UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

J.93

(03/98)

SERIE J: TRANSMISIONES DE SEÑALES RADIOFÓNICAS, DE TELEVISIÓN Y DE OTRAS SEÑALES MULTIMEDIOS

Servicios digitales auxiliares para transmisiones de televisión

---

Requisitos del acceso condicional en la distribución secundaria de televisión digital por sistemas de televisión por cable

Recomendación UIT-T J.93

(Anteriormente Recomendación del CCITT)

RECOMENDACIONES DE LA SERIE J DEL UIT-T

TRANSMISIONES DE SEÑALES RADIOFÓNICAS, DE TELEVISIÓN Y DE OTRAS SEÑALES MULTIMEDIOS

Recomendaciones generales	J.1–J.9
Especificaciones generales para transmisiones radiofónicas analógicas	J.10–J.19
Características de funcionamiento de los circuitos radiofónicos	J.20–J.29
Equipos y líneas utilizados para circuitos radiofónicos analógicos	J.30–J.39
Codificadores digitales para señales radiofónicas analógicas	J.40–J.49
Transmisión digital de señales radiofónicas	J.50–J.59
Circuitos para transmisiones de televisión analógica	J.60–J.69
Transmisiones de televisión analógica por líneas metálicas e interconexión con radioenlaces	J.70–J.79
Transmisión digital de señales de televisión	J.80–J.89
Servicios digitales auxiliares para transmisiones de televisión	**J.90–J.99**
Requisitos operacionales y métodos para transmisiones de televisión	J.100–J.109
Sistemas interactivos para distribución de televisión digital	J.110–J.129
Transporte de señales MPEG-2 por redes de transmisión de paquetes	J.130–J.139
Mediciones de la calidad de servicio	J.140–J.149
Distribución de televisión digital por redes locales de abonados	J.150–J.159

Para más información, véase la Lista de Recomendaciones del UIT-T.

RECOMENDACIÓN UIT-T J.93

REQUISITOS DEL ACCESO CONDICIONAL EN LA DISTRIBUCIÓN SECUNDARIA DE TELEVISIÓN DIGITAL POR SISTEMAS DE TELEVISIÓN POR CABLE

Resumen

La presente Recomendación examina los requisitos, soporte físico e interfaces de instrucción, políticas y procedimientos relativos al acceso condicional para la distribución secundaria de televisión digital y datos por los sistemas de cable.

Orígenes

La Recomendación UIT-T J.93 ha sido preparada por la Comisión de Estudio 9 (1997-2000) del UIT-T y fue aprobada por el procedimiento de la Resolución N.° 1 de la CMNT el 18 de marzo de 1998.

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Conferencia Mundial de Normalización de las Telecomunicaciones (CMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución N.° 1 de la CMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB.

ÍNDICE

Recomendación J.93

REQUISITOS DEL ACCESO CONDICIONAL EN LA DISTRIBUCIÓN SECUNDARIA DE TELEVISIÓN DIGITAL POR SISTEMAS DE TELEVISIÓN POR CABLE

(Ginebra, 1998)

1 Alcance

La presente Recomendación enumera los requisitos de los sistemas de acceso condicional (CA, *conditional access*) correspondientes a la distribución secundaria de televisión digital y señales de datos por un sistema de televisión por cable. Las características de acceso condicional efectivas seleccionadas para su aplicación en un sistema concreto deben obtenerse de los requisitos de ese sistema.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes.

[1] Recomendación UIT-T J.83 (1997), *Sistemas digitales multiprogramas para servicios de televisión, sonido y datos de distribución por cable*.

[2] Recomendación UIT-T J.84 (1997), *Distribución de señales digitales multiprogramas para servicios de televisión, sonido y datos a través de redes de antena colectiva de televisión por satélite* .

3 Definiciones

En esta Recomendación se definen los términos siguientes.

3.1 algoritmo: Proceso matemático que puede utilizarse para la aleatorización y desaleatorización de un tren de datos.

3.2 autenticación: Proceso destinado a permitir al sistema comprobar con certeza la identificación de una parte.

3.3 codificación de autorización: Palabra digital que describe la personalidad de la capacidad de acceso al servicio de la unidad decodificador de abonado.

NOTA – Esta palabra de código que se basa en el acceso al servicio autorizado por el sistema de facturación, determina qué claves se distribuyen a cada cliente, y se necesitan en el decodificador de abonado para autorizar la desaleatorización de algún programa específico.

3.4 sistema de acceso condicional (CA): El sistema completo para asegurar que los servicios por cable son accesibles sólo a quienes están autorizados a recibirlos, y que el pedido de tales servicios no está sujeto a modificación o rechazo.

3.5 criptoanálisis: Ciencia de la recuperación del texto en lenguaje claro de un mensaje sin acceso a la clave (a la clave electrónica en los sistemas criptográficos electrónicos).

3.6 ciclo de trabajo criptográfico: Máxima capacidad segura de un proceso criptográfico, basada en el número total de bits que pueden ser criptados con seguridad antes de que resulte aconsejable cambiar la clave.

3.7 desaleatorización: Proceso de invertir la función de aleatorización (véase aleatorización) para obtener imágenes, sonido y servicios de datos utilizables.

3.8 **clave electrónica**: Término que designa las señales de datos que se utilizan para controlar el proceso de desaleatorización en los decodificadores de abonado.

NOTA – Hay al menos tres tipos de claves electrónicas: las utilizadas para los trenes de señales de televisión, las utilizadas para proteger las operaciones del sistema de control, y las utilizadas para la distribución de claves electrónicas en el sistema de cable. Véase también "codificación de autorización", que también es efectivamente una clave.

3.9 **criptación**: Proceso de aleatorización de las señales para evitar el acceso no autorizado.

3.10 **servicio de conexión ordinaria permanente**: Servicio por abono que está siempre disponible para los abonados durante las horas de funcionamiento del sistema de distribución.

NOTA – En cambio, otros servicios, tales como filmes de pago por visión, sólo están disponibles durante un periodo de tiempo determinado.

3.11 **computador central**: Dispositivo con funcionalidad generalizada al que pueden conectarse módulos que contienen funcionalidad especializada.

3.12 **integridad**: Aptitud de una función para resistir su usurpación para uso no autorizado, o su modificación para conseguir resultados no autorizados.

3.13 **resistencia a la intrusión**: Aptitud de un objeto de soporte lógico para denegar el acceso físico, eléctrico, o por irradiación a funcionalidad interna por partes no autorizadas.

3.14 **módulo**: Pequeño dispositivo, que no funciona por sí mismo, destinado a realizar tareas especializadas en asociación con un computador central.

3.15 **no rechazo**: Proceso por el cual el emisor de un mensaje (por ejemplo, una petición de pago por visión) no puede negar haber enviado el mensaje.

3.16 **troceo unidireccional**: Algoritmo matemático por el que un mensaje de longitud variable se transforma en una palabra digital de longitud fija, de manera que es muy difícil calcular el mensaje original a partir de la palabra, y también muy difícil encontrar un segundo mensaje con la misma palabra.

3.17 **pago por visión**: Sistema de pago por el que el abonado puede pagar un programa individual o un periodo de tiempo especificado.

3.18 **piratería**: Acción de conseguir acceso no autorizado a programas, normalmente con el fin de revender dicho acceso para su recepción no autorizada.

3.19 **criptografía de claves públicas**: Técnica criptográfica basada en un algoritmo de dos claves, privada y pública, por el que un mensaje es criptado con la clave pública, pero puede ser descriptado con la clave privada. También conocido como sistema de clave privada-pública (PPK, *private-public key*).

NOTA – El conocimiento de la clave pública no revela la clave privada.

Ejemplo: La parte A diseñaría dicha clave privada y pública, y enviaría la clave pública abiertamente a todos quienes pudieran desear comunicar con la parte A, pero mantendría secreta la clave privada. Entonces, en tanto que cualquiera que tenga la clave privada puede criptar un mensaje para la parte A, sólo la parte A con la clave privada puede descriptar los mensajes.

3.20 **aleatorización**: Proceso de utilizar una función de criptación para hacer inutilizables las señales de televisión y de datos a las partes no autorizadas.

3.21 **signatura segura**: Proceso matemático por el cual puede determinarse el origen y la integridad de un mensaje transmitido.

NOTA – Si se utiliza un sistema de signatura segura, el originador no puede negar haber enviado el mensaje, y el receptor puede determinar si el mensaje ha sido modificado.

3.22 **tren de transporte**: Un tren de transporte MPEG-2.

4 Antecedentes

Con la aparición de la transmisión de televisión digital y de datos por cable, se necesitan nuevas normas para el subsistema de acceso (CA), o de seguridad, que ejecuta diversas funciones asociadas con este elemento del sistema. Hay numerosas actividades de normalización actualmente en curso en el mundo entero que tratan directamente el acceso condicional de la televisión por cable y de señales datos. Hay otras organizaciones que tratan de manera tangencial la seguridad de estas señales orientando los estudios a un tema más amplio que incluya también la televisión y los datos.

4.1 Televisión

Tal como ocurre hoy día con las transmisiones de televisión analógica por cable, hay variadas necesidades para los diferentes tipos de material de programación de televisión digital que serán transportados a las instalaciones del usuario por sistemas de distribución por cable. Son estos:

- Servicios de televisión de abono con conexión ordinaria permanente.
- Servicios de televisión de abono con conexión de canal con recargo.
- Servicios de televisión de transacción coherente, tales como pago por visión.
- Televisión de breve duración, que forma parte de una transmisión multimedios con fines comerciales, empresariales, o de comunicaciones.

La distribución por cable de programas de televisión presentan los dos mismos desafíos de seguridad básica que se dan en los sistemas de distribución de radiodifusión, por satélite, televisión de antena colectiva por satélite (SMATV, *satellite master antenna television*), y sistemas de distribución multipunto multicanal (MMDS, *multichannel multipoint distribution systems*), resultantes principalmente de la necesidad de instalar un decodificador operacional con material de manipulación actual en las instalaciones del usuario, uno de los cuales resulta también que es el pirata, donde puede sufrir un ataque sofisticado sin miedo de detección física. En un sistema estatal o militar tradicional de claves simétricas, esto equivale a dar al enemigo la clave criptográfica vigente. La adopción de medidas físicas, como son los microprocesadores de seguridad, hacen el trabajo más difícil, pero ninguna de estas contramedidas retrasará al profesional mucho tiempo. La distribución por cable tiene la ventaja de que al tratarse de un sistema cerrado, pueden aplicarse ciertas políticas y procedimientos tratados a continuación para hacer inútiles los esfuerzos del pirata.

Al establecer los requisitos de un sistema de acceso condicional (CA), debe prestarse atención a la evaluación de los riesgos y amenazas y los costes de capital y operacionales de las contramedidas recomendadas. El riesgo corresponde a lo que podría perderse si se viera comprometido el sistema CA. En el caso de sistemas de cable, el riesgo es la pérdida de ingresos del sistema por robo de señal, o la usurpación del control del sistema por una parte no autorizada. La amenaza es el individuo, la organización, o el mecanismo por el que las contramedidas del CA resultan comprometidas y el riesgo que se corre. Todas las contramedidas, aun si se trata solamente de procedimientos, representan algún coste para el sistema de cable operativo. Si el coste de anular la amenaza es demasiado grande con relación al riesgo, no hay entonces ninguna opción practicable.

4.2 Distribución secundaria de datos por cable

(Queda en estudio.)

5 Requisitos de acceso condicional en los sistemas de cable

El área general del acceso condicional (CA, *conditional access*), que se aplica a la distribución secundaria de televisión digital y datos por sistemas de cable, puede subdividirse y definirse como se muestra a continuación en el cuadro 1.

Cuadro 1/J.93 – Requisitos de acceso condicional y explicaciones

Requisito de acceso condicional	Explicación
Seguridad de la señal	Proporciona la criptación de las señales de televisión digital y/o de la correspondiente mensajería para impedir el acceso autorizado al contenido (véase 5.1)
Distribución de claves	Se refiere al subsistema que genera, distribuye y almacena las claves criptográficas para los codificadores del extremo de cabecera y para los decodificadores situados en las instalaciones del cliente (véase 5.2)
Signatura segura	Proceso por el cual se realizan la autenticación del usuario y el no rechazo transaccional (véase 5.3)
Integridad del sistema de control	Impide la usurpación del control del sistema por una entidad no autorizada (véase 5.4)
Codificación de autorización	Proceso por el cual la personalidad de acceso de la unidad decodificadora de abonado es protegida contra su modificación no autorizada (véase 5.5).

5.1 Requisitos de seguridad de la señal

Se requiere que cualquier canal de televisión digital o de datos transportado por un sistema operativo de cable sea susceptible de aleatorización mediante criptación digital, como opción de la gestión del sistema. El acceso a todos los servicios diferenciados debe controlarse mediante un proceso de aleatorización. Se aplican los siguientes requisitos generales a dichos procesos criptográficos:

- El proceso criptográfico elegido debe operar en un modo de clave privada-pública (PPK, *private-public key*) un modo de clave simétrica, no debe utilizar procesos PPK para distribuir claves secretas destinadas a transacciones específicas.
- El dispositivo criptográfico seleccionado para la aleatorización y desaleatorización de un tren de televisión o de datos asociado con una única portadora RF debe ser aplicable a los sistemas de distribución descritos en las Recomendaciones J.83[1] y J.84[2].
- El ciclo de trabajo del proceso criptográfico que soporta aleatorización debe ser suficiente para cumplir unos criterios adecuados de diseño criptográfico.
- El algoritmo criptográfico seleccionado para la aleatorización debe ser suficientemente resistente para hacer que un ataque criptográfico directo inicial y posteriormente efectuado por un tercero sea ineficaz por su coste y duración.
- Las características operativas del proceso criptográfico, tales como extensión de errores, latencia, velocidad de datos, variación de la velocidad de datos, y parámetros de interfaz deben ser optimizados a las características del tren de transporte MPEG-2 o de datos, según convenga.
- El algoritmo criptográfico seleccionado para la aleatorización de la señal debe ser aprobado para su utilización en todo el mundo.
- La tara del sistema de control requerida para la operación continua del algoritmo de aleatorización debe ser minimizada.
- El algoritmo debe diseñarse de manera que facilite los puntos de entrada de diagnóstico de soporte físico, soporte lógico y microprogramas necesarios para comprobaciones intensivas del sistema de seguridad y contra medidas antimanipulación.

5.2 Requisitos de distribución y almacenamiento de claves

El elemento raíz de todos los sistemas CA es la clave criptográfica binaria que se utiliza en unión de otros elementos de soporte físico y soporte lógico del sistema CA para limitar el acceso al contenido a los usuarios autorizados únicamente. La clave puede asignarse a un grupo o categoría de servicios de televisión compuesto por varios canales aleatorizados con la misma clave. La clave puede también asignarse a un canal de televisión, como en el caso de un programador aislado de programas con recargo. Una clave puede también asignarse a un cierto canal de televisión, pero sólo durante un periodo de tiempo previamente determinado, como en el caso de los servicios de pago por visión. Por tanto, se requiere que el mecanismo CA tenga la posibilidad de almacenar las múltiples claves que sean necesarias.

Además de las claves operacionales citadas, cada codificador o decodificador debe tener la capacidad de almacenar un número de identificación único permanente e inmodificable que pueda ser utilizado para la identificación de la unidad o como un tipo de clave para la radiodifusión de vía estrecha de señales a esa unidad. Para la televisión, puede ser necesario que los codificadores y decodificadores tengan la posibilidad de almacenar y utilizar claves adicionales o puede ser necesaria una compartimentalización del sistema para disminuir el riesgo resultante de los abonados piratas, un ejemplo del cual puede ser un sistema de claves troncales coherentes por el que algún elemento de la clave se cambia de acuerdo con la dirección troncal del abonado. El número exacto y la naturaleza de estas claves coherentes de un sistema es una característica que se deja a los vendedores de productos CA para su especificación.

Todas las claves, si son operacionales, del tipo identificador único, o coherentes del sistema, deben almacenarse en circuitos resistentes a la intrusión, con lo que es prohibitivo acceder por medios físicos, por irradiación, o por metodología criptográfica.

La longitud de cualquier clave depende de las características singulares y de las debilidades del algoritmo criptográfico seleccionado, pero debe ser suficientemente grande para protegerse contra ataques conocidos del sistema criptográfico durante un periodo que sea suficiente para cumplir los distintos requisitos de seguridad operacional del sistema.

La velocidad de datos efectiva necesaria para la transmisión del material de manipulación depende de los requisitos del ciclo de remanipulación, del tamaño del universo manipulado, del número de claves operacionales utilizadas, y de la longitud de las distintas claves. Estas especificaciones de diseño deben indicarse claramente en cualquier descripción de un sistema CA destinado a su utilización por sistemas de cable.

La distribución de claves puede realizarse dentro de banda mediante paquetes de datos dentro del tren de paquetes MPEG-2, o fuera de banda mediante una portadora de datos autónoma en el sistema. En cualquier caso, las transmisiones de distribución de claves representan un objetivo de gran valor para el pirata de señales, y deben protegerse en medida considerablemente mayor que el necesario para la seguridad de la señal de televisión. Si el algoritmo seleccionado para la seguridad de la señal no proporciona ese grado de protección, debe entonces utilizarse otro algoritmo para la distribución de claves. En todas las circunstancias, se utiliza una clave separada para la protección del sistema de distribución de claves. La protección del material de manipulación debe ser suficiente para resistir el compromiso durante un periodo consecuente con los requisitos de seguridad del sistema operativo de cable considerado.

5.3 Signatura segura

La signatura segura garantiza con certeza que los mensajes recibidos proceden de la fuente indicada, que no han de ser modificados, y que el remitente no puede negar haber enviado el mensaje. El proceso debe proteger los mensajes de control y de pedido que puedan ser enviados en cualquier sentido por la red de cable.

Hay varios ejemplos bien conocidos de esta clase de funcionalidad, que incluyen de manera no exhaustiva los algoritmos RSA (*Rivest-Shamir-Adleman*) o algoritmo de la signatura digital (DSA, *digital-signature-algorithm*). Estos sistemas incluyen un algoritmo de troceo unidireccional seguro que reduce el mensaje de longitud arbitraria a un trozo de longitud fija altamente distintivo del mensaje original, y que tiene las siguientes características:

- dado cualquier mensaje, es rápido y fácil calcular su trozo distintivo;
- dado cualquier trozo, es virtualmente imposible calcular el mensaje original;
- dado cualquier mensaje y su trozo, es virtualmente imposible encontrar otro mensaje que genere el mismo trozo.

Ciertos ataques clásicos sobre los trozos se limitan efectivamente al número de operaciones de análisis para atacar el algoritmo alrededor de $2^{(1/2 \text{ longitud del trozo})}$. Esto significa que un trozo de 64 bits puede descomponerse con 2^{32} operaciones, quizá un trabajo de una hora para un moderno computador personal de alta velocidad. Por esta razón, cualquier trozo utilizado para la función signatura segura en un sistema de cable debe ser de longitud suficiente para cumplir los requisitos operacionales del sistema.

5.4 Integridad del sistema de control

Esta funcionalidad se implementa para asegurar que no puedan introducirse en el sistema de control partes no autorizadas con fines de robo de señales o interrupción de servicios. Las señales de control en las que el riesgo de robo o interrupción es razonablemente bajo se criptan en su forma normal para su transmisión a un decodificador individual, un grupo de decodificadores, o globalmente a todos los decodificadores del sistema. Los mensajes de control que son de gran valor pueden someterse a contramedidas adicionales. El sistema de control exige una clave separada y distintiva de las utilizadas para la seguridad de la señal o a la distribución de claves.

5.5 Codificación de autorización

Además del proceso de proteger criptográficamente el material de programación, se requiere un proceso seguro para establecer la autorización de cada abonado. En el extremo de cabecera, esta personalidad del servicio determina qué claves criptográficas están autorizadas para su telecarga a cada abonado, y sirve en la unidad de abonado como protección contra la inserción no autorizada de claves criptográficas pirateadas desde una fuente exterior. Puede ser implementada por una técnica cualquiera elegida entre varias.

6 Fabricación y seguridad de distribución

El soporte lógico que es fabricado para el CA de las señales de televisión digital y de datos por sistemas de cable es necesario que satisfaga ciertas prácticas para asegurar la integridad de sus sistemas. Son éstas:

- toda la documentación del diseño de circuitos integrados y de vectores de prueba estará numerada y se someterá a comprobación de forma regular con documentación sobre cualesquiera elementos que falten para su examen por los posibles abonados;
- todos los circuitos integrados fabricados de uso en el soporte físico de CA serán auditados y cada elemento documentado en cuanto a su disposición final, incluida su integración en un dispositivo central y el número de serie de este dispositivo, su trayecto de distribución y la identificación de sistema operativo de cable en el que está operando. Además, todos los circuitos integrados se marcarán con un número de identificación distintivo invariable física y eléctricamente legible.

7 Recuperación tras el fallo y de compromiso

Por razones económicas, operacionales y de seguridad, es necesario que los circuitos o soporte lógico de CA puedan ser fácilmente suprimibles y sustituibles, sin tener también que sustituir el dispositivo central (o dispositivos centrales) con el (los) que interactúa. Tales sustituciones pueden ser necesarias debido al fallo de elementos mecánicos, eléctricos o de soporte lógico de la funcionalidad de CA, ya que las cambiantes estructuras comerciales y arquitecturales exigen una funcionalidad nueva o diferente, o porque se ha concebido y perpetrado algún ataque, que ha comprometido seriamente la seguridad, con el resultado de una pérdida inaceptable de ingresos o de control del sistema.

La amovibilidad implica que todos los circuitos y el soporte lógico de CA deben estar contenidos en un módulo que hace interfaz con un dispositivo central, tal como una unidad decodificadora situada sobre o detrás del aparato, un receptor de televisión o un VCR, un módem de datos o un computador personal. La sustituibilidad significa que no hay factores de interfaz, operacionales, legales o financieros que hagan imposible la sustitución de la funcionalidad de CA.

Para satisfacer estos requisitos, la interfaz entre el módulo CA amovible y el dispositivo central debe ser no propietario y de arquitectura abierta. Hay cierto número de tales interfaces y factores en forma de módulo comúnmente definidos para otras aplicaciones internacionales que pueden ser convenientes en este caso, por ejemplo, una especificación de interfaz común DVB (véase [I.3]) o la especificación definida por la National Renewable Security Standard (véase [I.4]). (Queda en estudio.)

8 Capacidad de garantía de claves

Si la legislación nacional de cualquier país exige la inclusión de una capacidad de garantía de claves dentro del sistema de CA, debe entonces incluirse funcionalidad para introducirla. En el momento de redactar esta Recomendación, no existe dicho requisito en ningún país que sea miembro de derecho de la UIT.

9 Políticas y procedimientos

Ningún sistema criptográfico es verdaderamente seguro sin un conjunto de políticas y procedimientos operacionales que respalden la función. El modo de implementar estas políticas y procedimientos en un sistema operativo de cable es dependiente de la situación. Por tanto, deben adoptarse las siguientes directrices con prácticas recomendadas y adaptarse a cada situación operacional en la forma necesaria.

- El personal que tiene acceso al sistema de control de CA y el extremo de cabecera de cable o al centro regional, que trata de oficio las unidades de abonado, debe someterse a un programa de fiabilidad humana.
- El acceso a elementos clave de sistemas de CA debe restringirse y mantenerse la vigilancia de dichas zonas.
- Los grandes sistemas de cable y las grandes aglomeraciones deben estar compartimentados por procedimientos criptográficos para reducir el área de operaciones de los abonados piratas.
- Los sistemas de CA no verificados cuya adquisición se considera deben ser sometidos a prueba por una organización de certificación independiente.
- Debe iniciarse y mantenerse un sistema de comprobación regular de seguridad.
- Deben implantarse procedimientos que permitan la captura de una unidad de CA ilegal activa, y la identificación del abonado pirata debe determinarse por examen del identificador distintivo de la unidad y de su código de autorización.

Apéndice I

Bibliografía

Se incluyen aquí las siguientes normas regionales e internacionales como información antecedente aplicable.

[I.1] ISO/CEI 13818-1:1996, *Generic coding of moving pictures and associated audio information: Systems*.

[I.2] ISO 7816: *Identification Cards*, Parts 1-6.

[I.3] Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications, *DVB A007*, July 1995.

[I.4] National Renewable Security Standard, *EIA/NCTA IS-679*, Parts A and B.

[I.5] Digital Video Broadcasting – Support for use of Scrambling and Conditional Access with Digital Broadcasting Systems, *EBU*.

[I.6] CCIR Report 1079-1 (1990), *General Characteristics of a Conditional Access Broadcasting System*.

[I.7] Recomendación UIT-T J.81 (1993), *Transmisión de señales de televisión digitales con codificación de componentes para las aplicaciones con calidad de contribución al tercer nivel jerárquico de la Recomendación UIT-T G.702*.

[I.8] Recomendación UIT-T J.91 (1994), *Métodos técnicos para asegurar la privacidad de las transmisiones internacionales de televisión a larga distancia*.

[I.9] UIT-T CE 9 Contribución Tardía D.19 (1997-2000): *The conditional access system of digital cable television in Japan*.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie B	Medios de expresión: definiciones, símbolos, clasificación
Serie C	Estadísticas generales de telecomunicaciones
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedios
Serie I	Red digital de servicios integrados
Serie J	**Transmisiones de señales radiofónicas, de televisión y de otras señales multimedios**
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos y comunicación entre sistemas abiertos
Serie Y	Infraestructura mundial de la información
Serie Z	Lenguajes de programación