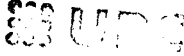




**ESCOLA TÈCNICA SUPERIOR D'ENGINYERIA
DE TELECOMUNICACIÓ DE BARCELONA**

**Seguridad en Redes de Banda Ancha. Contribución al Diseño y
Evaluación de un Sistema de Seguridad para la RDSI-BA**

TESIS DOCTORAL


BIBLIOTECA RECTOR GABRIEL FERRERIE
Campus Nord

Tesis Doctoral presentada en la Universitat
Politécnica de Catalunya para la obtención del
título de Doctor Ingeniero de Telecomunicación

Autor: **Jordi Forné Muñoz**

Director: **Dr. José Luis Melús Moreno**

ÍNDICE

CAPÍTULO 1. Introducción

1.1. Introducción	1-1
1.2. La Red Digital de Servicios Integrados de Banda Ancha (RDSI-BA)	1-2
1.2.1. Servicios	1-4
1.2.2. Modo de Transferencia Asíncrono	1-5
1.2.3. Estructura de la Celda MTA. Concepto de Conexión Virtual	1-5
1.2.4. Control de Congestión y Control de Errores en Redes MTA	1-8
1.3. Seguridad en Redes	1-10
1.3.1. Amenazas, Mecanismos y Servicios de Seguridad	1-11
1.3.1.1. Amenazas	1-11
1.3.1.2. Servicios de Seguridad	1-12
1.3.1.3. Mecanismos de Seguridad	1-14
1.3.2. Sistemas Criptográficos	1-15
1.3.2.1. Criptosistemas Simétricos	1-17
1.3.1.2. Criptosistemas de Clave Pública	1-17
1.3.3. Algoritmos y Aplicaciones Actuales	1-19
1.4. Motivación, Objetivos y Contribuciones de esta Tesis	1-20
1.5. Desarrollo de la Tesis	1-22
1.6. Artículos e Informes Técnicos Publicados	1-23

CAPÍTULO 2. Ubicación de los Servicios de Seguridad dentro del Modelo de Referencia de Protocolos de la RDSI-BA

2.1. Introducción	2-1
2.2. Modelo de Referencia OSI	2-2
2.3. Modelo de Seguridad de 4 Niveles	2-3
2.4. Modelo de Referencia de Protocolos para la RDSI-BA	2-4
2.5. Ubicación de los Servicios de Seguridad	2-7
2.5.1. Cifrado de la Información. Confidencialidad e Integridad	2-10
2.5.1.1. Cifrado por debajo del Nivel de Aplicación	2-12
2.5.1.2. Cifrado por encima del Nivel de Adaptación	2-14
2.5.1.3. Cifrado entre el Nivel de Adaptación y el Nivel MTA	2-15
2.5.1.4. Cifrado a Nivel Físico	2-19
2.5.2. Gestión de Claves	2-21

2.5.3. Autenticación	2-22
2.5.4. Control de Acceso	2-23
2.5.5. No Repudio	2-24
2.5.6. Resumen de las Posibilidades de Ubicación de los Servicios de Seguridad.....	2-24
2.6. Ejemplo: el Proyecto CRIPTO del PlanBA.....	2-25
2.6.1. Proyecto TEMA	2-26
2.6.2. Proyecto CRIPTO	2-28
2.6.2.1. Cifrado de la Información	2-28
2.6.2.2. Autenticación y Control de Acceso.....	2-29
2.6.2.3. Gestión de Claves.....	2-30
2.6.3. Arquitectura del Sistema de Seguridad.....	2-31
2.6.3.1. Ubicación del Cifrado	2-31
2.6.3.2. Arquitectura del Sistema de Seguridad Propuesto en el Proyecto CRIPTO	2-32
2.7. Conclusiones y Aportaciones	2-33

CAPÍTULO 3. Arquitectura del Sistema de Seguridad

3.1. Introducción	3-1
3.2. Escenarios a Proteger	3-2
3.3. Requisitos para el Sistema de Seguridad	3-3
3.4. Ubicación de los Servicios de Seguridad	3-8
3.4.1. Cifrado de la Información. Confidencialidad e Integridad	3-9
3.4.1.1. Cifrado debajo del Nivel de Aplicación	3-9
3.4.1.2. Cifrado entre Niveles MTA y AAL.....	3-10
3.4.1.3. Cifrado por encima de AAL.....	3-11
3.4.1.4. Conclusiones	3-11
3.4.2. Gestión de Claves.....	3-12
3.4.3. Autenticación	3-12
3.4.4. Control de Acceso y no Repudio.....	3-13
3.5. Arquitectura Propuesta	3-13
3.5.1. Ejemplo Simplificado de Operación	3-15
3.5.2. Compatibilidad con Interconexión de Redes.....	3-17
3.6. Negociación de Servicios de Seguridad	3-18
3.6.1. La interfaz de Programación de la Aplicación (API)	3-23
3.6.2. Primitivas de Comunicación entre Niveles SEC-APL.....	3-25
3.6.3. Ejemplo de Operación.....	3-26

3.6.3.1. Establecimiento de la Asociación de Seguridad	3-27
3.6.3.2. Comunicación Segura.....	3-28
3.6.3.3. Liberación de la Asociación de Seguridad	3-28
3.6.3.4. Intentos Frustrados de Establecer Asociación de Seguridad	3-28
3.7. Conclusiones y Aportaciones	3-30

CAPÍTULO 4. Coste de Servicios de Seguridad

4.1. Introducción	4-1
4.2. Coste de la Implantación de Servicios Seguridad.....	4-2
4.3. Coste de la Confidencialidad.....	4-3
4.4. Coste de la Integridad.....	4-8
4.5. Gestión Eficiente de Claves.....	4-9
4.5.1. Estructuras Globales de Certificación	4-10
4.5.2. Modelo Propuesto	4-12
4.5.3. Dimensionado de CA y del Número de Entidades Suscritas	4-14
4.5.4. Capacidad de Cálculo Óptima para CA.....	4-16
4.5.5. Modelo con Colas Finitas.....	4-17
4.6. Conclusiones y Aportaciones	4-18

CAPÍTULO 5. Autenticación y Gestión de Claves

5.1. Introducción	5-1
5.2. Gestión de Claves.....	5-2
5.2.1. Aspectos Generales de la Gestión de Claves.....	5-2
5.2.2. Autenticación	5-5
5.2.3. Aspectos Concretos de Gestión de Claves en la RDSI-BA	5-7
5.3. Protocolo Propuesto para la RDSI-BA.....	5-9
5.3.1. Notación	5-9
5.3.2. Protocolo Propuesto	5-10
5.3.3. Dimensionado de Tabla de Claves Públicas.....	5-13
5.3.4. Desarrollo del Protocolo Propuesto para el Proyecto CRIPTO.....	5-15
5.4. Comparación con otros Protocolos.....	5-16
5.4.1. X.509.....	5-17
5.4.2. Protocolo STS	5-18
5.5. Autenticación de Parámetros de Seguridad Negociados	5-19
5.6. Conclusiones y Aportaciones	5-20

CAPÍTULO 6. Conclusiones

6.1. Conclusiones	6-1
6.2. Líneas Futuras	6-5

ANEXO A. Especificación de Primitivas de Seguridad

Especificación de Primitivas de Seguridad.....	A-1
--	-----

ANEXO B. Coste Detallado de los Servicios de Seguridad

Coste Detallado de los Servicios de Seguridad	B-1
---	-----

REFERENCIAS BIBLIOGRÁFICAS

Referencias Bibliográficas.....	RB-1
---------------------------------	------

CAPÍTULO 1

Introducción

1.1 Introducción

La transferencia de datos mediante redes de comunicación es una práctica muy extendida en todos los ámbitos. El volumen de información que circula por las redes telemáticas actuales, así como el advenimiento de nuevas aplicaciones que requieren un gran ancho de banda, plantea la necesidad de redes de área extendida de banda ancha que ofrezcan alta velocidad de transmisión e integración de servicios.

Afortunadamente, los últimos avances tecnológicos en áreas como la microelectrónica, la tecnología de conmutación de paquetes y las comunicaciones por fibra óptica hacen posible el desarrollo de una red de servicios integrados de alta velocidad capaz de soportar de manera unificada servicios de voz, vídeo y datos.

Esta red recibe el nombre de Red Digital de Servicios Integrados de Banda Ancha (RDSI-BA), y el modo de transferencia asíncrono (MTA) ha sido adoptado por el Comité Consultivo Internacional de Telegrafía y Telefonía (CCITT) como el modo de transferencia universal para la RDSI-BA [CCI92a]. Este modo de transferencia está basado en la segmentación del flujo de la información en paquetes de longitud fija (denominados celdas), que son transmitidos en función de la demanda de la fuente, optimizándose así el ancho de banda utilizado.

MTA es esencialmente una técnica orientada a conexión. Ello significa que todas las características del servicio se negocian entre el usuario y la red durante el periodo de

establecimiento de conexión, y toda la información se encamina usando un circuito virtual asignado durante la duración total de la conexión. La información necesaria para el enrutamiento está ubicada en la cabecera de la celda, y ofrece una velocidad de transmisión mucho mayor que la proporcionada por las redes actualmente en funcionamiento. Baste señalar que se han especificado como velocidades de línea (para el interfaz usuario-red) tasas nominales de 155,52 y 622,080 Mbps.

La seguridad de la información es uno de los problemas importantes que se plantean en una red de tales dimensiones, en la que gran cantidad de usuarios acceden a multitud de recursos. Conviene destacar que esta preocupación es general en todas las redes existentes y que, pese a que las redes de datos en funcionamiento son en la mayoría de los casos inseguras, se está realizando a nivel mundial un gran esfuerzo para incorporar en ellas mecanismos de seguridad que controlen el acceso a recursos, garanticen integridad y confidencialidad de las comunicaciones, etc.

Este capítulo se dedica a dar una visión general sobre la RDSI-BA y sobre la seguridad en redes de comunicaciones. Ello proporcionará los antecedentes para el tema sobre el que versa este trabajo de Tesis, es decir, la seguridad en redes de banda ancha. Debe señalarse que el apartado 3 de este capítulo (Seguridad en Redes de Comunicaciones) fue parcialmente adelantado en [FOR95c]. Los dos últimos apartados exponen la motivación, objetivos y contribuciones de este trabajo de Tesis, y describen el desarrollo de este documento, es decir, hacen referencia a los capítulos restantes.

1.2 La Red Digital de Servicios Integrados de Banda Ancha (RDSI-BA)

El tipo de tráfico a soportar y la tecnología disponible en cada momento definen los requisitos para el diseño de una red de telecomunicación. En general, se deben soportar tres tipos de tráfico: voz, vídeo y ficheros de datos. Las redes de telecomunicación actuales están extremadamente especializadas para dar servicio con propiedad a un sólo tipo de tráfico. Debido a la naturaleza tan específica de dichas redes, éstas sufren un gran número de desventajas, siendo las más importantes [DEP93]:

- Dependencia del servicio: cada red es sólo capaz de transportar el servicio específico para el que fue diseñada. Sólo se pueden adaptar otros servicios, aunque de forma ineficiente, en un número muy limitado de casos y usando equipos adicionales

- **Inflexibilidad:** una red especializada presenta grandes dificultades para adaptarse a los cambios tecnológicos y a los requisitos que imponen los nuevos servicios
- **Ineficiencia:** los recursos propios de una red no pueden hacerse disponibles a otras redes

Además, esta situación conlleva un mayor coste económico ya que, por ejemplo, debe realizarse el mantenimiento de varias redes separadas en lugar de una única red.

Todos estos problemas ponen de relieve la necesidad de disponer de una red única capaz de transportar todos los servicios de forma integrada compartiendo eficientemente sus recursos entre los mismos.

El progreso tecnológico en campos tan diversos como sistemas de transmisión por fibra óptica, microelectrónica (VLSI) y tecnologías de conmutación, comunicación digital y procesado de la señal, ingeniería del *software* y aplicaciones, etc., junto con la creciente demanda de servicios y nuevas aplicaciones que requieren gran ancho de banda (supercomputación, teleradiología, visualización de la información, aplicaciones CAD, multimedia, interconexión de redes locales, ...) están proporcionando el impulso suficiente para la definición de una Red Digital de Servicios Integrados de Banda Ancha (RDSI-BA) [DEP93, LEE93].

La RDSI-BA se concibe como una red digital multipropósito, independiente de toda aplicación, basada en estándares internacionales y prevista como la base para conseguir una intercomunicación universal.

La recomendación I.113 del CCITT [CCI92b] define "banda ancha" como "un servicio o sistema que requiere canales de transmisión capaces de soportar tasas binarias superiores a la tasa primaria (1,5 Mbps, 2 Mbps)". En la actualidad las interfases RDSI-BA soportan hasta 622 Mbps con la posibilidad de definir velocidades superiores en un futuro próximo.

En [CCI92a] la UIT resume el concepto de RDSI-BA:

"La RDSI-BA soporta conexiones conmutadas, semipermanentes, permanentes, punto a punto y punto a multipunto y proporciona servicios según demanda, por reserva y permanentes. Las conexiones en RDSI-BA soportan servicios en modo circuito y en modo paquete de tipo mono y multimedia y de naturaleza no orientada a conexión en configuraciones bidireccionales y unidireccionales".

1.2.1 Servicios

En [CCI92c] se muestra una lista detallada de los servicios proporcionados por la RDSI-BA. Éstos se dividen en dos categorías:

- Servicios interactivos
 - Conversacionales (p.e., telefonía, videoconferencia, ...)
 - De mensajería (correo electrónico, correo electrónico multimedia, ...)
 - De consulta (bases de datos de imágenes médicas, ...)
- Servicios de distribución con o sin control de presentación por parte del usuario (entretenimiento, edición, ...)

Los servicios interactivos permiten comunicaciones entre usuario y usuario y entre usuario y servidor. Las comunicaciones se pueden dar en tiempo real o vía almacenamiento y retransmisión. En los servicios de distribución la información se distribuye desde una fuente central a un número ilimitado de usuarios autorizados. Algunos servicios de distribución proporcionan la información según una secuencia de entidades repetida cíclicamente permitiendo el control de los usuarios sobre el tiempo y el orden de la información presentada. Otros envían la información como un flujo continuo y no permiten el control por parte del usuario. La información presentada al usuario está sujeta al momento de conexión con el servicio.

La variedad de posibles servicios y aplicaciones en la RDSI-BA requiere una red con capacidad de transferencia universal para [HÄN91]:

- Proveer servicios que pueden emplear tasas binarias muy diferentes
- Soportar tráfico a ráfagas y de velocidad binaria variable
- Tener en cuenta tanto aplicaciones sensibles a retardo como a pérdida de información

Para cumplir los distintos requisitos impuestos a la RDSI-BA (gran variedad de tráfico, diversidad de servicios y requisitos de prestaciones, expansión futura, ...) se han propuesto varias técnicas como posibles esquemas de multiplexación y conmutación. Ello recibe el nombre de modo de transferencia y destacan los siguientes:

- El modo de transferencia síncrono (MTS) basado en técnicas de conmutación de circuitos
- El modo de transferencia asíncrono (MTA) basado en técnicas de conmutación de paquetes

1.2.2 Modo de Transferencia Asíncrono

MTA ha sido normalizado por la UIT-T como el modo de transferencia para la RDSI-BA.

MTA está basado en técnicas de multiplexación estadística por división en el tiempo y conmutación rápida de paquetes que transmite y encamina el tráfico mediante una dirección contenida en lo que se denomina un paquete de información. MTA utiliza pequeños paquetes de longitud fija, denominados celdas o células. Una celda MTA consta de 53 octetos, 5 de los cuales forman la cabecera del paquete (y contienen básicamente una dirección) y los 48 octetos restantes forman el campo de información.

El tiempo de transmisión de una celda se considera como la longitud de la ranura temporal en el múltiplex. El término multiplexación estadística se refiere al hecho de que varias conexiones pueden compartir un enlace de capacidad menor que la suma de sus requisitos de ancho de banda de pico. El término asíncrono se usa para reflejar que las celdas de una misma comunicación pueden aparecer a intervalos irregulares sobre los enlaces de la red [ONV94].

Al igual que en el resto de tecnologías de conmutación de paquetes se consigue mayor eficiencia en la utilización de los recursos que en el caso de conmutación de circuitos, ya que los usuarios acceden al canal de información cuando lo necesitan (bajo demanda = asincrónamente) y durante el tiempo en que lo necesitan (por supuesto si el canal ya está en uso, un nuevo usuario debe esperar hasta que consiga acceder). En cambio en el modo de transferencia síncrono (MTS) se identifican los datos de una determinada comunicación en base a una ranura temporal particular (se usa multiplexación por división en el tiempo) dentro de una trama, de ahí que no sea necesaria una cabecera que contenga la dirección de destino del mensaje. Además, las ranuras temporales en una trama MTS no se comparten entre llamadas. Por tanto, incluso cuando la fuente de tráfico está inactiva la ranura temporal correspondiente no puede ser utilizada por otro usuario.

1.2.3 Estructura de la Celda MTA. Concepto de Conexión Virtual

Como ya se enunció anteriormente, la celda MTA tiene 53 octetos de longitud, 5 de los cuales constituyen la cabecera de la celda que consta de varios campos de información tal como se aprecia en la Figura 1.1. Ello es así para el interfaz usuario-red [ATM93], en el caso de la interfaz red-red o nodo-nodo, el campo GFC se dedica también a VPI.

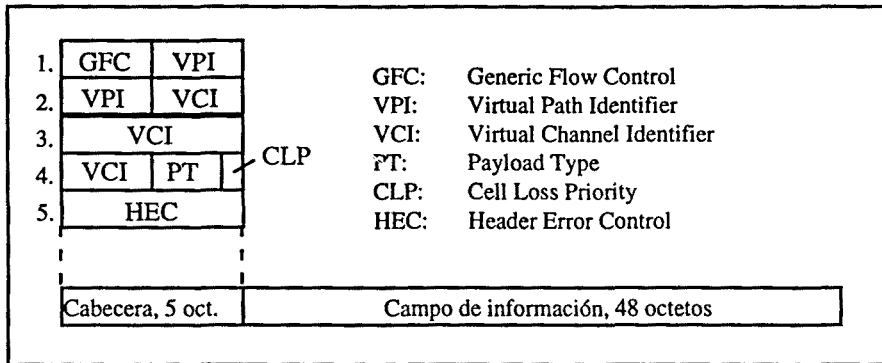


Figura 1.1. Estructura de la celda MTA.

La funcionalidad asociada a los distintos campos de la cabecera está reducida al máximo (básicamente encaminamiento) para garantizar un proceso rápido en los nodos de la red. De los cinco octetos que forman la cabecera, tres contienen información de encaminamiento, dos para lo que se denomina identificador de canal virtual (VCI, *Virtual Channel Identifier*) y un octeto para el identificador de camino virtual (VPI, *Virtual Path Identifier*). El resto de la cabecera consiste en un campo de control de flujo genérico (GFC, *Generic Flow Control*), tres *bits* para un identificador del tipo de información útil que transporta la celda (PTI, *Payload Type Identifier*), un *bit* de prioridad frente a pérdida de celdas (CLP, *Cell Loss Priority*) y ocho *bits* para un campo de control de errores en la cabecera (HEC, *Header Error Control*).

Tal y como corresponde a una tecnología de conmutación de paquetes, la cabecera contiene principalmente información para transportar las celdas MTA de un nodo al siguiente. Sin embargo, en lugar de especificarse explícitamente las direcciones de fuente/destino, las celdas MTA se etiquetan mediante números identificadores de conexión virtual (VCI/VPI), ello permite identificar las conexiones mediante un número menor de *bits* y conseguir un encaminamiento universal. El nodo destino se especifica mediante una secuencia de pasos en el proceso de encaminamiento que se determina en el momento de establecer la conexión correspondiente.

MTA es, por tanto, un modo orientado a conexión. La comunicación se divide en tres fases: la fase de establecimiento donde se reservan los recursos necesarios (en el caso en que éstos estén disponibles, en caso contrario la conexión simplemente se rechaza), la fase de transferencia de la información y la fase de liberación de recursos y de la conexión. Las celdas MTA de una misma comunicación viajan por la misma ruta durante toda la duración de la transmisión (ello resulta favorable frente a un modo no orientado a conexión, para evitar el resecuenciamiento de paquetes en servicios de tiempo real). Dicha ruta se especifica en la fase de establecimiento de la llamada. La cabecera de la celda MTA contiene en cada momento la información que la red necesita para encaminar la celda sobre la ruta preestablecida.

Un camino virtual consta de varios canales virtuales (ver Figura 1.2).

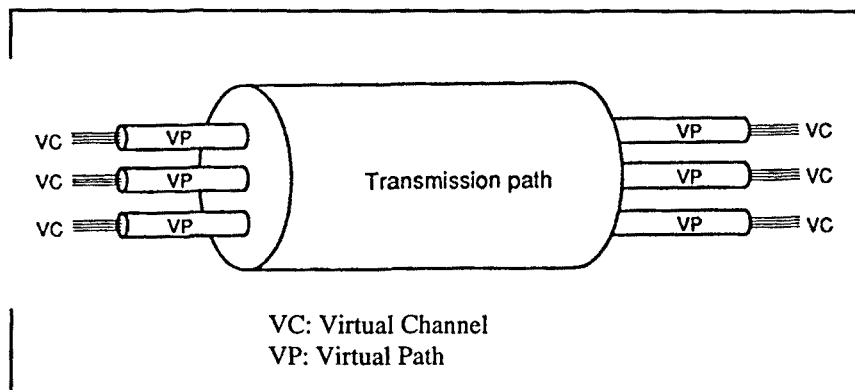


Figura 1.2. Relación entre camino virtual y canal virtual.

La distinción en la etiqueta de direccionamiento entre VCI y VPI permite a la red usar una notación más corta y compacta para las rutas con más tráfico (p.e., enlaces entre grandes ciudades) gracias al identificador VPI, a la vez que con el identificador VCI se preserva la identidad de cada canal individual dentro del camino de comunicación. Ello permite que los equipos utilizados en la transmisión traten las llamadas sólo en base al campo VPI, sin la necesidad de operar con el resto del campo de direccionamiento (VCI) hasta que el enlace general llega a su destino final, donde el tráfico correspondiente a cada canal se distribuye de acuerdo a su VCI.

El resto de campos en la cabecera se usa para controlar el flujo del tráfico generado en la parte de red de usuario (sólo en el interfaz usuario-red), para discernir el tipo de información que transportan las celdas (celdas de usuario o celdas propias de la red), y para marcar cuál es la prioridad de las celdas frente a pérdidas y poder, así, ejercer alguna acción sobre las mismas en caso de congestión. Finalmente, se utiliza un octeto para detectar errores en la cabecera (básicamente de la dirección) a través de la red.

MTA usa el concepto de conexión virtual [LAN94], estableciendo conexiones virtuales entre cada par de nodos de conmutación intermedios en la transmisión desde un extremo fuente a un extremo destino. Estas conexiones se denominan virtuales para distinguirlas de los circuitos o canales dedicados como en el caso del Modo de Transferencia Síncrono (MTS). En MTA el enlace no se reserva únicamente a un usuario de modo que cada vez que un usuario no está ocupando el enlace otro usuario activo puede acceder a él y utilizarlo.

Las conexiones MTA sólo existen como conjuntos de tablas de encaminamiento que se mantienen en cada conmutador y que están indexadas en función de la etiqueta de direccionamiento (VCI/VPI) de la cabecera de las celdas. Las etiquetas de direccionamiento en MTA tienen sólo un significado local, en cuanto que sólo son relevantes entre dos equipos de conmutación MTA adyacentes. Cuando se establece un camino virtual, a cada conmutador se le proporciona un conjunto de tablas de búsqueda (indexadas por los identificadores de camino/canal virtual) para identificar una celda de entrada por su etiqueta de direccionamiento presente en la cabecera, encaminarla a través de la red de conmutación hasta su puerto de salida destino, reescribiendo la dirección de entrada por una nueva etiqueta que será usada por el siguiente conmutador en la ruta de transmisión y que de nuevo la reconocerá como un índice de su propia tabla (Fig. 3).

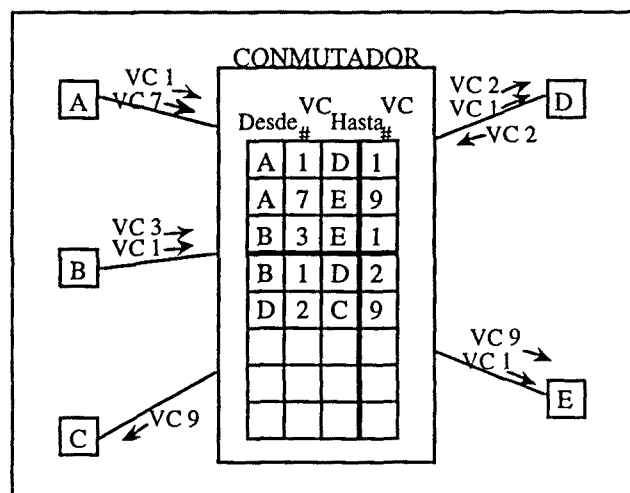


Figura 1.3. Tablas de búsqueda en el conmutador.

La celda pasará de conmutador a conmutador por la ruta preestablecida en la fase de establecimiento de la conexión, pero dicha ruta es virtual en cuanto a que las facilidades de transporte sólo se le dedican mientras la celda las atraviese.

El Modo de Transferencia Asíncrono puede aumentar la eficiencia permitiendo que varias conexiones virtuales compartan los mismos recursos físicos.

1.2.4 Control de Congestión y Control de Errores en Redes MTA

Las fuentes de tráfico a ráfagas generan celdas a prácticamente su velocidad de pico durante intervalos de tiempo cortos e inmediatamente después permanecen

inactivas sin generar paquetes. En una red donde se accede bajo demanda y se usa multiplexación estadística pueden alcanzarse condiciones de congestión muy severas si un número elevado de fuentes de tráfico se activan simultáneamente [BAE91].

Por otra parte, y debido a los enlaces de alta velocidad, el retardo de propagación se hace significativo respecto al tiempo de transmisión y al tiempo de proceso que conlleva la ejecución de los protocolos de comunicación. Por tanto, las redes MTA utilizan protocolos simplificados e intentan desplazar el peso de los protocolos que actualmente se ejecutan de enlace a enlace hacia capas superiores del modelo de referencia de protocolos OSI [TAN89] para que el proceso se lleve a término de extremo a extremo.

En general, los esquemas de control de congestión pueden clasificarse en esquemas de control reactivo y esquemas de control preventivo. El control reactivo reacciona a la condición de congestión después de que ésta ocurra e intenta devolver la red a un nivel de utilización aceptable. Usualmente, ello se consigue indicando a las fuentes que disminuyan su carga de tráfico mediante señales de control (*feedback*).

Los esquemas de control preventivo intentan prevenir la congestión antes de que ésta ocurra controlando el flujo de tráfico en los puntos de acceso a la red. Ello se realiza de dos formas (o combinando ambas), mediante control de admisión y cumplimiento del ancho de banda.

El control de admisión se encarga de determinar, en el momento de establecer la llamada, cuándo debe aceptarse o rechazarse una nueva conexión (se basa en las características del tráfico de la nueva conexión y de la carga de la red en ese momento).

El cumplimiento del ancho de banda se refiere a monitorizar las conexiones individuales para asegurarse de que el flujo de tráfico está de acuerdo con lo que se declaró en el establecimiento de la llamada.

Debido a los efectos de los canales de alta velocidad, puede resolverse que el control preventivo es más efectivo que el control reactivo en las redes MTA. Asimismo, ello conduce a que las redes MTA sean redes que operan en modo orientado a conexión.

Aunque, en principio, MTA puede utilizarse sobre cualquier medio físico, fue desarrollado pensando en redes basadas en tecnología óptica, como por ejemplo, la jerarquía digital síncrona JDS [LEE93, SDH93].

El uso de fibra óptica como medio de transmisión, a parte de proporcionar anchos de banda elevados (tasas binarias altas) y mejores relaciones de atenuación (mayor distancia entre repetidores) también se caracteriza por ser un medio de bajo

ruido. Ello implica que la tasa de errores en el canal sea a su vez baja y, por tanto, que los esquemas de control de errores usados en la actualidad sean reexaminados.

Los esquemas de control de errores pueden llevarse a la práctica entre nodos intermedios o entre extremos de la comunicación. Si el control de errores se realiza entre nodos la retransmisión de celdas erróneas o perdidas sólo tiene lugar entre nodos de conmutación adyacentes. Ello involucra un tiempo de proceso en la ejecución de los protocolos correspondientes.

Nótese que si el medio es ruidoso y el control de errores no se realizase en cada nodo, podría darse el caso de que ningún paquete llegase a su destino y el caudal se reduciría al mínimo ya que el sistema no haría más que retransmitir paquetes erróneos. Por tanto, cuando el medio es ruidoso el controlar los errores en cada nodo resulta lo más acertado.

Si el control de errores tiene lugar sólo entre los nodos fuente y destino un paquete erróneo es enviado durante todo el recorrido de la comunicación malgastando recursos, sin embargo, si el medio presenta bajo ruido esta situación no ocurre con frecuencia y se tienen efectos positivos como es el aligerar el tiempo de proceso en los nodos ya que no es necesario verificar en cada nodo la existencia o no de errores y desencadenar las operaciones necesarias para tal menester. Por otra parte, también disminuyen los requisitos de almacenamiento y retardo en los nodos intermedios.

MTA sigue esta última opción y sólo incorpora control de errores nodo a nodo para la cabecera de las celdas, pero no sobre el campo de información haciendo, por tanto, uso de la mejor tasa de errores que proporcionan los medios de transmisión óptica.

1.3 Seguridad en Redes de Comunicaciones

Las redes de comunicaciones actuales permiten la conectividad de un gran número de usuarios que pueden estar situados en cualquier parte del mundo, tanto para transmisión de voz (red telefónica), imágenes (redes de distribución de televisión, TV vía satélite) como para la transmisión de datos entre ordenadores (redes locales, metropolitanas, así como redes a nivel mundial, como por ejemplo Internet). La explosión de servicios ofrecidos por estas redes, especialmente las de datos, ha incrementado la dependencia de individuos y organizaciones de la transmisión de datos por estas redes. Esta dependencia ha despertado la conciencia de la necesidad de protección de la información y de garantizar la autenticidad de datos y mensajes.

En este apartado se presentan las amenazas a la seguridad en redes de comunicaciones, así como los servicios de seguridad requeridos y los mecanismos necesarios para proveer estos servicios. Entre estos mecanismos destacan los criptográficos, tanto los sistemas convencionales (simétricos) como los de clave pública (asimétricos). Por último se introducen algunos de los algoritmos y aplicaciones criptográficas más extendidos en la actualidad o de los que se prevé una mayor utilización en los próximos años.

1.3.1 Amenazas, Mecanismos y Servicios de Seguridad

1.3.1.1 Amenazas

Las amenazas a la seguridad en una red de comunicaciones pueden caracterizarse modelando el sistema como un flujo de información desde una fuente, como pueda ser un fichero o usuario, a un destino, que pudiera ser otro fichero o usuario, tal como se muestra en la Figura 1.4. Los cuatro tipos genéricos de ataques a la seguridad son los siguientes:

- *Interrupción:* Una parte del sistema resulta destruida o no disponible en un momento dado. Ejemplos de este tipo de ataque pueden ser la destrucción de una parte del hardware o el corte de una línea de comunicación.
- *Intercepción:* Una entidad no autorizada accede a una parte de la información. La parte no autorizada puede ser una persona, una máquina o un programa. Ejemplos de este tipo de ataques son la escucha del canal, ya sea el típico "pinchazo" de la línea telefónica, la intercepción vía radio de comunicaciones móviles o la copia ilícita de ficheros o programas transmitidos a través de redes de datos utilizando analizadores de redes.
- *Modificación:* Una entidad no autorizada no sólo accede a una parte de la información, sino que además es capaz de modificar su contenido. Ejemplos de estas modificaciones son la alteración de ficheros de datos, alteración de programas y modificación de mensajes mientras son transmitidos por la red.
- *Fabricación:* Una entidad no autorizada envía mensajes haciéndose pasar por un usuario legítimo.

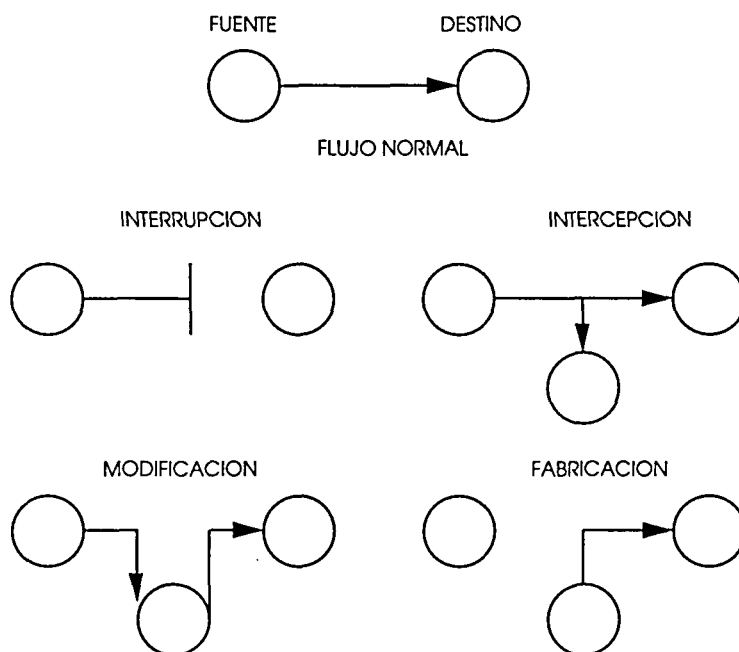


Figura 1.4. Amenazas a la seguridad

Otra clasificación útil es dividir los ataques en términos de pasivos y activos. En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación. Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos que se verán más adelante.

En los ataques activos el atacante altera las comunicaciones. Pueden subdividirse en cuatro categorías: suplantación de identidad, donde el intruso se hace pasar por una entidad diferente; reactuación, donde uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no autorizado; modificación de mensajes, donde el intruso varía los datos transmitidos y degradación fraudulenta del servicio, donde el intruso intenta impedir que los entes dialogantes puedan realizar correctamente su función, mediante destrucción o retardo de mensajes o la introducción de mensajes espúreos con el fin de congestionar la red.

1.3.1.2 Servicios de seguridad

Para hacer frente a las amenazas a la seguridad del sistema, se definen una serie de servicios que realzan la seguridad de los sistemas de proceso de datos y de transferencia de información de una organización. Estos servicios hacen uso de uno o

varios mecanismos de seguridad. Una clasificación útil de los servicios de seguridad, definida por ISO/IEC 7498-2 [ISO88], es la siguiente:

- *Confidencialidad*: Requiere que la información sea accesible únicamente por las entidades autorizadas
- *Autenticación*: Requiere una identificación correcta del origen del mensaje, asegurando que la entidad no es falsa
- *Integridad*: Requiere que la información sólo pueda ser modificada por las entidades autorizadas. La modificación incluye escritura, cambio, borrado, creación y reactuación de los mensajes transmitidos
- *No repudio*: Requiere que ni el emisor ni el receptor del mensaje puedan negar la transmisión
- *Control de acceso*: Requiere que el acceso a la información sea controlado por el sistema destino

Ninguno de estos servicios anteriores fue concebido específicamente para entornos de comunicación de datos. Todos ellos tienen analogías no electrónicas, que emplean mecanismos familiares a cualquier persona, como se muestra en la Tabla 1.1.

Servicio de seguridad	Ejemplo mecanismo no electrónico
Autenticación	Carné con identificación fotográfica Huellas dactilares
Control de acceso	Llaves y cerrojos
Confidencialidad	Tinta invisible Carta lacrada
Integridad	Tinta indeleble.
No repudio	Firma notariada Correo certificado

Tabla 1.1. Analogías no electrónicas de servicios de seguridad.

1.3.1.3 Mecanismos de seguridad

No existe un único mecanismo capaz de proveer todos los servicios anteriormente citados, pero la mayoría de ellos hacen uso de técnicas criptográficas basadas en el cifrado de la información. Los más importantes son los siguientes:

- *Intercambio de autenticación.* Corroborar que una entidad, ya sea origen o destino de la información, es la deseada
- *Cifrado.* Garantiza que la información no es inteligible para individuos, entidades o procesos no autorizados
- *Integridad de datos.* Este mecanismo implica el cifrado de una cadena comprimida de datos a transmitir. Este mensaje se envía al receptor junto con los datos ordinarios. El receptor repite la compresión y el cifrado posterior de los datos y compara el resultado obtenido con el que le llega, para verificar que los datos no han sido modificados
- *Firma digital.* Este mecanismo implica el cifrado, por medio de la clave secreta del emisor, de una cadena comprimida de datos que se va a transferir. La firma digital se envía al receptor junto con los datos ordinarios. Este mensaje se procesa en el receptor, para verificar su integridad
- *Control de acceso.* Esfuerzo para que sólo aquellos usuarios autorizados accedan a los recursos del sistema o a la red
- *Tráfico de relleno.* Consiste en enviar tráfico espúreo junto con los datos válidos para que el enemigo no sepa si se está enviando información, ni qué cantidad de datos útiles se está transfiriendo
- *Control de encaminamiento.* Permite enviar determinada información por determinadas zonas consideradas clasificadas. Asimismo posibilita solicitar otras rutas, en caso que se detecten persistentes violaciones de integridad en una ruta determinada

En la Tabla 1.2 se muestra una relación de los mecanismos de seguridad y los servicios de seguridad que hacen uso de ellos.

	Autenticación	Control de acceso	Confidencialidad	Integridad	No repudio
Intercambio de autenticación	S	N	N	N	N
Cifrado	S	N	S	S	N
Firma digital	S	N	N	S	S
Integridad de datos	N	N	N	S	S
Control de acceso	N	S	N	N	N
Tráfico de relleno	N	N	S	N	N
Control de encaminamiento	N	N	S	N	N

Tabla 1.2. Relación entre servicios de seguridad y mecanismos relacionados.

1.3.2 Sistemas Criptográficos

Los sistemas de protección física son un mecanismo práctico para salvaguardar los equipos terminales de posibles ataques. Sin embargo, dada la dispersión geográfica de los sistemas de transmisión en redes, una protección de este tipo conllevaría un alto coste económico, haciéndolos totalmente desaconsejables en estos casos. Los sistemas criptográficos, por otra parte, son muy útiles para la seguridad en redes de datos, ya que permiten paliar muchas de las posibles vulnerabilidades que éstas presentan.

En la Figura 1.5 se presenta un esquema de la transmisión segura de un mensaje M entre dos entidades, a través de un canal inseguro.

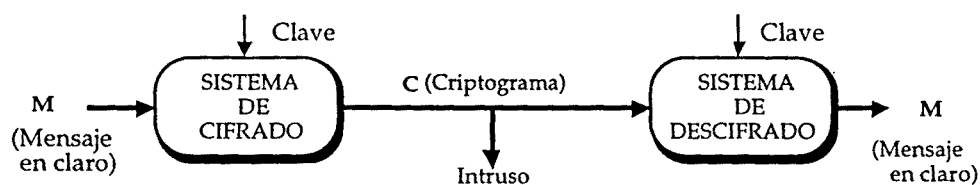


Figura 1.5. Esquema de transmisión segura de un mensaje.

Los sistemas criptográficos de este esquema son los encargados de calcular el mensaje cifrado C, a partir del mensaje en claro M y de la "clave de cifrado"; y de

realizar el proceso inverso, el descifrado, y así determinar M a partir del mensaje cifrado y la "clave de descifrado". Estas dos claves, como ya veremos más adelante, no tienen que ser necesariamente iguales.

Cuando un sistema criptográfico utiliza en el descifrado la misma clave que en el cifrado, se dice que utiliza un "cifrado simétrico"¹. Por el contrario, si la clave de descifrado es distinta a la clave de cifrado el sistema estará empleando un "cifrado asimétrico".

Un sistema de criptografía simétrico es una familia de transformaciones inversibles (E_k), donde emisor y receptor usan la misma clave k . La clave k ha tenido que ser puesta previamente en conocimiento de las dos partes mediante el uso de un canal secreto. Esta clave necesita, pues, ser distribuida con antelación a la comunicación. El coste y el retardo, impuestos por esta necesidad, son los principales obstáculos para la utilización de la criptografía de clave secreta en grandes redes.

Entre los algoritmos simétricos podemos destacar los de cifrado en bloque y los de cifrado de flujo. Estos últimos son los más indicados para entornos de alta velocidad de transmisión. Los algoritmos simétricos de cifrado en bloque son los más usados en redes de datos, y se pueden clasificar entre públicos y privados. El algoritmo simétrico público más utilizado en la práctica es el DES (*Data Encryption Standard*) [NBS77], aunque existen otros algoritmos secretos estandarizados por organismos americanos, europeos, etc.

En un sistema de clave pública, el cifrador utiliza una clave P , mientras que el descifrador utiliza una clave distinta S . La clave P es pública, y la clave S es privada e incalculable a partir de P en un tiempo prudente. El sistema asimétrico posibilita la comunicación en un sentido; para realizar la comunicación en sentido contrario se necesita otro par de claves secreta-pública. La principal característica que hace interesantes a estos métodos frente a los sistemas criptográficos simétricos, es que no se precisa el intercambio de secretos entre los dos comunicantes. Los algoritmos de clave pública se basan en la teoría de números y de cuerpos finitos. Gracias a este fundamento matemático es posible demostrar la seguridad computacional de estos métodos.

Los algoritmos de clave pública sólo se utilizan para cifrar comunicaciones en los que la velocidad no sea un requisito crítico. Esto se debe a la baja velocidad de cifrado que presentan las realizaciones de estos algoritmos. Sin embargo estos algoritmos son útiles para la transmisión de claves por medios inseguros entre sistemas que utilicen algoritmos simétricos, ya que en la distribución de claves la velocidad no es

¹ En realidad también se habla de "cifrado simétrico" cuando las claves de cifrado y descifrado son diferentes, pero el conocimiento de una de ellas permite fácilmente reconstruir la otra.

crítica. Uno de los algoritmos asimétricos más utilizados es el *RSA (Rivest-Shamir-Adleman)* [RIV77].

1.3.2.1 Criptosistemas simétricos

Los criptosistemas simétricos se caracterizan por el hecho que se emplea la misma clave en las transformaciones de cifrado y descifrado. Para proporcionar confidencialidad, un criptosistema simétrico actúa de la siguiente forma. Dos sistemas A y B desean comunicarse de forma segura, y mediante un proceso de distribución de claves, ambos comparten un conjunto de bits que será usado como clave. Esta clave será secreta para cualquier otro individuo, entidad,... distinto de A y de B. Así pues, cualquier mensaje intercambiado entre A y B irá cifrado usando dicha clave.

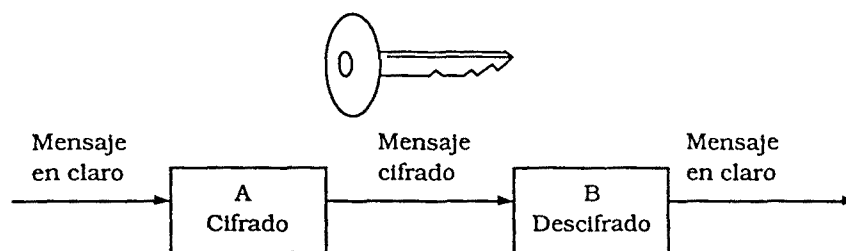


Figura 1.6. Criptosistema simétrico.

Los criptosistemas simétricos han sido utilizados en redes comerciales desde el principio de los 70. El estándar americano DES (*Data Encryption Standard*) es el criptosistema de este tipo que mayor popularidad ha alcanzado.

1.3.2.2 Criptosistemas de clave pública

El concepto de criptografía de clave pública fue introducido por Whitfield Diffie y Martin Hellman en 1976 [DIF76]. A diferencia de los criptosistemas simétricos, los algoritmos de clave pública utilizan pares de claves complementarias para separar los procesos de cifrado y descifrado. Una clave, la privada, se mantiene secreta, mientras que la clave pública puede ser conocida. El sistema tiene la propiedad que a partir del conocimiento de la clave pública no es posible determinar la clave privada. Este enfoque con dos claves permite simplificar la gestión de claves, minimizando el número de claves que deben ser gestionadas y permitiendo su distribución a través de sistemas no protegidos. En una red con n usuarios, si se usa cifrado de clave simétrica se precisan $n(n-1)/2$ claves, mientras que si se emplea cifrado de clave pública bastan $2n$ claves.

Potencialmente hay dos modos de uso de los criptosistemas de clave pública, dependiendo del uso que se haga de la clave privada (cifrado o descifrado). Por una

parte cualquier usuario puede enviar un mensaje de forma confidencial a un receptor (p.e. B) cifrando su contenido con la clave pública del receptor, que será el único capaz de descifrarlo por ser el único conocedor de la clave privada (en caso contrario la gestión de claves estaría mal hecha. Por otro lado cualquier usuario (p.e. A) puede autenticar el origen y contenido de un mensaje cifrándolo con su clave secreta, ya que prueba su identidad como único poseedor de esta clave. Cualquier receptor puede verificar la autenticidad del mensaje descifrándolo con la clave pública del emisor. La Figura 1.7 ilustra el proceso.

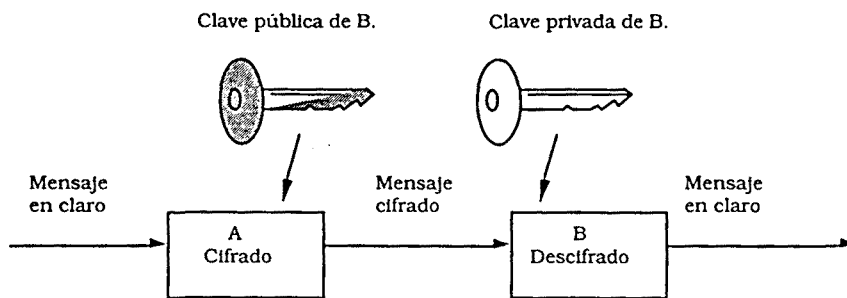


Figura 1.7a. Confidencialidad mediante criptografía de clave pública.

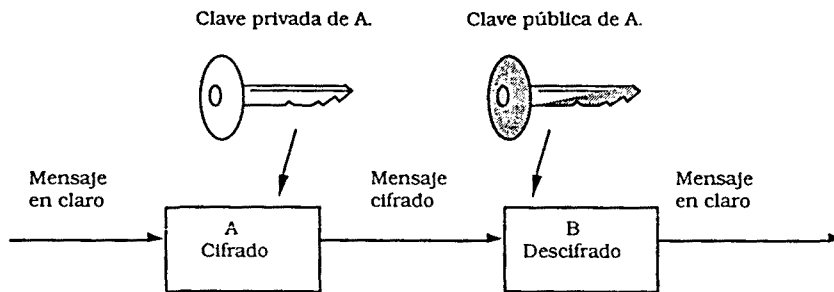


Figura 1.7b. Autenticación mediante criptografía de clave pública.

Los criptosistemas de clave pública ofrecen muchas más posibilidades a los diseñadores que los de clave simétrica. La idea fundamental de los criptosistemas de clave pública consiste en utilizar funciones unidireccionales con trampa (en inglés, *trapdoor one-way function*). Una función $y=f(x)$ se denomina unidireccional si:

- A cada valor de x le corresponde una y
- Dado un valor de x es fácil calcular la y
- Dado un valor de y es difícil calcular la x

Se dice que un problema es “fácil” o “difícil” en función del coste de CPU que precise su resolución. Una función $y=f(x)$ se denomina unidireccional con trampa si:

- A cada valor de x le corresponde una y
- Dado un valor de x es fácil calcular la y
- Dado un valor de y es fácil calcular la x conociendo cierta información (clave) y difícil sin esta información

Una de las primeras candidatas a función unidireccional con trampa fue el logaritmo discreto. El cálculo de la función exponencial discreta $y=a^x \bmod p$, es relativamente fácil de cálculo, incluso para valores grandes de x . En cambio, su función inversa, el logaritmo discreto $x=\log_a y \bmod p$ es difícilmente calculable si p es primo y $p-1$ tiene un factor primo grande.

Algunos problemas que generan funciones unidireccionales, y algoritmos que hacen uso de ellos se presentan en la Tabla 1.3.

BASADOS EN ...	ALGORITMO
Logaritmos discretos.	Diffie-Hellman Massey - Omura. ElGamal
Factorización	R.S.A.
Logaritmos elípticos	Miller.
Residuosidad cuadrática	Métodos probabilísticos

Tabla 1.3. Algoritmos que hacen uso de funciones unidireccionales.

Una mayor información sobre los algoritmos precedentes puede encontrarse en [DIF76, ELG85, RIV77, MIL87].

1.3.3 Algoritmos y Aplicaciones Actuales

Aparte del DES y el RSA, presentados anteriormente, los algoritmos criptográficos de los que se prevé una mayor utilización para ofrecer los servicios de confidencialidad y autenticidad en redes de datos son el IDEA (*International Data Encryption Algorithm*) [LAI90, LAI91, LAI92a], desarrollado como esquema de cifrado

convencional más seguro que el DES; el SKIPJACK [BRI93], propuesto por la administración norteamericana y que se implementa en el polémico chip Clipper; y el LUC [SMI93a, SMI93b], un criptosistema de clave pública comparable al RSA en cuanto a seguridad y funcionalidad.

De todas las aplicaciones de red, el correo electrónico es la usada más ampliamente. Por ello existe una gran demanda de servicios de confidencialidad y autenticación para esta aplicación. Actualmente existen dos esquemas que probablemente alcanzarán una gran expansión en pocos años: PGP (*Pretty Good Privacy*) [LEV93, STA95], y PEM (*Privacy-Enhanced Mail*) [RFC1421, RFC1422, RFC1423, RFC1424].

PGP es resultado del esfuerzo de una única persona, Phil Zimmermann, y provee servicios de confidencialidad y autenticación que pueden ser usados por aplicaciones de correo electrónico y de archivo de ficheros. Esta disponible libremente a través de Internet para un gran número de plataformas, que incluyen DOS, Windows, UNIX y Macintosh entre otras. Además utiliza algoritmos que se han mostrado altamente seguros al examen público durante años. En concreto utiliza RSA para cifrado con clave pública, IDEA para cifrado simétrico y MD5 [RFC1321] como función de hash.

Por otra parte, PEM es un borrador de estándar Internet que provee servicios de seguridad para aplicaciones de correo electrónico y posibilita varios esquemas de distribución de claves. Es un servicio extremo a extremo transparente a los distintos elementos intermedios de transmisión de correo. El diseño de PEM permite el empleo de distintos algoritmos criptográficos. Para ello los mensajes incluyen identificadores de los algoritmos usados. Para proporcionar integridad, se añade un código de hash calculado mediante MD2 [RFC1319] o MD5. Se emplea cifrado asimétrico, el algoritmo usado es RSA y el código de hash constituye una firma digital. Si se emplea cifrado simétrico se utiliza el algoritmo DES. El servicio de confidencialidad se consigue siempre mediante cifrado simétrico utilizando el algoritmo DES.

1.4 Motivación, Objetivos y Contribuciones de esta Tesis

Como se ha apuntado anteriormente, el estudio de arquitecturas de seguridad para redes de transmisión de datos adquiere cada día mayor importancia, a pesar de que en general se considera la seguridad un mal necesario más que una inversión que reporte beneficios. Por otra parte, es un hecho constatado que el mundo de las telecomunicaciones camina decididamente hacia la Red Digital de Servicios Integrados de Banda Ancha, que se espera que sea la red pública del futuro.

Sin embargo, aun cuando muchos de los mecanismos de seguridad que se utilizan en las redes actuales son igualmente aplicables en redes de banda ancha, no existe ninguna propuesta global que defina mecanismos y servicios de seguridad para este tipo de redes. En este sentido, la primera contribución de este trabajo de tesis es el estudio de la ubicación de servicios de seguridad dentro de la arquitectura de la red, evaluando las ventajas e inconvenientes de las posibles opciones. Se consideran especialmente aquellas opciones en las que los mecanismos utilizados sean comunes para toda la información multimedia (voz, vídeo y datos), ya que esta solución permite una integración global y a la vez modular de todos los servicios. Conviene señalar que estas soluciones integradas exigen en cualquier caso el uso de cifradores de gran velocidad. Hasta hace muy poco únicamente los cifradores en flujo [RUE86, BRU84, PIP82] parecían capaces de conseguir una velocidad de cifrado acorde con la de transmisión de la RDSI-BA. Hoy en día la tecnología actual parece que finalmente permite la utilización de cifradores en bloque en estos entornos [STE95].

Una vez analizadas las distintas posibilidades de ubicación de los servicios de seguridad dentro de la torre de protocolos MTA, se propone la arquitectura completa de un sistema integrado de seguridad para la RDSI-BA. Para ello se justifican una serie de requisitos que debe cumplir el sistema propuesto y se estudia la ubicación de los servicios de seguridad que mejor se adapta a ellos. A continuación se propone la arquitectura de un sistema de seguridad para RDSI-BA, que es otra contribución importante de esta Tesis. Este sistema de seguridad presenta un interfaz con las aplicaciones (API) para que éstas soliciten los servicios de seguridad que requieran con los parámetros apropiados. Para ello se definen una serie de primitivas de petición de servicios de seguridad, así como un protocolo para su negociación en un sistema distribuido.

Un tema prácticamente nuevo, del que conocemos pocas publicaciones (notables ejemplos son [GON93, REC96, SIR94, SOR93b, YAH93, ZOR94]) es la evaluación del coste que la introducción del sistema de seguridad conlleva, tanto en degradación de prestaciones en la red como en el coste económico que supone. Así, la siguiente aportación importante es la evaluación del coste que supone la implantación de servicios de seguridad en la red. Aunque este estudio se centra en la RDSI-BA, por coherencia con el resto de la Tesis, la metodología empleada es fácilmente exportable a otro tipo de redes y algunos resultados son generalizables.

En el estudio anterior se muestra la necesidad de métodos eficientes de gestión de claves para la viabilidad económica de la implantación de un sistema de seguridad en una red pública multidominio con un gran número de usuarios. Por ello la última aportación de esta tesis consiste en la propuesta de sistemas eficientes de gestión de

claves para la RDSI-BA. El principal objetivo será demostrar la eficiencia más que la seguridad, puesto que el diseño de protocolos de gestión de claves y la evaluación de su seguridad es un tema ampliamente estudiado durante los últimos años [BAN89, GON90, NES90, ZHE93]. Para garantizar la seguridad de los protocolos que se propongan, se parte de un protocolo conocido considerado seguros por la comunidad científica internacional, del que se proponen modificaciones y para aumentar su eficiencia sin disminuir su seguridad. Ejemplos de protocolos seguros y eficientes se adelantaron en [FOR95a, FOR96b].

En resumen, como contribución fundamental de este trabajo de Tesis se ha propuesto una arquitectura global de seguridad para la RDSI-BA.

1.5 Desarrollo de la Tesis

En el primer capítulo se han presentado las bases de la RDSI-BA y se han revisado conceptos generales de seguridad en redes de comunicación, con especial incidencia en los servicios genéricos de seguridad definidos en [ISO88] y los mecanismos para proveer estos servicios.

En el capítulo 2 se presenta el Modelo de Referencia de Protocolos (MRP) de la RDSI-BA, y se analizan diferentes opciones para la ubicación de los servicios genéricos de seguridad dentro de esta arquitectura de red, comentando ventajas e inconvenientes de cada una de ellas. Como motivación de este estudio, y también como ejemplo concreto, se presenta el proyecto CRIPTO del Plan Nacional de Banda Ancha (PLANBA).

En el capítulo 3 se sientan una serie de requisitos que debe cumplir el sistema de seguridad que se proponga. En relación con el estudio del capítulo anterior se escoge la ubicación de los servicios de seguridad que mejor cumple esta serie de requisitos. Seguidamente se propone una arquitectura del sistema de seguridad y su interfaz con las aplicaciones, que consiste en una serie de primitivas mediante las cuales las aplicaciones sensibles solicitan servicios de seguridad con ciertos parámetros de calidad.

En el capítulo 4 se estudia el coste que supone la implantación de estos servicios de seguridad, tanto para la red (incremento de tráfico, existencia de centros servidores de seguridad, etc.), como para los usuarios (tiempo de cálculo y proceso de los algoritmos de seguridad, uso de hardware específico, etc.). Se llega a la conclusión de que el coste asociado a la gestión de claves es necesario para evaluar cada uno de los servicios de seguridad, y que además es un coste que crece al aumentar el número de usuarios.

En el capítulo 5 se propone un protocolo de gestión de claves eficientes desde el punto de vista de minimización de los costes estudiados en el capítulo 4. Para su optimización se ha tenido en cuenta que se trabaja sobre una red pública orientada a conexión con un gran número de usuarios conectados (como es el caso de la RDSI-BA). Ello hace que este estudio sea generalizable a redes que cumplan estas dos características (como por ejemplo Internet).

En el capítulo 6 se remarcan las conclusiones más importantes de este trabajo de investigación y se proponen futuras líneas de actuación que quedan abiertas.

Finalmente se adjuntan 2 anexos. En el anexo A se presenta una especificación detallada en notación ASN.1 de las primitivas de seguridad mediante las cuales las aplicaciones solicitan servicios de seguridad. En el anexo B se presenta una relación detallada del coste que supone ofrecer servicios de seguridad en una red de comunicaciones.

1.6 Artículos e Informes Técnicos Publicados

A continuación se presenta la serie de publicaciones a las que ha dado lugar este trabajo de tesis:

- [CEÑ96] S. Ceña, "Seguridad en Comunicaciones TCP/IP. Desarrollo de un Protocolo Autenticado de Gestión de Claves", Proyecto Final de Carrera, UPC, ETSETB, Director del Proyecto: J. Forné, Junio 1996.
- [CRU95] E. Cruselles, M. Soriano, J. Forné, J.L. Melús, "Secure Communications in Broadband Networks". *Proceedings of the Third International Conference on Telecommunication Systems. Modelling and Analysis*. Nashville, USA Marzo 1995.
- [CRUZ93] L. de la Cruz, Ll. Cedó, J. Forné, "Implementación de un Sistema de Seguridad en una Red Local Ethernet". URSI-93. Valencia. 1993
- [CRUZ94] L. de la Cruz, "Diseño y realización del módulo de cifrado y del protocolo de seguridad para un bridge cifrador sobre redes Ethernet", Proyecto Final de Carrera, UPC, ETSETB, Director del Proyecto: J. Forné, Junio 1994.
- [FOR91] J. Forné, F. Recacha, X. Simón, M. Soriano, "Desarrollo de un Sistema de Seguridad para la red UPCNet basado en bridges cifradores", I Congreso Nacional de Criptología, Palma de Mallorca. Sep. 1991.

- [FOR93] J. Forné, M. Soriano, Melús, Recacha, "Hardware Implementation of a Secure Bridge in Ethernet Environment". *Proceedings of the Globecom'93*, Houston, USA. Nov. 1993.
- [FOR94a] J. Forné, J. L. Melús, F. Recacha, M. Soriano, "The Cripto Project: Security in Broadband Communications". Poster presentado en ESORICS'94 (European Symposium on Research in Computer Security), Brighton, England. Nov 1994.
- [FOR94b] J. Forné, F. Recacha, "Gestión de Claves en un Terminal Multimedia para RDSI-BA". III Reunión Española sobre Criptología. Barcelona, Noviembre 1994.
- [FOR94c] J. Forné, "Autopistas seguras para la información". *Suplemento de Ciencia y Tecnología de LA VANGUARDIA*. 26 Noviembre 1994.
- [FOR95a] J. Forné, F. Recacha, M. Soriano, J.L. Melús, "The Cripto Project Architecture: A Spanish Experience in Broadband Networks Security". *Proceedings of the ICC'95*. Seattle, Washington. USA. Junio 1995.
- [FOR95b] J. Forné, M. Soriano, F. Recacha, J. L. Melús, "Seguridad en redes de banda ancha", revista MUNDO ELECTRONICO. Num. 260. Oct. 1995.
- [FOR95c] J. Forné, M. Soriano, J. L. Melús, "Criptografía y seguridad en redes de comunicación", revista NOVATICA, Ago. 1995
- [FOR96a] J. Forné, J. L. Melús, "An Integrated Solution for Secure Communications over B-ISDN". *Communications and Multimedia Security. Joint Working Conference IFIP TC-6 and TC-11*. CHAPMANN-HALL. 1996.
- [FOR96b] J. Forné, J. L. Melús, D. Rebollo, "Gestión Eficiente de Claves en Grandes Redes" Actas de la IV Reunión Española sobre Criptología. Valladolid. 1996.
- [FOR96c] J. Forné, J. L. Melús, D. Rebollo, "Securing Multimedia Applications over B-ISDN". *Proceedings of the PROMS'96 (3rd International Workshop on Protocols for Multimedia Systems)*. Madrid. 1996.
- [PAL94] E. Pallarés, "Desenvolupament del mòdul de gestió de claus i d'administració per a un bridge segur", Proyecto Final de Carrera, UPC, ETSETB, Director del Proyecto: J. Forné, Junio 1994.
- [PLA92] J. Forné, J. L. Melús, F. Recacha, M. Soriano, "Informe Previo del Subproyecto de Gestión de Clave", *Informe Técnico del proyecto CRIPTO del Plan Nacional de Banda Ancha (PLANBA)*. 1992.

- [PLA93] J. Forné, J. L. Melús, F. Recacha, M. Soriano, "PLANBA. Proyecto CRIPTO. Subproyecto Gestión de Claves. Primer Informe", *Informe Técnico del proyecto CRIPTO del Plan Nacional de Banda Ancha (PLANBA)*. 1993.
- [PLA94a] J. Forné, J. L. Melús, F. Recacha, M. Soriano, "Autenticación y Gestión del Claves en Redes de Comunicaciones", *Informe Técnico del proyecto CRIPTO del Plan Nacional de Banda Ancha (PLANBA)*. 1994.
- [PLA94b] J. Forné, J. L. Melús, F. Recacha, M. Soriano, "Elección de un Protocolo Criptográfico para la Red de Banda Ancha", *Informe Técnico del proyecto CRIPTO del Plan Nacional de Banda Ancha (PLANBA)*. 1994.
- [PLA95a] J. Forné, J. L. Melús, F. Recacha, M. Soriano, "T.2.2.2/2. Diseño funcional del conjunto operador/protocolo criptográfico", *Informe Técnico del proyecto CRIPTO del Plan Nacional de Banda Ancha (PLANBA)*. 1995.
- [PLA95b] J. Forné, J. L. Melús, F. Recacha, M. Soriano, "T.2.3.1/R1. Estudio de integración de la gestión de claves", *Informe Técnico del proyecto CRIPTO del Plan Nacional de Banda Ancha (PLANBA)*. 1995.
- [PLA95c] J. Forné, J. L. Melús, F. Recacha, M. Soriano, "T.2.3.1/R2. Especificación Funcional del Módulo de gestión de claves", *Informe Técnico del proyecto CRIPTO del Plan Nacional de Banda Ancha (PLANBA)*. 1995.
- [PLA95d] J. Forné, J. L. Melús, F. Recacha, M. Soriano, "T.2.3.1/R3. Especificación de características lógicas para el diseñador industrial", *Informe Técnico del proyecto CRIPTO del Plan Nacional de Banda Ancha (PLANBA)*. 1995.
- [PLA95e] J. Forné, J. L. Melús, F. Recacha, M. Soriano, "PLANBA. Proyecto CRIPTO. Subproyecto Gestión de Claves. Informe Final", *Informe Técnico del proyecto CRIPTO del Plan Nacional de Banda Ancha (PLANBA)*. 1995.
- [REB96] D. Rebollo, "Seguridad en Internet. Desarrollo de una plataforma de negociación de servicios de seguridad para sistemas UNIX", Proyecto Final de Carrera, UPC, ETSETB, Director del Proyecto: J. Forné. 1996.
- [REC93] F. Recacha, J. L. Melús, X. Simón, M. Soriano, J. Forné, "Secure Communications in Extended Ethernet Environments" *IEEE Journal on Selected Areas in Communications*. Volume 11. Number 5. June 1993

- [REC95] F. Recacha, J. Forné, J.L. Melús, "A solution to secure inter-networking with Metropolitan Area Networks" Minutes of the EEC DG XIII/B (InfoSec) WorkShop on Security Dependability and Safety of Communications Systems and Services, Brussels. June 1995.
- [SOR93a] M. Soriano, J. Forné, J.L. Melús, F. Recacha, "Implementation of a security system in a local area network environment". *Proceedings of the 18th Annual Conference on Local Computer Networks..* Minneapolis, USA. Sept 1993
- [SOR93b] M. Soriano, J. Forné, F. Recacha, J.L. Melús, "A particular solution to provide secure communications in an ethernet environment". *Proceedings of the 1st ACM Conference on Computer and Communications Security.* Virginia, USA. Nov. 1993.
- [SOR96] M. Soriano, J. Forné, J.L. Melús, "Linear Complexity Stability in Stream Ciphering for High Speed Networks." *Proceedings of the 4th. International Conference on Telecommunications Systems.* Nashville, USA, Marzo 1996.

CAPÍTULO 2

Ubicación de los Servicios de Seguridad dentro del Modelo de Referencia de Protocolos de la RDSI-BA

2.1 Introducción

Las comunicaciones actuales se basan en arquitecturas de protocolos a diferentes niveles, especialmente para la transmisión de datos. El modelo de Interconexión de Sistemas Abiertos (OSI, *Open Systems Interconnection*) es la base de las arquitecturas que utilizan protocolos estratificados. El Modelo de Referencia Básico (ISO/IEC 7498-1) [ISO84] establece este modelo arquitectónico.

La ubicación de los servicios de seguridad dentro de una arquitectura de protocolos estratificada es compleja y a menudo sujeta a controversia [LAM89]. Diferentes estándares contemplan esta problemática (por ejemplo, ISO 7498-2 [ISO88] y IEEE 802.10 [IEE89, IEE91, IEE92]). Sin embargo, estos estándares dejan muchas opciones abiertas. Es conveniente que algunos servicios se ofrezcan a diferentes niveles en diferentes escenarios de aplicación, mientras que otros sería incluso conveniente que se ofreciesen en varios niveles en un mismo escenario. En este sentido W. Ford [FORD94] plantea un modelo de seguridad de cuatro niveles que, bajo nuestro punto de vista, se adecua mejor a las implicaciones de seguridad de las redes reales.

En cualquier caso la ubicación de los servicios de seguridad en la RDSI-BA es un tema completamente nuevo y de especial interés si se tiene en cuenta que el futuro de las telecomunicaciones camina inexorablemente hacia este tipo de redes. Por ello en este capítulo se estudian diferentes posibilidades para la ubicación de los servicios de seguridad definidos por [ISO88] (ver Capítulo 1, apartado 1.3.1.2) dentro del modelo de referencia de protocolos para la RDSI-BA.

2.2 Modelo de Referencia OSI

A la hora de realizar una descripción de la estructura y funcionalidad de los protocolos de comunicación de datos frecuentemente se utiliza como referencia un modelo de arquitectura desarrollado por la Organización Internacional de Estándares (ISO) [ISO84].

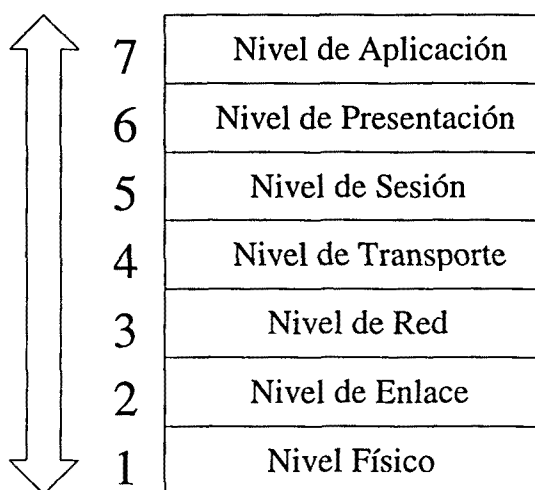


Figura 2.1. Niveles del Modelo de referencia OSI.

Este modelo de arquitectura, comúnmente conocido como Modelo de Referencia OSI (*Open Systems Interconnection Reference Model*) supone una referencia básica a la hora de discutir acerca de comunicaciones, siendo los términos definidos por este modelo tan conocidos y tan ampliamente difundidos, que se nos hace difícil el poder discutir acerca de comunicación de datos sin utilizar la terminología OSI.

El Modelo de Referencia OSI contiene siete niveles que definen las funciones de los protocolos de comunicación de datos, que están estructurados unos encima de otros a modo de pila, tal y como muestra la Figura 2.1. Cada uno de los niveles representa una función desarrollada cuando se transfieren datos entre aplicaciones cooperantes dentro de una misma red.

Cada uno de estos niveles no representa un único protocolo, sino que cada nivel contiene múltiples protocolos, que proporcionan un servicio acorde con la función correspondiente a ese nivel. Por otra parte estos niveles son los encargados de enviar información desde una aplicación local a una remota. La información pasa por cada uno de los niveles superiores de la pila a los inferiores hasta que es transmitida a nivel físico a través de la red.

En el extremo opuesto de la comunicación la operación se realiza en el sentido contrario, es decir, es recogida de los niveles inferiores hacia los superiores. Cada uno de los niveles individuales no necesita conocer el funcionamiento de los niveles inferiores o superiores. Este aislamiento entre niveles permite poder añadir nuevas aplicaciones sin tener que variar la red física o instalar nuevo hardware sin necesidad de modificar el software de aplicación que ya teníamos.

2.3 Modelo de Seguridad de 4 Niveles

La Figura 2.2 muestra un par de sistemas extremos que se comunican a través de una serie de subredes. Cada una de estas subredes emplea la misma tecnología de comunicaciones, pudiendo ser redes de área local (LANs, *Local Area Network*) particulares, o bien redes de área extendida (WANs, *Wide Area Network*). Un ejemplo típico es un sistema extremo conectado a una LAN privada que tiene un dispositivo de interconexión (*gateway*) a una WAN pública. Finalmente el otro sistema extremo se encuentra también en una LAN conectada también a la WAN pública.

En este escenario, Ford [FORD94] plantea un modelo de seguridad que consta de los siguientes cuatro niveles, como se muestra en la Figura 2.2:

- (a) *Nivel de aplicación*: Elementos de protocolos de seguridad dependientes de la aplicación.
- (b) *Nivel de sistema extremo*: Elementos de protocolos de seguridad que protegen extremo a extremo.
- (c) *Nivel de subred*: Elementos de protocolos de seguridad que protegen sobre una subred considerada menos fiable que el resto.

(d) *Nivel de enlace*: Elementos de protocolos de seguridad dentro de una subred concreta, que protegen un enlace que se considera menos fiable que el resto.

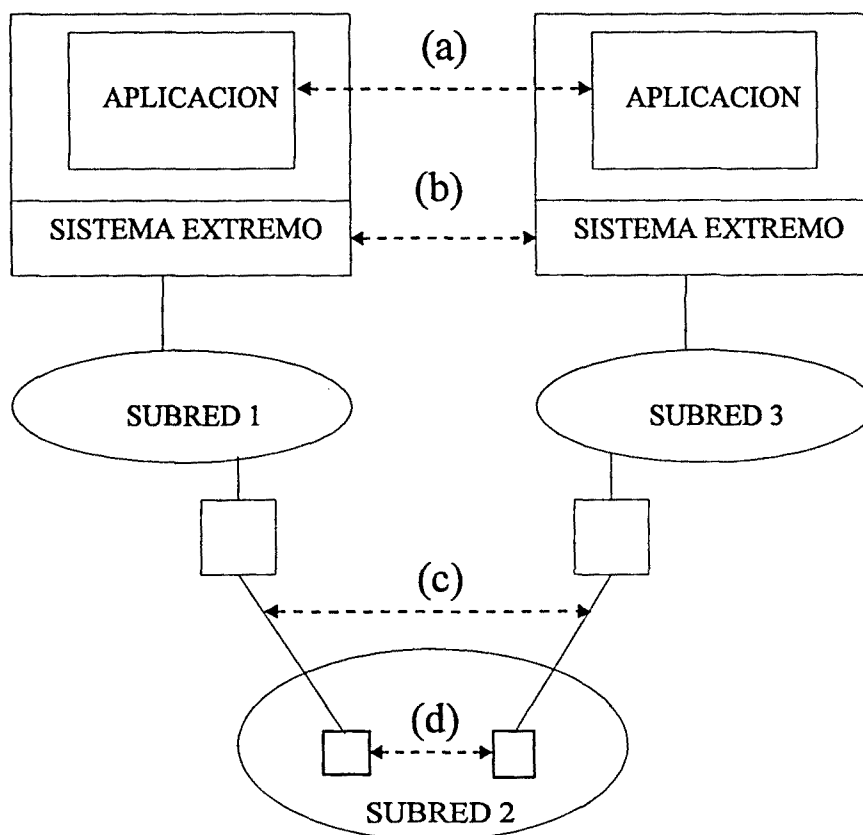


Figura 2.2. Modelo de seguridad de 4 niveles.

2.4 Modelo de Referencia de Protocolos para la RDSI-BA

La figura 2.3 muestra el modelo de referencia de protocolos (MRP) para la RDSI-BA. En la figura 2.4 se ilustran las funciones de cada capa según se describe en las recomendaciones I.321 e I.413 del CCITT [CCI92d, CCI92e].

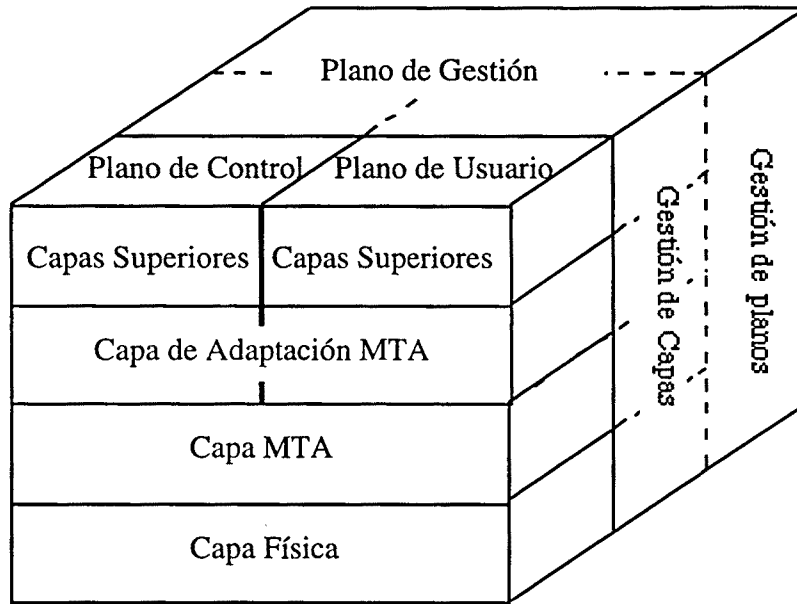


Figura 2.3: Modelo de referencia de protocolos para la RDSI-BA.

Layer Management	Higher layer functions	Higher layers	
	Convergence	CS	AAL
Segmentation and reassembly	SAR		
Generic flow control Cell header generation/extraction Cell VPI/VCI traslation Cell multiplex and demultiplex	ATM		
Cell rate decoupling HEC sequence generation/verification Cell delination Transmission frame adaptation Transmission frame generation/recovery	TC	Physical layer	
Bit timing	PM		
Physical medium			

CS: Convergence Sublayer
PM: Physical Medium
SAR: Segmentation and Reassembly sublayer
TC: Transmission Convergence

Figura 2.4: Funciones de la RDSI-BA en relación al MRP de la RDSI.

El modelo de referencia de protocolos consta de tres planos: el plano de usuario, el plano de control y el plano de gestión. El plano de usuario hace referencia a la transferencia de información de usuario e incluye mecanismos como control de flujo y recuperación de errores. El plano de control se encarga del control de las llamadas y conexiones. Es decir, comporta todas aquellas funciones de señalización necesarias para establecer, supervisar y liberar llamadas y conexiones.

El plano de gestión es el responsable de funciones de operación y mantenimiento de la red. La gestión de planos realiza funciones de gestión relativas al sistema global y proporciona la coordinación necesaria entre planos. No posee una estructura de capas. La gestión de capas realiza funciones de gestión que tienen que ver con los recursos y parámetros que residen en sus entidades de protocolo (p.e., meta-señalización). También maneja flujos de información de operación y mantenimiento, pero específicos a cada capa en cuestión.

En la actualidad se han definido con claridad tres capas del modelo de referencia: la capa física, la capa MTA y la capa de adaptación MTA. Las capas superiores se encuentran todavía en fase de estudio.

La capa física (PL, *Physical Layer*) se divide en dos subcapas: la subcapa del medio físico (PM, *Physical Medium*) y la subcapa de convergencia a la transmisión (TC, *Transmission Convergence*) [CCI92f]. La subcapa PM incluye todas aquellas funciones dependientes del medio físico en cuestión (p.e., conversión electro-óptica). La subcapa TC efectúa todas las funciones necesarias para transformar un flujo de celdas en un flujo de entidades de datos (por ejemplo *bits*), compatible con el esquema de multiplexación del sistema de transmisión.

La capa de adaptación MTA (AAL, *ATM Adaptation Layer*) [CCI92g, CCI92h] tiene como función básica el aislar las capas superiores de las características propias de la capa MTA. Se encarga de adaptar los datos procedentes de niveles superiores a un formato que pueda ser manipulado por la capa MTA. La capa AAL se organiza en dos subcapas. La subcapa de convergencia (CS, *Convergence Sublayer*) y la subcapa de segmentación y reensamblado (SAR, *Segmentation And Reassembly*). La subcapa SAR tiene como misión el segmentar los datos de las capas superiores en un formato compatible con el campo de información de usuario de una celda MTA (48 octetos), o recíprocamente, el reensamblar dichos campos de información en unidades de datos de protocolo (PDU, *Protocol Data Unit*) de la capa superior.

La subcapa CS es independiente del servicio y realiza funciones necesarias para soportar aplicaciones específicas (p.e., recuperación de reloj en servicios de vídeo insertando palabras de sincronización). Actualmente se han definido cinco tipos de capa AAL respondiendo a una clasificación en cuatro tipos de servicios que tiene en cuenta los siguientes parámetros: relación de sincronismo entre fuente y destino, tasa binaria (constante o variable) y modo de conexión (orientado o no orientado a conexión).

Seguidamente y de forma muy resumida se comentan las cuatro clases de servicios definidos por el CCITT y alguna noción sobre los cinco tipos de capa AAL:

- Clase 1: aplicaciones de tasa binaria continua (constante) tal como la telefonía por modulación de impulsos codificados (PCM).
- Clase 2: aplicaciones no de datos y de tasa binaria variable tal como vídeo digital comprimido.
- Clase 3: aplicaciones de datos orientadas a conexión.
- Clase 4: aplicaciones de datos no orientadas a conexión.

Los distintas capas AAL son:

- AAL-1: definida para soportar aplicaciones de clase 1.
- AAL-2: definida para soportar aplicaciones de clase 2.
- AAL-3/4: cuando se aceptó que un solo protocolo AAL podía usarse para soportar servicios de datos orientados a conexión y en modo datagrama (no orientados a conexión) se especificó la capa AAL-3/4 para tratar ambos servicios.
- AAL-5: como resultado de la complejidad asociada con la capa AAL-3/4, se propuso el nivel AAL-5, también conocido como capa de adaptación simple y eficiente (SEAL, *Simple and Efficient Adaptation Layer*). Proporciona funciones más limitadas (detección de error pero no recuperación) y posee menores requisitos en cuanto al proceso que implica y al ancho de banda que necesita.

La capa MTA es independiente del medio físico y de los servicios que transporta. Se encarga de las funciones relacionadas con la información presente en la cabecera de la celda MTA y que, por tanto, son necesarias para el tratamiento lógico de dicha celda MTA [CC192i]. La identificación de canales virtuales y la detección de errores en la cabecera de la celda son ejemplos de dichas funciones.

Antes de pasar a la siguiente sección, debe destacarse que no existe una correspondencia clara entre el modelo de referencia de protocolos para la RDSI-BA y el modelo de protocolos OSI de 7 niveles y que la compatibilidad entre los mismos es difícil y aún no ha sido dilucidada.

2.5 Ubicación de los Servicios de Seguridad

En la sección anterior se ha presentado el modelo de referencia de protocolos para la RDSI-BA. Se ha comentado que las capas superiores a la capa de adaptación

(AAL) aún no han sido claramente definidas, aunque parece que al menos transitoriamente deberán ser compatibles con protocolos actuales de comunicaciones, como el TCP/IP. En cualquier caso es claro que el plano de usuario constará de una capa de aplicación (correspondiente al nivel 7 del modelo de referencia OSI) y una serie de niveles intermedios entre ésta y el nivel AAL. La figura 2.5 caracteriza la torre de protocolos para el plano de usuario de la RDSI-BA.

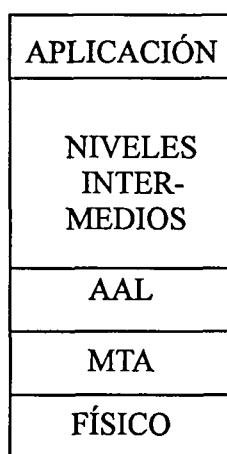


Figura 2.5. Modelo de Referencia de Protocolos para el plano de usuario de la RDSI-BA.

En este apartado se comparan diferentes opciones para la ubicación de los servicios de seguridad dentro del plano de usuario de la RDSI-BA (Figura 2.5). Se estudia únicamente la inclusión de los servicios en el plano de usuario, puesto que las demás opciones supondrían interactuar con aspectos de control y gestión de red cuando en realidad muchos de ellos están aún en fase de definición. Por otra parte, para evitar redefinir la funcionalidad de las capas mostradas en la figura 2.5, no se considera la posibilidad de integrar los servicios de seguridad dentro de alguna de ellas. En su lugar, se propondrán nuevos niveles de seguridad a insertar entre las diferentes capas, de forma que el resto de niveles no se modifiquen y se pueda actuar de forma transparente.

Teniendo en cuenta lo anteriormente expuesto, la figura 2.6 presenta las principales opciones para la ubicación de los servicios de seguridad en la arquitectura de protocolos de la RDSI-BA.

APLICACIÓN
SEGURIDAD
NIVELES INTER-MEDIOS
AAL
MTA
FÍSICO

Figura 2.6a

APLICACIÓN
NIVELES INTER-MEDIOS
SEGURIDAD
AAL
MTA
FÍSICO

Figura 2.6b

APLICACIÓN
NIVELES INTER-MEDIOS
AAL
SEGURIDAD
MTA
FÍSICO

Figura 2.6c

APLICACIÓN
NIVELES INTER-MEDIOS
AAL
MTA
SEGURIDAD
FÍSICO

Figura 2.6d

Tal como apunta [FORD94], en general la ubicación de los servicios de seguridad a niveles más altos o más bajos presenta los siguientes compromisos:

- *Mezcla de tráfico:* Como resultado de la multiplexación, existe una mayor tendencia de tener datos procedentes de diferentes usuarios o aplicaciones a niveles bajos que a niveles más altos. Si se desea que usuarios y aplicaciones especifiquen individualmente la protección requerida para sus datos, entonces es preferible la ubicación de los servicios de seguridad a niveles más altos. Si se desea cierto grado de protección de toda la información independientemente de su procedencia, esto se consigue más fácilmente a niveles más bajos.
- *Conocimiento de la ruta:* A niveles más bajos, existe un mayor conocimiento de las características de seguridad de diferentes rutas y enlaces. La ubicación de servicios de seguridad a niveles bajos puede ser más efectiva y eficiente en entornos en los que los requisitos de seguridad varíen fuertemente de unos enlaces o subredes a otros.
- *Número de puntos de protección:* La ubicación de los servicios de seguridad en el nivel más alto (nivel de aplicación) requiere una implementación de seguridad para cada aplicación en cada sistema extremo. La ubicación a niveles más bajos facilita la posibilidad de instalar los servicios de seguridad en un número menor de puntos, reduciendo el coste. Sin embargo, la ubicación a nivel de enlace supone la implantación de los servicios de seguridad en todos los nodos intermedios.
- *Protección de cabeceras de protocolos:* La ubicación de seguridad a los niveles más altos no protege las cabeceras de los protocolos de nivel inferior, que pueden ser sensibles en ciertos casos. Ello permite por ejemplo ataques por análisis de tráfico.

- *Asociación con origen/destino*: Algunos servicios de seguridad, como autenticación del origen de datos o no repudio, dependen de la asociación de los datos con su origen o destino. Esta asociación se consigue más fácilmente a niveles más altos, especialmente el de aplicación.

Si se desea proteger la información que circula entre terminales conectados a una red RDSI-BA, la arquitectura del terminal puede jugar un papel fundamental en el diseño de un sistema de seguridad [CRU95, FOR95a]. La elección de una opción u otra de las presentadas en la figura 2.6 será mejor o peor en función de la arquitectura particular del terminal.

A continuación se comparan las principales opciones para ubicar el cifrado de la información (necesaria para ofrecer servicios de integridad y confidencialidad), la gestión de claves (necesaria para todos los servicios de seguridad) y la autenticación, control de acceso y no repudio, según la arquitectura MTA.

2.5.1 Cifrado de la Información. Integridad y Confidencialidad

El cifrado de la información es un mecanismo fundamental para proporcionar los servicios de integridad y confidencialidad.

El servicio de confidencialidad se ofrecerá típicamente cifrando en el origen toda la información con una clave secreta que únicamente será compartida con el receptor legítimo. La alta velocidad de la red imposibilita el uso de criptosistemas de clave pública para el cifrado del “grueso de la información” (en inglés, *bulk ciphering*), ya que la tecnología actual limita las velocidades de encriptación de estos sistemas bastante por debajo de las de las típicas aplicaciones multimedia sobre la RDSI-BA. Por ello es necesario el uso de criptosistemas simétricos capaces de procesar (cifrar y descifrar) toda la información a una velocidad al menos tan rápida como la de red, requisito imprescindible para no degradar las aplicaciones en tiempo real. Hoy en día los cifradores en flujo [RUE86] parecen ser la mejor alternativa tecnológica para alcanzar altas velocidades de cifrado a un coste razonable [CRU95, GUI94], aunque [STE95] apunta la posibilidad de utilizar cifradores en bloque.

Existen dos opciones principales para proporcionar el servicio de integridad, que son las siguientes:

- Se cifra una cadena comprimida función de la información con una clave secreta. Esta cadena se envía conjuntamente con la información a transmitir. El receptor repite la compresión de los datos recibidos y cifrado de esta cadena

con la misma clave que en emisión. Posteriormente compara con la cadena cifrada enviada y decide que la información es íntegra si ambas cadenas coinciden. La compresión y cifrado deben cumplir ciertas propiedades para garantizar una buena seguridad. Las principales opciones consisten en la utilización de un *checksum* criptográfico (que realiza la compresión y cifrado, con propiedades similares a los algoritmos criptográficos) o la utilización de una función de *hash* y el posterior cifrado del resultado de esta función. Para una mayor información sobre checksum y funciones de hash puede consultarse por ejemplo [STA95].

- Ofrecer el servicio de confidencialidad conjuntamente al de integridad, con un único cifrado. Para ello es necesario disponer de un algoritmo de cifrado en bloque que difunda los errores (aleatorios o intencionados) de forma que la variación de un bit en el texto en claro provoque una incertidumbre total en la variación del criptograma (es decir, cada bit del criptograma debe tener una probabilidad de variar $\frac{1}{2}$) y viceversa. Asimismo es necesario que cada bloque contenga información redundante para que en el proceso de descifrado pueda verificarse la integridad del bloque comprobando únicamente la integridad de esta información redundante. Es necesario que la longitud de la información redundante sea lo suficientemente grande como para garantizar una tasa de error no detectado baja. Conviene destacar que esta opción no puede implementarse en cifradores en flujo, ya que estos algoritmos no provocan difusión.

Una variante de la segunda opción que puede resultar interesante desde un punto de vista económico es aprovechar como información-redundante las cabeceras de protocolos de nivel superior. Si se cifra por ejemplo el campo de datos de nivel MTA, todas las cabeceras de nivel superior estarán cifradas. Suponiendo que los protocolos de nivel superior sean fiables será posible detectar ataques a la integridad bajo ciertas condiciones. Así, si un bloque de información contiene una cabecera que forme parte de un protocolo fiable con detección de errores, será imposible modificar un bit del criptograma sin que esto afecte a la cabecera y esta modificación sea detectada¹. Para ello es necesario que todos los bloques de información cifrada contengan ciertas cabeceras, lo cual no siempre es fácil de conseguir.

¹ De hecho esto será interpretado por el protocolo fiable que corresponda como un error en la transmisión y la PDU no se pasará a niveles superiores. Dependiendo del mecanismo de corrección de errores de ese protocolo, puede solicitarse una retransmisión de la información. Si el protocolo ofrece mecanismos de control de flujo, puede ser relativamente robusto a ataques por reactuación.

Otra posibilidad es garantizar cierto grado de integridad como efecto colateral del cifrado utilizado para ofrecer confidencialidad. Esta aproximación supone redundancia en la información y juega con el hecho de que el atacante no conseguirá crear un criptograma que corresponda a un texto en claro coherente. Sin embargo la detección de ataques a la integridad sólo es posible para información de alta redundancia (por ejemplo, ficheros de texto o imágenes) y cuando exista una entidad inteligente (por ejemplo, un usuario) que realice esta detección. Por ello creemos que esta forma indirecta de proporcionar integridad es claramente desaconsejable, y en lo sucesivo no será considerada.

Es de resaltar que en cualquiera de las opciones anteriores es necesario el procesamiento de toda la información, al igual que para el servicio de confidencialidad, y que los mecanismos que se utilizan son muy similares. Por ello se estudia conjuntamente la ubicación de ambos servicios dentro del MRP de la RDSI-BA, puesto que conllevan el procesamiento del grueso de la información. La figura 2.7 presenta las cuatro posibilidades que serán consideradas, en consonancia con la figura 2.6.

APLICACIÓN
CIFRADO
NIVELES INTER-MEDIOS
AAL
MTA
FÍSICO

Figura 2.7a

APLICACIÓN
NIVELES INTER-MEDIOS
CIFRADO
AAL
MTA
FÍSICO

Figura 2.7b

APLICACIÓN
NIVELES INTER-MEDIOS
AAL
CIFRADO
MTA
FÍSICO

Figura 2.7c

APLICACIÓN
NIVELES INTER-MEDIOS
AAL
MTA
CIFRADO
FÍSICO

Figura 2.7d

2.5.1.1 Cifrado por debajo del nivel de aplicación

La primera posibilidad es ubicar el cifrado inmediatamente debajo del nivel de aplicación, tal como se observa en la figura 2.7a. En esta situación, los datos procedentes de aplicaciones sensibles se cifran en el terminal origen antes de ser transmitidos a los niveles intermedios, a continuación son encapsulados con los protocolos de comunicaciones correspondientes y finalmente son transmitidos a través de la red. En el extremo destinatario se realiza el proceso inverso, de modo que los datos

son descifrados justo antes de ser entregados al nivel de aplicación. Esta solución presenta las siguientes ventajas:

- La cantidad de datos a cifrar es menor, ya que las cabeceras introducidas por los niveles por debajo del nivel de aplicación no son procesadas.
- Las unidades de información a cifrar son mayores que a niveles inferiores, en particular mucho mayores que en la opción 7c. Ello permite que diferentes aplicaciones puedan compartir fácilmente un único dispositivo cifrador de forma eficiente². Para más detalles sobre el efecto de la longitud de datos en la eficiencia ver capítulo 4 de esta memoria de Tesis.
- La gestión de claves se simplifica, ya que se asocia una clave con cada aplicación.
- Si se desea ofrecer estos servicios en función de la aplicación, a este nivel la interfaz con la aplicación es más sencilla, y se facilita que las aplicaciones soliciten los servicios requeridos (en este caso confidencialidad, o integridad, o ambos) con los parámetros deseados. En el caso de que se requiera integridad o confidencialidad sólo en unos campos selectivos de la aplicación, entonces los servicios de seguridad deberían integrarse dentro de la propia aplicación, o la aplicación debería interactuar estrechamente con este nivel de seguridad.
- Permite la compatibilidad (interconexión segura) con sistemas conectados a otro tipo de redes (LANs, MANs o WANs), ya que este nivel está por encima de cualquier tecnología de red particular.
- Esta solución es la única posible cuando los servicios de seguridad deben atravesar dispositivos a nivel de aplicación. Existen aplicaciones, como el caso del correo electrónico, que involucran más de dos sistemas finales. En este entorno se hace necesario proteger el contenido del mensaje, algo que sólo puede hacerse a nivel de aplicación. Sin embargo conviene señalar que en muchos de estos casos puede ser más conveniente ofrecer los servicios de seguridad integrados dentro de las aplicaciones sensibles.

Entre los inconvenientes más importantes que presenta esta opción se encuentran los siguientes:

² La mayoría de cifradores, especialmente si se trata de dispositivos hardware, requieren un tiempo inicial para su funcionamiento. Este tiempo incluye la carga de claves (o el tiempo necesario para su conmutación, si han sido previamente cargadas) y una serie de instrucciones para su funcionamiento. Si las unidades de datos son pequeñas y cada una de ellas requiere una conmutación de claves, el tiempo total dedicado al cifrado puede ser pequeño con lo que el cifrado se hará poco eficiente.

- En algunos casos, la arquitectura del terminal multimedia impone que aplicaciones de audio y vídeo accedan directamente a los niveles inferiores, impidiendo esta solución (ver [FOR95a]). Lógicamente podría ubicarse la seguridad a este nivel para aplicaciones de datos que lo requieran, y dotar de mecanismos alternativos de seguridad para el resto de aplicaciones de audio y vídeo. Sin embargo, ello aumentaría el coste al requerir un mayor número de puntos de protección.
- Deberá diseñarse un nivel de seguridad específico, que deberá tener un interfaz diferente para cada posible familia de protocolos de comunicaciones por debajo del nivel de aplicación (por ejemplo, TCP, etc.). Este incremento necesario del número de puntos de protección es, sin lugar a dudas, el principal inconveniente de adoptar la opción 7a.

2.5.1.2 Cifrado por encima del nivel de adaptación

La segunda opción que se contempla es ubicar los servicios de integridad y confidencialidad inmediatamente por encima de la capa de adaptación AAL, tal como se indica en la figura 2.7b. Esta opción presenta las siguientes ventajas:

- Al igual que ocurría en la opción 7a, los bloques de información son de mayor tamaño que a niveles más bajos, mejorando la eficiencia del proceso de cifrado.
- Sólo existen 4 niveles de adaptación (AAL-1, AAL-2, AAL-3/4 y AAL-5) a través de los cuales cualquier tipo de información multimedia accede a la RDSI-BA. Ello hace que a este nivel sólo sea necesario diseñar cuatro interfaces diferentes entre el nivel de seguridad y el de adaptación, a diferencia de la opción 2.7a, donde debía diseñarse un interfaz diferente para cualquier protocolo disponible a nivel inferior sobre el que se estableciesen comunicaciones seguras.
- La segmentación y reensamblado de las unidades de información se lleva a cabo en la capa AAL, concretamente en el subnivel SAR (*Segmentation and Reassembly*). El ofrecer integridad por encima de la capa AAL presenta muchas ventajas, ya que este servicio precisa incluir información adicional (expandir el mensaje). La ubicación por debajo de la capa de adaptación (opciones 7c y 7d) obligaría a crear nuevas celdas y a que la capa que provea el servicio de integridad las procese repitiendo funciones de segmentación y reensamblado, lo cual es poco aconsejable. El servicio de confidencialidad no sufre esta limitación, al no implicar necesariamente una expansión de los mensajes. Sin embargo en muchas ocasiones puede ser conveniente ofrecer

integridad y confidencialidad a un mismo nivel lógico en aras de una mayor sencillez del sistema de seguridad.

- La identificación de la aplicación origen o destino de los datos es más sencilla a este nivel que a niveles inferiores.
- El nivel de adaptación provee mecanismos de detección y corrección de errores, según el tipo de servicio que se requiera, además de control de flujo. Ello facilita la utilización de ciertos algoritmos de cifrado, como por ejemplo cifradores en flujo síncronos.

Como inconvenientes principales se destacan los siguientes:

- No es posible ofrecer servicios de seguridad a equipos terminales conectados a redes que no sean MTA. Ello es debido a que otras redes no tendrán el nivel AAL, y la interconexión de equipos será posible gracias a que se compartirán protocolos de niveles superiores, como el TCP/IP.
- Permite ciertos ataques de análisis de tráfico, al permanecer en claro las cabeceras AAL y ATM.

2.5.1.3 Cifrado entre el nivel de adaptación y el nivel MTA

La tercera opción es la ubicación del proceso de cifrado entre los niveles AAL y MTA, tal como se muestra en la figura 2.7c. El cifrado se realiza sobre todo el campo de datos de las celdas MTA mientras que las cabeceras se mantienen en claro. De esta forma se puede ofrecer el servicio de confidencialidad.

La implementación del servicio de integridad a este nivel presenta grandes inconvenientes.

Por una parte la introducción de información redundante para ofrecer este servicio presenta el problema de expansión de la información y la necesidad de repetir operaciones de segmentación y reensamblado, tal como se mencionó en el apartado 2.5.1.2. Una posibilidad puede ser insertar celdas de comprobación de la integridad cada cierto número de celdas normales. La información no se podrá pasar a un nivel superior como “íntegra” hasta no recibir estas celdas y comprobar la integridad del conjunto de celdas anteriores. Ello provoca un retardo aparte de un incremento de tráfico, y deberá realizarse cierto grado de control de flujo a este nivel.

Por otra parte el intentar ofrecer este servicio sin una expansión de la información presenta importantes problemas de implementación y de seguridad. La única posibilidad viable sería que cada bloque cifrado contuviese información redundante fácilmente verificable. Ello en general sólo ocurre si cada bloque de información contiene cabeceras de protocolos de nivel superior, que serán posteriormente comprobadas en el nivel correspondiente.

Sin embargo esta posibilidad es muy difícil de realizar, ya que precisa longitudes de bloques de cifrado tales que cada bloque incluya las cabeceras de protocolos de nivel superior. A nivel de celdas MTA se debería trabajar con bloques de cifrado de 48 bytes. De esta forma la comprobación de la integridad de las cabeceras AAL por el nivel de adaptación implicaría la integridad de todo el campo de datos de la celda MTA. Un problema es que no todos los niveles de adaptación incluyen cabeceras en cada celda (en concreto el AAL 5 no lo hace). Además los otros niveles incluyen una longitud pequeña de esta información, con lo que el nivel de seguridad es pequeño. Otro problema añadido es que esta técnica no es posible con cifradores en flujo, y no es evidente encontrar cifradores en bloque que manejen bloques de 48 bytes y que a la vez sean rápidos. Por todo ello no es aconsejable ofrecer integridad a este nivel.

A partir de ahora, pues, se presentan las ventajas y desventajas de ofrecer confidencialidad a este nivel.

Existen dos opciones principales ofrecer confidencialidad a este nivel. La primera de ellas consiste en cifrar el campo de datos de todas las celdas con una única clave, independientemente del destino, tal como se muestra en la figura 2.8. La segunda opción (figura 2.9) consiste en utilizar una clave diferente en función del destino de la celda, que a este nivel viene dado por camino y canal virtual.

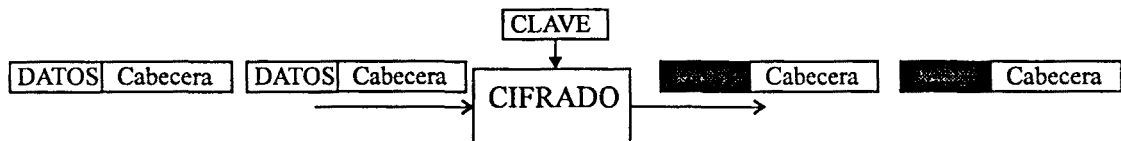


Figura 2.8. Cifrado del campo de datos de todas las celdas MTA con una única clave, independientemente de la cabecera.

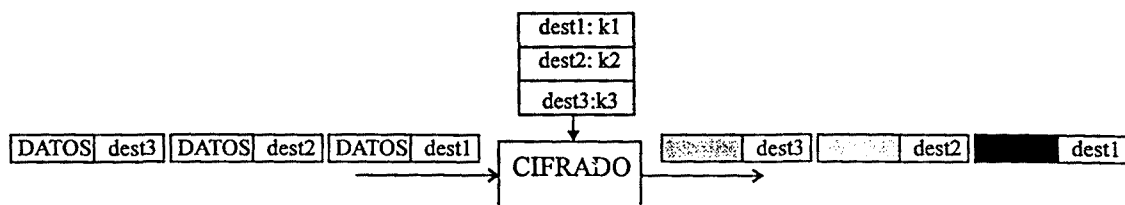


Figura 2.9. Cifrado del campo de datos de cada celda MTA con una clave diferente para cada destino.

Ambas soluciones pueden adoptarse en el nodo extremo (típicamente un terminal multimedia) o en nodos intermedios especializados en ofrecer servicios de seguridad. Esta última opción puede ser especialmente interesante desde un punto de vista económico, ya que un único nodo cifrador puede ofrecer servicios de seguridad a varios terminales. La figura 2.10 ilustra la conveniencia de esta opción.

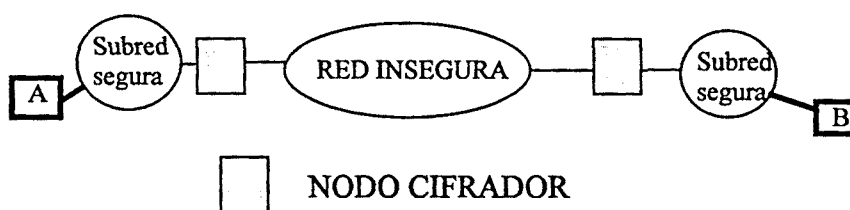


Figura 2.10. Ubicación de los servicios de seguridad en nodos intermedios de interconexión de subredes seguras a través de redes inseguras.

La opción presentada en la figura 2.10 debe tenerse muy en cuenta a la hora de interconectar subredes seguras a través de la RDSI-BA. Ejemplos de entornos de interconexión de subredes seguras pueden ser redes locales corporativas (no necesariamente han de ser redes MTA), o redes departamentales de tipo campus, como por ejemplo el entorno descrito en [REC93]. La filosofía para el diseño de un sistema de seguridad a este nivel puede ser similar a la utilizada en el proyecto CryptoNet [FOR91, FOR93, REC93, SOR93a, SOR93b, REC96]. Como ya se apuntó en alguna de las anteriores referencias, esta filosofía presenta las siguientes ventajas:

- El diseño del dispositivo de seguridad es independiente del número y tipo de nodos extremos conectados a la red
- Los servicios de confidencialidad e integridad se ofrecen de forma transparente a los usuarios y equipos conectados a cualquiera de las subredes seguras
- Las subredes seguras pueden ser de cualquier tipo (Ethernet, Token Ring, DQDB, ATM LAN, etc.). Únicamente es necesario que la red insegura utilice la tecnología MTA

- Los dispositivos de cifrado son compartidos por varios equipos, con lo cual el coste total del sistema de seguridad se reduce
- Se permite la coexistencia de tráfico seguro con tráfico inseguro
- La corporaciones que requieran servicios de seguridad y estén dispuestas a asumir su coste pueden instalar dispositivos de seguridad, que permitirán la coexistencia de tráfico inseguro y la conexión con corporaciones que no incorporen el sistema de seguridad

Sin embargo, en un entorno de aplicación como la RDSI-BA esta solución presenta un importante inconveniente que no existía en un entorno de red local de datos como en el que se enmarca el proyecto CryptoNet, y que debe ser considerado en detalle. Una red digital de servicios integrados soporta tráfico de distinta naturaleza con diferentes requisitos de calidad de servicio (QoS). Cada tipo de tráfico puede tener sus propios requerimientos de seguridad, de forma que aplicaciones de audio pueden requerir especialmente confidencialidad mientras que aplicaciones de datos utilizadas para comercio electrónico pueden requerir fundamentalmente integridad y autenticidad.

Una solución a este problema parece ser el ofrecer ambos servicios a todo el tráfico. Sin embargo esta opción, aparte de poco eficiente, continua presentando un problema importante. Cada tipo de tráfico tiene unas características y, por lo tanto, debe negociar unos parámetros de QoS propios. Mientras que en aplicaciones de datos es importante una tasa de error baja, otras aplicaciones en tiempo real como la telefonía requieren en su lugar un retardo y una variación del retardo pequeños.

La utilización de cifradores en flujo en el entorno mostrado en la figura 2.10 presenta los siguientes problemas:

- La red garantiza únicamente el orden de recepción para las celdas pertenecientes a un mismo canal virtual. Dado que en el cifrado en flujo es característica fundamental que se mantenga el orden de bits entre el cifrado y el descifrado, la opción presentada en la figura 2.8 (una misma clave para todos los trayectos virtuales) debe ser inmediatamente descartada si se pretende utilizar cifradores en flujo
- Trabajando a este nivel puede haber pérdidas de tramas, lo cual obligaría a trabajar con cifradores robustos a estas pérdidas. En caso de utilizarse cifradores en flujo, estos deberían funcionar en modo autosincronizante. En modo síncrono la pérdida de una única celda en la red provocaría la desincronización en recepción y, a partir de este momento toda la información recibida sería errónea después de su descifrado. El modo de funcionamiento

autosincronizante permitiría la resincronización al cabo de unas cuantas celdas (dependiendo del período de resincronización). Como efecto negativo presenta una importante expansión de errores

La utilización de una única clave de cifrado independientemente del destino para el entorno de la figura 2.10 parece, pues, conducir a la utilización de algoritmos de cifrado en bloque³. El requisito para obtener buenas características es que la longitud del campo de datos de la celda MTA (48 bytes) sea múltiplo de la longitud del bloque de cifrado. Ello evita que en un mismo bloque de cifrado se mezcle información perteneciente a diferentes celdas (que pueden tener destinos diferentes). Ejemplos de algoritmos de cifrado en bloque que cumplen esta característica son el DES [NBS77] y el IDEA [LAI90, LAI91, LAI92a]. Ambos algoritmos trabajan con bloques de mensajes de 64 bits, con lo que una celda MTA contiene exactamente 6 bloques cifrados, como se muestra en la figura 2.11.

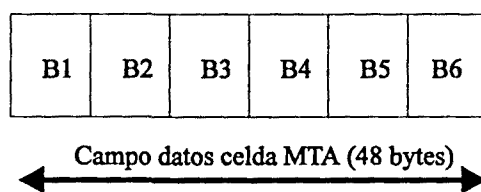


Figura 2.11. Bloques de cifrado (DES o IDEA) dentro de una celda MTA.

2.5.1.4 Cifrado a nivel físico

La ubicación del cifrado a nivel físico, tal como se muestra en la figura 2.7d, supone el cifrado de todos los bits antes de ser transmitidos por la línea. La ubicación de los servicios de seguridad a este nivel modela la red como un conjunto de conmutadores unidos por enlaces físicos, cada uno de los cuales se protege individualmente.

El servicio de confidencialidad puede ofrecerse fácilmente a cada uno de los enlaces de esta forma. En cambio, el servicio de integridad es difícilmente ubicable a este nivel, y al menos sufriría todos los inconvenientes expuestos en el punto 5.1.3. La

³ Si bien esta solución parecía tecnológicamente inviable al inicio del proyecto CRIPTO de PLANBA (1992), parece que hoy en día (1996) son posibles realizaciones hardware de dispositivos capaces de cifrar a velocidades compatibles con la de la red. En concreto [STE95] menciona un prototipo capaz de cifrar en DES modo CBC a velocidades del orden de Gigabits por segundo.

única solución plausible consistiría en introducir bits adicionales en la línea para poder utilizar un código comprobador de la integridad.

Para el servicio de confidencialidad, esta solución presenta las siguientes ventajas:

- Se protege todo tipo de tráfico (información de usuario, de control o de gestión) que se transmita sobre el enlace físico
- Permite ofrecer servicios de seguridad de forma transparente a todos los protocolos de nivel superior. De hecho el único parámetro de red que condiciona esta solución es la velocidad de transmisión, que impondrá una velocidad de cifrado
- Ofrece protección natural contra ataques por análisis de tráfico, ya que todas las cabeceras se transmiten cifradas impidiendo que un atacante conozca el destino de la información
- Es posible proteger la información sólo sobre enlaces críticos

Sin embargo esta opción presenta los siguientes inconvenientes:

- La información debe descifrarse en cada conmutador MTA para consultar la información de enrutamiento perteneciente a la cabecera MTA. Ello implica dos inconvenientes. El primero es el incremento de procesado que esto implica, ya que cada unidad de información deberá cifrarse y descifrarse $N+1$ veces siendo N el número de conmutadores por los que pasa la celda. El segundo es que no se ofrece protección contra ataques dentro de los conmutadores, ya que allí la información está en claro
- Se debe ofrecer el mismo nivel seguridad a toda la información, independientemente de su naturaleza, ya que a este nivel no es posible ofrecer un interfaz para que las aplicaciones demanden niveles de seguridad
- La información de todos los usuarios se cifra con la misma clave
- La distribución de claves puede ser bastante costosa, al igual que la protección de los conmutadores de la red

2.5.2 Gestión de Claves

La gestión de claves es el mecanismo mediante el cual se negocia una o varias claves para cifrar una comunicación. Juega un papel fundamental para proporcionar los servicios de confidencialidad e integridad. De los muchos aspectos que engloba la gestión de claves (ver capítulo 5, para mayor detalle), el aspecto más relacionado con la ubicación lógica en la red es la distribución de claves. Esta distribución debe realizarse previamente a la comunicación para poder ofrecer los servicios de seguridad. Existen básicamente dos tipos de protocolos de distribución de claves:

- *Intercambio directo*: La información para establecer la clave se intercambia entre las dos entidades involucradas en la comunicación. Posteriormente esta clave (o conjunto de claves) se utilizará para proteger los datos a transmitir entre ellos
- *Intercambio con un centro de gestión de claves*: Durante el proceso de establecimiento de las claves, se intercambia información con un centro de gestión de claves

En el caso de intercambio con un centro, el nivel de aplicación parece ser la única opción viable, ya que el centro de gestión de claves estará representado por una entidad a nivel de aplicación. La opción a utilizar en una red orientada a conexión como la RDSI-BA es abrir una conexión de corta duración con el centro para realizar la distribución de claves.

En el caso de intercambio directo deben considerarse dos alternativas:

1. El intercambio de claves se hace a nivel de aplicación. Ello implica que debe abrirse una conexión para negociar las claves que se utilizarán para proteger la conexión sobre la que transcurre la comunicación
2. La gestión de claves se realiza al mismo nivel que los servicios de seguridad que se den (es decir, en cualquiera de las opciones presentadas en la figura 2.6), previamente a la transmisión de datos. La forma más sencilla parece la inclusión de la gestión de claves en los procedimientos de establecimiento de conexión. En la RDSI-BA esta aproximación significa la ubicación de la distribución de claves en el plano de control del MRP. Seguidamente toda la transferencia de datos de usuarios pertenecientes al plano de usuario se protegerá con estas claves

La opción (2) puede resultar más eficiente bajo cierto punto vista (no es necesario establecer una conexión adicional). Sin embargo su adopción supone introducir modificaciones en la señalización (plano de usuario) que permitan la gestión de claves. En cualquier caso parece que la libertad de negociación de parámetros de seguridad (entre ellos las claves) puede ser bastante más limitada utilizando el plano de control que el de usuario, a no ser que se modificase excesivamente el plano de control para incluir la negociación exhaustiva de parámetros de seguridad. En el capítulo 3 de esta Tesis se muestra como una conexión adicional puede ser utilizada para negociar un gran número de parámetros de seguridad, entre los que se incluye las claves de sesión.

Puede ser conveniente ofrecer servicios de seguridad únicamente a aquellas aplicaciones que manipulan información crítica, independientemente del nivel al que luego se ofrezcan estos servicios. En consecuencia, la gestión de claves debería ubicarse a nivel de aplicación para obtener una interfaz adecuada con los usuarios y las aplicaciones.

2.5.3 Autenticación

Autenticación es el servicio de seguridad que garantiza la identidad de las entidades involucradas en la comunicación. En el entorno de redes de comunicaciones se distinguen dos tipos de autenticación:

- *Autenticación de entidad*: Que asegura de la identidad de las entidades participantes en una comunicación
- *Autenticación de origen de información*: Que asegura que una unidad de información proviene de cierta entidad

Para autenticación de entidad, la ubicación del servicio de autenticación dentro del MRP de la RDSI-BA dependerá de la entidad que quiera autenticarse. Si quieren autenticarse diferentes aplicaciones individualmente, el servicio de autenticación deberá ubicarse a nivel de aplicación. Lo mismo ocurre si se desea identificación de usuarios individualmente o si se desea que la autenticación soporte control de acceso basado en la identidad de individuos.

Para la autenticación de sistemas extremos (por ejemplo, terminales) parece más conveniente la ubicación a niveles más bajos. Si desea autenticarse únicamente el extremo comunicante será suficiente con la ubicación de este servicio entre los niveles MTA y AAL, mientras que si desea autenticarse también las cabeceras del nivel de adaptación del que proviene el servicio, la autenticación deberá darse por encima del

nivel AAL. En entornos de interconexión de redes la autenticación de entidad deberá darse por encima del nivel donde se defina el identificador de entidad en el entorno de interconexión. En Internet, por ejemplo, la autenticación deberá darse por encima del nivel IP (o por encima de TCP si quiere autenticarse el *socket* completo).

Por encima de nivel físico únicamente podremos autenticar enlaces físicos individuales entre diferentes nodos de la red.

Para la autenticación de una conexión puede ser muy útil integrar la autenticación en el mecanismo de establecimiento de la conexión. En la RDSI-BA esta solución pasaría por la integración de los mecanismos de autenticación en el plano de control. Otra solución consiste en autenticar las entidades por una conexión de datos independiente, que comporta la ventaja de no interferir con la señalización definida para la red (es decir, se realiza de forma transparente para la red).

El mecanismo de distribución de claves deberá estar autenticado. Por ello es interesante ubicar la autenticación en el nivel de aplicación para, al igual que la gestión de claves, proporcionar una interfaz sencilla a usuarios y aplicaciones. En realidad una autenticación mutua será necesaria durante el proceso de negociación de una clave de sesión con la cual posteriormente proporcionar cualquier servicio de seguridad. Posteriormente, toda la comunicación cifrada con esta clave estará también autenticada, con lo que se podría asegurar autenticación de origen de datos.

La criptografía asimétrica proporciona una serie de ventajas sobre la criptografía simétrica cuando es usada para la autenticación. Entre estas ventajas se encuentran un soporte más natural para la autenticación ante receptores múltiples, un mejor soporte para el servicio de no repudio y el eliminar la necesidad de claves secretas proporcionadas por un servidor central.

2.5.4 Control de Acceso

Autorización es la cesión de derechos, por el propietario o controlador de un recurso, de que otros usuarios accedan a ese recurso. El control de acceso es un medio para controlar esta autorización, evitando que usuarios no autorizados accedan a recursos (información, capacidad de cálculo, nodos de comunicaciones, entidades físicas, etc.).

Si el control de acceso se desea hacer en función de usuarios finales, el nivel de aplicación es sin lugar a dudas la mejor alternativa para ubicar este servicio.

Sin embargo, esta alternativa es a veces costosa en grandes redes con muchos usuarios, ya que supone que los sistemas accedan a información distribuida necesaria para identificar a estos usuarios. Por eso muchas veces se controla el acceso en función del nodo extremo, permitiéndose por ejemplo acceder a una subred privada en función del dominio de la red donde se ubique el usuario que pretende acceder al sistema. Este control de acceso puede realizarse a niveles más bajos, como por encima de AAL y entre MTA y AAL.

2.5.5 No Repudio

El servicio de no repudio ofrece protección a un usuario frente a que otro usuario niegue posteriormente que en realidad se realizó cierta comunicación. Esta protección se realiza por medio de una colección de evidencias irrefutables que permitirán la resolución de cualquier disputa. En concreto el no repudio de envío protege al emisor de que el receptor niegue haber recibido el mensaje, mientras que el no repudio de origen protege al receptor de que el emisor niegue haber enviado el mensaje. La criptografía de clave pública y más concretamente las firmas digitales juegan un papel esencial en este servicio. El proceso de no repudio involucra árbitros de confianza neutrales y aceptados por ambas partes involucradas.

La ubicación del servicio de no repudio es bastante simple. Debe ser ubicado a nivel de aplicación, ya que es un servicio específico de algunas aplicaciones y además se aplica únicamente a algunos campos del protocolo de aplicación.

2.5.6 Resumen de las posibilidades de ubicación de los servicios de seguridad

La tabla 2.1 resume en cierta forma lo discutido en el apartado 5 de este capítulo.

	Debajo de aplicación	Encima de nivel AAL	Entre niveles MTA y AAL	Entre niveles MTA y físico
Confidencialidad	Posible	Posible	Posible	Posible
Integridad	Posible	Posible	Muy desaconsejable	Muy desaconsejable
Autenticación	Autenticación de aplicaciones y usuarios finales. Soporte de control de acceso basado en identidad. Autenticación entidad extrema desde aplicación de datos	Autenticación de conexión desde plano de control (por encima de AAL 5)	Autenticación de equipos extremos	Autenticación de un enlace físico entre nodos intermedios (difícilmente útil para usuarios)
Control de acceso	Control de acceso basado en identificación de usuarios y aplicaciones	Control de acceso a equipos extremos	Control de acceso a equipos extremos y nodos intermedios	NO
No repudio	Necesario ubicarlo a nivel de aplicación	NO	NO	NO
Gestión de claves	Preferible	Posible	Posible	Posible

Tabla 2.1. Posibilidades de ubicación de los servicios de seguridad y gestión de claves en el MRP de la RDSI-BA.

2.6 Ejemplo: El Proyecto CRIPTO del Plan Nacional de Banda Ancha (PlanBA)

La discusión del apartado 2.5 deja muchas opciones abiertas y apunta las ventajas e inconvenientes que comporta la adopción de diferentes alternativas. Sin embargo, a la hora de diseñar un sistema concreto de seguridad deben concretarse los

servicios de seguridad que se ofrecerán (que dependerán de las amenazas presentes en la red y de las posibilidades tecnológicas y económicas de cubrir estas amenazas). Una vez concretados los servicios, el siguiente paso es escoger su ubicación lógica dentro de la arquitectura de red. Para ello deben valorarse las ventajas e inconvenientes anteriormente descritas, y en función de ellas escoger un nivel adecuado para la implantación de estos servicios.

Como ejemplo de lo anteriormente expuesto nos permitimos presentar un proyecto que se desarrolló en el marco del Plan Nacional de Banda Ancha (PlanBA), el proyecto CRIPTO [FOR95a].

El propósito del Plan nacional de Banda Ancha (1992-1995) fue promover el desarrollo conjunto entre centros de investigación públicos y privados en el área de las comunicaciones de banda ancha. Dos proyectos enmarcados en este plan fueron TEMA y CRIPTO. El propósito del primero fue el de desarrollar un terminal multimedia mientras que el del segundo fue el proveer servicios de seguridad en la operación y comunicaciones de estos terminales multimedia conectados a RDSI-BA.

En la elección de la ubicación lógica de los servicios de seguridad dentro de la torre de protocolos MTA la arquitectura del terminal multimedia definida por otro proyecto (TEMA) jugó un papel esencial. Por ello es interesante que se presente brevemente esta arquitectura.

2.6.1 Proyecto TEMA

Uno de los objetivos del Plan nacional de banda ancha fue el desarrollo de un terminal multimedia que permitiese a los usuarios el acceso a la RDSI-BA y sirviese de plataforma para desarrollar nuevos servicios y aplicaciones. [MAR93] presenta alguno de estos servicios.

En la figura 2.12 se aprecia que la arquitectura del terminal multimedia consta de dos módulos: una estación de trabajo y un módulo auxiliar conectados entre sí por un enlace Ethernet. Mientras que las aplicaciones de datos se encuentran normalmente sobre la estación de trabajo, las aplicaciones que utilizan audio y vídeo utilizan dispositivos de entrada/salida ubicados en el Módulo Auxiliar. En este módulo se encuentran también los elementos necesarios para realizar la conexión a RDSI-BA.

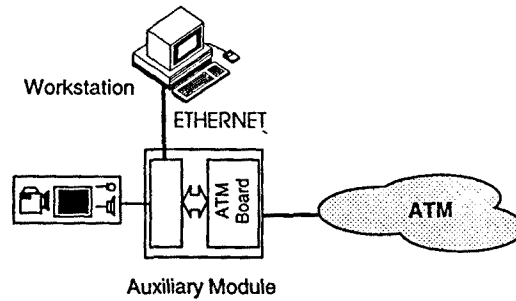


Figura 2.12. Estructura del terminal multimedia definido por el proyecto TEMA.

La figura 2.13 presenta la arquitectura física del módulo auxiliar, que como se verá más adelante condiciona la ubicación de los servicios de seguridad.

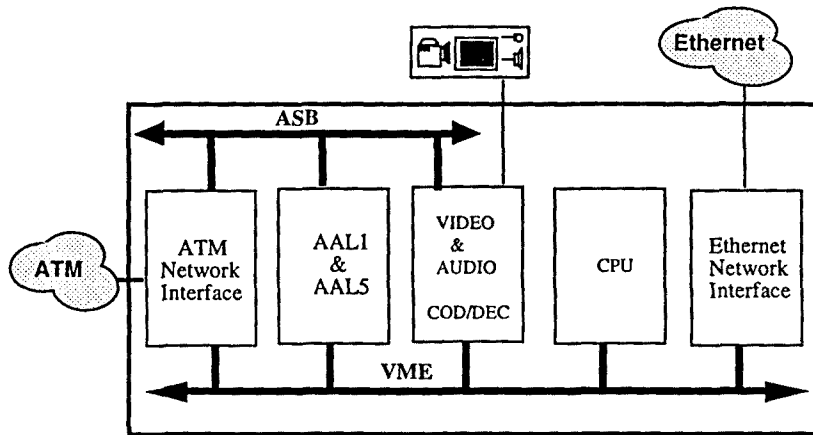


Figura 2.13. Arquitectura física del módulo auxiliar del terminal multimedia TEMA.

Las aplicaciones de vídeo y audio acceden a sus correspondientes codificadores y decodificadores (por ejemplo, MPEG, JPEG, etc.). Una vez codificada, esta información se envía a las tarjetas que integran los niveles de adaptación MTA (AAL-1 y AAL-5) a través del bus VME. Las aplicaciones de datos ubicadas en la workstation acceden al módulo auxiliar a través de una interfaz Ethernet. Desde la CPU del módulo auxiliar estos datos se envían a las tarjetas AAL y ATM a través del bus VME para que sean encapsulados con los protocolos propios de la RDSI-BA. El bus síncrono MTA (ASB) permite la transmisión de tráfico bidireccional MTA entre el interfaz de red MTA y el resto de componentes que permiten la adaptación de diferentes servicios estándar de banda ancha. La capacidad de transmisión de este bus es de 160 Mbit/s en cada dirección.

2.6.2 Proyecto CRIPTO

El principal objetivo del proyecto CRIPTO fue demostrar la viabilidad de la integración de servicios de seguridad en el terminal multimedia a fin de conseguir comunicaciones seguras en la red PlanBA. Los servicios de seguridad contemplados son la confidencialidad e integridad en el transporte de información sensible, autenticación entre terminales, gestión de claves sobre la misma red y control de acceso de los usuarios de cada terminal. Está previsto además que en un futuro se puedan prestar servicios tales como firma digital de documentos utilizando para ello los mecanismos diseñados en principio para la gestión de claves. El proyecto CRIPTO se dividió básicamente en tres partes: cifrado de la información, control de acceso y gestión de claves.

2.6.2.1 Cifrado de la información

El servicio de confidencialidad se ofrece mediante un cifrador en flujo [RUE86]. Se realiza un cifrado hardware en varios ASICs especialmente diseñados para esta aplicación [GUI94]. La figura 2.14 muestra un esquema del cifrador utilizado.

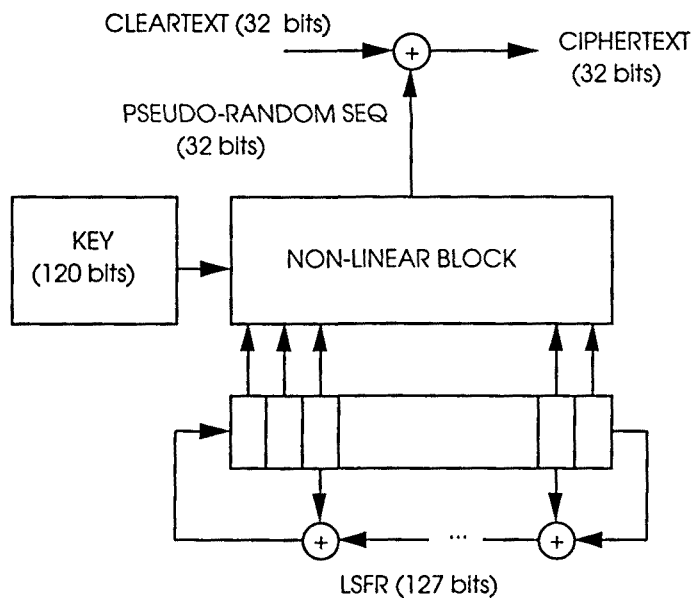


Figure 14. Estructura del cifrador en flujo utilizado en el proyecto CRIPTO.

El cifrador en flujo está compuesto por un registro de desplazamiento realimentado linealmente (LFSR, *Linear Feedback Shift Register*), y un bloque no lineal utilizado para obtener diferentes salidas (32) a partir de cada estado del LFSR. El bloque

no lineal utiliza una clave de 120 bits, mientras que el estado del LFSR debe inicializarse mediante una semilla de 127 bits, que constituirá su estado inicial. Todo ello provoca la utilización de claves de sesión de 247 bits (127+120).

El dispositivo ha sido diseñado para poder trabajar tanto en modo síncrono como autosincronizante. El modo autosincronizante es necesario ya que como se verá más adelante el cifrado se decidió ubicar entre los niveles MTA y AAL (es decir, se adoptó la opción mostrada en la figura 2.7c de este capítulo). Como se ha comentado en el apartado 5.1.3, a este nivel no se garantiza el flujo de la información, es decir, pueden perderse celdas en la red. Si se utilizase un cifrador en flujo en modo síncrono, la pérdida de una celda provocaría una desincronización del cifrado en recepción que ya no podría volver a recuperarse. Un cifrador en flujo en modo autosincronizante recupera el sincronismo al cabo de cierto tiempo, por lo que la pérdida de una celda únicamente provoca un bloque de errores. Este modo de funcionamiento tiene como inconveniente provocar una expansión de los bits erróneos en todo el bloque.

2.6.2.2 Autenticación y control de acceso

El control de acceso de los usuarios a los terminales es un punto clave para garantizar la seguridad del sistema. Es esencial que usuarios no autorizados no puedan acceder a ciertos recursos, como terminales o servidores, a la vez que es necesario controlar los permisos de acceso a la información (lectura, modificación o ejecución de programas). Para ello es fundamental garantizar una identificación segura de los usuarios. Ello puede conseguirse mediante mecanismos apropiados de autenticación. En nuestro entorno se deben considerar tres tipos de autenticación:

- Autenticación entre usuarios
- Autenticación de terminal ante usuario y de usuario ante terminal (identificación)
- Autenticación entre terminales

La primera opción (autenticación entre usuarios finales), implica que ambos usuarios que participan en una comunicación se autentican mutuamente⁴. Cada usuario del sistema de seguridad deberá tener asociadas unas credenciales (claves asociadas a identificador de usuarios) que deberán ser guardadas en dispositivos seguros tales como

⁴Para el caso de comunicaciones punto a punto. Para comunicaciones multipunto deberá, al menos, autenticarse mutuamente emisor y cada uno de los receptores, o puede ser necesaria una autenticación de todos ante todos, para servicios tales como la teleconferencia.

tarjetas inteligentes. Esta opción proporciona el mejor nivel de seguridad, pero el coste de la gestión de claves puede ser muy alto si el número de usuarios es muy alto.

Otro aspecto importante es la identificación de usuarios por parte de los terminales. Una autenticación mutua sería conveniente en el caso de que los usuarios no confiaran a priori en los terminales. Una combinación de identificación y autenticación entre terminales puede usarse en ciertas ocasiones para proporcionar autenticación entre usuarios finales. Esto es posible porque dos terminales mutuamente autenticados podrán confiar que el usuario que se ha identificado correctamente en el otro terminal sea quien pretende ser. Esta es precisamente la opción que se escogió para el proyecto CRIPTO.

La criptografía asimétrica proporciona una serie de ventajas sobre la criptografía simétrica cuando es usada para la autenticación. Entre estas ventajas se encuentran un soporte más natural para la autenticación ante receptores múltiples, un mejor soporte para el servicio de no repudio y el eliminar la necesidad de claves secretas proporcionadas por un servidor central.

En la mayoría de sistemas actualmente en funcionamiento la identificación de usuarios está basada en sistemas de logins y passwords, con claros problemas de seguridad. En el proyecto CRIPTO se propone la utilización de seguridad criptográfica para la identificación de los usuarios en los terminales multimedia. Los mecanismos que se desarrollaron para la verificación de la identidad de los usuarios están basados en PINs (o BIOPINs) y tarjetas inteligentes que contienen claves criptográficas protegidas contra la lectura. Cada usuario autorizado deberá poseer una tarjeta inteligente para poder identificarse ante los terminales en los que esté registrado. El equipo para físico para la introducción de PINs y reconocimiento de información biométrica (huellas digitales) se conecta a la estación de trabajo de cada terminal multimedia a través de un puerto serie (RS-232), lo que permite que este equipo pueda ser reutilizado en otros entornos.

2.6.2.3 Gestión de Claves

Las claves secretas requeridas por el cifrado en flujo (claves de sesión) deben ser negociadas por los dos terminales implicados. Esta negociación se realiza sobre la misma red utilizando protocolos de gestión de claves. Puesto que la red es en principio insegura, estos protocolos deben ser protegidos utilizando algún mecanismo criptográfico adecuado. En la solución adoptada se utiliza el algoritmo de clave pública RSA [RIV77] utilizando para ello una implementación *hard/soft* basada en un procesador DSP56001 de Motorola. Durante la gestión de claves se produce una

autenticación bidireccional de los terminales involucrados. En el capítulo 5 de esta tesis se especifica el protocolo de gestión de claves utilizado en este proyecto.

2.6.3 Arquitectura del Sistema de Seguridad

2.6.3.1 Ubicación del cifrado

Como se ha señalado anteriormente, una decisión importante que condiciona el proyecto CRIPTO es la ubicación del cifrado de la información en el MRP de la RDSI-BA. Dado que se desea incorporar la seguridad en los terminales extremos, deben considerarse las posibilidades mostradas en las figuras 2.7a, 2.7b y 2.7c. La opción de la figura 2.7d debe ser inmediatamente descartada, ya que no permite un cifrado extremo a extremo. Todas las ventajas e inconvenientes señalados en el apartado 2.5 debieron ser consideradas. De todos modos, el punto que más influyó en la ubicación final del cifrado de la información fue la estructura particular del terminal multimedia.

La ubicación del cifrado inmediatamente debajo del nivel de aplicación (figura 2.7a) facilitaría enormemente el interfaz con la aplicación y el establecimiento de asociaciones de seguridad. Sin embargo esta solución debió ser abandonada inmediatamente debido a la particular arquitectura del terminal multimedia. Mientras que muchas aplicaciones de datos se encapsulan en protocolos de comunicaciones (como TCP/IP) en la estación de trabajo, otro tipo de aplicaciones multimedia (vídeo y audio) acceden directamente al módulo auxiliar. En consecuencia no existe a este nivel un único punto donde el dispositivo cifrador pudiese ofrecer seguridad a toda la información multimedia.

La siguiente posibilidad que se estudió fue la ubicación del cifrado justo por encima del nivel AAL (figura 2.7b). Esta solución parecía buena, ya que el cifrador podría ubicarse en el módulo auxiliar del terminal multimedia, donde se ubican las tarjetas que ofrecen los diferentes niveles de adaptación. La mejor solución parecía la conexión de una tarjeta de cifrado al bus VME que se encargaría del cifrado y descifrado de la información que tuviese como origen o destino las tarjetas AAL. Desafortunadamente, esta solución tiene los siguientes inconvenientes importantes:

1. Se provoca un incremento del tráfico en el bus VME. De esta manera, este bus podía llegar a convertirse en el "cuello de botella" del terminal multimedia
2. Se definieron algunos servicios que accedían al terminal directamente a través del bus ASB. Por lo tanto, este tráfico no accedía al bus VME y, por lo tanto, no podía ser cifrado

Este último motivo forzó la ubicación lógica del cifrado entre el nivel MTA y el nivel de adaptación (figura 2.7c). Todo tipo de información que accede a la red debe pasar forzosamente por el bus ASB, que no es más que una extensión de la propia red: las celdas MTA viajan a través de este bus en palabras de 16 bits, con el mismo formato que en la red MTA. Por lo tanto, toda la información multimedia (datos, voz y vídeo) puede cifrarse en este punto. De esta forma, la clave es seleccionada en función del identificador de trayecto virtual (VPI y VCI) de la celda MTA, y se cifra todo el campo de datos de la celda, dejando las cabecera en claro para que sea posible el enrutamiento de la información.

Para resolver los problemas apuntados en el apartado 5.1.3 debidos a la pequeña longitud de las unidades de datos a este nivel y los fuertes requisitos de rapidez de conmutación de claves para un cifrador a este nivel⁵ se optó por integrar en el ASIC de cifrado varios cifradores en flujo que trabajarían en paralelo, y limitar el número de comunicaciones cifradas simultáneas que podían ser cifradas al número de cifradores que se integrasen en la tarjeta de cifrado. De otra forma con la tecnología del momento (1993-1994) no hubiese sido posible solucionar el problema anteriormente señalado.

2.6.3.2 Arquitectura del sistema de seguridad propuesto en el proyecto CRIPTO

La integración de la arquitectura de seguridad sobre la del terminal multimedia TEMA se presenta de forma esquemática en la figura 2.15. Dado que uno de los requisitos del proyecto es que sólo las aplicaciones que lo requieran sean protegidas, se ubicó la gestión de claves en el nivel de aplicación. De esta forma se simplifica la construcción de una interfaz adecuada con las aplicaciones. Así pues, la entidad de gestión de claves es una aplicación más situada en la estación de trabajo. Puesto que esta aplicación requiere de mecanismos de cifrado RSA, utiliza un módulo físico para llevar a cabo los cálculos RSA de forma eficaz, conectado a la estación de trabajo mediante un puerto serie RS-232. Hay que señalar que este módulo de cifrado RSA está ubicado en una misma caja con el módulo físico de control de acceso y comparte con él un puerto serie.

⁵ Máxime teniendo en cuenta que se trata de un cifrador en flujo que utiliza claves muy largas y que cada vez que se conmute de canal debe guardarse además el estado del LFSR.

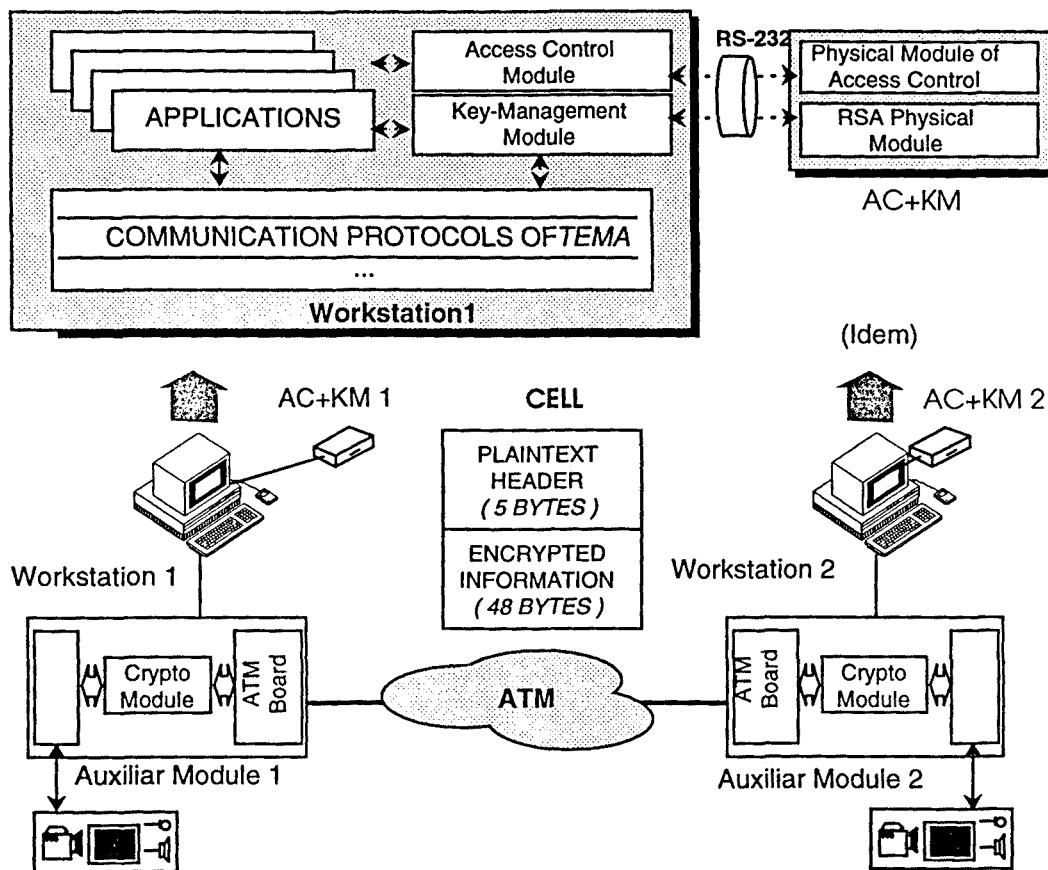


Figura 2.15. Arquitectura del sistema de seguridad propuesto.

Un problema fundamental en una estructura como la propuesta, donde la gestión de claves se ubica a nivel de aplicación y el servicio de confidencialidad se ofrece por encima del nivel MTA, es la asociación de seguridad, es decir, como se transmiten las claves desde el nivel de aplicación al nivel que proporciona el cifrado, y como a este nivel se identifica la clave que debe utilizarse en función de las cabeceras disponibles.

2.7 Conclusiones y Aportaciones

En este capítulo se han comparado diferentes posibilidades para la ubicación de servicios genéricos de seguridad definidos por [ISO88] (autenticación, confidencialidad, control de acceso, integridad y no repudio) dentro del modelo de referencia (MRP) de protocolos de la red digital de servicios integrados de banda ancha (RDSI-BA) [CCI92d, CCI92e]. Se ha estudiado la inclusión de los servicios de seguridad en el plano de usuario definido por el MRP para no interactuar con la señalización y gestión de red, muchos de cuyos aspectos están actualmente en fase de definición.

Se ha optado por intercalar niveles de seguridad entre las diferentes capas definidas por el MRP. De esta forma no es necesaria la modificación de ninguno de los niveles definidos, sino que la inclusión de estas capas de seguridad ofrece servicios de seguridad de forma transparente a los protocolos de nivel superior. La inclusión de un nivel de confidencialidad entre el nivel MTA y AAL, por ejemplo, haría que para los diferentes protocolos del nivel de adaptación (AAL-1, AAL-2, AAL-3/4 y AAL-5), el nivel MTA ofreciese este servicio. La tabla 2.1 resume las principales opciones para la ubicación de cada uno de estos servicios, así como del mecanismo de gestión de claves. Algunos de estos resultados se adelantaron en [CRU95] y [FOR95b]. Este trabajo es totalmente novedoso, y éstas son las dos primeras publicaciones que conocemos hagan referencia a este tema.

Existen también otra serie de factores que condicionan la ubicación de los servicios de seguridad. Como ejemplo se presenta la ubicación lógica del cifrado que se adoptó en el proyecto CRIPTO perteneciente al Plan Nacional de Banda Ancha (PlanBA). En este proyecto la arquitectura del terminal multimedia definido jugó un papel decisivo en la ubicación del cifrado. Se presenta también la arquitectura de seguridad del proyecto CRIPTO, en la definición de la cual participamos de forma relevante [FOR95a]. Por las noticias que tenemos, este proyecto fue pionero a nivel mundial en contemplar aspectos de seguridad en redes MTA. Durante el desarrollo del proyecto (1993-1994) no se conocen publicaciones a nivel internacional que hagan referencia a estudios de este tipo, aunque publicaciones posteriores [STE95, DEN95] muestran la existencia de proyectos similares desarrollados en paralelo. [STE95] en concreto hace referencia a un proyecto para ofrecer servicios de seguridad a una red MTA experimental, en concreto la *North Carolina Information Highway* (NCIH). Ello muestra el interés de ofrecer servicios de seguridad en una tecnología que está llamada a representar el futuro de las telecomunicaciones.

CAPÍTULO 3

Arquitectura del Sistema de Seguridad

3.1 Introducción

En el capítulo anterior se estudiaron diferentes alternativas para la ubicación de los servicios de seguridad en la arquitectura de la RDSI-BA, enumerando ventajas e inconvenientes de cada una de ellas. En este capítulo se propone un sistema de seguridad para proteger las comunicaciones entre terminales multimedia conectados a través de la RDSI-BA, en un escenario que se detalla en la sección 2.

Para ello en primer lugar se razonan una serie de requisitos a exigir al sistema de seguridad que se proponga. Seguidamente, en consonancia con las alternativas propuestas en el capítulo anterior y en función de esta serie de requisitos, se estudia la mejor ubicación posible de cada uno de los servicios de seguridad.

Una vez elegida la ubicación de cada uno de los servicios, se propone la arquitectura de un sistema de seguridad distribuido capaz de ofrecer servicios de seguridad de forma integrada para todo tipo de aplicaciones multimedia que puedan ofrecerse sobre terminales conectados a la RDSI-BA.

Una característica fundamental del sistema propuesto es que permite negociar servicios y niveles de seguridad en función de requerimientos específicos de las aplicaciones. Los mecanismos de seguridad finalmente empleados para proteger la comunicación se negociarán entre los terminales involucrados en función de los solicitados por las aplicaciones sensibles (que incluirán parámetros de calidad de servicio) y de la disponibilidad de mecanismos de seguridad en los terminales.

Seguidamente se especifican las primitivas mediante las que las aplicaciones sensibles negociarán servicios de seguridad con el sistema de seguridad, y las primitivas que definen las comunicaciones entre las entidades que negocian los parámetros de seguridad en función de la disponibilidad de los terminales involucrados.

Por último se presenta un ejemplo de operación del sistema de seguridad.

Gran parte de lo expuesto en este capítulo fue adelantado en parte en [FOR96a] y en parte en [FOR96c].

3.2 Escenario a Proteger

Aunque la RDSI-BA permite la conexión de terminales que soporten únicamente voz, vídeo o datos, se espera que los terminales multimedia sean el soporte a través del cual servicios de datos, vídeo y voz accederán a la futura red de banda ancha.

La figura 3.1 muestra dos terminales multimedia que se comunican a través de la red de banda ancha. Cada terminal posee una interfaz adecuada para aplicaciones de vídeo y audio, y para conectarse a la RDSI-BA

El escenario presentado en la figura 3.1 será muy habitual en la futura RDSI-BA, donde es de esperar que se soporten un gran número de servicios. Muchos de estos servicios de banda ancha requerirán servicios de seguridad tales como autenticación, confidencialidad, control de acceso, integridad o no repudio, cuya implementación deberá hacer uso de los mecanismos de seguridad apropiados.

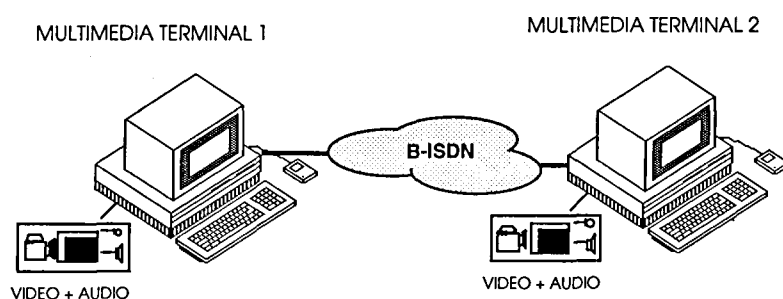


Figura 3.1. Escenario A: terminales multimedia directamente conectados a la RDSI-BA.

Aunque el propósito de este capítulo es proponer un sistema de seguridad para terminales multimedia directamente conectados a la RDSI-BA, tal como muestra la figura 3.1 (escenario A), no se puede olvidar la existencia de escenarios de

interconexión de redes. Este tipo de escenarios será muy habitual, especialmente durante los inicios de la tecnología MTA, cuando muchos usuarios utilizarán la red para aplicaciones de interconexión de LANs y MANs a alta velocidad. Con el tiempo se espera que la tecnología MTA vaya sustituyendo la tecnología actual de las redes locales, con lo que el escenario A será cada vez más popular.

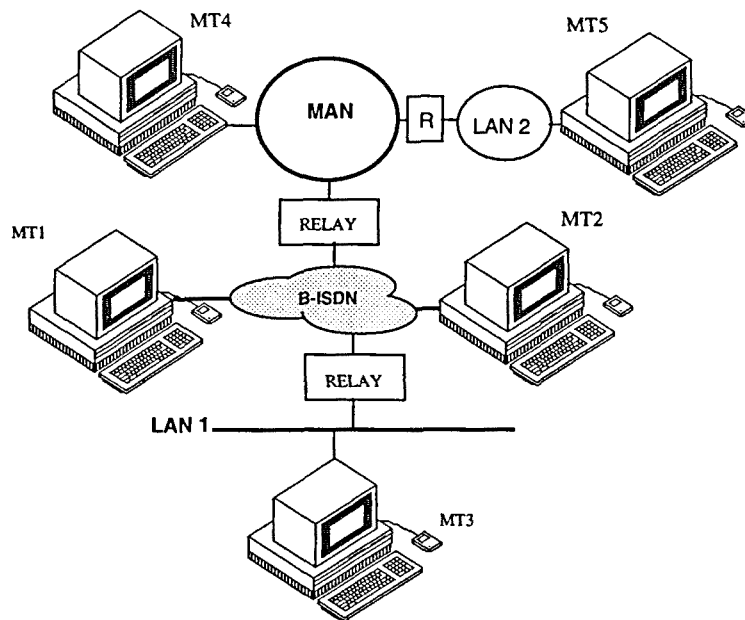


Figura. 2. Escenario B: algunos terminales están directamente conectados a la RDSI-BA, mientras que otros acceden a ella a través de redes locales y metropolitanas.

La figura 3.2 ilustra un escenario de interconexión de redes que denominamos escenario B. Puede observarse que los terminales multimedia MT1 y MT2 acceden directamente a la red de banda ancha, MT3 accede a través de una red de área local, MT4 a través de una red metropolitana y MT5 a través de una LAN conectada a la RDSI-BA mediante una MAN.

El sistema de seguridad que proponemos para el escenario A deberá poder coexistir con el escenario de interconexión B.

3.3 Requisitos para el Sistema de Seguridad

El sistema de seguridad que se propone deberá cumplir las siguientes premisas:

- *REQUISITO 1. El sistema de seguridad debe ofrecer servicios de seguridad únicamente a las aplicaciones sensibles*

No tiene sentido el cifrado de toda la información no clasificada, a la vez que es ineficiente desde un punto de vista económico. Por otra parte las necesidades de servicios de seguridad varían enormemente entre diferentes aplicaciones. Mientras que integridad y autenticidad son esenciales para aplicaciones tales como comercio electrónico, otro tipo de aplicaciones requieren otro tipo de servicios como confidencialidad o no repudio. Desde este punto de vista, ofrecer todos los servicios de seguridad para cada aplicación sería complicado, ineficiente y comportaría un coste elevado.

Como consecuencia el sistema de seguridad deberá disponer de una interfaz con las aplicaciones (API), a través de la cual las aplicaciones sensibles soliciten los servicios de seguridad requeridos.

- *REQUISITO 2. Debe existir una correspondencia entre las aplicaciones y las claves de sesión utilizadas*

Distintas aplicaciones requerirán servicios y niveles de seguridad diferentes. Por ello deberán utilizarse claves diferentes para ofrecer servicios de seguridad a información procedente de distintas aplicaciones.

La compartición de claves por distintas aplicaciones es desaconsejable incluso cuando éstas requieran los mismos servicios con el mismo grado de seguridad. Ello es debido a que diferentes aplicaciones requerirán en general distintos parámetros de calidad de servicio (QoS), tales como tasa, probabilidad de pérdida de celda, retardo o variaciones del retardo, etc. Si se utilizase una única clave de cifrado y un único dispositivo cifrador para todas ellas se impediría mantener diferentes parámetros de QoS para las diferentes aplicaciones.

Bajo nuestro punto de vista, la seguridad es otro parámetro similar a los de QoS y, por lo tanto, sería interesante incluir aspectos de seguridad durante el periodo de negociación de QoS en la estructura de señalización de la B-ISDN. Sin embargo, como ya ha sido previamente mencionado, ello implicaría una modificación de la señalización que consideramos fuera del ámbito de este trabajo.

- *REQUISITO 3. El mecanismo de cifrado debe ser rápido*

La velocidad de transmisión de la información en una red de banda ancha es muy elevada. Ello obliga a que el proceso de cifrado sea muy rápido; de otra forma constituiría un cuello de botella y se perderían tramas. En consecuencia, es evidente la necesidad de un cifrador de alta velocidad.

Actualmente, los cifradores en flujo [RUE86] son una buena opción para conseguir mecanismos de cifrado rápidos. Las técnicas de cifrado en flujo consisten en generar una secuencia pseudoaleatoria que se suma al mensaje (módulo 2), obteniéndose así el texto cifrado. La misma secuencia pseudoaleatoria se genera en el receptor, y al sumarle el texto cifrado se obtiene el mensaje en claro.

Como se ha comentado en el capítulo 2, puede ocurrir que no exista garantía de sincronización en recepción (es decir, puede que se pierda información). En tales circunstancias, si se selecciona un cifrador en flujo, debería ser capaz de trabajar en modo autosincronizante. La figura 3.3 muestra el esquema de un cifrador en flujo síncrono y un cifrador autosincronizante.

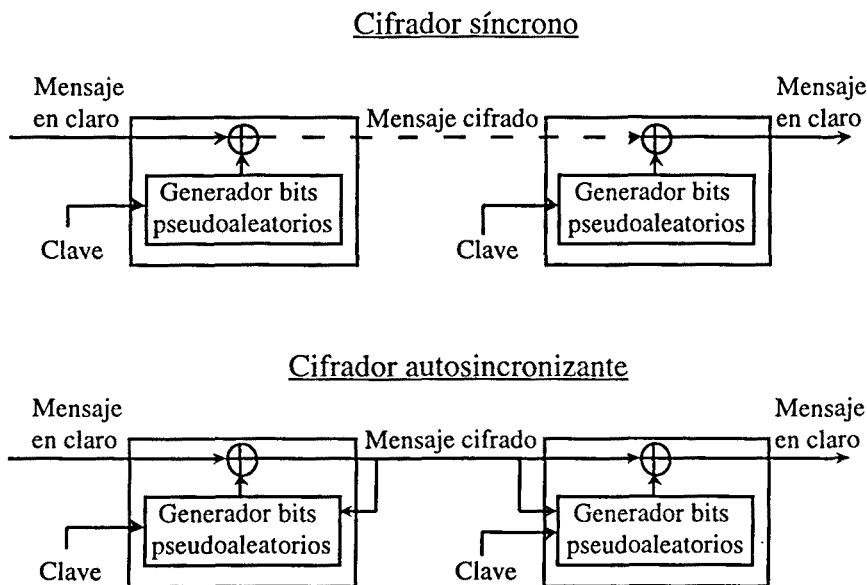


Figura 3.3. Cifradores en flujo síncrono y autosincronizantes.

Una de las características de los cifradores síncronos es que si se pierde un bit en el texto cifrado, el mensaje restante a partir de dicho bit se recibirá incorrectamente. Sin embargo, en los cifradores autosincronizantes la secuencia pseudoaleatoria depende del

texto cifrado, permitiendo que cuando hay pérdidas el sistema sea capaz de recuperarse al cabo de n bits, siendo n la memoria del cifrador.

La alta velocidad de las aplicaciones de banda ancha hace necesaria realizaciones hardware de estos cifradores en flujo. Ejemplos de cifradores en flujo ideados para este entorno se presentan en [CRU95] y [GUI94]. Debe mencionarse que los últimos avances tecnológicos en la integración hardware parecen permitir también el diseño de cifradores en bloque para estas velocidades [STE95].

En cualquier caso es impensable con la tecnología actual alcanzar velocidades de cifrado de centenares de Mbit/s empleando criptosistemas de clave pública. Sin embargo los algoritmos asimétricos (criptografía de clave pública) pueden ser usados por aplicaciones que no requieren alta velocidad para ofrecer servicios específicos como no repudio. Los algoritmos de clave pública son igualmente muy útiles para autenticación y gestión de claves, donde la velocidad de encriptado no es esencial.

- *REQUISITO 4. La codificación de fuente (compresión de datos) debe realizarse previamente al cifrado, y el cifrado previamente a la codificación de canal (control de errores)*

La figura 3.4 muestra el orden correcto para los procesos de compresión, cifrado y codificación de canal, tanto en emisión como en recepción.

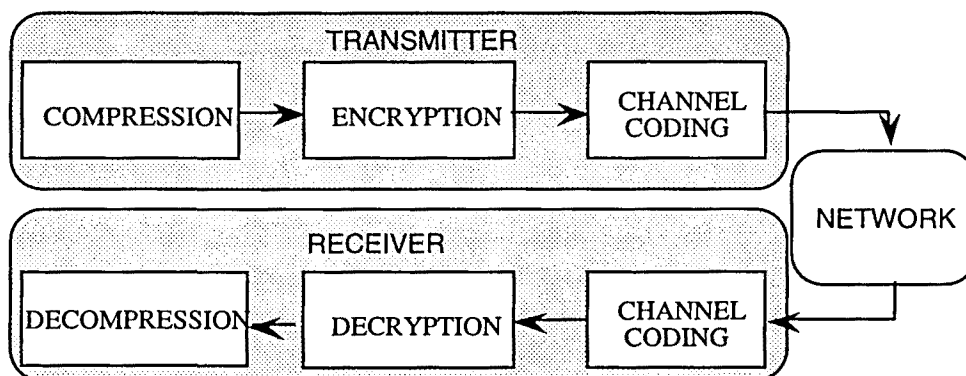


Figura 3.4. Orden para compresión de fuente, cifrado y codificación de canal, tanto en el emisor como en el receptor.

El cifrado de la información previamente a su compresión presenta dos inconvenientes principales:

- La salida de un algoritmo de cifrado tiene la apariencia de aleatoria, imposibilitando cualquier compresión posterior.
- La correlación del texto en claro puede ser utilizada para ataques eficientes: incluso no conociendo mensajes en claro, podría invertirse el algoritmo de cifrado maximizando la correlación del texto en claro estimado. Shannon [SHA49] mostró que este tipo de ataque no es posible en el caso de que los datos sean independientes, lo cual puede aproximarse mediante la compresión de fuente previa al cifrado.

Muchos algoritmos de cifrado, como por ejemplo el DES, provocan difusión: el cambio de un único bit en el texto cifrado provoca que estadísticamente cambien la mitad de los bits de texto en claro, y viceversa. Esta propiedad es ampliamente utilizada para proporcionar el servicio de integridad, bien mediante un algoritmo de cifrado, o bien mediante una función de *hash* que cumple esta propiedad. Debido a ello, la codificación de canal debe llevarse a cabo después del cifrado. De otra forma, una probabilidad de error pequeña en el canal provocaría una probabilidad de error alta en el mensaje descifrado (es decir, tendríamos una importante expansión de errores, efecto totalmente indeseable). Esto no podría evitarse debido a que los mecanismos de integridad no son capaces de diferenciar errores aleatorios de ataques intencionados, y actúan suponiendo un canal libre de errores, hecho que puede ser aproximado mediante la codificación de canal oportuna.

Este requisito es general excepto para ciertas aplicaciones de criptología para radiodifusión de televisión digital (ver [MAC95]), en las cuales se muestra el interés de desarrollar nuevos esquemas donde codificación de fuente se desarrolle en combinación con codificación de canal y codificación criptográfica, con el objeto de alcanzar ciertas características, como transparencia y potabilidad de código (en inglés, *transcodability*).

- *REQUISITO 5. El sistema de seguridad debe constituir una solución integrada capaz de ofrecer servicios de seguridad a todo tipo de servicios y aplicaciones multimedia*

El sistema de seguridad que se proponga debe ser capaz de ofrecer servicios de seguridad a todo tipo de información multimedia (datos, voz y vídeo) independientemente de su naturaleza.

Ello permitirá la propuesta de un solución integrada, cuyo coste es menor. La utilización de una solución diferente para cada tipo de tráfico de aplicaciones o de protocolos de nivel inferior, obligaría al diseño de diferentes sistemas de seguridad, cada

uno de ellos específico para un tipo de tráfico. El coste total de la seguridad sería la suma de los costes de cada uno de los sistemas, suponiendo que fuesen compatibles.

- *REQUISITO 6. El sistema de seguridad debe permitir la compatibilidad con entornos de interconexión como el entorno B*

El sistema de seguridad debe ser lo suficientemente flexible como para permitir la interconexión segura con redes que no utilicen tecnología MTA. Se exigirá el cumplimiento de dos condiciones:

- Si los servicios de seguridad se ofrecen en los terminales extremos en otras redes, el sistema de seguridad debería permitir la existencia de este tráfico seguro sin volver a repetir servicios de seguridad ya ofrecidos.
 - Tráfico inseguro proveniente de otras debería tener la posibilidad de solicitar servicios de seguridad para su paso a través de la RDSI-BA. Esta característica es muy interesante para aplicaciones de interconexión de redes a través de la futura red de banda ancha.
- *REQUISITO 7. Se deben utilizar mecanismos de seguridad extremo a extremo*

Esta solución se considera mejor que los mecanismos de enlace desde el punto de vista de la seguridad proporcionada, a pesar de que las medidas de enlace puedan ofrecer un grado de anonimato mucho mayor, ya que ocultan la identidad de las entidades extremas involucradas. Una medida de enlace implicaría el cifrado de todo el enlace con la misma clave de sesión, independientemente de las aplicaciones, lo cual es contrario a los requisitos 1 y 2.

Por otra parte, ello permite ofrecer la seguridad a los usuarios como un valor añadido de su terminal, sin necesidad de modificar los nodos de la red.

3.4 Ubicación de los Servicios de Seguridad

En este apartado se presentan las principales opciones para la ubicación del mecanismo de cifrado (necesario para ofrecer los servicios de confidencialidad e integridad al grueso de la información), así como la correcta ubicación de los

mecanismos de gestión de claves y de los servicios de autenticación, control de acceso y no repudio.

En lugar de una discusión general como en el capítulo 2, aquí únicamente se considera si cada una de las opciones permite alcanzar los requisitos presentados en el apartado 3.3. En cualquier caso todas las ventajas e inconvenientes enumeradas en el capítulo anterior de forma general, son igualmente aplicables.

3.4.1 Cifrado de la Información. Confidencialidad e Integridad

Los servicios de confidencialidad e integridad hacen uso del mecanismo de cifrado. Por razones de simplicidad del sistema de seguridad finalmente propuesto, se intentará la ubicación de ambos servicios a un mismo nivel, que será donde se realice el proceso de cifrado del grueso de la información (*bulk encryption*). Por ello, la ubicación de estos servicios vendrá determinada por la ubicación del mecanismo de cifrado.

Dado que únicamente se contempla la implantación de servicios de seguridad en terminales multimedia extremos, no tiene sentido la opción de ubicar el cifrado por debajo del nivel MTA, con lo cual no será considerada a diferencia del capítulo anterior.

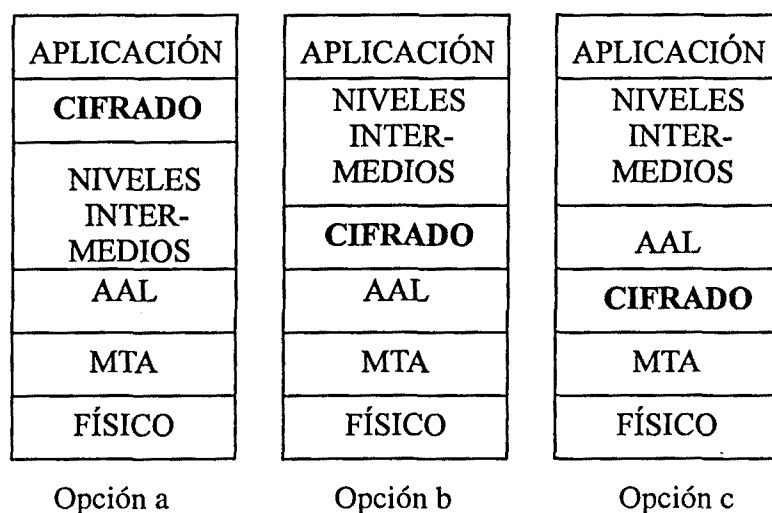


Figura 3.5. Tres posibles ubicaciones del mecanismo de cifrado.

3.4.1.1 Cifrado debajo del nivel de aplicación

La primera posibilidad a considerar es la ubicación del cifrado justo por debajo del nivel de aplicación, tal como se muestra en la figura 3.5a. En este caso la

información multimedia procedente de aplicaciones sensibles será cifrada en el terminal origen antes de ser enviada a niveles inferiores. La información cifrada es posteriormente encapsulada mediante los correspondientes protocolos de comunicación y transmitida por la red. En recepción se lleva a cabo el proceso contrario y la información es descifrada justo por debajo del nivel de aplicación. Como se mencionó en el capítulo 2, esta opción presenta una serie de ventajas respecto a las otras: en primer lugar, la cantidad de información a cifrar es menor, puesto que no se procesan las cabeceras que añaden los protocolos por debajo del nivel de aplicación, circunstancia que facilita la consecución del requisito 3. Por otra parte la asociación de claves dependientes de la aplicación se facilita enormemente, consistiendo fundamentalmente en que cada aplicación sensible negocie una clave de sesión y posteriormente la información sea cifrada con esta clave. En esta opción, pues, los requisitos 1 y 2 son fáciles de conseguir. Los requisitos 4 y 7 también se cumplen y, además, esta es la única opción que cumple completamente el requisito 6¹.

Sin embargo, esta opción difícilmente integrará todo tipo de servicios multimedia, como exige el requisito 5. En efecto, adoptar esta solución implica la realización de un nivel específico de seguridad para todo tipo de protocolos que pudiesen ubicarse por debajo del nivel de aplicación, o la integración de los servicios dentro de cada aplicación.

3.4.1.2 Cifrado entre niveles MTA y AAL

La figura 3.5c sitúa el cifrado entre los niveles MTA y AAL. Esta es la ubicación más baja posible para mecanismos extremo a extremo, tal como exige el requisito 7. En efecto, para poder proveer servicios extremo a extremo es requisito indispensable que las cabeceras de las celdas MTA viajen en claro por la red, permitiendo el enrutado de la información².

Esta opción cumple fácilmente el requisito 5, ya que toda la información debe acceder al nivel MTA antes de ser enviada por la red. Los requisitos 1 y 2 también pueden cumplirse, aunque será necesario el diseño de primitivas que accedan directamente al nivel MTA desde el nivel de aplicación durante la asociación de la clave de sesión a la aplicación correspondiente, lo cual puede ser complicado.

¹ En realidad, esta es la mejor opción posible para el escenario B.

² De hecho el cifrado de enlace es desaconsejable desde del punto de vista de la seguridad, puesto que la información es descifrada en cada nodo de la red, donde puede ser objeto de ataque, como establece el requisito 7.

Si esta opción se adopta finalmente, cabe esperar que unidades de información pequeñas (celdas MTA) procedentes de diferentes aplicaciones accedan al dispositivo de cifrado en períodos de tiempo especialmente reducidos. Como consecuencia del requisito 2, si se utiliza un único dispositivo de cifrado la clave de sesión deberá conmutarse muy rápidamente³, o bien deberán usarse diversos dispositivos de cifrado en paralelo. En cualquier caso los requerimientos para el cifrador son muy fuertes, máxime teniendo en cuenta que además debe tratarse de un cifrador de muy alta velocidad (requisito 3). En consecuencia el coste del dispositivo cifrador en esta opción será mucho mayor que en las otras.

Por otra parte esta opción es contraria al requisito 4 por ubicar el cifrado por debajo del nivel AAL, que es el encargado del manejo de los errores de transmisión (es decir, la codificación de canal). Además debe recordarse que en el capítulo 2 ya se apuntó que la ubicación del servicio de integridad por debajo del nivel AAL es poco recomendable, puesto que este nivel se encarga de gestionar segmentación y reensamblado.

3.4.1.3 Cifrado por encima del nivel AAL

La ubicación del cifrado inmediatamente encima del nivel AAL (Figura 3.5b) permite alcanzar los requisitos 1 y 2 de forma mucho más natural que la opción c. Además, a este nivel las unidades de información son mayores, con lo que el requisito 3 es mucho más fácil de alcanzar, ya que se aumenta la eficiencia de cifrado⁴. El resto de requisitos, con la notable excepción del sexto, son fácilmente alcanzables.

En realidad esta opción representa la ubicación más alta posible del cifrado que cumple el requisito 5. Ello es debido a que el nivel AAL es el más alto definido por RDSI-BA y, por lo tanto, todos los servicios y aplicaciones multimedia deben acceder a la red de banda ancha a través de este nivel. Las consideraciones acerca de si esta opción es compatible o no con el requisito 6 se presentan en el apartado 3.5.2.

3.4.1.4 Conclusiones

A modo de resumen, la Tabla 3.1 muestra los requisitos que cumple cada una de las opciones anteriores. Puede verse claramente que la opción b es mejor que la c para este conjunto de requisitos y, por lo tanto, la opción c debe ser descartada. La opción a

³En el peor caso, cada celda consecutiva pertenecerá aplicaciones diferentes y, debido al requisito 2, la clave deberá ser conmutada cada 48 bytes (longitud del campo de datos de una celda MTA).

⁴Para mayor información consultése el capítulo 4 de esta tesis.

también parece interesante, pero la imposibilidad de cumplir con el requisito 5 hace que sea descartable, principalmente porque en este estudio se busca una solución integrada.

En resumen, la opción b es la que resulta más atractiva. En concordancia con ella, se definirá un nivel de seguridad por encima del protocolo AAL que ofrezca confidencialidad e integridad entre aplicaciones de comunicaciones de banda ancha, de forma transparente para los protocolos de nivel superior.

	<i>Opción a</i>	<i>Opción b</i>	<i>Opción c</i>
REQUISITO 1	Muy fácil	Relativamente fácil	Más difícil
REQUISITO 2	Muy fácil	Relativamente fácil	Más difícil
REQUISITO 3	Si	Si	Fuertes requisitos para el cifrador. Integridad muy complicada
REQUISITO 4	Si	Si	NO
REQUISITO 5	NO	Si	Si
REQUISITO 6	Si	Permite coexistencia	Permite coexistencia
REQUISITO 7	Si	Si	Si

Tabla 3.1. Requisitos que cumplen cada una de las opciones para la ubicación del cifrado.

3.4.2 Gestión de Claves

En consonancia con el requisito 1 sólo se proporcionarán servicios de seguridad a las aplicaciones sensibles. La ubicación de la gestión de claves a nivel de aplicación facilita enormemente la consecución de este objetivo, ya que permite una interfaz adecuada con usuarios y aplicaciones sensibles.

3.4.3 Autenticación

Al igual que ocurre con la gestión de claves, la ubicación de la autenticación a nivel de aplicación proporciona una interfaz sencilla a usuarios y aplicaciones. En realidad una autenticación mutua es necesaria durante el proceso de negociación de claves de sesión.

Como ya se comentó en el capítulo anterior, la criptografía asimétrica proporciona una serie de ventajas sobre la criptografía simétrica cuando es usada para la autenticación. Entre estas ventajas se encuentran un soporte más natural para la autenticación ante receptores múltiples, un mejor soporte para el servicio de no repudio y eliminar la necesidad de claves secretas proporcionadas por un servidor central.

3.4.4 Control de Acceso y no Repudio

Estos servicios son específicos de algunas aplicaciones, y en general hacen uso de criptografía de clave pública. Por ello su ubicación más correcta es en el nivel de aplicación, conjuntamente con gestión de claves y autenticación. El situar el control de acceso a nivel de aplicación permite realizarlo en función de la identificación de usuarios y aplicaciones particulares.

3.5 Arquitectura Propuesta

En la figura 3.6 se muestra la arquitectura propuesta para el sistema de seguridad. Por simplicidad se hace uso únicamente del plano de usuario definido en el modelo de referencia de protocolos para la RDSI-BA [CCI92d]. De esta forma el sistema de seguridad propuesto no interfiere con señalización y gestión de red.

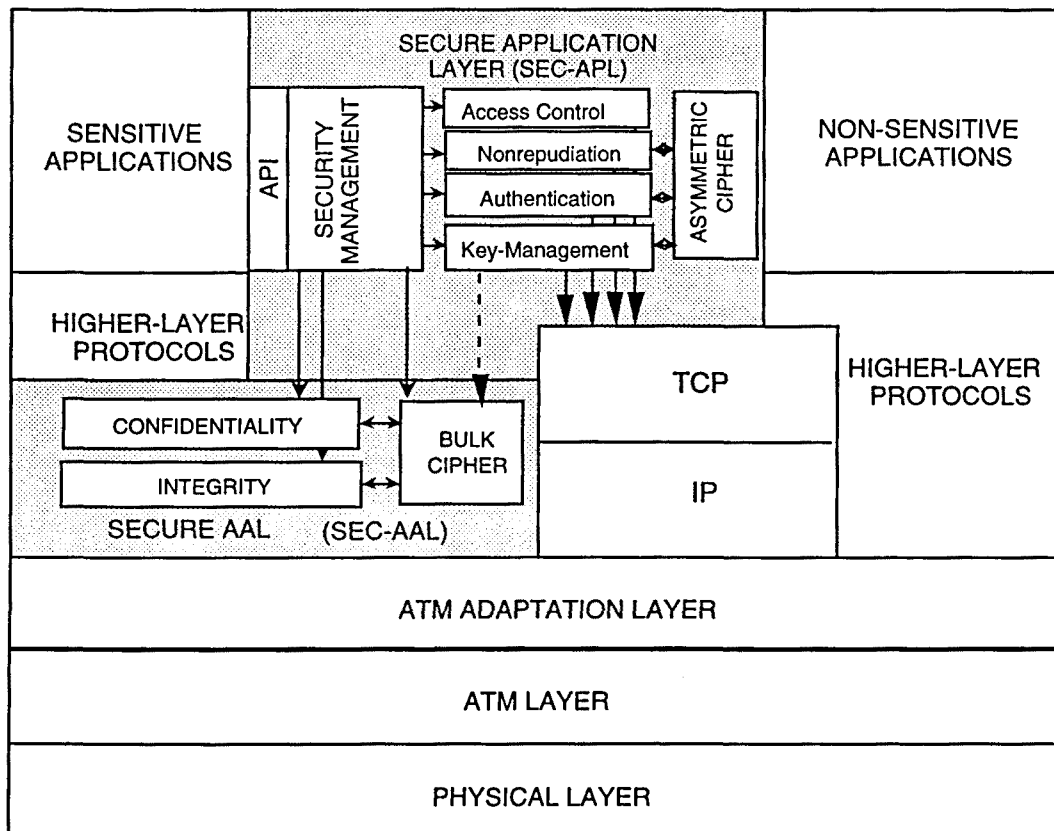
Una utilización de los planos de control y de gestión hubiese permitido la integración de la gestión de la seguridad dentro de la gestión de red, lo que comportaría una serie de ventajas, entre las que destacan que los servicios de seguridad podrían ser negociados como parámetros de calidad de servicio (QoS) durante el periodo de establecimiento de la llamada, a la vez que estos servicios podrían integrarse en la gestión de red para lograr una gestión segura. Sin embargo, esta opción comportaría una redefinición de la señalización y gestión de red, que aún siendo un reto interesante queda fuera del ámbito de este trabajo de investigación.

El protocolo de seguridad esta formado por dos niveles: el nivel seguro AAL (SEC-AAL) y el nivel de aplicación seguro (SEC-APL).

En el nivel más bajo, la capa SEC-AAL se ubica por encima del nivel AAL y es independiente de los protocolos superiores, lo que significa que cualquier protocolo de alto nivel puede ubicarse por encima del nivel SEC-AAL de forma transparente. Este nivel proporciona los mecanismos de cifrado a la vez que proporciona los servicios de

confidencialidad e integridad. Ofrece a los protocolos de nivel superior la misma interfaz que los niveles AAL convencionales (AAL-1, AAL-2, AAL-3/4 y AAL-5), además de unos servicios de seguridad extra de forma totalmente transparente para aplicaciones no sensibles. Será necesario definir 4 niveles SEC-AAL, cada uno de los cuales ofrezca a los protocolos de nivel superior la misma interfaz que cada una de las capas AAL definidas.

El nivel SEC-APL se ubica a nivel de aplicación. Proporciona el mecanismo de cifrado asimétrico y la gestión de claves, a la vez que los servicios de autenticación, control de acceso y no repudio. Las aplicaciones sensibles solicitarán los servicios de seguridad que necesiten mediante una interfaz de programación de la aplicación (API), que especifica una serie de primitivas de seguridad. Para ello estas aplicaciones deberán modificarse de tal forma que sean capaces de solicitar los servicios requeridos. Sin embargo, una vez negociados los parámetros de seguridad, éstos se ofrecerán de forma transparente a las aplicaciones.




 SECURITY SYSTEM

Figura 3.6 Arquitectura del sistema de seguridad.

3.5.1 Ejemplo Simplificado de Operación

A continuación se muestra el funcionamiento del sistema de seguridad, a través de un ejemplo simplificado. En este ejemplo se supone que no existe negociación de parámetros de seguridad, es decir, la aplicación solicita un servicio de seguridad con unos parámetros (algoritmo, longitud de claves, etc.) que se consideran conocidos a priori. Más adelante se propondrá un sistema de seguridad más sofisticado donde estos parámetros serán negociados.

Supongamos que una aplicación ejecutándose sobre un terminal multimedia local (representada a la izquierda de la Figura 3.6) solicita una conexión confidencial con una aplicación remota ejecutándose sobre un terminal remoto. Para ello se debe establecer previamente una conexión insegura, y posteriormente transformar esta conexión insegura en una conexión segura mediante la negociación de parámetros de seguridad a través de un canal de datos independiente⁵. La Figura 3.7 muestra los pasos que se llevan a cabo para esta negociación, que son los siguientes:

1. La aplicación (AP) solicita el servicio de confidencialidad al módulo de gestión de seguridad (SMM, *Security Management Module*) a través de la interfaz de programación de la aplicación (API) mediante el envío de una primitiva de seguridad.
2. El SMM activa el módulo de gestión de claves (KMM, *Key Management Module*) para que negocie una clave de sesión (SK, *Session Key*) para cifrar la conexión.
3. El módulo de gestión de claves negocia una clave de sesión con la entidad remota siguiendo un protocolo de gestión de claves autenticado, utilizando el cifrador asimétrico (AC, *Asymmetric Cipher*). Este protocolo de gestión de claves se encapsula sobre un protocolo fiable de comunicaciones (por ejemplo, TCP/IP). Cuando este protocolo finalice, los módulos de gestión de claves local y remoto habrán acordado la clave de sesión (SK) con la que cifrar la conexión, proporcionando confidencialidad.
4. Esta SK y su identificador de aplicación (AI, *Application Identifier*) se envían al módulo de confidencialidad situado en el nivel SEC-AAL para que cargue esta clave en el cifrador (BC, *Bulk Cipher*).

⁵ Otra opción interesante consiste en negociar los parámetros de seguridad durante el periodo de establecimiento de la conexión. Sin embargo, esta solución requiere la utilización del plano de control (señalización), por lo que ha sido descartada con el objetivo de no modificar la señalización.

5. Se envía un reconocimiento a la aplicación para indicarle que el módulo de confidencialidad ya está preparado para ofrecer dicho servicio.
6. La aplicación inicia la conexión confidencial enviando la información a través del protocolo de comunicaciones que utilice de igual forma que haría en el caso de una conexión insegura. Cuando la información alcanza el nivel SEC-AAL, su AI provoca que el módulo de confidencialidad la redireccione hacia el cifrador adecuado para ser cifrada con la clave correspondiente (cada AI tiene asociada una clave de sesión).
7. Una vez cifrada la información se envía al nivel AAL correspondiente para ser transmitida por la red.

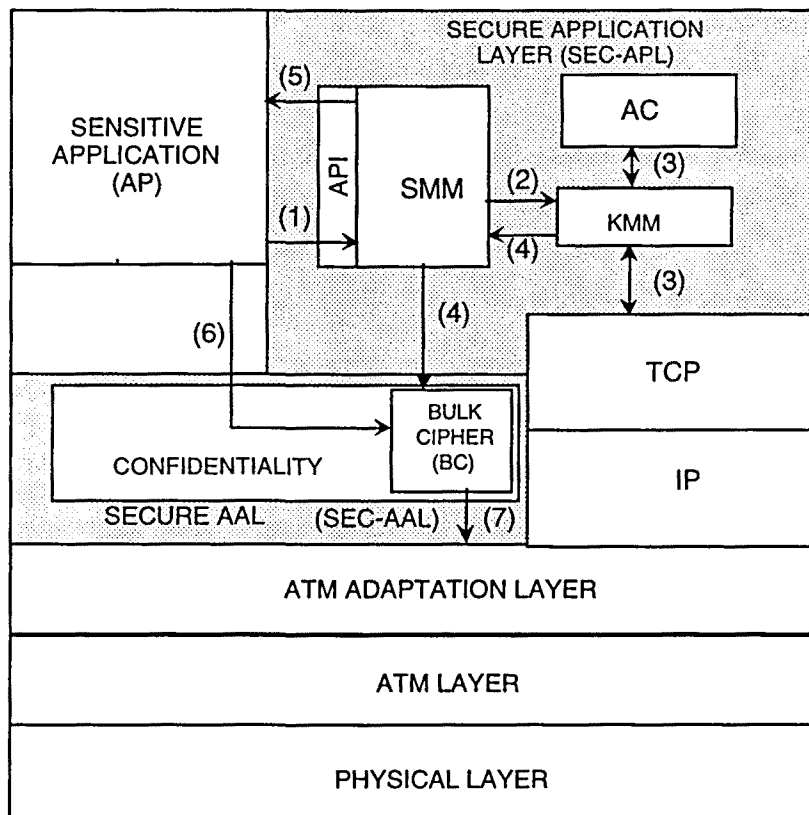


Figura 3.7. Ejemplo de los pasos a seguir para establecer una conexión confidencial.

En el terminal remoto se lleva a cabo un proceso similar y la información se descifra con la misma clave de sesión. Cuando la conexión confidencial finaliza, la aplicación informa al módulo de gestión de seguridad (SMM) y éste libera el recurso de cifrado y deshace la asociación entre SK y AI. Para aplicaciones no sensibles el sistema de seguridad es transparente.

3.5.2 Compatibilidad con Interconexión de Redes

A continuación se estudia si el sistema de seguridad propuesto es capaz de cumplir el requisito 6: “*El sistema de seguridad debe permitir la compatibilidad con entornos de interconexión como el entorno B*”.

Dos sistemas son capaces de comunicarse entre ellos debido a que existe un canal que los une y a que comparten un protocolo común. En la RDSI-BA este protocolo está especificado por el Modelo de Referencia de Protocolos (CCITT I.321). Los sistemas conectados a otro tipo de redes comparten otros protocolos que especifican las comunicaciones dentro de cada red. La interconexión de sistemas pertenecientes a redes diferentes es posible debido a que los sistemas comparten una familia de protocolos ubicada a niveles más altos. Un ejemplo de estos protocolos a niveles superiores es la familia TCP/IP, utilizada por *Internet* para construir el mayor escenario de interconexión jamás visto. En esta red se asocia una dirección IP a cada nodo (ya sea intermedio o extremo), que se utiliza para el enrutamiento de la información a través de una red virtual, denominada *Internet*, independientemente de la red física a la que esté conectado cada sistema. Para el estudio del requisito de interconexión se puede asumir, sin pérdida de generalidad, que los sistemas a interconectar comparten la familia de protocolos TCP/IP, es decir, se comunican a través de *Internet*.

Como ejemplo, supongamos que los terminales MT1 y MT3 de la figura 3.2 están conectados a *Internet* (es decir, ambos usan TCP/IP) y que MT1 abre una conexión con MT3 (por ejemplo, una sesión *telnet*). Para ofrecer confidencialidad e integridad a toda la conexión, el requisito 7 nos conduce a situar el cifrador por encima del nivel IP (en efecto, las cabeceras IP deben permanecer en claro para permitir el enrutado de la información a través de la red). El cumplimiento conjunto de los requisitos 4 y 5 situaría el cifrado encima de un protocolo fiable (por ejemplo, TCP)⁶. En cualquier caso MT3 nunca podrá usar el sistema de seguridad propuesto en este capítulo, debido a que no está conectado directamente a la RDSI-BA y, consecuentemente, no puede acceder al nivel SEC-AAL. Para permitir compatibilidad, el cifrado debe ubicarse entre los niveles IP y de aplicación, de acuerdo con un protocolo de seguridad específico de *Internet*.

El requisito de compatibilidad significa que el sistema de seguridad propuesto debe permitir la coexistencia con otros protocolos de seguridad ofrecidos a niveles superiores. En nuestro sistema esto puede alcanzarse fácilmente debido a que se ofrecen servicios de seguridad a petición de las aplicaciones. Si estos servicios de seguridad se

⁶ Existe un protocolo para *Internet*, denominado SSL (*Secure Socket Layer*), que ubica el cifrado a este nivel.

ofrecen a niveles superiores, entonces la aplicación no solicitará servicios de seguridad al SMM del nivel SEC-APL, con lo que el nivel SEC-AAL considerará la aplicación como no sensible.

El otro requerimiento de compatibilidad es permitir la interconexión segura de LANs y MANs a través de la RDSI-BA. Esto puede conseguirse fácilmente si los dispositivos que interconectan la RDSI-BA con otras redes ofrecen los niveles SEC-APL y SEC-AAL. Un diseño de este tipo podría seguir la filosofía que se utilizó en el proyecto CryptoNet [FOR91, FOR93, REC93, SOR93a, SOR93b], donde dispositivos de interconexión (en este caso *bridges*) fueron utilizados para la interconexión segura de redes a través de una red insegura.

3.6 Negociación de los Servicios de Seguridad

Como se mencionó anteriormente, una aplicación sensible inicia una petición de comunicación segura enviando una primitiva al nivel SEC-APL del terminal multimedia local. Esta primitiva debe especificar, entre otros, los siguientes parámetros:

- *Servicio de seguridad*: confidencialidad, integridad, autenticación, control de acceso, no repudio, o una combinación de ellos
- *Nivel de seguridad*: Para usuarios no expertos puede especificarse como un nivel genérico (por ejemplo, un número entre 1 y 5). Un nivel más bajo significa un nivel menor de seguridad, mientras que niveles más altos requieren generalmente mayor capacidad de cálculo o proporcionan menor ancho de banda. El nivel SEC-APL transforma este nivel de seguridad en un algoritmo criptográfico y una longitud de clave, si estos parámetros no son implícitamente especificados por el usuario
- *Algoritmo*: Usuarios y aplicaciones expertas pueden especificar el algoritmo a usar para proporcionar cada uno de los servicios requeridos. No es de esperar que usuarios inexpertos especifiquen este parámetro
- *Longitud de claves*: Usuarios y aplicaciones expertas pueden especificar también la longitud de la clave criptográfica a usar, si es que esta no queda determinada por el algoritmo. No es de esperar que usuarios inexpertos especifiquen este parámetro

- *Velocidad*: Ciertos niveles de seguridad (o ciertos algoritmos y longitudes de clave) no pueden ofrecerse a cierta velocidad. Por ello, la velocidad debe especificarse para detectar incompatibilidades
- *Probabilidad de error*: Dependiendo del algoritmo criptográfico utilizado, la probabilidad de error puede expandirse. Por ejemplo, si se usa un cifrador en bloque, un único bit erróneo durante la transmisión se transforma en todo un bloque erróneo después del descifrado. Otro tipo de algoritmos, como los cifradores en flujo síncronos, no presentan expansión de errores. En cualquier caso se debe especificar la máxima tasa de error aceptable después del descifrado, que puede comprometer el uso de ciertos algoritmos dada una probabilidad de error del canal
- *Retardo*: El procesado necesario para ofrecer los servicios de seguridad requeridos, introducirá un retardo en la comunicación. El usuario debe especificar el máximo retardo permisible que a su vez condiciona los algoritmos a utilizar. Una especificación restrictiva de este parámetro puede ser incompatible con cierto nivel de seguridad
- *Entorno*: Este parámetro especifica aspectos tales como versión de protocolos de gestión de claves usados, autoridades y centros de certificación y confianza, etc.
- *Parámetros dependientes del servicio*: Los parámetros anteriores son genéricos para todos los servicios de seguridad. Existen sin embargo otros parámetros que son específicos de cada servicio. Ejemplos de este último tipo serían el modo de autenticación a usar (de un sentido, bidireccional o haciendo uso de centros de confianza), la clase de repudio (de origen o destino), el formato utilizado para dar firma digital, etc.

Los usuarios tienen la opción de especificar únicamente algunos de estos parámetros. En particular es probable que los usuarios con conocimientos limitados de criptografía especifiquen únicamente el servicio de seguridad, el nivel de seguridad, y quizás, velocidad, retardo y probabilidad de error.

Además diferentes clases de servicios requieren diferentes parámetros de seguridad. Por ejemplo, mientras que confidencialidad y retardo acotado pueden ser requerimientos para ciertos servicios de tasa constante (CBR, *Constant Bit Rate*), como telefonía a 64 kbits/s o vídeo no comprimido a tasa constante; otros servicios de datos ABR (*Available Bit Rate*) como transferencia de ficheros o correo electrónico pueden requerir principalmente integridad.

La figura 3.8 resume el funcionamiento del sistema de seguridad.

Cuando el nivel SEC-APL recibe una primitiva, debe verificar si es posible ofrecer simultáneamente todos los servicios solicitados con los parámetros deseados. En caso contrario, debe proponer a la aplicación un nuevo conjunto de parámetros. Por ejemplo, si una aplicación solicita un algoritmo específico y este algoritmo no se encuentra disponible, el nivel SEC-APL debe proponer una lista de los algoritmos disponibles que puedan proporcionar los mismos servicios a ser posible con el mismo nivel de seguridad.

El proceso no finaliza si el módulo SEC-APL local es capaz de ofrecer los servicios solicitados. En ese caso el nivel local debe consultar al nivel SEC-APL remoto sobre la posibilidad de ofrecer estos servicios por parte del terminal remoto, así como si la aplicación remota está dispuesta a aceptar una comunicación segura con la aplicación local.

A partir de aquí se ejecuta un protocolo mediante el cual ambos niveles SEC-APL negocian los algoritmos para ofrecer los servicios solicitados.

En primer lugar el módulo SEC-APL remoto envía al módulo local una lista priorizada de los algoritmos y mecanismos disponibles para ofrecer estos servicios. Para ello debe escoger de entre todas las opciones que tenga disponibles las que considere que mejor cumplen las especificaciones al menor coste posible. Ello implica la consulta a unas bases de datos locales y la utilización de unas funciones de coste que tendrán en cuenta, entre otros aspectos, los siguientes:

- La velocidad y el retardo al que pueden ofrecerse los diferentes algoritmos y mecanismos (que a su vez pueden ser combinación de mecanismos elementales)
- El consumo de CPU o utilización de dispositivos *hardware*
- La expansión de mensajes que supone la utilización de ciertos mecanismos

Con esta información y consultando bases de datos locales, el módulo SEC-APL local lleva a cabo un algoritmo de decisión para decidir el conjunto de mecanismos y algoritmos que se aplicarán. Si se encuentra un conjunto adecuado, se envía la propuesta final al SEC-APL remoto, que debería aceptarla si se ha utilizado su propuesta anterior. Si esto no es posible, debe repetirse la propuesta con otro conjunto de algoritmos.

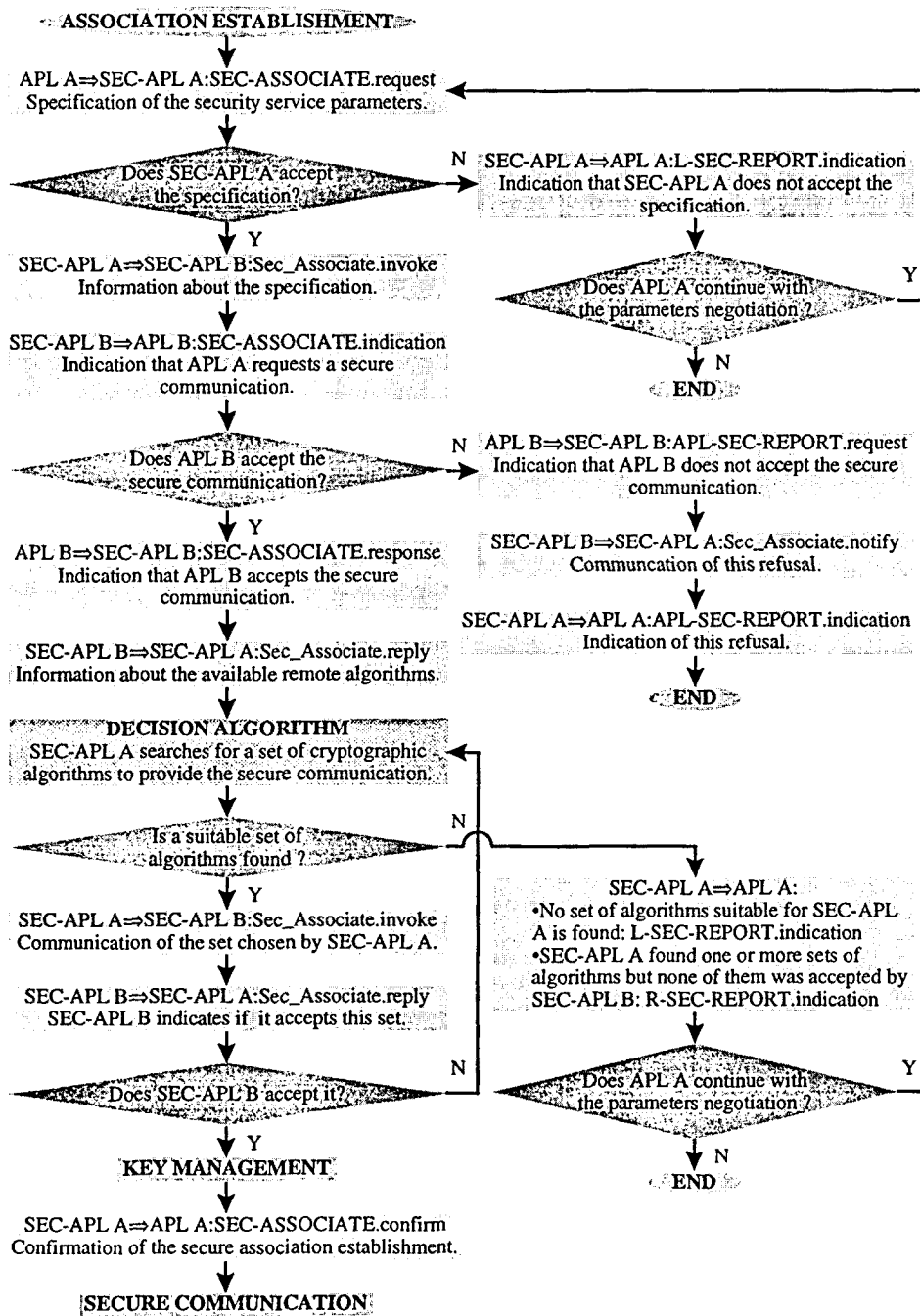


Figura 3.8 Diagrama de flujo de funcionamiento del sistema de seguridad

Si al cabo de cierto número de mensajes ambos niveles SEC-APL no consiguen negociar unos parámetros comunes, se concluye este proceso. En este caso el módulo local sugiere a la aplicación un nuevo conjunto de parámetros, asegurándole en este caso que el nivel SEC-APL remoto podrá aceptarlos.

En caso de no poder ofrecerse ciertos servicios de seguridad con los parámetros solicitados, es importante informar a la aplicación sobre si la imposibilidad proviene del módulo SEC-APL local o del remoto. Si el problema es local no se podrá hacer nada, y en ese caso probablemente deberán aceptarse los parámetros sugeridos por el módulo local. Sin embargo, si el problema reside en el terminal remoto, quizás en un entorno distribuido se pueda conectar con otro servidor que proporcione los servicios solicitados.

Otro aspecto importante es indicar si la imposibilidad de ofrecer un servicio con los parámetros solicitados es transitoria o permanente. Pudiera ser que el terminal utilizase *hardware* específico de cifrado, y que este *hardware* estuviese ocupado sirviendo a otra aplicación, siendo temporalmente imposible ofrecer cierta velocidad de encriptado, que en cambio será sencilla de alcanzar cuando se libere este *hardware*. Otro ejemplo es un servidor ocupado que temporalmente no puede ofrecer ciertos servicios.

Una vez negociados los parámetros de seguridad, ambos niveles SEC-APL negocian una clave o conjunto de claves con las que ofrecer los servicios solicitados. Para ello deben utilizar protocolos autenticados de gestión de claves, que deben cumplir, entre otros, los siguientes requerimientos:

- *Confidencialidad de datos:* Las claves secretas deben mantenerse confidenciales durante sus transmisión por la red
- *Detección de modificación:* Deben detectarse modificaciones no autorizadas durante la transmisión
- *Detección de reactuación:* El reenvío no autorizado de mensajes es uno de los principales ataques a protocolos de gestión de claves, por lo que debe ser detectado
- *Autenticación:* La entidad involucrada debe ser quien pretende ser

Durante la negociación de claves no sólo es fundamental que se autentifique la identidad de las entidades involucradas, sino que también se deben autenticar los parámetros de seguridad anteriormente negociados y comprobar su integridad. Además, puede ser que se acceda a centros de certificación y otras entidades de confianza. En el capítulo 5 de esta tesis se muestra que una infraestructura de clave pública es muy útil para implementar protocolos de negociación de claves en la RDSI-BA.

Una vez concluida la negociación de claves, se informa a la aplicación que la asociación de seguridad ya ha sido establecida. A partir de entonces, se inicia la

comunicación segura. Cualquiera de las aplicaciones involucradas pueda solicitar la liberación de la asociación de seguridad.

Si un nivel SEC-APL detecta una violación de seguridad (por ejemplo, detecta una modificación o una reactuación) durante el proceso de gestión de claves o durante la comunicación segura, se debe advertir a las aplicaciones involucradas.

3.6.1 La Interfaz de Programación de la Aplicación (API)

En este apartado se muestra la forma en la que las aplicaciones sensibles solicitan servicios de seguridad al nivel de aplicación segura (SEC-APL).

Se define la interfaz de programación de la aplicación (API) como el mecanismo a través del cual software de nivel de aplicación interactúa con el sistema de seguridad. En nuestro caso, esta API define un conjunto de funciones primitivas que serán usadas por las aplicaciones para solicitar servicios de seguridad o para informar al sistema de seguridad de ciertos acontecimientos. También permite que el sistema de seguridad informe a las aplicaciones de ciertos eventos, como pueda ser el que un canal seguro está disponible. Para la definición de estas funciones primitivas utilizamos una terminología similar a la usada por el modelo de referencia OSI [ISO84]. La Tabla 3.2 nos muestra las primitivas definidas para que las aplicaciones soliciten servicios de seguridad.

<i>Servicio</i>	<i>Elemento de servicio</i>	<i>Primitivas</i>
Security association	SEC-ASSOCIATE	Request; Indication; Response, Confirm
Confirmed security release	SEC-RELEASE	Request, Indication; Response; Confirm
Local SEC-APL report	L-SEC-REPORT	Indication
Remote SEC-APL report	R-SEC-REPORT	Indication
Remote application report	APL-SEC-REPORT	Request; Indication
Unconfirmed security release	SEC-ABORT	Request; Indication

Tabla 3.2. Servicios, elementos de servicio y primitivas para ofrecer servicios de seguridad a las aplicaciones.

El primer servicio que se presenta es la asociación de seguridad. Una asociación de seguridad es una asociación, entre dos o más sistema, que establece un modelo y una

definición del formato de la información entre ambos sistemas (por ejemplo, identificadores de entidades, algoritmos seleccionados, claves y parámetros). Esta asociación de seguridad constituye el soporte para una protección consistente de una secuencia de transferencia de datos [FORD94]. Se propone la implementación de esta asociación de seguridad como un elemento de servicio con confirmación (*SEC-ASSOCIATE*), que define cuatro primitivas de seguridad (*SEC-ASSOCIATE.request*; *SEC-ASSOCIATE.indication*; *SEC-ASSOCIATE.response*; *SEC-ASSOCIATE.confirm*).

El segundo servicio es la liberación de la asociación de seguridad. Se define nuevamente como un elemento de servicio con confirmación (*SEC-RELEASE*), que es utilizado para la liberación de la asociación de seguridad una vez finaliza la conexión segura. Se le asocian cuatro primitivas, que son las siguientes : *SEC-RELEASE.request*; *SEC-RELEASE.indication*; *SEC-RELEASE.response*; y *SEC-RELEASE.confirm*.

Por último se definen una serie de primitivas para indicar a la aplicación que los servicios de seguridad no pueden ser ofrecidos, al menos con los parámetros solicitados : *L-SEC-REPORT.indication*; *R-SEC-REPORT.indication*, *APL-SEC-REPORT.request* y *APL-SEC-REPORT.indication*.

El servicio de informe del módulo *SEC-APL* local (*L-SEC-REPORT*) utiliza la primitiva *L-SEC-REPORT.indication* para informar a la aplicación que el módulo de seguridad local no puede ofrecer los servicios de seguridad solicitados, al menos con los parámetros requeridos. Se indica además si esta imposibilidad es temporal o permanente, a la vez que sugiere un nuevo conjunto de parámetros que ofrezcan un nivel de seguridad parecido.

El servicio de informe del módulo de seguridad remoto (*R-SEC-REPORT*) utiliza la primitiva *L-SEC-REPORT.indication* para indicar a la aplicación que el nivel de seguridad *SEC-APL* remoto no es capaz de ofrecer los servicios de seguridad solicitados. De igual forma que en el caso anterior, esta función indica además si esta imposibilidad para ofrecer estos servicios es temporal o permanente, a la vez que sugiere un nuevo conjunto de parámetros que ofrezcan un nivel de seguridad parecido.

El servicio de informe de la aplicación remota (*APL-SEC-REPORT*) indica que la aplicación remota no acepta la conexión segura. Utiliza las dos primitivas siguientes: *APL-SEC-REPORT.request* y *APL-SEC-REPORT.indication*.

Una especificación completa de estas primitivas según la notación ASN.1 [ISO8824] se adjunta en el anexo 1 de esta tesis.

3.6.2 Primitivas de Comunicación entre Niveles SEC-APL

En el apartado anterior se ha presentado la interfaz que ofrece el nivel SEC-APL a las aplicaciones sensibles. Se ha definido como un conjunto de primitivas a través de las cuales las aplicaciones sensibles solicitan servicios de seguridad. Para la negociación de estos servicios de seguridad las entidades SEC-APL se comunican entre ellas de acuerdo a un Protocolo de Gestión de la Seguridad. Este protocolo define una serie de primitivas de comunicación para transferir mensajes entre dos niveles SEC-APL cooperantes:

A continuación se presentan las primitivas que se proponen para las comunicaciones entre niveles SEC-APL local y remoto. Además de las primitivas que se usen para la gestión de claves, se definen las siguientes:

- *Sec_Associate invoke*: Petición de una asociación de seguridad (por parte de la entidad origen)
- *Sec_Associate reply*: Aceptación de una asociación de seguridad (por parte de la entidad destino)
- *Sec_Associate notify*: Rechazo de una petición de asociación de seguridad. Notificación de la detección de una violación de seguridad (por parte de la entidad destino)
- *Sec_Release invoke*: Petición de liberación de una asociación de seguridad (tanto por parte de la entidad origen como de la entidad destino)
- *Sec_Release reply*: Reconocimiento de liberación de una asociación de seguridad (tanto por parte de la entidad origen como de la entidad destino)
- *Sec_Abort notify*: Notificación de una liberación de seguridad no confirmada (tanto por parte de la entidad origen como de la entidad destino)

Las 3 primeras primitivas (*Sec_Associate **) se utilizan para negociar la asociación de seguridad, incluyendo servicios, algoritmos y parámetros. Las dos siguientes (*Sec_Release **) se utilizan para liberar la asociación de forma confirmada, mientras que la última (*Sec_Abort notify*) se utiliza para una notificación no confirmada.

Estas primitivas definen las estructuras de los mensajes intercambiados entre niveles SEC-APL cooperantes para negociar parámetros de seguridad y para liberar las asociaciones de seguridad. Estos niveles utilizan protocolos de comunicaciones

ordinarios (por ejemplo TCP/IP) para abrir conexiones y para negociar claves de forma segura. Durante la fase de gestión de claves se lleva a cabo una autenticación mutua de ambas entidades, sin la cual no se podría confiar en nada de lo anteriormente negociado.

3.6.3 Ejemplo de Operación

La figura 3.9 presenta un ejemplo de los pasos que se llevan a cabo para establecer una comunicación segura y las primitivas que entran en juego. Se supone que previamente se ha establecido una asociación entre las aplicaciones A y B con lo que se ha establecido una conexión insegura.

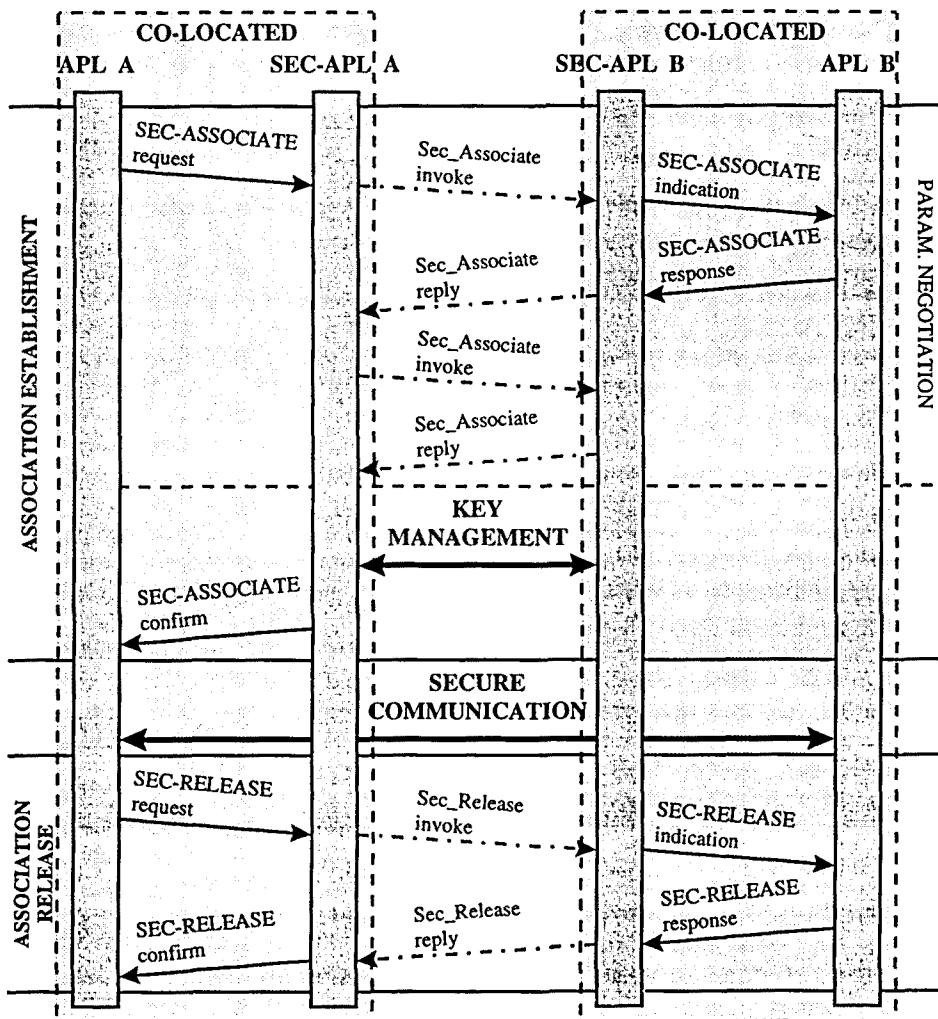


Figura 3.9. Ejemplo de establecimiento de una comunicación segura y primitivas involucradas.

Los pasos para convertir la conexión insegura en conexión segura son los siguientes:

3.6.3.1 Establecimiento de la asociación de seguridad

En primer lugar la aplicación local A solicita al nivel SEC-AAL local una comunicación segura con la aplicación remota B. Para ello envía al nivel SEC-APL A, ubicado en el mismo terminal, la primitiva *SEC-ASSOCIATE.request* indicando los parámetros solicitados.

Suponiendo que el nivel SEC-APL A acepta los parámetros solicitados, lo notifica al nivel remoto SEC-APL B, mediante la primitiva de comunicaciones *Sec_Associate invoke*. Seguidamente, el nivel SEC-APL B envía la primitiva *SEC-ASSOCIATE.indication* a la aplicación B situada también en el terminal remoto.

Si la aplicación B acepta la comunicación segura, responde al nivel SEC-APL B con la primitiva *SEC-ASSOCIATE.response*. Posteriormente, el nivel SEC-APL B envía un mensaje al nivel SEC-APL A mediante la primitiva de comunicaciones *Sec_Association reply* indicando que el terminal remoto puede aceptar la petición de asociación de seguridad. Este mensaje contiene información acerca de los algoritmos criptográficos disponibles por SEC-APL B para ofrecer los servicios solicitados.

A partir de aquí se inicia un algoritmo de decisión mediante el cual ambas entidades SEC-APL acuerdan un conjunto adecuado de algoritmos, que se intenta ofrezcan los servicios solicitados con un coste mínimo. [REB96] detalla diferentes algoritmos de decisión y su implementación. En la figura 3.9 se muestra el comportamiento de uno de los posibles algoritmos.

En este algoritmo si el nivel SEC-APL A encuentra un conjunto adecuado de algoritmos de seguridad entre los propuestos por SEC-APL B, debe enviárselo a través de la primitiva de comunicaciones *Sec_Associate invoke*. Si el nivel SEC-APL B finalmente acepta esta propuesta, debe confirmarlo mediante el envío de la primitiva de *Sec_Associate reply*.

Seguidamente, ambas entidades SEC-APL llevan a cabo un protocolo de gestión de claves, a través del cual negocian de forma segura una clave o conjunto de claves, a la vez que autentifican su identidad y la integridad de los parámetros de seguridad anteriormente negociados. Una vez concluida la gestión de claves, el nivel SEC-APL A informa de ello a la aplicación A mediante la primitiva *SEC-ASSOCIATE.confirm*.

3.6.3.2 Comunicación segura

Cuando la aplicación A recibe la primitiva *SEC-ASSOCIATE.confirm* la asociación de seguridad ha concluido. A partir de aquí los servicios de seguridad se ofrecen de forma transparente para la aplicación, que actúa como si se tratase de una comunicación insegura, enviando la información a los protocolos de nivel inferior.

Sin embargo, dado que el nivel SEC-AAL ha recibido la identificación de la asociación de seguridad, ofrece los servicios de seguridad (confidencialidad e integridad, o ambos) a toda la información que proceda de la aplicación A.

3.6.3.3 Liberación de la asociación de seguridad

Cualquiera de las aplicaciones puede liberar la asociación de seguridad mediante la primitiva *SEC-RELEASE.request*. Este proceso implica la activación de la primitivas *SEC-RELEASE.indication*, *SEC-RELEASE.response* y *SEC-RELEASE.confirm* entre las aplicaciones y los niveles SEC-APL, así como el intercambio de mensajes a través de la red mediante las primitivas de comunicaciones *Sec_Release invoke* y *Sec_Release reply*.

3.6.3.4 Intentos frustrados de establecer asociación de seguridad

Las figuras 3.10, 3.11 y 3.12 muestran intentos no exitosos de establecer asociaciones de seguridad, así como las primitivas utilizadas para notificar esta situación.

El caso más simple es el mostrado en la figura 3.10, donde el nivel SEC-APL local no acepta los parámetros solicitados por la aplicación A mediante la primitiva *SEC-ASSOCIATE.request*. En esta situación no es necesario el intercambio de mensajes a través de la red.

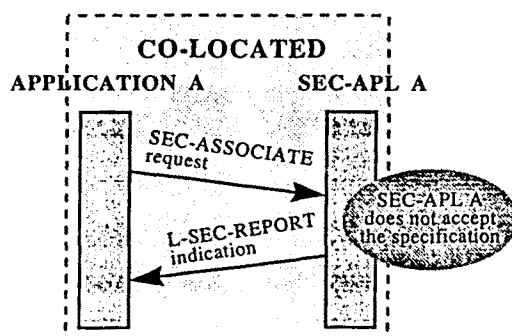


Figura 3.10. El nivel SEC-APL local no puede ofrecer los servicios de seguridad solicitados.

Otra posibilidad es que el nivel SEC-APL remoto no acepte los algoritmos que propone el nivel SEC-APL local, tal como muestra la figura 3.11. En este caso entra en juego la primitiva *R-SEC-REPORT.indication*.

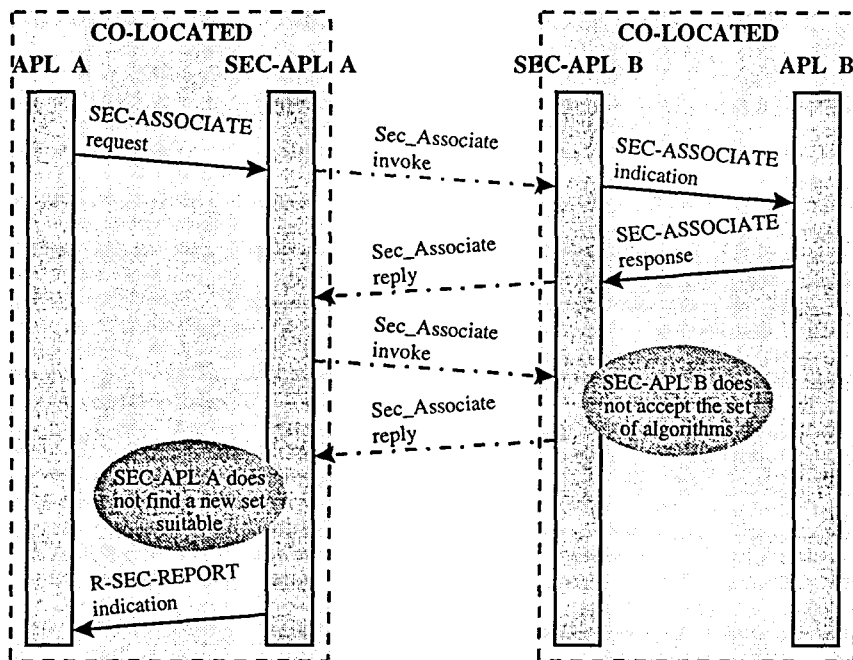


Figura 3.11. El nivel SEC-APL remoto no puede ofrecer los servicios de seguridad solicitados.

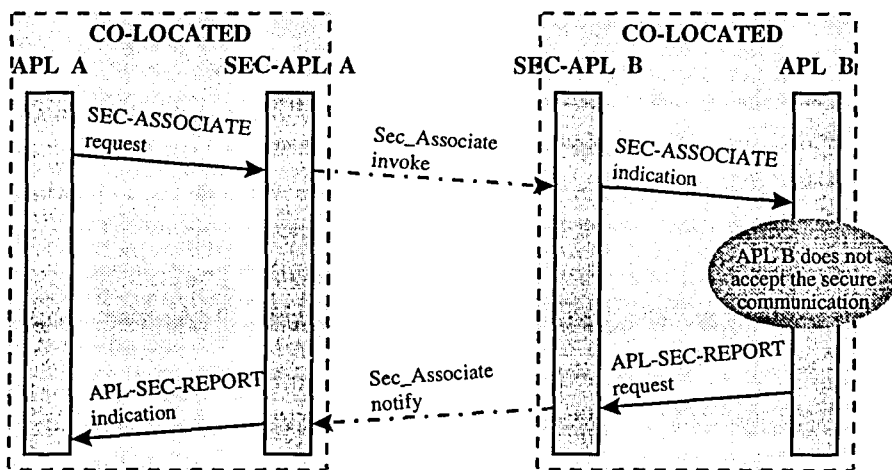


Figura 3.12. La aplicación remota no acepta la conexión segura.

La figura 3.12 muestra la posibilidad que la aplicación remota no acepte la conexión segura. En ese caso la primitiva *APL-SEC-REPORT.indication* entra en juego.

3.7 Conclusiones y Aportaciones

En este capítulo se presenta una solución integrada capaz de ofrecer servicios de seguridad para todo tipo de servicios y aplicaciones que hagan uso de la futura RDSI-BA. Se han sentado una serie de requisitos para el sistema de seguridad, en base a los cuales se ha decidido la ubicación de los servicios de confidencialidad e integridad por encima de la capa AAL del modelo de referencia de protocolos de la RDSI-BA. También se ha decidido la ubicación a nivel de aplicación de los servicios de control de acceso, no repudio y autenticación, así como del mecanismo de gestión de claves.

Seguidamente se propone un sistema de seguridad que, además de ofrecer servicios de seguridad a aplicaciones multimedia sensibles de todo tipo, es también transparente para las aplicaciones que utilicen otros protocolos de seguridad. De esta forma se hace posible la comunicación segura entre terminales pertenecientes a diferentes redes locales o metropolitanas que se comuniquen a través de la RDSI-BA.

El sistema de seguridad permite que aplicaciones sensibles transformen una conexión insegura en una conexión segura mediante la negociación de unos parámetros de seguridad y de unos identificadores de la asociación a través de una conexión de datos paralela. Ello posibilita la integración de toda la seguridad en el plano de usuario del MRP de la RDSI-BA, sin necesidad de modificar el plano de control (señalización).

El sistema de seguridad se compone de dos niveles, el SEC-AAL y el SEC-APL.

El nivel más bajo, el SEC-AAL se ubica encima del nivel de adaptación MTA, y es independiente de los protocolos de nivel superior. Cualquier familia de protocolos de nivel superior puede ubicarse por encima del nivel SEC-AAL de forma transparente, ya que les ofrece la misma interfaz que el nivel de adaptación convencional. Este nivel proporciona el mecanismo de cifrado y los servicios de confidencialidad e integridad.

El nivel SEC-APL se ubica a nivel de aplicación, y ofrece el mecanismo de gestión de claves y los servicios de control de acceso, no repudio y autenticación. En este nivel se ubica también toda la gestión de seguridad. Las aplicaciones sensibles solicitan servicios de seguridad especificando ciertos parámetros a través de una interfaz de programación de la aplicación (API). Esta API define una serie de primitivas de seguridad para negociar servicios de seguridad entre aplicaciones y el nivel SEC-APL.

Para comunicaciones punto a punto los niveles SEC-APL situados en el terminal origen y en el destino intercambian una serie de mensajes para negociar unos parámetros de seguridad compatibles con unos niveles de calidad de servicio solicitados. Debe cuidarse especialmente la negociación de las claves, siendo necesario el uso de protocolos autenticados de gestión de claves. En el capítulo 5 de esta tesis se propone un protocolo de gestión de claves que puede ser usado en este entorno. La generalización de negociación de parámetros de seguridad para comunicaciones multipunto con la propuesta de sistemas de negociación de claves asociados es un campo abierto que puede constituir una futura línea de trabajo.

Se han definido también una serie de primitivas de comunicaciones que definen los mensajes intercambiados entre ambos niveles SEC-APL durante la fase de negociación de la asociación de seguridad y liberación de esta asociación.

La filosofía del diseño del sistema de seguridad y de la interfaz entre las aplicaciones y el nivel SEC-APL puede exportarse a otras redes. El nivel SEC-APL en concreto es directamente exportable a otro tipo de redes, se ha desarrollado en un sistema de seguridad para *Internet*⁷ [REB96], ofreciendo prácticamente la misma API a las aplicaciones que el sistema propuesto. Ello permite refinar los algoritmos de negociación de servicios de seguridad, y sobre este entorno se ha verificado el comportamiento del sistema y se ha refinado la especificación de las primitivas de seguridad del anexo A.

⁷ Este sistema de seguridad para Internet se ha desarrollado para servicios orientados a conexión que utilizan el protocolo TCP.

CAPÍTULO 4

Coste de Servicios de Seguridad

4.1 Introducción

En los capítulos anteriores se han estudiado diferentes posibilidades para la ubicación de los servicios de seguridad definidos por ISO/IEC 7498-2 [ISO88] en la RDSI-BA y se ha propuesto la arquitectura de un sistema de seguridad que ofrece estos servicios a aplicaciones que se comuniquen a través de esta red.

La implantación de estos servicios de seguridad en redes abiertas en las que no puede garantizarse seguridad física supone un coste añadido, tanto en elementos adicionales e incremento de tráfico en la red como en requerimientos para las entidades que participan de estos servicios, a costa de *hardware* específico adicional o a costa de capacidad de cálculo de su procesador. La evaluación del coste de la seguridad es requisito necesario para estudiar la viabilidad económica de cada servicio según las necesidades de los usuarios. Curiosamente, se trata de un tema prácticamente nuevo, del que conocemos pocos trabajos (notables excepciones son [GON93, SOR93b, SIR94, YAH93, ZOR94, REC96]).

En este capítulo se presentan métodos para evaluar el coste que supone la implantación de estos servicios, tanto en coste computacional para las entidades extremas como en incremento de tráfico en la red. Aunque este estudio se centra en la RDSI-BA, por coherencia con el resto de la Tesis, la metodología empleada es fácilmente exportable a otro tipo de redes y algunos resultados son generalizables.

4.2 Coste de la Implantación de Servicios de Seguridad

La Tabla 4.1 resume el coste que suponen los distintos servicios de seguridad, tanto para la entidad involucrada como para la red. Conviene resaltar que todos ellos requieren un mecanismo de gestión de claves cuyo coste, señalado en la Tabla 4.2, deberá añadirse a cada uno de ellos. Por brevedad, se han omitido ciertos detalles y se han presentado únicamente los que se consideran más importante. En el anexo B se presentan tablas mucho más completas y detalladas.

SERVICIO DE SEGURIDAD	COSTE PARA LA ENTIDAD	COSTE PARA LA RED
Autenticación (de entidad y de origen de los datos)	Cifrado y generación de MACs Generación de números aleatorios o mantenimiento de relojes Gestión de claves	Servidores de autenticación Intercambio de mensajes de autenticación Gestión de claves
Confidencialidad	Cifrado de información sensible con alto coste en tiempo de cálculo Gestión de claves	Suponiendo que el cifrado no incrementa longitud de mensaje, no hay coste adicional asociado Gestión de claves
Control de acceso	Mecanismos de autenticación Mecanismos de integridad Gestión de claves	Mecanismos de autenticación Mecanismos de integridad Gestión de claves
Integridad	Protocolo de integridad (función de compresión del mensaje y cifrado) con alto coste de cálculo Gestión de claves	Incremento longitud de mensajes debido a ICVs (información redundante) Gestión de claves
No repudiación (de origen y de entrega)	Almacenamiento de firmas digitales o de reconocimientos de entrega Resolución de disputas Gestión de claves	Conexión con árbitro (firmas digitales y resolución de disputas) Incremento de longitud y número de mensajes Gestión de claves

Tabla 4.1. Coste de los servicios de seguridad.

El mecanismo de la gestión de claves no sólo es especialmente relevante por tomar parte, de una forma u otra, en todos los servicios de seguridad, sino que además destaca por el crecimiento de su coste con el número de entidades en la red. Por ello, es de vital importancia en grandes redes su optimización.

GESTIÓN DE CLAVES	COSTE PARA LA ENTIDAD	COSTE PARA LA RED
Claves públicas (maestras)	Almacenamiento de propia pareja de claves privada y pública Tabla autenticada de claves públicas de entidades registradas Almacenamiento de certificados y lista de revocaciones Gestión de tabla de claves públicas (búsqueda, actualización) Comprobaciones y actualizaciones en lista de revocaciones Obtención de certificados de entidades no registradas y su verificación	Autoridades de certificación o centros de distribución de certificados (terceras partes de confianza) Conexión y tráfico de entidad con una o varias terceras partes para obtención de certificados Conexiones y tráfico para comunicación de listas certificadas de revocaciones
Claves de sesión	Almacenamiento de clave de sesión Protocolo autenticado que incluye distribución de claves de sesión	Posible participación de un centro de distribución de claves Protocolo autenticado que incluye distribución de claves de sesión

Tabla 4.2. Coste de la gestión de claves.

Conviene estudiar especialmente el coste de los servicios que se ofrecen a un mayor volumen de información. En la arquitectura propuesta en el capítulo 3, estos servicios son los ofrecidos por el nivel SEC-AAL, es decir, confidencialidad e integridad. Ambos implican el procesado de toda la información, y por ello a continuación se estudian más detalladamente.

4.3 Coste de la Confidencialidad

El cifrado de la información es el mecanismo de seguridad utilizado para ofrecer el servicio de confidencialidad. Este mecanismo implica el procesado de toda la información en función de una clave secreta compartida por emisor y receptor¹.

Cada entidad debe realizar el proceso de cifrado y/o descifrado, lo que supone un coste importante en tiempo de cálculo o requiere *hardware* adicional. Este coste se

¹ Por simplicidad no se considera la criptografía de clave pública, ya que no es adecuada para el cifrado del grueso de la información en redes de gran velocidad.

incrementa al aumentar la velocidad de la red, ya que se precisa una velocidad de cifrado mayor. En la RDSI-BA en concreto, son necesarios cifradores *hardware* específicos para aplicaciones que generen un tráfico del orden de decenas de Mbit/s.

En caso de utilizar un dispositivo *hardware* y claves diferentes en función de la aplicación o entidad destino, es muy importante el estudio de la eficiencia de este proceso de cifrado en función de la longitud de los bloques a cifrar con la misma clave.

Un cifrador con una velocidad de cifrado (v_{cifrado}), una vez cargada la clave y lanzado el proceso de cifrado, precisa un tiempo de cifrado (T_{cifrado}) para cifrar un bloque de información de longitud L , de acuerdo con la ecuación (4.1).

$$T_{\text{cifrado}} = \frac{1}{v_{\text{cifrado}}} \cdot L \quad (4.1)$$

Sin embargo, cada vez que se conmute de clave es necesario un tiempo para la inicialización de este proceso (T_{conm}) que será suma del tiempo necesario para la carga de la nueva clave en el dispositivo cifrador ($T_{\text{carga_clave}}$), y del tiempo de ejecución de las instrucciones de cifrado ($T_{\text{instrucciones}}$), como se muestra en (4.2).

$$T_{\text{conm}} = T_{\text{carga_clave}} + T_{\text{instrucciones}} \quad (4.2)$$

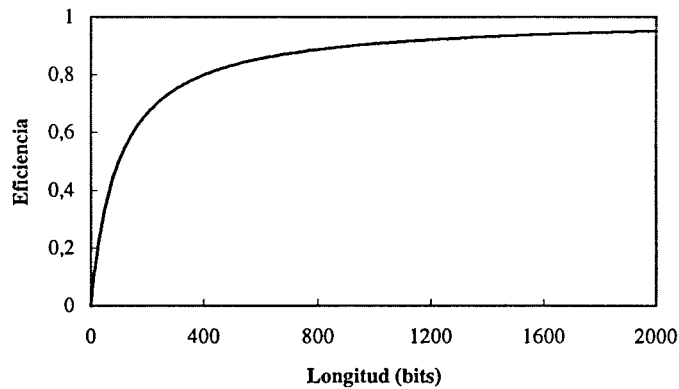
Definimos eficiencia de tiempo de cifrado (E_{TC}) como el cociente entre el tiempo que realmente el dispositivo trabaja a su velocidad de cifrado máxima y el tiempo total.

$$E_{TC} = \frac{T_{\text{cifrado}}}{T_{\text{total}}} = \frac{T_{\text{cifrado}}}{T_{\text{conm}} + T_{\text{cifrado}}} = \frac{L/v_{\text{cifrado}}}{T_{\text{conm}} + L/v_{\text{cifrado}}} = \frac{L}{T_{\text{conm}} \cdot v_{\text{cifrado}} + L} \quad (4.3)$$

Por ejemplo, para una $v_{\text{cifrado}} = 200 \text{ Mbit/s}$ y $T_{\text{conm}} = 0,5 \mu\text{s}$, se obtiene la siguiente eficiencia²:

$$E_{TC}(L) = \frac{L}{100 + L} \quad (4.4)$$

² Estos son valores cercanos a los necesarios para un dispositivo *hardware* que cifrase celdas MTA conmutando de clave en un enlace a 155 Mbit/s en la RDSI-BA. Si bien el valor de velocidad de cifrado parece alto, el valor de T_{conm} parece más difícil de alcanzar con la tecnología actual, a no ser que las claves hayan sido previamente cargadas en el dispositivo y se realice una conmutación *hardware*.



Gráfica 4.1. Eficiencia de tiempo de cifrado en función de la longitud de bits cifrados con una misma clave (para $v_{\text{cifrado}} = 200 \text{ Mbit / s}$ y $T_{\text{conn}} = 0,5 \mu\text{s}$).

La gráfica 4.1 muestra la forma de E_{TC} para los valores del ejemplo. Puede verse claramente que la eficiencia crece al aumentar la longitud de la información cifrada con la misma clave, tendiendo asintóticamente a 1.

Definimos la velocidad efectiva de cifrado ($v_{\text{ef_cif}}$) como el producto de la eficiencia de tiempo de cifrado por la velocidad de cifrado, como se muestra en (4.5).

$$v_{\text{er_cif}} = E_{TC} \cdot v_{\text{cifrado}} \quad (4.5)$$

Esta velocidad efectiva de cifrado es un parámetro importante, ya que se debe asegurar que alcance al menos la velocidad de transmisión de la red. Su dependencia con L es la misma que la de E_{TC} (gráfica 4.1). Por ello es conveniente ubicar el cifrado a un nivel en el que L sea grande y, por lo tanto, la eficiencia sea alta, como se comentó en el capítulo 2.

La función presentada en la gráfica 4.1 presupone que la longitud de entrada al algoritmo de cifrado puede tomar cualquier valor. Esto es cierto para algunos cifradores en flujo, pero no lo es para los cifradores en bloque. Estos últimos sólo aceptarán entradas de longitud (L') múltiplo de la longitud de un bloque de cifrado (M).

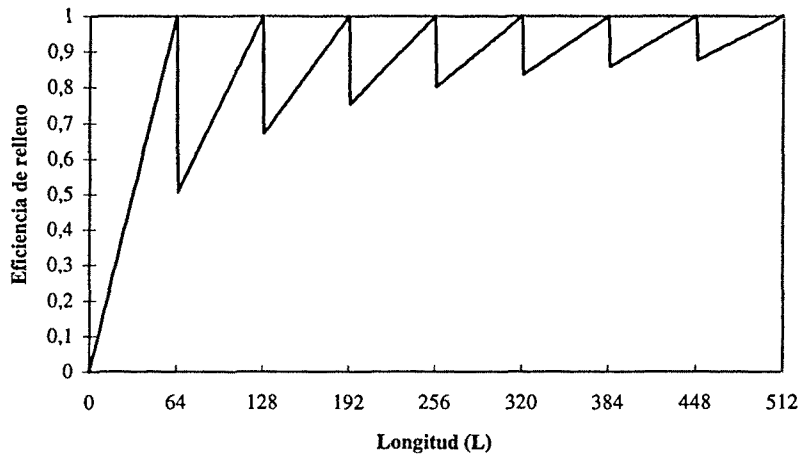
$$L' = n \cdot M \quad \text{con } n \text{ natural} \quad (4.6)$$

Para longitudes de entrada diferentes a las expresadas en (4.6) deben añadirse unos bits de “relleno” (*padding*) para conseguir una longitud múltiplo de M . Ello provoca una expansión del mensaje y, consecuentemente, un incremento de tráfico.

Definimos la eficiencia de relleno ($E_{padding}$) como el cociente entre los bits de información originales (L) y los bits totales (L') incluyendo el relleno, como muestra (4.7).

$$E_{padding} = \frac{L}{L'} = \frac{L}{M \cdot \left\lceil \frac{L}{M} \right\rceil} \quad (4.7)$$

Un valor típico es $M=64$ bits, longitud de bloque utilizada por ejemplo por DES e IDEA, los algoritmos en bloque más populares actualmente. La gráfica 4.2 muestra la forma de $E_{padding}(L)$ para $M=64$.



Gráfica 4.2. Eficiencia de relleno ($E_{padding}$) para cifrado en bloque de longitud $M=64$ bits.

El parámetro $E_{padding}$ permite estimar el incremento relativo de tráfico que provocará el cifrado ($\frac{\Delta T}{T}$), según la expresión (4.8):

$$\frac{\Delta T}{T} = \frac{L' - L}{L} = \frac{\frac{L}{E_{padding}} - L}{L} = \frac{1 - E_{padding}}{E_{padding}} \quad (4.8)$$

La gráfica 4.2 muestra que $E_{padding}$ toma valores máximos para tamaños de información $L = n \cdot M$. Sin embargo, dependiendo del nivel donde se efectúe el cifrado no siempre es posible garantizar esta condición (puede ser que las unidades de

información sean de tamaño variable). En estos casos es interesante observar que (4.9) constituye una cota inferior para $E_{padding}(L)$.

$$E_{padding}(L) > \frac{\left\lfloor \frac{L}{M} \right\rfloor}{\left\lfloor \frac{L}{M} \right\rfloor + 1} \quad (4.9)$$

De (4.8) y (4.9) puede deducirse el valor mínimo de la longitud de los mensajes a cifrar con una misma clave (L) para obtener un incremento relativo de tráfico acotado ($\Delta T/T \leq K$). En efecto, de (4.8) obtenemos:

$$E_{padding} \geq \frac{1}{K+1} \quad (4.10)$$

Mientras que de (4.9) se obtiene,

$$\left\lfloor \frac{L}{M} \right\rfloor > \frac{E_{padding}}{1 - E_{padding}} \Rightarrow L > \frac{M \cdot E_{padding}}{1 - E_{padding}} \quad (4.11)$$

Sustituyendo en (4.11) el valor mínimo de $E_{padding}$ dado por (4.10) que garantiza un incremento relativo de tráfico menor que K, se obtiene la siguiente cota:

$$L > \frac{M}{K} \quad (4.12)$$

Por ejemplo, para $M=64$ (DES o IDEA) de (4.12) se obtiene que se garantiza un incremento relativo de tráfico menor que el 5 % ($K=0,05$) para longitudes de información $L > 1280$ bits, mientras que para garantizar un incremento relativo menor que el 1% ($K=0,01$) se requieren longitudes $L > 6400$ bits.

Como conclusión conviene remarcar que ambas eficiencias definidas (E_{TC} y $E_{padding}$) crecen con L, de lo cual se deduce la conveniencia de aumentar la longitud de los bloques de información a cifrar con una misma clave. Ello comporta una mayor velocidad efectiva de cifrado (v_{ef_cif}) y un incremento relativo de tráfico ($\Delta T/T$) menor para cifradores en bloque. En la RDSI-BA las unidades de información son muy pequeñas (48 bytes) a nivel de celdas MTA, con lo cual E_{TC} es pequeña, mientras que

$E_{padding}$ también será pequeña a no ser que M sea divisor del tamaño de celda³. Por ello es preferible la ubicación del cifrado a niveles superiores, tal como se apuntó en el capítulo 2.

4.4 Coste de la Integridad

La posibilidad más utilizada para detectar ataques a la integridad de la información consiste en cifrar una cadena comprimida función de la información con una clave secreta. Esta cadena se envía conjuntamente con la información a transmitir. El receptor repite la compresión de los datos recibidos y cifrado de esta cadena con la misma clave que en emisión. Posteriormente compara con la cadena cifrada enviada y decide que la información es íntegra si ambas cadenas coinciden. La compresión y cifrado deben cumplir ciertas propiedades para garantizar una buena seguridad. Las principales opciones consisten en la utilización de un *checksum* criptográfico (que realiza la compresión y cifrado, con propiedades similares a los algoritmos criptográficos) o la utilización de una función de *hash* y el posterior cifrado del resultado de esta función.

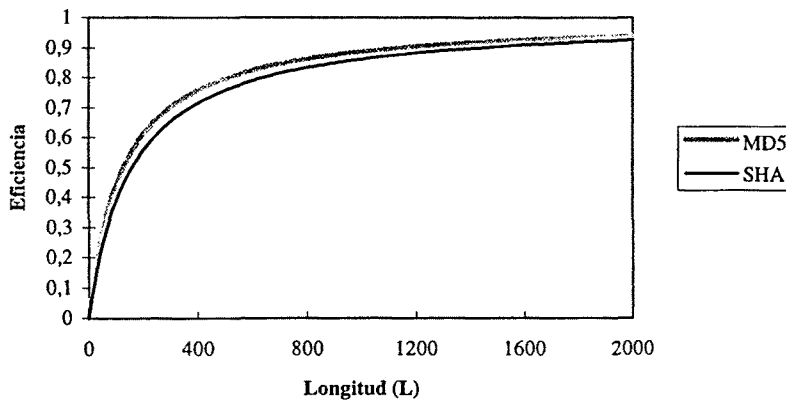
En cualquier caso se transforma un mensaje inicial de longitud L variable en una cadena comprimida de longitud fija M , y se transmite por la red un mensaje de longitud total $L'=L+M$. Así, ofrecer el servicio de integridad supone un incremento de la longitud de los mensajes a transmitir.

De forma similar al caso de confidencialidad podemos definir una función de eficiencia de integridad ($E_{integridad}$) como la relación entre la longitud de la información original (L) y la longitud que se transmite por la red (L'), según (4.13).

$$E_{integridad} = \frac{L}{L + M} \quad (4.13)$$

Valores típicos de M son 128 bits (MD5) y 160 bits (SHA). La gráfica 4.3 muestra la forma de $E_{integridad}(L)$ para ambos casos.

³ En realidad puede conseguirse una $E_{padding}=1$ si se utilizan bloques de cifrado de longitud M divisor del tamaño de celda, circunstancia que se da por ejemplo para $M=64$ bits (longitud de DES e IDEA).



Gráfica 4.3. $E_{integridad}$ en función de L para MD5 y SHA.

La gráfica 4.3 muestra que $E_{integridad}$ es siempre mayor para MD5 que para SHA, ya que este último algoritmo utiliza una información redundante (M) mayor. De igual forma puede verse que la eficiencia crece al aumentar L , lo que aconseja la ubicación del servicio de integridad a niveles altos en redes de comunicaciones, donde la información se maneja en bloques de mayor tamaño.

El incremento relativo de tráfico debido a la integridad en función de la $E_{integridad}$ viene dado por:

$$\frac{\Delta T}{T} = \frac{L-L}{L} = \frac{\frac{L}{E_{integridad}} - L}{L} = \frac{1 - E_{integridad}}{E_{integridad}} \quad (4.14)$$

Notar que la expresión (4.14) es similar a (4.8).

4.5 Gestión Eficiente de Claves

Como se mostró en el apartado 4.2, la minimización del coste de la gestión de claves es muy importante por ser éste un mecanismo necesario para proporcionar todos los servicios de seguridad. Por ello en este apartado se pretende evaluar y reducir el coste de la gestión de claves en la RDSI-BA. El estudio es general para cualquier gran red digital multidominio, como Internet o la RDSI de banda estrecha.

Una parte importante es la optimización del protocolo de negociación de claves de sesión. Para ello es necesario minimizar:

- El número de conexiones⁴ (se accederá lo mínimo posible a recursos de confianza)
- El número de mensajes intercambiados
- La longitud de estos mensajes
- El número y complejidad de operaciones criptográficas involucradas

Un protocolo eficiente atendiendo a estos criterios se presenta en el capítulo 5.7 de esta tesis, donde se detalla como se ha optimizado su coste.

Este protocolo utiliza certificados con claves públicas de tamaño variable. La longitud de certificados es general en todo protocolo de clave pública para ser independiente de la gran importancia la evaluación y optimización del coste que representa el uso de las autoridades de certificación. Por ello en primer lugar se han estudiado los modelos globales de certificación, para posteriormente proponer un protocolo que permita relacionar parámetros de seguridad con parámetros de coste.

4.5.1 Estructuras Globales de Certificación

La utilización de firmas digitales basadas en criptografía asimétrica es necesaria para conseguir mecanismos fiables de autenticación en entornos de red. La entidad que verifique la firma digital deberá confiar en la clave pública del emisor del proceso de verificación. La mejor solución a este problema es la utilización de las Autoridades de Certificación (CA, *Certification Authority*), que son entidades a las que confían tanto el que realiza la firma como el que la verifica. Como ejemplo una compañía puede certificar a sus empleados, una universidad a sus profesores o una ciudad a sus ciudadanos.

La principal labor de una CA es firmar con su clave privada correspondencia entre usuarios y sus claves públicas. Esta correspondencia firmada (como por ejemplo otros campos, como por ejemplo período de validez) se denomina certificado. El formato de certificados más ampliamente aceptado es el definido por el estándar X.509 [CCI89].

En grandes redes no existe un único punto común de confianza para todos los usuarios. Para resolver este problema, las claves públicas de los usuarios pueden ser certificadas por otras CAs, con lo que se crea una red de confianza de autoridades. Estas estructuras de confianza pueden ser utilizadas para verificar firmas digitales.

⁴ Este criterio es de gran importancia en todos los protocolos de autenticación de la IESM-04.

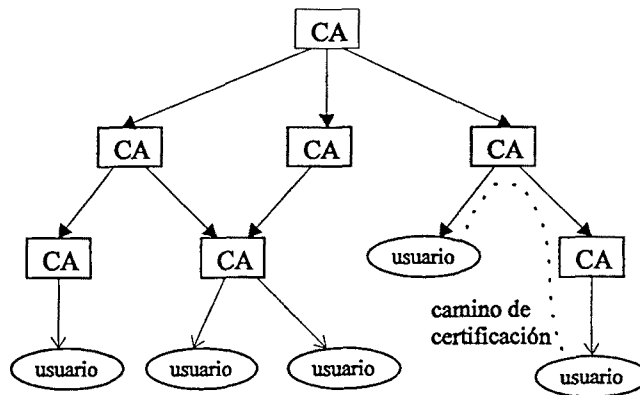


Figura 4.1. Ejemplo de estructura jerárquica de CAs.

En una estructura jerárquica cada CA es certificado por otro CA perteneciente a un nivel inmediatamente superior, hasta llegar a la raíz del árbol. Es posible que un par de CAs certifiquen un CA de un nivel inferior. Esta estructura proporciona caminos de certificación entre individuos. De esta forma se permite obtener un punto común de confianza que permita verificar la clave pública de las respectivas CAs.

Las flechas de la figura 4.1 muestran el sentido en que son emitidos los certificados. La cadena de certificados termina en un punto (la raíz del árbol), cuya clave pública no puede ser certificada. En la clave pública de la raíz deben confiar todos los usuarios, y debe ser distribuida de forma auténtica e íntegra independientemente de la red. Esta clave podría ser publicada en diarios de gran tirada, o anunciada en canales de TV, o en boletines oficiales.

En ocasiones es conveniente la revocación de certificados previamente a su expiración por las siguientes razones:

- La clave secreta de un usuario se ha comprometido
- El usuario ya no es certificado por esta CA (por ejemplo, porque ya no pertenece a una compañía)
- La clave secreta del CA se ha comprometido

Cada CA debe mantener una lista de certificados revocados que no han expirado. Estas listas debe ser públicas, y deben estar firmadas digitalmente por el emisor de los certificados.

Cuando un usuario recibe un certificado en un mensaje, debe determinar si el certificado ha sido revocado. Para ello deberá consultar la lista de certificados revocados.

4.5.2 Modelo Propuesto

Uno de los mayores costes en un escenario de clave pública es el asociado a la comunicación de las listas de revocación, es decir, las listas autenticadas de certificados inválidos [CHO94]. La necesidad de tales listas disminuye si se utiliza un tiempo de expiración de certificado suficientemente reducido, de forma que en la ventana temporal entre el instante de invalidación de una clave pública y el de su expiración no sea probable el uso ilegítimo de dicha clave. No obstante, la disminución del período de validez de un certificado supone la desventaja de hacer necesaria con mayor frecuencia su actualización.

A continuación se propone un modelo bastante sencillo que permite el dimensionado óptimo del número de entidades suscritas en cada centro de certificación, así como de la capacidad de cálculo (es decir, tiempo máximo de emisión de un certificado) a exigir a éste.

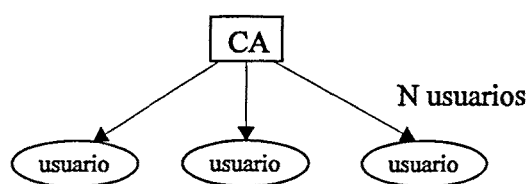


Figura 4.2. Escenario básico con un único CA.

Se considera un escenario básico donde únicamente existe un CA para todas las entidades suscritas en la red, tal como se muestra en la figura 4.2. Cada usuario conoce la clave pública con la que CA emite sus certificados, y confía en CA. Cada usuario guarda un certificado de su clave pública emitido por CA. En la negociación de claves los usuarios involucrados (que denominaremos A y B) intercambian sus certificados y posteriormente negocian claves de sesión de forma auténtica, utilizando por ejemplo el siguiente protocolo⁵:

Mensaje_1 : $A \Rightarrow B$ $\{ \text{CERT}\{S, A, P_A, T_{\text{exp}}\}_{S_S} \}$
 Mensaje_2 : $B \Rightarrow A$ $\{ \{B, N_B\}_{P_A}, \text{CERT}\{S, B, P_B, T_{\text{exp}}\}_{S_S} \}$
 Mensaje_3 : $A \Rightarrow B$ $\{ N_B, N_A \}_{P_B}$
 Mensaje_4 : $B \Rightarrow A$ $\{ N_A \}_{P_A}$

⁵ Este es el protocolo que se propone en el apartado 5.3 de esta tesis, denominado Protocolo_2. De todas formas, este estudio es general para cualquier protocolo autenticado de gestión de claves en que ambos usuarios intercambien certificados. Para detalles del protocolo y de la notación utilizada remitimos al capítulo 5.

Si el certificado de un usuario ha expirado, éste deberá obtener un nuevo certificado de CA antes de iniciar el protocolo.

Se considera que el tiempo de expiración es lo suficientemente reducido como para hacer innecesario el uso de listas de revocación. Ello permite utilizar un modelo más sencillo, en el cual no es preciso contemplar el tráfico de revocación. En este caso el tiempo de validez de un certificado es un claro parámetro de seguridad. Cuanto menor sea éste más reducida será la probabilidad de que ocurra alguna circunstancia que fuerce a que el certificado deje de ser válido. Igualmente la ventana temporal para un posible ataque también será menor.

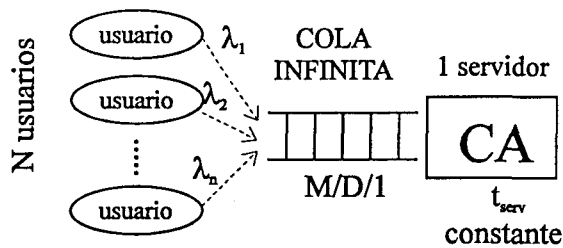


Figura 4.3. Modelo del escenario básico con cola infinita.

La figura 4.3 muestra un modelo para el escenario básico presentado en la figura 4.2 con las consideraciones anteriores. CA se ha modelado como un servidor con una cola infinita⁶ y un tiempo de servicio a una petición de certificado constante, que llamaremos t_{serv} . El tiempo de servicio será el tiempo que dedicará CA para emitir un certificado. Se ha considerado constante, ya que el proceso de emisión implica una firma digital de longitud fija cuyo tiempo de emisión puede considerarse constante⁷. La duración de la comunicación puede tener una gran varianza, pero las comunicaciones entre usuarios y CA pueden implementarse mediante procesos en paralelo con necesidades de capacidad de cálculo despreciables respecto a la emisión de certificados.

Denominaremos μ a la capacidad de cálculo del centro, que será $\mu=1/ t_{serv}$, es decir, la inversa del tiempo de servicio.

Cada usuario posee un certificado de su clave pública con un período de validez T_{exp} . Podría por lo tanto suponerse que cada usuario genera una petición de certificado

⁶ Para información general sobre teoría de colas puede consultarse por ejemplo [KLE75].

⁷ En realidad puede haber una pequeña variación en función de la relación de 1s y 0s que contenga el mensaje a firmar, pero para longitudes grandes puede considerarse equiprobable (de hecho el mensaje a firmar será la salida de una checksum criptográfico, con lo que $P(0)=P(1)$).

cada intervalo de tiempo T_{exp} . Sin embargo, es posible que un usuario no necesite un nuevo certificado justo cuando éste ha expirado (no iniciará inmediatamente una comunicación segura), por lo que se considera un tiempo de expiración *efectivo* $T'_{exp} > T_{exp}$.

En estas circunstancias, si el número de usuarios (N) es grande se puede suponer que la estadística de llegada de peticiones de certificados a CA puede caracterizarse según un proceso aleatorio de Poisson. De esta forma, la probabilidad de que se produzcan k peticiones durante un intervalo de tiempo t viene dada por la siguiente expresión:

$$P_k(t) = \frac{\lambda \cdot t^k}{k!} \cdot e^{-\lambda t} \quad (4.15)$$

de tasa,

$$\lambda = \frac{N}{T'_{exp}} \quad (4.16)$$

De esta forma la cola infinita del servidor de certificados (CA) presentado en el modelo de la figura 4.3 puede modelarse como una cola M/D/1.

4.5.3 Dimensionado de CA y del Número de las Entidades Suscritas

Siguiendo el modelo de cola infinita presentado en el apartado anterior, en este apartado se estudia el compromiso existente entre el número de entidades (N), el tiempo de validez de un certificado (T_{exp}) y la capacidad de cálculo de CA (μ) o el tiempo de servicio de una petición de certificado ($1/\mu$). Dada la sencillez del modelo propuesto se obtienen soluciones analíticas.

Se tiene pues una cola M/D/1. Sea T el tiempo medio total de generación del certificado y espera en cola. A partir de la fórmula de Pollakzec-Khinchin :

$$T = \frac{\lambda \cdot t_{serv}^2}{2(1 - \lambda \cdot t_{serv})} + t_{serv} \quad \frac{\lambda}{\mu} = \frac{N}{T'_{exp}} \cdot t_{serv} < 1 \quad (4.17)$$

En (4.17) se caracteriza un parámetro de calidad del sistema como el tiempo medio de generación de certificado y espera en cola (T), en función del número de

usuarios (N), de un parámetro que caracteriza la capacidad de cálculo CA (t_{serv}) y de un parámetro de seguridad (T'_{exp}). La relación λ/μ debe ser inferior a la unidad⁸.

Como ejemplo supongamos que CA es capaz de generar un certificado firmado digitalmente en 30 segundos ($t_{serv}=30$ s), y que para garantizar un nivel suficiente de seguridad al sistema es necesario fijar un T'_{exp} de 10 horas ($T'_{exp}=36.000$ s). La tabla 4.3 muestra diferentes valores de T para los parámetros anteriores y diferentes valores de λ/μ .

λ/μ	N	T (segundos)	T' (segundos)
0,5	600	45	45,779
0,7	840	65	65,989
0,8	960	90	91,272
0,9	1080	165	159,35

Tabla 4.3. Tiempo medio de generación de certificado más espera en cola para $t_{serv}=30$ segundos y $T'_{exp}=10$ horas.

En la tercera columna de la tabla 4.3 se muestra el valor del retardo medio (T) que se obtiene de sustituir los parámetros anteriores en la expresión (4.17). En la cuarta columna se muestra el valor (T') que se obtiene de simular el sistema con la ayuda del simulador SES/Workbench [SES92] para un período de simulación de 10^6 segundos. Se puede observar que los valores simulados son muy cercanos a los previstos por (4.17).

Si se toma como límite para el tiempo medio T_{max} , es decir, $T \leq T_{max}$, se tienen las cotas siguientes :

$$N \leq \frac{2 \left(T_{max} - \frac{1}{\mu} \right)}{\frac{1}{\mu} \left(2 T_{max} - \frac{1}{\mu} \right)} T'_{exp} \tag{4.18}$$

⁸ Este sería el máximo valor que podría absorber CA con una estadística de generación de peticiones constante.

En (4.18) puede verse el compromiso entre el nivel de seguridad (T'_{exp} pequeño) y el número de usuarios que puede atender el centro de certificación dada su capacidad de cálculo μ , en función del retardo medio admisible T_{max} .

4.5.4 Capacidad de Cálculo Óptima para CA

La expresión (4.18) del apartado anterior permite dimensionar el número máximo de usuarios por CA. Sin embargo, muchas veces N vendrá fijado por razones de ubicación geográfica y dominios de seguridad, por lo que otro problema quizás más interesante es el dimensionado del centro de certificación dado el número N de usuarios que debe atender y el parámetro de seguridad T'_{exp} . Para ello, (4.19) nos da una cota del tiempo de servicio, que depende también del parámetro de calidad T_{max} .

$$t_{serv} = \frac{1}{\mu} \leq \frac{1 + \lambda T_{max} - \sqrt{1 + (\lambda T_{max})^2}}{\lambda} \quad (4.19)$$

A continuación se muestra una metodología para hallar el coste óptimo de CA. Para ello es necesario establecer una relación entre el coste de CA (C_{CA}) y su capacidad de cálculo (μ) de la forma:

$$C_{CA} = f(\mu) \quad (4.20)$$

Una aproximación de segundo orden de esta dependencia es la siguiente :

$$C_{CA} = C_0 + C_1 \mu + C_2 \mu^2 \quad (4.21)$$

si CU_{CA} representa el coste del centro de certificación repartido entre todas las entidades, se tiene, tomando N máximo dado en (4.18) :

$$CU_{CA} = \frac{C_{CA}}{N} = \frac{1}{T'_{exp}} \frac{(2 T_{max} \mu - 1) (C_0 + C_1 \mu + C_2 \mu^2)}{2 \mu (T_{max} \mu - 1)} \quad (4.22)$$

La expresión (4.22) es sólo válida en el intervalo de μ dado por (4.19). Es interesante encontrar un mínimo de esta expresión, ya que supondrá una minimización del coste por usuario de la presencia de CA. Para ello pueden seguirse métodos numéricos, o simplemente derivar (4.22) e igualar a 0, con lo que se obtiene:

$$2 C_2 T_{\max}^2 \mu^4 - 4 C_2 T_{\max} \mu^3 - (2 C_0 T_{\max}^2 + C_1 T_{\max} - C_2) \mu^2 + 2 C_0 T_{\max} \mu - C_0 = 0 \quad (4.23)$$

Obsérvese de (4.23) que el valor óptimo de μ no depende de T'_{exp} (si que depende, en cambio, CU_{CA}). Si $C_2=0$ (aproximación lineal de $f(\mu)$), no existe el mínimo buscado, ya que la función CU_{CA} es monótona estrictamente decreciente en $(1/T_{\max}, +\infty)$.

Dados los parámetros de seguridad T'_{exp} y de calidad T_{\max} , la minimización según μ en la expresión (4.22) permite hallar la capacidad de cálculo del centro de certificación que minimiza su coste por entidad, y el número N de entidades dependientes de dicho centro. En general, representando el coste del centro o autoridad de certificación según (4.20), se debe minimizar la siguiente expresión:

$$CU_{CA} = \frac{C_{CA}}{N} = \frac{1}{T'_{\text{exp}}} \frac{(2 T_{\max} \mu - 1)}{2 \mu (T_{\max} \mu - 1)} \cdot f(\mu) \quad (4.24)$$

4.5.5 Modelo con Colas Finitas

Se ha visto que el modelo básico de la figura 4.3 permite optimizar el número de CAs a introducir en la red para ofrecer servicios de seguridad a los usuarios en una gran red multidominio como la RDSI-BA. Mediante la utilización de teoría de colas para una cola infinita se ha llegado a unos resultados donde se ha tomado como parámetro de calidad el tiempo medio de espera en cola. En un sistema real puede ser más conveniente considerar colas finitas y acotar la probabilidad de que una petición de certificado no sea atendida debido a que la cola esté llena. Por ello en la figura 4.4 se presenta un nuevo modelo con una cola finita de longitud L .

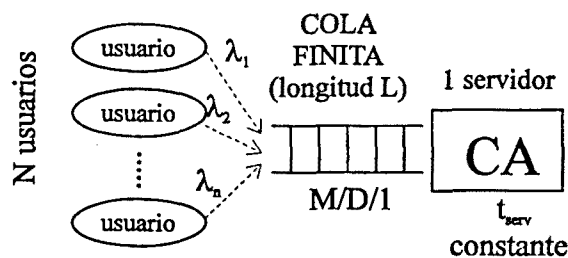


Figura 4.4. Modelo del escenario básico con cola finita.

Se ha simulado el sistema de la figura 4.4 para $L=5$ posiciones, $t_{serv}=30$ segundos y $T'_{exp}=10$ horas. Para un período de simulación de 10^6 segundos se han obtenido las probabilidades de no atención a petición de certificado mostradas en la tabla 4.4.

λ/μ	N	Peticiones atendidas	Peticiones no atendidas	Probabilidad de no atención
0,5	600	16789	16	$9,52 \cdot 10^{-4}$
0,7	840	23165	195	0,008
0,8	960	26134	544	0,020
0,9	1080	28550	1316	0,044

Tabla 4.4. Probabilidad de no atención a petición de certificados con cola finita de 5 posiciones, para $t_{serv}=30$ segundos y $T'_{exp}=10$ horas.

4.6 Conclusiones y Aportaciones

La evaluación del coste que implica la introducción de servicios de seguridad en una arquitectura de red es de vital importancia para el estudio de la viabilidad económica de la implantación de estos servicios. En efecto, los usuarios considerarán la seguridad como un servicio de valor añadido que ofrece la red y decidirán su contratación en función del coste que les suponga.

En este capítulo se han presentado algunos elementos de coste necesarios para ofrecer estos servicios de seguridad (ver tablas 4.1 y 4.2). Para el caso concreto de confidencialidad e integridad se ha evaluado cuantitativamente el coste de su introducción, mediante la definición de funciones de eficiencia que permiten cuantificar el impacto que estos servicios provocarán tanto a los usuarios finales como a la red.

Posteriormente se ha contemplado el mecanismo de gestión de claves, que es sin duda el factor clave para permitir comunicaciones seguras en grandes redes multidominio como la RDSI-BA. En este sentido se ha introducido un modelo basado en teoría de colas que permite evaluar el coste de un sistema de gestión de claves basado en una estructura jerárquica de autoridades de certificación, a la vez que permite el correcto dimensionado del número de usuarios por centro de certificación y de la

capacidad de cálculo óptima del centro en función de su coste. Este modelo fue adelantado en [FOR96b].

Ello ha permitido relacionar parámetros de coste con parámetros de seguridad, lo que constituye un trabajo original en un campo muy poco trabajado.

Un estudio detallado podría conducirnos a la elección de modelos más elaborados, siendo el presente estudio una guía que sienta las bases del método que se seguiría para optimizar el coste de la gestión de claves. Sería también interesante un modelo que contemplase un escenario de centros de certificación organizados jerárquicamente como los definidos por CCITT X.509 apto para grandes redes, dimensionando el número de niveles jerárquicos. Para ello sería necesario modelar el tráfico cursado entre niveles, que en general podría tener una estadística bastante diferente del considerado para un único nivel.

