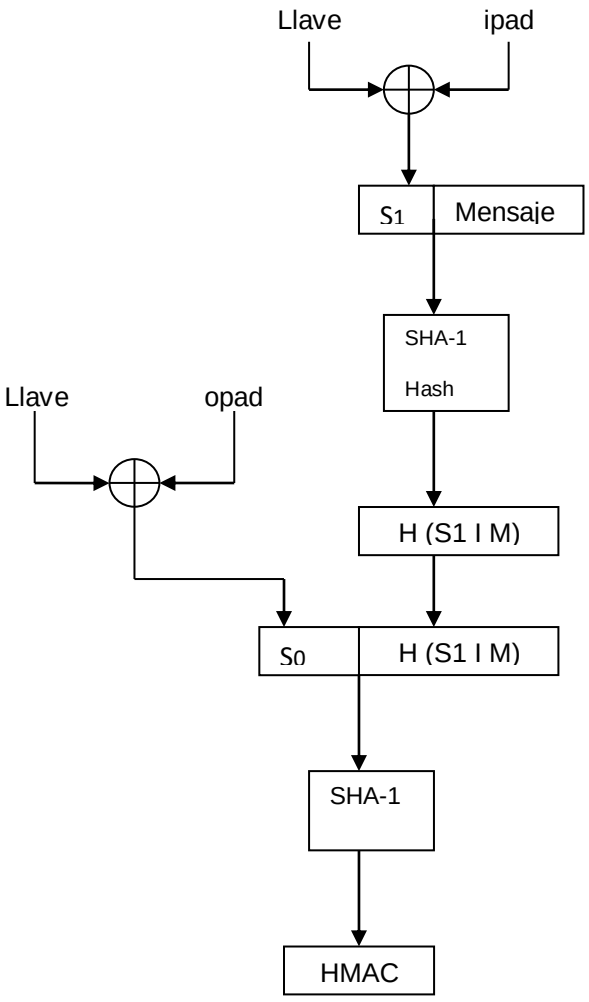
Dos claves de código de mensaje de autenticación hash son utilizadas, una para los enlaces de subida y bajada, las cuales son incluidas para permitir la creación de claves HMAC durante el proceso de intercambio de TEKs. La llave que va de la EB a la ES se utiliza para crear una clave HMAC del mensaje que es enviado, mientras que la llave que va desde la ES a la EB es usada para crear una clave HMAC del mensaje recibido, permitiendo que el mensaje recibido sea autenticado. La llave de subida se obtiene concatenando el valor Hexadecimal 0x3A repetido 64 veces, el AK luego calcula la función hash SHA-1 de este valor creando una clave HMAC de 160 bits. La llave de bajada es calculada de la misma manera, pero el valor Hexadecimal 0x5C es concatenado ahora con la AK [2].

AUTENTICACION

CODIGO DE AUTENTICACION DE MENSAJE HASH. Las claves HMAC son usadas para proveer autenticación en los mensajes. Usando HMAC el receptor puede verificar quien esta enviando el mensaje. Esto es posible porque se crea una clave HMAC del

mensaje que se ha enviado usando una llave conocida solamente por el transmisor y receptor, cuando el receptor obtiene el mensaje, este se calcula con la propia clave HMAC del mensaje usando la misma llave y comparando el que se calculo con el recibido desde el transmisor, si la clave HMAC es igual, entonces, la transmisión es confirmada. HMAC esta creada como una función de la llave y el mensaje. La figura D.2 muestra el proceso de creación de claves HMAC.

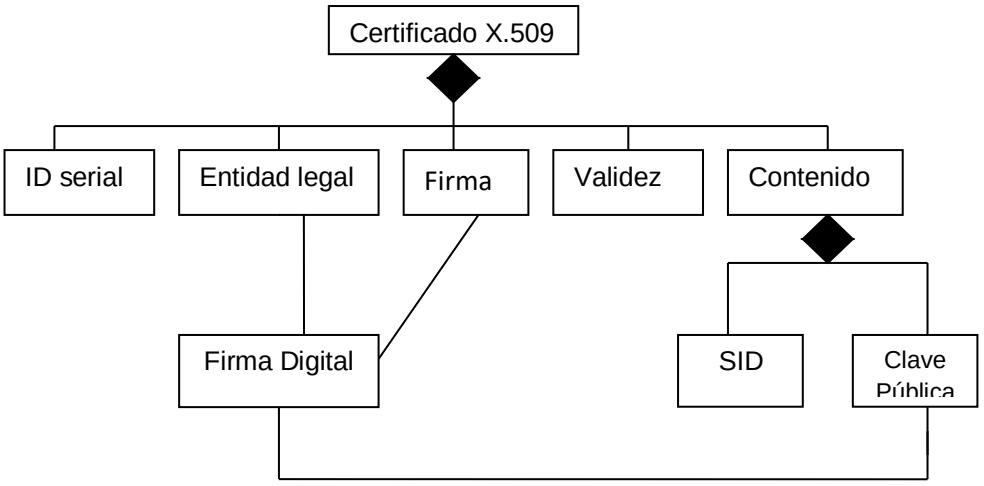
Figura D.2 Creación de claves HMAC



Primero, la llave hash, definida en la SA de autorización, es creada con la función XOR con un ipad, este ipad es el byte 0x36 repetido 20 veces hasta coincidir con el tamaño de la llave hash. El valor de estos 160 bits son añadidos al comienzo del mensaje. Para calcular la función hash el estándar define el uso de la función SHA-1. La clave hash es una función XOR con un opad, este opad es el byte 0x5C repetido 20 veces hasta que es igual en tamaño a la llave hash. El valor de los 160 bits son adicionados al comienzo de la salida anterior a la llave hash. Estos dos valores están en las llaves hash produciendo entonces las claves HMAC.

CERTIFICADOS X.509. Los certificados X.509 son utilizados para permitir a la EB identificar a la ES. Hay dos tipos de certificados: certificados del fabricante y de la ES. Un certificado de fabricante el cual identifica el dispositivo fabricado por este. Una ES puede emitir su propio certificado o lo puede hacer una tercera parte. El certificado de una ES es generalmente creado y firmado por el fabricante de la estación, este es usado para identificar la ES e incluir la dirección MAC de esta en el equipo. La EB puede utilizar este certificado para verificar el certificado de la ES, permitiendo identificar la legitimidad del equipo. Los certificados X.509 en el estándar se muestra en un diagrama de clases (figura D.3) describiendo la estructura de estos.

Figura D.3 Diagrama de clases para el certificado X.509

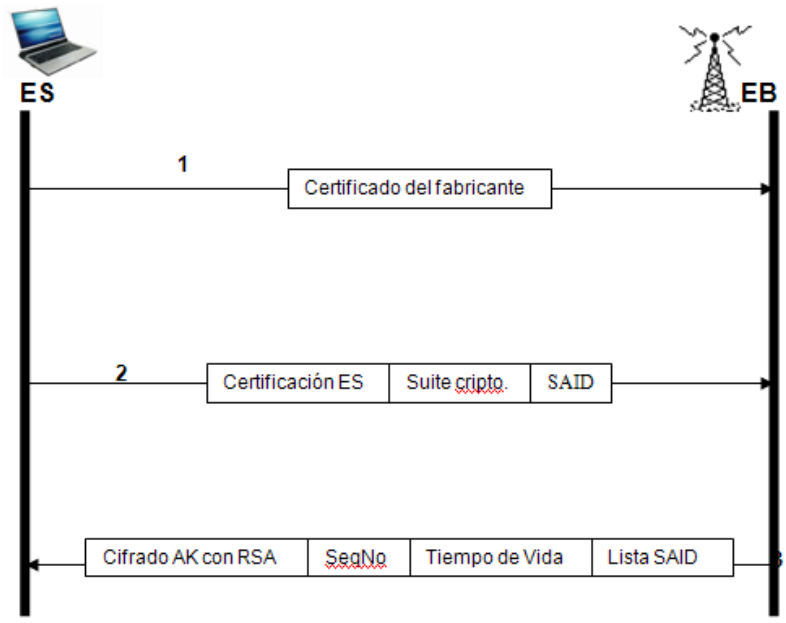


PRIVACIDAD Y GESTION DE CLAVES.

Las Estaciones suscriptoras utilizan el protocolo PKM para obtener la autorización y el material para intercambiar claves desde la Estación Suscriptora. El PKM se puede romper en dos partes, una manipulando la autorización de las Estaciones suscriptoras y el intercambio de AK, otra forma es manipulando el intercambio de TEKs.

AUTORIZACION E INTERCAMBIO DE AK. La autorización del protocolo PKM es usado para intercambiar una AK desde la EB hacia la ES, una vez la ES recibe una autorización inicial, esta acción continua haciéndose periódicamente. El intercambio de AK es llevado a cabo usando tres mensajes, los cuales se muestran en la figura D.4.

Figura D.4 Autorización PKM [2]



La ES inicia el intercambio enviando un mensaje contenido en el certificado X.509 del fabricante de la ES hacia la EB, este mensaje es estrictamente informativo y puede ser ignorado por esta. Sin embargo, la EB puede ser configurada solamente para permitir el acceso a dispositivos de confianza del fabricante.

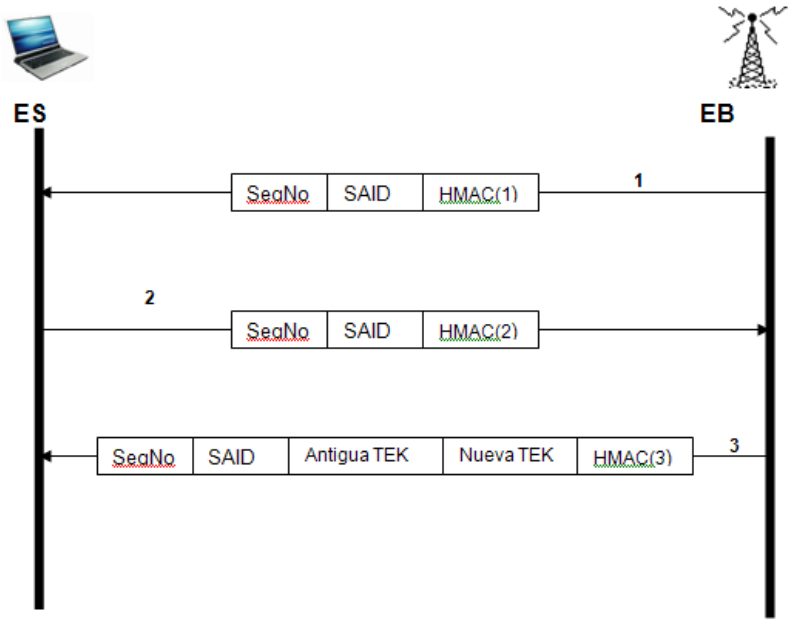
El segundo mensaje es enviado desde la ES a la EB inmediatamente después de que el primer mensaje se envío, este mensaje es solicitado por una AK y una lista de SAIDs que identifican las SA de la ES autorizadas para participar. Hay tres partes en este mensaje: Certificados X.509 que emite el fabricante, algoritmos criptográficos soportados por la ES, y el SAID de la SA primaria.

La EB utiliza el certificado de la ES para determinar si está autorizada, si es así, la EB responderá con el tercer mensaje. La EB usa la calve publica de la ES, la cual se obtiene desde esta certificación para cifrar la AK utilizando el algoritmo RSA. El cifrado AK también está incluido en este mensaje con el SeqNo el cual diferencia sucesivas AK, el tiempo de vida y una lista de SAID de la SAs estáticas que autorizan a la ES a participar en la comunicación con la EB.

INTERCAMBIO DE TEK. Una vez la ES ha sido autorizada, se establece una SA para cada SAID en la lista recibida desde la EB. Esto es llevado a cabo inicialmente en el intercambio de TEKs. Una ves la SA es establecida, la ES periódicamente refrescará el material de las claves. La EB puede también reforzar el intercambio de claves si es necesario, en la figura D.5, se muestra en proceso de intercambio de TEK.

El primer mensaje de un intercambio de TEKs es opcional y permite a la EB forzar el intercambio de claves. Hay tres partes en el mensaje: SeqNo que se refiere al AK utilizado en la creación de HMAC, el SAID se refiere a las SA que se utilizan para el refuerzo de claves, y la HMAC que permite a la ES autenticar mensajes.

Figura D.5 Intercambio de TEK

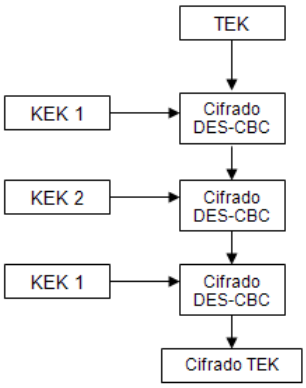


El segundo mensaje es enviado por la ES en respuesta al primer mensaje o si esta solicita el refresco del material de las claves. Hay tres partes en este mensaje: SeqnNo se refiere a la AK usada en la creación de la HMAC, el SAID se refiere a cualquiera de los SAID recibidos en el primer mensaje o una de las SAs desde la lista SAID de la ES autorizada, y la clave HMAC que permite la autenticación del mensaje de la EB.

Si la HMAC en el segundo mensaje es válida, entonces, la EB enviará el tercer mensaje. Como en el primer mensaje, una SeqNo, el SAID, y la HMAC están incluidas, adicionalmente a esto la antigua y nueva TEK son adicionadas. La antigua TEK reitera los parámetros de la SA activa mientras la nueva se usa una vez la activa expira. La EB cifra las dos claves TEK usando el algoritmo DES en modo ECB con el KEK que está incorporado con la SA.

La figura D.6 muestra el proceso de cifrado KEK, en la sección x se describirá como las KEK son creadas.

Figura D.6 Proceso de cifrado TEK [2]



Aquí, KEK 1 y KEK 2 son el grupo de 64 bits calculados para formar el KEK de 128 bits, estas dos claves son usadas en el cifrado con el algoritmo 3 DES en donde el TEK es el primero en ser cifrado usando el KEK 1. La salida se descifra usando el KEK 2 y luego se cifra usando el KEK 1, este proceso es llevado a cabo en la antigua y nueva clave TEK para producir el cifrado de las claves TEKs.