UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

T.36

Enmienda 1
(04/99)

SERIE T: TERMINALES PARA SERVICIOS DE TELEMÁTICA

Capacidades de seguridad para su utilización con terminales facsímil del grupo 3

Enmienda 1

Recomendación UIT-T T.36 – Enmienda 1

(Anteriormente Recomendación del CCITT)

RECOMENDACIONES UIT-T DE LA SERIE T

TERMINALES PARA SERVICIOS DE TELEMÁTICA

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

RECOMENDACIÓN UIT-T T.36

CAPACIDADES DE SEGURIDAD PARA SU UTILIZACIÓN CON TERMINALES FACSÍMIL DEL GRUPO 3

ENMIENDA 1

Resumen

La enmienda 1 a la Recomendación T.36 define el modo anulación asociado con el sistema de criptación HKM/HFX.

Orígenes

La enmienda 1 a la Recomendación UIT-T T.36 ha sido preparada por la Comisión de Estudio 8 (1997-2000) del UIT-T y fue aprobada por el procedimiento de la Resolución N.º 1 de la CMNT el 1 de abril de 1999.

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 *empresa de explotación reconocida (EER)* designa a toda persona, compañía, empresa u organización gubernamental que explote un servicio de correspondencia pública. Los términos *Administración*, *EER* y *correspondencia pública* están definidos en la *Constitución de la UIT (Ginebra, 1992).*

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

CAPACIDADES DE SEGURIDAD PARA SU UTILIZACIÓN CON TERMINALES FACSÍMIL DEL GRUPO 3

ENMIENDA 1

(Ginebra, 1999)

1) Subcláusula A.2.2

Modifíquese A.2.2 como sigue:

A.2.2 Funciones

La gestión de claves se efectúa mediante el sistema definido en el anexo C/T.36. Se definen tres procedimientos:

1) el modo registro (véase C.4);

2) el modo transmisión segura (véase C.5); y

3) el modo contraorden (véase C.7).

El registro establece secretos mutuos y permite que todas las transmisiones posteriores se efectúen con seguridad. En las transmisiones posteriores, el sistema HKM proporciona autenticación mutua, una clave secreta de sesión para la confidencialidad y la integridad de los documentos, la confirmación de recibo o la confirmación o denegación de la integridad de los documentos.

La confidencialidad de los documentos se obtiene utilizando el sistema de cifrado definido en el anexo D/T.36. El cifrado utiliza una clave de doce cifras decimales que sea aproximadamente equivalente a 40 bits.

La integridad del documento se obtiene mediante el sistema definido en el anexo E/T.36. Este anexo define el algoritmo de troceo, incluidos los correspondientes cálculos y el intercambio de información.

2) Nueva subcláusula C.7

Añádase una nueva cláusula C.7 con el texto siguiente:

C.7 Modo anulación

El modo anulación permite que los operadores de terminales se comuniquen independientemente y en secreto, utilizando dos terminales facsímil seguros conformes con la Recomendación T.36, sin necesidad de un proceso de registro entre los dos terminales. Se efectúa evitando los procedimientos automáticos de gestión de claves del modo seguro (véase C.5). No se genera ninguna primitiva mutua, no se extrae ningún número de criptación y no se establece ninguna clave de sesión secreta. En lugar de ello, el usuario terminal introduce una clave de sesión secreta de 12 cifras previamente dispuesta en el terminal emisor, que se utiliza como una cifra portadora para proporcionar confidencialidad de documentos. El usuario terminal en el terminal receptor, introduce la misma clave mutuamente convenida que se utiliza con la cifra portadora para descriptar el documento recibido.

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 y aspectos generales de soporte lógico para sistemas de telecomunicación