UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T M.3320

(04/97)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE M: RGT Y MANTENIMIENTO DE REDES: SISTEMAS DE TRANSMISIÓN, CIRCUITOS TELEFÓNICOS, TELEGRAFÍA, FACSÍMIL Y CIRCUITOS ARRENDADOS INTERNACIONALES

Red de gestión de las telecomunicaciones

Marco de los requisitos de gestión para la interfaz de la RGT

Recomendación UIT-T M.3320

(Anteriormente Recomendación del CCITT)

RECOMENDACIONES DE LA SERIE M DEL UIT-T

RGT Y MANTENIMIENTO DE REDES: SISTEMAS DE TRANSMISIÓN, CIRCUITOS TELEFÓNICOS, TELEGRAFÍA, FACSÍMIL Y CIRCUITOS ARRENDADOS INTERNACIONALES

Introducción y principios generales de mantenimiento y organización del mantenimiento	M.10–M.299
Sistemas internacionales de transmisión	M.300–M.559
Circuitos telefónicos internacionales	M.560–M.759
Sistemas de señalización por canal común	M.760–M.799
Circuitos internacionales utilizados para transmisiones de telegrafía y de telefotografía	M.800–M.899
Enlaces internacionales arrendados en grupo primario y secundario	M.900–M.999
Circuitos internacionales arrendados	M.1000–M.1099
Sistemas y servicios de telecomunicaciones móviles	M.1100–M.1199
Red telefónica pública internacional	M.1200–M.1299
Sistemas internacionales de transmisión de datos	M.1300–M.1399
Designaciones e intercambio de información	M.1400–M.1999
Red de transporte internacional	M.2000–M.2999
Red de gestión de las telecomunicaciones	**M.3000–M.3599**
Redes digitales de servicios integrados	M.3600–M.3999
Sistemas de señalización por canal común	M.4000–M.4999

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

RECOMENDACIÓN UIT-T M.3320

MARCO DE LOS REQUISITOS DE GESTIÓN PARA LA INTERFAZ DE LA RGT

Resumen

Esta Recomendación describe un marco general y establece los requisitos básicos de gestión para el desarrollo y utilización de la interfaz RGT-X.

Orígenes

La Recomendación UIT-T M.3320 ha sido preparada por la Comisión de Estudio 4 (1997-2000) del UIT-T y fue aprobada por el procedimiento de la Resolución N.° 1 de la CMNT el 19 de abril de 1997.

Palabras clave

Aspectos internacionales, consideraciones sobre la seguridad, intercambio de información de gestión, interfaz RGT-X.

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 ha recibido/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 M.3320

MARCO DE LOS REQUISITOS DE GESTIÓN PARA LA INTERFAZ DE LA RGT

(Ginebra, 1997)

1 Introducción

Este conjunto de requisitos identifican la parte aplicable al intercambio de información (a través de una interfaz RGT-X automatizada), entre Administraciones para lograr una gestión de red y del servicio de extremo a extremo conjunta. Puede ampliarse para incluir los requisitos de gestión de red de cliente que pueden añadir nueva información para intercambio entre Administraciones. Esta Recomendación se basa en la definición de la interfaz X que aparece en la Recomendación M.3010.

1.1 Alcance

La presente Recomendación forma parte de una serie de Recomendaciones relativas a la transferencia de información para la gestión de las redes y servicios de telecomunicaciones. El objetivo de esta Recomendación es definir un marco general relativo a los requisitos funcionales, de servicio y a nivel de red para el intercambio de información sobre la RGT entre Administraciones. La Recomendación presenta igualmente el marco general de utilización de la interfaz RGT-X para el intercambio de información entre Administraciones, empresas de explotación reconocidas, otros operadores de redes, suministradores de servicios, clientes y otras entidades.

1.2 Referencias

1.2.1 Referencias normativas

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.

– Recomendación UIT-T M.3010 (1996), *Principios para una red de gestión de las telecomunicaciones.*

– Recomendación UIT-T M.3020 (1995), *Metodología de especificaciones de la interfaz de la red de gestión de las telecomunicaciones.*

– Recomendación UIT-T M.3200 (1997), *Servicios de gestión y zonas gestionadas de telecomunicación de la RGT: Descripción general.*

– Recomendación UIT-T M.3400 (1997), *Funciones de gestión de la red de gestión de las telecomunicaciones.*

– Recomendación UIT-T Q.811 (1997), *Perfiles de protocolo de capa inferior para las interfaces Q3 y X.*

– Recomendación UIT-T Q.812 (1997), *Perfiles de protocolo de capa superior para las interfaces Q3 y X.*

– Recomendación UIT-T X.160 (1996), *Arquitectura del servicio de gestión de red de cliente para redes públicas de datos*.

– Recomendación UIT-T X.161 (1997), *Definición de servicios de gestión de red de cliente en redes públicas de datos*.

– Recomendación UIT-T X.200 (1994), *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de referencia básico: El modelo básico.*

– Recomendación X.800 del CCITT (1991), *Arquitectura de seguridad para la interconexión de sistemas abiertos para aplicaciones del CCITT*.

– Recomendación UIT-T X.811 (1995), *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Marcos de autenticación.*

1.2.2 Otras referencias

– Recomendación F.435 del CCITT (1991), *Servicio de mensajería con intercambio electrónico de datos*.

– Recomendación M.1520 del CCITT (1992), *Intercambio normalizado de información entre Administraciones*.

– Recomendación UIT-T M.3000 (1994), *Visión de conjunto de las Recomendaciones relativas a la red de gestión de las telecomunicaciones.*

– Recomendación UIT-T M.3100 (1995), *Modelo genérico de información de red.*

– Recomendación UIT-T X.162 (1997), *Definición de la información de gestión para el servicio de gestión de red de cliente en redes públicas de datos que se ha de utilizar con la interfaz CMNc*.

– Recomendación UIT-T X.163 (1995), *Definición de la información de gestión para el servicio de gestión de red de cliente en las redes públicas de datos que se ha de utilizar con la interfaz CMNe*.

– Recomendación UIT-T X.509 (1997), *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marco de autenticación.*

– Recomendación UIT-T X.741 (1995), *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Objetos y atributos para el control de acceso.*

– Recomendación UIT-T X.802 (1995), *Tecnología de la información – Modelo de seguridad de capas más bajas*.

– Recomendación UIT-T X.803 (1994), *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de seguridad de capas superiores.*

– Recomendación UIT-T X.810 (1995), *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Visión general*.

– Recomendación UIT-T X.812 (1995), *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Marco de control de acceso.*

– Recomendación UIT-T X.813 (1996), *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Marco de no rechazo.*

– Recomendación UIT-T X.814 (1995), *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Marco de confidencialidad*.

– Recomendación UIT-T X.815 (1995), *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Marco de integridad.*

– Recomendación UIT-T X.816 (1995), *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Marco de auditoría y alarmas de seguridad*.

– ISO 9735:1988, *Electronic data interchange for administration, commence and transport (EDIFACT) – Application level syntax rules.*

– ISO 11166-1:(1994), *Banking – Key management by means of asymmetric algorithms – Part 1: Principles, procedures and formats*.

– ISO 9979:(1991), *Data cryptographic techniques – Procedures for the registration of cryptographic algorithms*.

1.3 Abreviaturas

En esta Recomendación se utilizan las siguientes siglas.

AI Información sobre autenticación (*authentication information*)

CMISE Elemento de servicio común de información de gestión (*common management information service element*)

CNM Gestión de red de cliente (*customer network management*)

CPE Equipo en los locales del cliente (*customer premises equipment*)

DAF Función de acceso al directorio (*directory access function*)

DSF Función del sistema de directorio (*directory system function*)

ICF Función de conversión de la información (*information conversion function*)

LAN Red de área local (*local area network*)

LLA Arquitectura lógica por capas (*logical layered architecture*)

MAF Función de aplicación de gestión (*management applications function*)

MCF Función de comunicación de mensaje (*message communication function*)

OSF Función del sistema de operaciones (*operations system function*)

OSI Interconexión de sistemas abiertos (*open system interconnection*)

RCD Red de comunicaciones de datos

RGT Red de gestión de las telecomunicaciones

ROA Empresa de explotación reconocida (*recognized operating agency*)

SF Función de seguridad (*security function*)

SMK Conocimiento de gestión compartido (*shared management knowledge*)

WAN Red de área amplia (*wide area network*)

1.4 Definiciones

En esta Recomendación se definen los términos siguientes.

1.4.1 interfaz X de la RGT: Interfaz física aplicada en los puntos de referencia x seleccionados (véase la Recomendación M.3010). El punto de referencia x es el punto situado entre dos OSF que se encuentran en distintas RGT.

1.4.2 Administración: Organismo de un gobierno designado para representar a dicho gobierno y sus intereses en la UIT. Cabe señalar que a veces se trata de la Administración de CTT y a veces de otro organismo. La entidad del gobierno actúa para administrar a escala nacional, y en coordinación con la UIT, las denominaciones, numeración, direccionamiento, contabilidad y otras normas de carácter internacional de la UIT.

1.4.3 administración: Puede utilizarse para referirse de manera general a las entidades propietarias o que pueden explotar RGT destinadas al servicio público o a su utilización como redes privadas.

1.4.4 operador de red: Organismo que explota una red de telecomunicaciones. Un operador de red puede ser un suministrador de servicio y viceversa y puede que proporcione, o no, servicios de telecomunicaciones concretos.

1.4.5 usuario de la RGT: Entidad que desempeña al menos el cometido de un gestor en relación con una RGT. En el contexto de la RGT, un usuario puede establecer interfaz con un suministrador de servicio o un operador de red RGT a través de la interfaz X, siempre que el usuario disponga de un sistema o de una red de gestión RGT o similar (véase también la Recomendación M.3020).

1.4.6 suministrador de servicio: Referencia general a una entidad que proporciona servicios de telecomunicaciones a los clientes y a otros usuarios mediante el pago de una tarifa o por contrato. Un suministrador de servicio puede explotar o no una red y puede ser o no cliente de otro suministrador de servicio.

1.4.7 cliente: Organización que tiene relaciones comerciales con un suministrador de servicio para la prestación de servicios de red. Un cliente puede englobar uno o más usuarios finales de los servicios de telecomunicaciones.

1.4.8 requisitos de gestión: Tarea específica asociada a entidades identificables. En el sentido UIT, se aplica a los miembros de la UIT que por consenso acuerdan aceptar los principios y disposiciones indicados en la Recomendación de la UIT.

1.4.9 servicio de gestión: (Véase la Recomendación M.3020).

1.4.10 caso de acceso: En el contexto de la interfaz X se trata del conjunto de condiciones, políticas y factores del entorno comercial donde va a aplicarse dicha interfaz.

2 Requisitos de arquitectura y comunicaciones

En esta cláusula se detallan las especificaciones de los requisitos para complementar y suplementar los perfiles de protocolo y la arquitectura de la interfaz RGT-X que figuran en las Recomendaciones de las series M.3000 y Q.800.

Un sistema no RGT puede interfuncionar con un sistema de la RGT a través de una interfaz X si proporciona funcionalidad y mensajes RGT para dicha interfaz.

2.1 Requisitos de organización

Los distintos casos de acceso a la interfaz RGT-X pueden describirse en términos del conjunto de condiciones, políticas y factores del entorno comercial en que debe aplicarse la interfaz X. Este

conjunto de condiciones o requisitos puede considerarse en gran medida en términos de las organizaciones que estudian la utilización de la interfaz RGT-X.

Los requisitos de organización para gestionar un conjunto de recursos a través o entre RGT incluye la subdivisión del entorno de gestión según la jurisdicción, los criterios geográficos, los criterios tecnológicos, las políticas de actuación, las razones de organización y las distintas áreas funcionales. Las características de una interfaz X vienen definidas fundamentalmente por los servicios de gestión RGT proporcionados a través de la misma. Sin embargo, las consideraciones estudiadas en esta subcláusula pueden tener influencia sobre los servicios de gestión proporcionados a través de una interfaz X y sobre los medios mediante los que son proporcionados.

La RGT puede tener distintos propietarios, a saber:

– Administraciones nacionales;
– administraciones que son operadores de redes internacionales;
– empresas de explotación reconocidas por la UIT;
– suministradores de servicios de valor añadido, organizaciones industriales con acceso limitado a operadores de red local/nacional;
– clientes y usuarios no abonados.

Desde un punto de vista administrativo, la interfaz X puede variar según los límites geográficos o jurisdiccionales de la forma siguiente:

– dentro de la compañía;
– entre compañías;
– intranacional;
– internacional.

2.2 Requisitos de interfuncionamiento organizativo

Los distintos casos de acceso en que puede aplicarse la interfaz RGT-X también pueden describirse en términos de:

– los requisitos reales para el interfuncionamiento entre RGT;
– la relación comercial o de colaboración entre propietarios de RGT; y
– el tipo y función del modelo de gestión que puede utilizarse.

El conjunto de requisitos de la interfaz RGT-X debe tener en cuenta el interfuncionamiento entre RGT para soportar las siguientes aplicaciones entre administraciones y los siguientes servicios comerciales proporcionados a los clientes:

– interfuncionamiento RGT pública-RGT pública para soportar diversas aplicaciones entre administraciones;
– interfuncionamiento RGT pública-RGT privada para soportar varios servicios comerciales;
– interfuncionamiento RGT pública-red de gestión "similar a la RGT" pública/privada.

Los diferentes usos de la interfaz RGT-X se han agrupado en los siguientes modelos. Cada configuración se considera como un modelo de gestión único.

Cuadro 1/M.3320 – Clasificación de los modelos de gestión de la interfaz X

Modelo de gestión	Relación de colaboración
Modelo de gestión cooperativa	Entre pares
Modelo de gestión conjunta	Gestor-Agentes
Modelo de gestión de red de cliente	Gestor-Agente, Cliente-Suministrador de servicio

Las diferencias entre estos conceptos afectan el tratamiento de los aspectos administrativos, de control y de seguridad/de perfil. Las diferencias entre modelos también son causa de las variaciones de los requisitos funcionales y de gestión del servicio.

2.2.1 Modelo de gestión cooperativa

Cuando dos o más operadores de redes deben compartir en una relación entre pares el tipo de interfuncionamiento RGT utilizado por la interfaz X se habla de modelo de gestión cooperativa.

Como el concepto RGT ha sido diseñado para soportar redes de telecomunicaciones, el propietario o el operador de la red es el actor principal de dicha red dentro de una relación de colaboración. En este modelo de gestión, un operador de red necesita una asociación de interfaz RGT-X con otro operador de red. Normalmente ello exigirá un acuerdo bilateral que permita a ambas partes establecer y delimitar claramente las funciones realizadas por la interfaz X.

Los requisitos de gestión cooperativa en la interfaz X utilizada entre entidades pares son los siguientes:

– toman parte dos o más operadores de red y uno o más de dichos operadores pueden desempeñar o no el cometido de un suministrador de servicio, también;

– es necesario llegar a un acuerdo contractual para el establecimiento de la interfaz X y la aplicación de las funciones de interfuncionamiento RGT;

– es necesario llegar a un acuerdo contractual para cada servicio de telecomunicaciones y su gestión respectiva;

– los acuerdos bilaterales pueden diferir entre las distintas partes, por ejemplo en un grupo amplio, dos partes pueden negociar contratos individuales para el intercambio de información de gestión a través de la interfaz X;

– el operador de red proporciona una visión de la gestión del servicio cuando uno o más operadores de red solicitan el servicio;

– cada parte mantiene el control de sus recursos pero proporciona los medios para su utilización por otras partes, según acuerdo bilateral;

– dos o más operadores de red soportan los cometidos de gestor y agente recíprocos.

En la figura 1 se representa un ejemplo de modelo de gestión cooperativa.

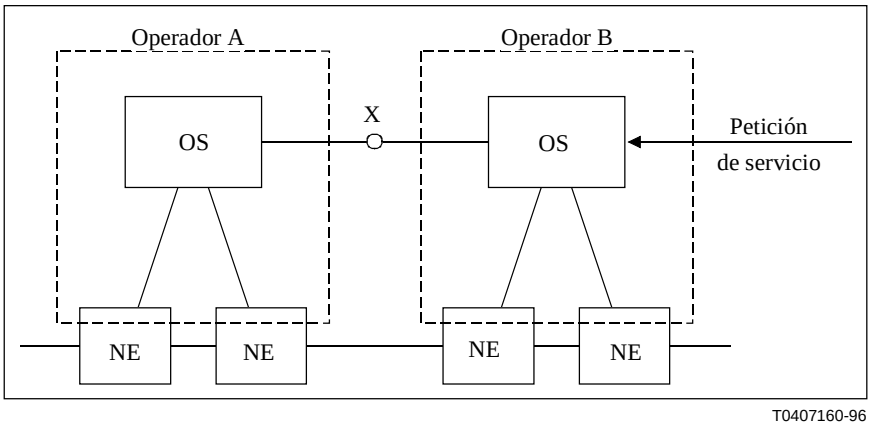


Figura 1/M.3320 – Ejemplo de gestión cooperativa a través de la interfaz X

2.2.2 Modelo de gestión conjunta

En este modelo de gestión, un grupo de operadores de red puede acordar centralizar las funciones en un solo emplazamiento o en una sola entidad operacional. Esta agrupación funcional entre operadores de red recibe el nombre de gestión conjunta. Otras relaciones de colaboración entre operadores pueden permanecer o no de la misma forma que en el modelo de gestión cooperativa dependiendo de las funciones que se hayan centralizado. Las funciones de interfuncionamiento RGT reales pueden semejarse a una configuración de un solo gestor y diversos agentes.

A continuación se describen diversos casos que ha hecho posible la gestión conjunta utilizando la interfaz RGT-X:

– dos o más operadores establecen una sociedad cooperativa bajo una sola jurisdicción;

– los socios reparten los beneficios según un acuerdo de repartición acordado con arreglo a los recursos utilizados;

– la información sobre gestión del servicio se proporciona al cliente a través de un suministrador de servicio de algún tipo;

– el suministrador de servicio gestiona los asuntos externos (acuerdos con propietarios no-partes) sobre los servicios de telecomunicaciones acordados;

– los asuntos de gestión entre la entidad central y los recursos contratados por los socios se gestionan a través de la interfaz X.

La figura 2 representa un ejemplo de modelo de gestión conjunta.

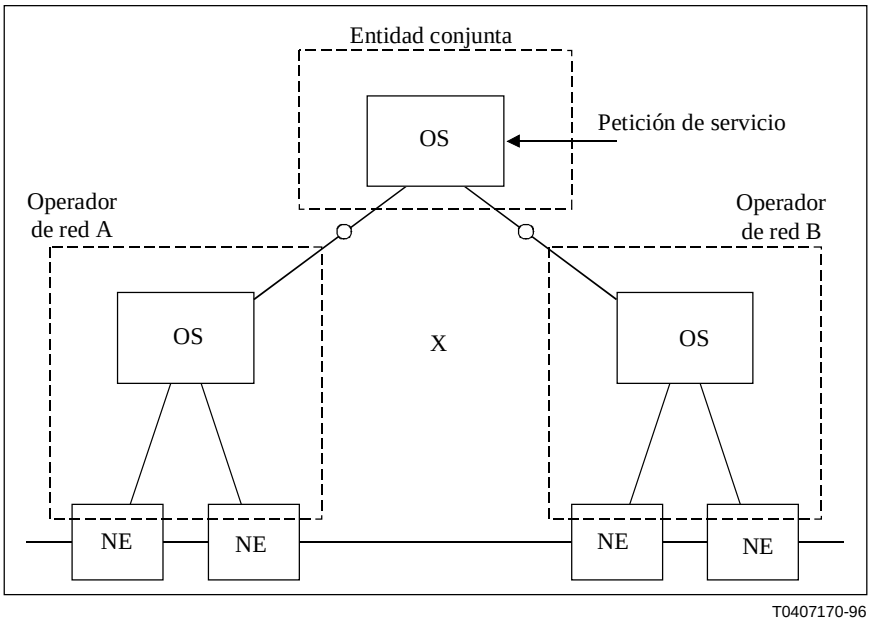


Figura 2/M.3320 – Ejemplo de gestión conjunta a través de la interfaz X

2.2.3 Modelo de gestión de red de cliente

Un suministrador de servicio puede ofrecer servicios de gestión a un cliente mediante tarifas o a través de otro acuerdo comercial. En este caso, el usuario especifica al propio suministrador de servicio y, por consiguiente, puede considerársele como un cliente. Este concepto en asociación con la interfaz RGT-X puede bautizarse como gestión de red de cliente. La relación de colaboración puede considerarse, en consecuencia, como una asociación de suministrador a cliente.

La relación del tipo suministrador de servicio-cliente establecida utilizando el modelo de gestión de red de cliente RGT puede describirse en las siguientes líneas:

– suministrador de servicio y cliente implicados;

– mediante suscripción, tarifa o contrato, el suministrador de servicio garantiza unos ciertos derechos de gestión (información, acceso, características, etc.) a un cliente;

– el volumen de información proporcionada y los derechos garantizados a través de la interfaz X pueden variar según el acuerdo de servicio al que haya llegado un suministrador de servicio y cada uno de sus clientes;

– los clientes se comunican normalmente al menos con un gestor y pueden tener funcionalidad de agente dependiendo del ámbito del acuerdo de servicio particular establecido con el suministrador de servicio.

La figura 3 representa un ejemplo del modelo de gestión de red de cliente.

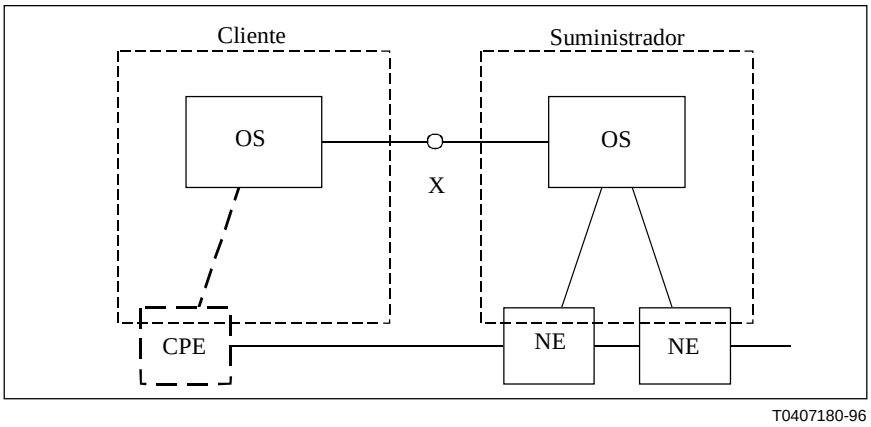


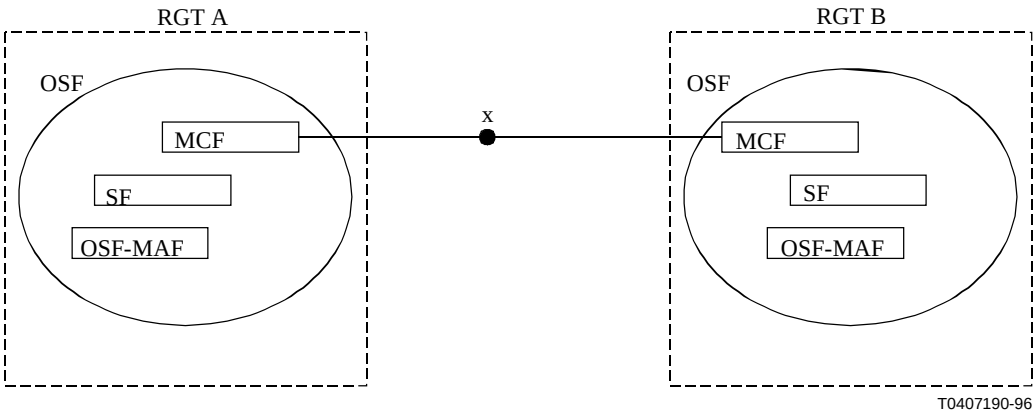
Figura 3/M.3320 – Ejemplo del tipo de gestión de red de cliente de la interfaz X

Obsérvese que un cliente puede explotar su propio equipo (CPE) en su entorno RGT o "similar a RGT".

Cuando el punto de referencia x se encuentra situado entre una RGT y un sistema de gestión distinto de la RGT, será invisible en el lado RGT; es decir, el sistema distinto de la RGT representará una funcionalidad similar a la RGT y soportará los protocolos y mensajes de la RGT.

2.3 Aspectos del bloque función

El bloque de función del sistema de operaciones en el punto de referencia x de la RGT incluirá las componentes funcionales obligatorias y opcionales indicadas en la figura 4.



OSF-MAF Función del sistema de operaciones – Función de aplicación de gestión (*operations system function – management application function*)
MCF Función de comunicación de mensaje (*message communication function*)
SF Función de seguridad (*security function*)

Figura 4/M.3320 – Bloques de función RGT básica en los puntos de referencia x de la RGT

2.4 Requisitos de denominación y direccionamiento

Considerando que cualquier RGT puede interfuncionar con otras varias RGT, es necesario identificar toda entidad gestionable, independientemente de su emplazamiento en términos de las RGT. Es preciso asignar nombres unívocos globales a las entidades gestionables en las relaciones entre RGT.

Las entidades RGT que participan en las comunicaciones de la interfaz X deben poder aceptar dichos nombres unívocos.

Los operadores de red y los usuarios que utilizan denominación global deberán asegurarse de que su nombre es único en todo el mundo.

Los requisitos para la estructura del formato de denominación global para la interfaz RGT-X son los siguientes:

– País que va recibir el mensaje RGT.

– Nombre/código de la organización que identifica el operador de red internacional.

– Recurso o servicio identificado dentro de la organización.

Para soportar las comunicaciones de datos entre RGT, pueden utilizarse puntos de acceso al servicio de red (NSAP, *network service access point*) u otras direcciones de capa de red a fin de identificar sin ambigüedades las entidades del sistema extremo que se comunican (es decir, los OS y los NE). Las direcciones de capa de red están asignadas de forma jerárquica por la ISO/UIT-T, y pueden estructurarse de forma diferente en las RGT que se comunican.

La RGT puede traducir el nombre global a la dirección de capa de red (por ejemplo, a través de directorios).

2.5 Servicios de comunicaciones

2.5.1 Aspectos del servicio interactivo

La Recomendación Q.812 define los servicios interactivos para la interfaz RGT-X proporcionados por el elemento de servicio común de información de gestión (CMISE: X.710).

El CMISE se organiza alrededor de dos tipos de servicios:

– los servicios de notificación de gestión pueden utilizarse para informar de cualquier suceso sobre un objeto gestionado que señale el usuario CMISE;

– los servicios de operación de gestión definen las operaciones para crear, recoger, modificar, suprimir o llevar a cabo otras acciones sobre el objeto gestionado.

2.5.2 Aspectos del servicio de transferencia de ficheros

La Recomendación Q.812 define los servicios de transferencia de fichero para la interfaz RGT-X como indican las partes 1 a 4 de la publicación ISO 8571, Transferencia y gestión de ficheros.

Las estructuras de fichero soportadas suponen la utilización de los cuatro siguientes tipos de documentos:

– ficheros binarios sin estructurar;

– ficheros de texto estructurados;

– ficheros de texto sin estructurar;

– ficheros ordenados secuencialmente (estos ficheros están constituidos por una secuencia de registros sin ninguna posibilidad de acceder directamente a un registro determinado; cada registro está compuesto por campos de distinto tipo).

2.5.3 Aspectos del servicio de directorio

La Recomendación Q.812 define los servicios de directorio para la interfaz RGT-X proporcionados por las Recomendaciones de la serie X.500. Los sistemas de directorio pueden definir una arquitectura que permite la distribución de la base de datos del directorio a un número en principio ilimitado de sistemas extremos OSI. A pesar de su distribución física, el usuario o la aplicación final que invoque el servicio de directorio debe considerar al directorio como una sola unidad lógica.

Los servicios de directorio pueden aplicarse a través del punto de referencia x. La Recomendación M.3010 describe la relación general de las componentes funcionales de directorio dentro del marco RGT. Los servicios de directorio que se extiendan más allá de los límites de una RGT utilizarán el punto de referencia x. Estos servicios pueden emplearse siempre que la disponibilidad mundial de la información sea fundamental para el funcionamiento de un sistema o servicio o sea beneficioso para la calidad de funcionamiento de un sistema o servicio.

Los bloques de función RGT pueden utilizar opcionalmente las componentes funcionales de directorio para implementar la función de directorio necesaria. Esto se modela en la arquitectura funcional RGT como componentes funcionales RGT que pueden estar contenidas en bloques de función RGT específicos que requieran la funcionalidad de directorio. La figura 5 representa la integración del directorio y la RGT.

Dependiendo de la arquitectura elegida, DSF-DSF o DAF-DSF [función de sistema de directorio (DSF, *directory system function*), función de acceso al directorio (DAF, *directory access function*)] pueden establecerse asociaciones a través del punto de referencia x. La asociación puede establecerse entre DSF/DAF de bloques de función RGT de distintas RGT o entre DSF/DAF de un bloque de función RGT y otro bloque de función similar a la RGT fuera de una RGT específica.

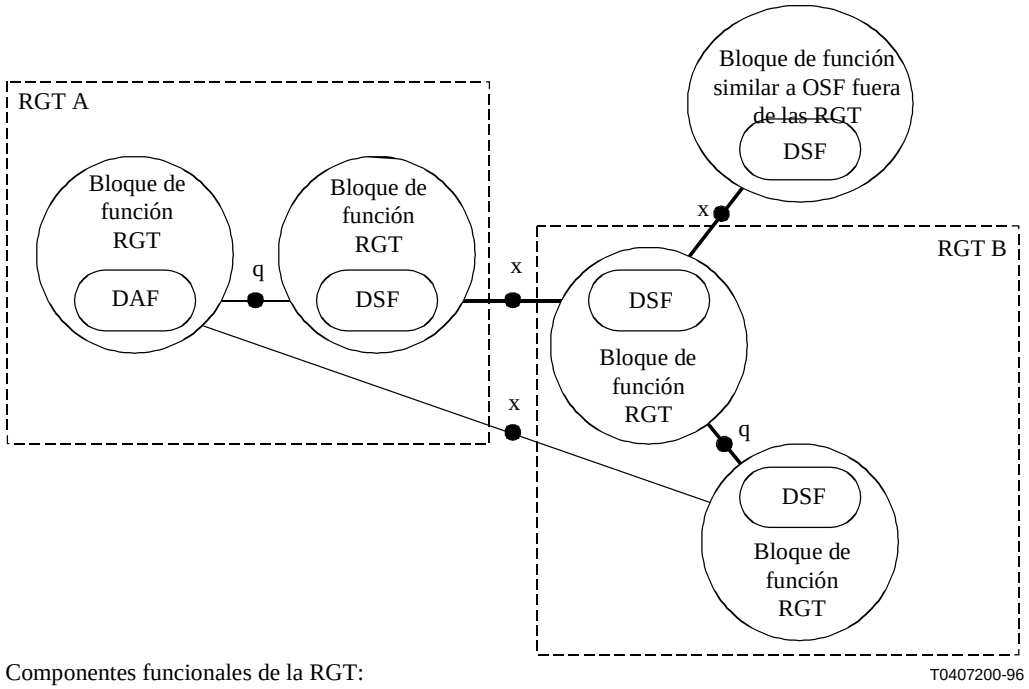


Figura 5/M.3320 – Aplicación de la arquitectura de directorio a la interfaz RGT-X

2.5.4 Aspectos del servicio de almacenamiento/retransmisión

Quedan en estudio.

2.6 Aspectos de la red de comunicaciones de datos

En la Recomendación Q.811, Protocolo de capa inferior de la RGT para las interfaces Q3 y X, se definen las distintas redes de comunicaciones de datos (RCD) actualmente reconocidas para apoyo de las interfaces RGT-X. El tipo de RCD y la topología de la red se deciden por acuerdo de los propietarios de RGT de forma bilateral o multilateral, teniendo en cuenta la seguridad, la redundancia de la red y otras condiciones. Sin embargo, los diseñadores de la RGT pueden aprovechar las directrices indicadas a continuación.

Las aplicaciones de la interfaz RGT-X pueden utilizar uno o más perfiles/pilas de protocolo de capa inferior RGT basados en criterios de selección tales como calidad de funcionamiento y seguridad.

Para la interfaz RGT-X se han identificado los siguientes requisitos de la RCD:

a) Las RGT pueden interfuncionar a través de una amplia variedad de tecnologías e interconexión de redes, incluidas las WAN y las LAN.

b) Los perfiles de capa inferior de la Recomendación Q.811 pueden utilizarse en las interfaces X.

c) La comunicación punto a punto debe soportarse por la transferencia de fichero interactiva y de bloque.

d) La comunicación punto a multipunto puede ser necesaria para satisfacer ciertos requisitos asociados con los servicios de gestión de algunas zonas gestionadas.

e) Deben soportarse comunicaciones locales, nacionales e internacionales.

f) La interconexión de redes permite que las RCD utilicen distintos protocolos de capa inferior para comunicarse. Los métodos de interconexión de redes RCD definidos en la Recomendación Q.811 son aplicables a la interfaz X.

3 Requisitos del servicio de gestión

En esta cláusula se indican los requisitos de gestión para la utilización de la interfaz RGT-X. Los requisitos de gestión deberán organizarse adecuadamente para asegurar que se interpretan convenientemente las necesidades de los usuarios RGT. Las siguientes subcláusulas son de interés para los usuarios RGT. Se indican los aspectos internacional y de usuario para establecer una clasificación más detallada de las diversas necesidades específicas a varias relaciones.

3.1 Áreas gestionadas de telecomunicaciones

La interfaz X puede soportar el intercambio de información de gestión para las áreas gestionadas de telecomunicaciones (como se define en la Recomendación M.3200).

3.2 Relación con la metodología RGT

Esta subcláusula describe el marco general para las actividades de la interfaz RGT-X indicadas bajo las tareas 0, 1 y 2 de la metodología RGT de la Recomendación M.3020. En esa subcláusula se indicarán los requisitos generales para la interfaz RGT-X. Los requisitos generales para los servicios de gestión se incluyen en el formato de la plantilla sobre directrices para la definición de servicios de gestión (GDMS, *guidelines for the definition of management services*) de las Recomendaciones de la serie M.3200. Los anexos a esta Recomendación relativos a consideraciones específicas al punto de

referencia quedan en estudio. Estos requisitos se agrupan con otros en las descripciones de servicio de gestión de RGT que se utilizan para activar los pasos de planificación de la TIB-X.

3.3 Categorías de los requisitos de gestión

La presente Recomendación reconoce a los suministradores de servicio que pueden ofrecer servicios al usuario final como se definen en las Recomendaciones UIT-T. Esta Recomendación reconoce a los operadores de red que pueden explotar redes como se define en las Recomendaciones de la UIT. Los suministradores de servicio ofrecen servicios a los clientes e interactúan con los operadores de redes para soportar sus servicios. (NOTA – La misma organización puede actuar como operador de red y como suministrador de servicio.)

La gestión soportada por la interfaz X puede agruparse en las aplicables entre cometidos y dentro de los mismos. Es decir, un conjunto de servicios de gestión puede definirse como aplicable entre el operador de red, entre los suministradores de servicio, entre suministradores de servicio y clientes y entre operadores de redes y vendedores de sus equipos.

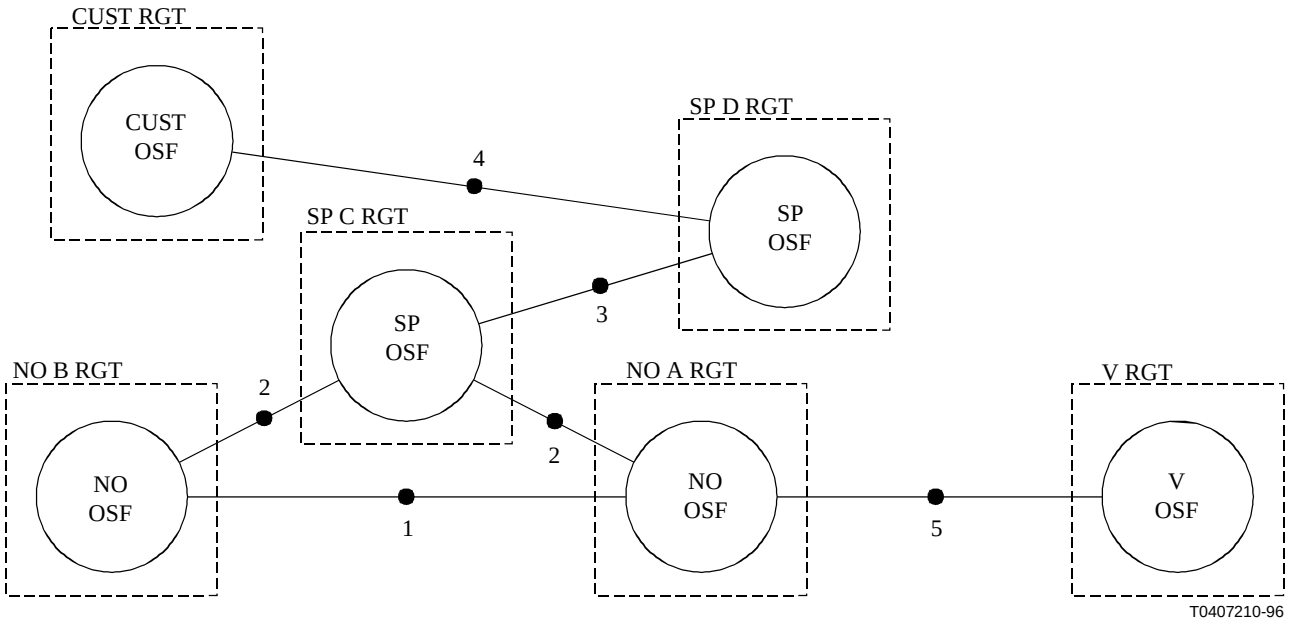
La intersección entre los participantes en estos servicios de gestión se caracteriza por los distintos modelos de gestión definidos en la cláusula 2 y se muestran en el cuadro 2 dando algunos ejemplos en la figura 6.

Una organización determinada (propietaria de una RGT) puede actuar en más de una de estas categorías; es decir, un operador de red puede también actuar como un suministrador de servicio. Los requisitos de gestión también pueden especificarse en términos de categorías específicas. La razón para introducir las categorías de requisitos de gestión es que el intercambio de información a través de la interfaz X puede entenderse mejor teniendo en cuenta estas categorías.

Obsérvese que para una determinada categoría de requisitos de gestión puede ser aplicable más de un modelo de gestión. La asignación de las categorías primaria o secundaria es hipotética y no vinculante.

Cuadro 2/M.3320 – Ejemplos de pares de relaciones

N.°	Categorías de los requisitos de gestión	Modelos de gestión		
		Cooperativa	Conjunta	CNM
1	Operador de red – Operador de red	P	S	S
2	Operador de red – Suministrador de servicio	S	S	P
3	Suministrador de servicio – Suministrador de servicio	S	S	P
4	Suministrador de servicio – Cliente	S	S	P
5	Operador de red – Vendedor del equipo	S	S	P*
P Opción primaria P* Opción primaria pero en sentido inverso S Opción secundaria				



NO Operador de red (*network operator*)
SP Suministrador de servicio (*service provider*)
CUST Cliente (customer)
V Vendedor (al operador de red)
OSF Función del sistema de operaciones (*operations system function*)

Figura 6/M.3320 – Ejemplos de pares de relaciones de las categorías de gestión

3.3.1 Categoría de requisitos de gestión operador de red a operador de red

La siguiente lista, no exhaustiva, contiene los servicios relativos a la red de información que puede que los operadores deseen intercambiar a través de una interfaz X para acomodar los actuales procedimientos de operador dentro de la red mediante una interfaz RGT automatizada.

FM: Gestión de alarma
Problemas de tasación
Gestión de tráfico (parte FM)
Procedimiento de escala
Prueba

CM: Gestión de tráfico (parte CM)
Un solo punto de contacto
Administración del cliente
Circuito/establecimiento del sistema/puesta en servicio/puesta en servicio de la red
Restablecimiento

AM: Contabilidad
Intercambio de facturación

PM: Calidad de funcionamiento de la red
Gestión de tráfico (parte PM)
Gestión de la calidad del servicio

SM: Usuarios autorizados

Se concede prioridad a la identificación de la necesidad más urgente del soporte del intercambio de información del operador dentro de la red a través de una interfaz X. La mayor prioridad se da a la especificación de la interfaz X para la utilización del operador dentro de la red; la segunda prioridad son las necesidades de una versión del operador del cliente de red de la interfaz X.

a) gestión de averías para conmutación y transmisión;

b) mantenimiento, FM, PM para líneas arrendadas (líneas privadas internacionales);

c) un solo punto de contacto;

d) puesta en servicio;

e) facturación electrónica.

Actualmente, en un entorno previo a la RGT, otras Recomendaciones UIT-T identifican la información intercambiada entre operadores de redes. En ese sentido, la Recomendación M.1520 resume las Recomendaciones pertinentes de las series E y M que requieren el intercambio de información entre los operadores de red. La interfaz RGT-X debe satisfacer estos posibles requisitos de intercambio de información actualmente definidos y debe soportar futuros requisitos adicionales, ampliándose el número de categorías de requisitos de gestión.

3.3.2 Categoría de requisito de gestión operador de red – suministrador de servicio

Los operadores de red pueden proporcionar una interfaz a los suministradores de servicio para:

– Permitir a los suministradores de servicio el acceso a la información sobre los recursos de red en las áreas de gestión de averías y de calidad de funcionamiento.

– Permitir a los suministradores de servicio solicitar al operador de red que soporte un servicio con los recursos de red en el área de gestión de la configuración y ofrezca información sobre tales configuraciones.

– Soportar las funciones de gestión de la contabilidad.

– Soportar las funciones de gestión de la seguridad.

3.3.3 Categoría de requisito de gestión suministrador de servicio – suministrador de servicio

La categoría de requisito de gestión suministrador de servicio-suministrador de servicio es necesaria para proporcionar intercambio de información de gestión de servicio entre los suministradores de servicio a fin de soportar un entorno comercial determinado.

3.3.4 Categoría de requisito de gestión cliente a suministrador de servicio

Los clientes desean utilizar la capacidad de gestión de una forma común en el entorno de multioperadores y multiservicios para extraer la información de gestión y llevar a cabo las operaciones de gestión. Como ejemplo puede citarse el intercambio de datos relativos al cliente, incluida la información sobre servicio y gestión.

3.3.5 Categoría de requisito de gestión operador de red – vendedor

Algunas veces el operador de red es capaz de proporcionar los servicios de gestión como un operador a otras entidades que no poseen o explotan una red de telecomunicaciones. A estas entidades puede considerárselas como usuarios y puede ser personal de mantenimiento de vendedor, entidades contratadas etc. A menudo, un contrato de servicio entre el vendedor y el operador determinará los derechos y privilegios que el personal del vendedor puede tener con la propiedad del operador de red. En este caso, cabe esperar que el operador de red actúe en el papel de agente o servidor y el usuario actúe en el papel de gestor o solicitante. Hay que indicar que este modelo se ajusta más al mantenimiento de red que a la puesta en funcionamiento del servicio al usuario final.

3.4 Conocimiento de gestión compartido para la interfaz X

Cada interfaz RGT puede clasificarse dependiendo del modelo de información en el que se basa la relación gestor/agente (en particular, véase 3.3 de la Recomendación M.3010, Conocimiento de gestión compartido). En el caso de la interfaz X se especificarán muchos modelos distintos de información, correspondientes a los diversos requisitos funcionales.

La disponibilidad de tal conocimiento de gestión compartido es un requisito previo al funcionamiento de la interfaz X y, por consiguiente, la RGT debe proporcionar e identificar los medios para establecerle.

4 Consideraciones relativas a la seguridad

En esta cláusula se identifican los requisitos de seguridad para el intercambio de información de gestión así como la gestión de los mecanismos de seguridad que soportarán el intercambio de información de gestión. La presente cláusula:

– describe las condiciones que repercutirán notablemente en el grado de seguridad que debe o puede aplicarse en una determinada instancia de utilización de la interfaz RGT-X;

– identifica las amenazas contra la seguridad y los riesgos conexos al intercambio de información en la interfaz RGT-X, así como los riesgos contra la propia RGT;

– identifica los requisitos funcionales y las capacidades de seguridad opcional específicas a la interfaz RGT-X;

– explica los servicios de seguridad que se utilizarán en la interfaz RGT-X para considerar las amenazas, riesgos y requisitos identificados;

– identifica los requisitos, características y funciones adicionales para gestionar los servicios de seguridad que soportan la interfaz RGT-X;

– se centra en la utilización de la interfaz RGT-X para el intercambio de material importante sin comprometer la integridad de la propia interfaz RGT-X;

– documenta los procedimientos para utilizar el registro de algoritmos criptográficos de la ISO.

4.1 Ámbito y objetivos de la seguridad

Esta subcláusula trata únicamente de los aspectos relativos a la seguridad específicos a la utilización, mantenimiento y soporte de la interfaz RGT-X. La presente Recomendación no define los requisitos de seguridad para la interfaz Q3 OS-OS u OS-NE o para las aplicaciones o configuraciones de la interfaz F.

Estos aspectos de la seguridad se relacionan con la especificación de la componente funcional RGT denominada función de seguridad incluida en el bloque de función OSF de soporte como describe la Recomendación M.3010.

Estos aspectos de seguridad también están relacionados con los servicios de gestión RGT que suponen el intercambio de información entre diversas RGT. Estos aspectos deben igualmente constituir las bases de las funciones de seguridad indicadas en la Recomendación M.3400, Funciones de gestión RGT. Estos aspectos de seguridad también deben considerarse un requisito para el servicio de gestión RGT, "Gestión de la seguridad RGT".

Esta subcláusula señala además los requisitos aplicables al conjunto de protocolo RGT para la interfaz X descrito en las Recomendaciones Q.811 y Q.812. Los objetivos de seguridad genéricos considerados para la interfaz RGT-X incluyen la autenticación, el control de acceso, la confidencialidad, la integridad y las auditorías de no rechazo y de seguridad.

4.1.1 Consideraciones de aplicación

Cada aplicación de la interfaz X debe estudiarse detalladamente como parte de la metodología de interfaz RGT para determinar del mejor modo posible la forma de resolver las amenazas contra la seguridad, solventar los riesgos y satisfacer los requisitos de seguridad.

No todos los mecanismos de seguridad son necesarios para todas las aplicaciones. Una aplicación puede utilizar un modelo de gestión de interfaz RGT-X particular. La aplicación puede incluir uno o más servicios de gestión RGT, conjuntos de función de gestión y funciones de gestión RGT. Los servicios de comunicaciones y las condiciones medioambientales deben derivar en decisiones relativas a la seguridad de la interfaz. Cada uno de los servicios de gestión proporcionados por una aplicación de la interfaz RGT-X debe descomponerse hasta el nivel funcional, antes de tomar una decisión sobre los requisitos de seguridad.

4.1.2 Consideraciones sobre la implementación

Las prácticas de seguridad pueden ser distintas según las Administraciones de los diversos países. Además, una Administración puede que no aplique las mismas rutinas de seguridad que otras Administraciones. Por consiguiente, no pueden establecerse unos requisitos de seguridad generales para todos los países que pretendan utilizar la interfaz RGT-X.

Las políticas de seguridad que pueden diferir de un país a otro incluyen los mecanismos de autenticación permisible, el tipo o la robustez de las técnicas de cifrado o de criptografía utilizadas, la longitud de las claves de cifrado, etc.

Puede que se necesiten procedimientos adicionales de interfuncionamiento para separar limitaciones prácticas y de otro tipo derivadas de las diferencias en las políticas de seguridad, en las tecnologías del sistema de seguridad y en las redes de comunicaciones de datos. Para una implementación en particular puede que sea preciso aplicar unos requisitos de seguridad adicionales.

Las consideraciones de seguridad para la implementación que deben tenerse en cuenta para resolver el tema de la seguridad en una implementación concreta de la interfaz X incluyen los siguientes puntos:

– políticas de seguridad nacional;
– tecnología de seguridad disponible en los distintos países;
– configuración RCD, red especializada y redes conmutadas;
– redes públicas de datos conmutadas y redes privadas conmutadas;
– número de redes o nodos intermedios utilizados en la configuración RCD;
– tipo y configuración de RCD tales como SS7, OSI/X.25, TCP/IP, LAN/WAN, RDSI, etc.

4.2 Amenazas contra la seguridad

Debe realizarse un detallado análisis de todas las amenazas que puedan identificarse.

Las amenazas contra la seguridad identificadas en esta Recomendación se basan en los conceptos definidos en ISO 7498-2 e ISO/CEI 10181. Las amenazas pueden suponer un riesgo para la seguridad e incluyen lo siguiente.

4.2.1 Divulgación de la información

La amenaza contra la confidencialidad de la información supone el acceso a la información por una entidad no autorizada. La información puede adquirirse por dicha entidad de forma ilegítima como por ejemplo capturando mensajes en tránsito o por acceso no autorizado a la información contenida en el sistema. Por ejemplo:

– divulgación de CMIP u otras unidades de datos de protocolo sin la autorización adecuada o por partes no autorizadas.

4.2.2 Acceso no autorizado

Esta amenaza incluye el acceso no autorizado a sistemas y recursos dentro de los sistemas tales como datos y programas informáticos. Una vez logrado el acceso no autorizado a través de la interfaz X, puede provocarse una avería en el sistema interrumpiendo el funcionamiento normal del mismo. Puede perderse, modificarse o divulgarse información sensible e importante que en último término puede poner en peligro el normal desarrollo de las actividades comerciales.

4.2.3 Simulación

Esta amenaza consiste en la pretensión de una entidad de pasarse por otra entidad distinta para acceder así a la información o adquirir privilegios adicionales.

4.2.4 Amenazas a la integridad de la información

Las amenazas a la integridad de la información incluyen la fabricación o modificación no autorizada de la información que reside en los sistemas así como de información en tránsito. Por ejemplo, la reproducción, reflexión, reordenación, inserción, supresión, creación o modificación de datos antes o durante la transmisión.

4.2.5 Denegación del servicio

Se produce cuando una entidad no puede llevar a cabo sus funciones o impide que otras entidades realicen las suyas. Ello puede traducirse en una denegación de acceso a la RGT o en una denegación de comunicación por desbordamiento de la RGT. En una red compartida, esta amenaza puede concretarse como una aparición de tráfico adicional que inunda la red, impidiendo a otros usuarios su utilización o retardando su tráfico.

4.2.6 Rechazo

Negación por una de las entidades que interviene en una comunicación de haber participado en toda o en parte de la comunicación.

4.2.7 Fraude

Se produce fraude cuando una parte no autorizada utiliza un recurso o servicio provocando una pérdida de uno o más usuarios de la RGT. En el caso de gestión de clientes esa situación es especialmente crítica puesto que complica la precisión de la facturación y prestación del servicio.

4.3 Requisitos de seguridad

Se producen riesgos contra la seguridad cuando una o ambas RGT o la RCD que proporciona la interfaz X están expuestas a una o más amenazas de seguridad. El primer paso para contrarrestar las amenazas de seguridad es llevar a cabo una evaluación del riesgo contra la seguridad. En el apéndice I se ilustra un método para realizar una evaluación de la seguridad.

4.3.1 Requisitos de identificación

Las RGT deben proporcionar las capacidades adecuadas para la identificación de los usuarios en el entorno RGT. Estas capacidades pueden ser necesarias para soportar la auditoría de todas las acciones y actividades de los usuarios en la red y para proporcionar la entrada al control de autenticación y acceso.

Como requisitos básicos de seguridad para la identificación pueden citarse los siguientes:

– los usuarios de la red deberán tener nombres (o ID de usuarios) inequívocos a efectos de identificación para soportar la contabilidad y auditoría individual;

– una RGT deberá enviar el nombre del usuario de las comunicaciones a través de dominios o límites jurisdiccionales, así como el identificador RGT.

4.3.2 Requisitos de privacidad

Deben soportarse los requisitos de privacidad para asegurar que no se compromete la información confidencial. Como requisitos de privacidad básicos pueden citarse los siguientes:

– capacidad de la RGT para cifrar información sensible transmitida en el interior o a través de RGT, así como información sensible almacenada internamente en una RGT;

– la RGT debe ser capaz de proporcionar confidencialidad de extremo a extremo de los datos transmitidos en el interior o a través de distintas RGT;

– la RGT debe cifrar la información sensible cuando se utilice tecnología de difusión;

– la RGT debe tener la capacidad de distribuir y gestionar de forma segura el material importante.

4.3.3 Requisitos de autenticación

Las RGT deben proporcionar las capacidades adecuadas para permitir la corroboración de los usuarios. Algunas de estas capacidades son genéricas en su naturaleza e independientes del tipo del mecanismo de autenticación utilizado, mientras que otras no lo son.

La autenticación es un requisito obligatorio cuando se conmutan en su totalidad o en parte disposiciones de red, para las interfaces RGT-X. En las disposiciones de red especializadas de extremo a extremo donde las identidades de ambas partes de la RGT es evidente, la autenticación puede considerarse opcional.

Como requisitos de autenticación pueden citarse:

– la RGT debería poder autenticar a los usuarios;

– la RGT no deberá soportar los medios para evitar el mecanismo de autenticación;

– la RGT deberá preservar la confidencialidad de toda la información de autenticación (AI, *authentication information*) secreta. Cuando se almacene internamente en una RGT, esta información de autenticación deberá protegerse contra el acceso no autorizado. Cierta información de autenticación (por ejemplo, las palabras clave cifradas) no deben estar disponibles en texto claro incluso para usuarios muy privilegiados;

– cada usuario de la RGT debe tener una información de autenticación única;

– esta información de autenticación no deberá enviarse en forma de texto claro en el interior o a través de la RGT salvo cuando así lo exija el mecanismo de autenticación concreto utilizado; por ejemplo, contraseñas de una sola utilización y algunos mecanismos de pregunta-respuesta;

– la RGT deberá preservar la integridad de toda la información de autenticación almacenada internamente;

– la RGT deberá tener la capacidad de proporcionar una autenticación adecuada de los usuarios que deseen llevar a cabo funciones administrativas "críticas" y otras funciones de explotación, administración, mantenimiento y puesta en servicio (OAM&P);
– la RGT deberá ser capaz de incorporar y soportar esquemas de autenticación incluidos los que se basan en simples acuerdos bilaterales, servidores de terceros de confianza y contraseñas.

Cabe señalar que los sistemas de confianza y las configuraciones se consideran un tema de implementación sujeto a negociación bilateral. Algunos modelos de gestión pueden exigir la utilización de terceros de confianza. Por el contrario, el modelo de gestión cooperativa puede depender del acuerdo de únicamente dos partes.

4.3.4 Requisitos del control de acceso

Las RGT deben incluir las capacidades para controlar (conceder o denegar) el acceso a diversos recursos de telecomunicaciones basándose en las identidades de los usuarios adecuadamente autenticadas. Los requisitos para utilizar los procedimientos de control de acceso dependen del servicio de gestión real ofrecido. Como directrices para utilizar el control de acceso en la interfaz RGT-X pueden citarse:

– una RGT no deberá permitir a los usuarios el acceso a ninguno de los recursos del sistema de la red a menos que se hayan identificado y autenticado adecuadamente;
– una RGT deberá proporcionar la capacidad de control de acceso a los recursos de la RGT a todos los niveles de granularidad;
– una RGT deberá incorporar y soportar la prestación de control de acceso a diversas clases (AI, *authentication information*) de usuario incluidos, entre otros, los usuarios individuales, los grupos, los cometidos y los delegados;
– una RGT tendrá la capacidad de filtrar el acceso a los recursos basándose en cualquier combinación de entidad de origen/dirección del solicitante, operación solicitada, entidad/dirección de destino; así como el perfil de autorización;
– una RGT deberá poder incorporar y soportar mecanismos para conceder o denegar el acceso a cualquier usuario basándose en información contextual (por ejemplo, el tiempo);
– una RGT deberá controlar el acceso a las aplicaciones y llevar a cabo el control del encaminamiento, la configuración y el flujo.

4.3.5 Requisitos de integridad

Los requisitos básicos para la integridad de la red, los datos y el sistema son los siguientes:

– la RGT deberá poder asociar con fiabilidad cualquier recurso de la red (datos, procesos) con su creador/propietario original. Deben establecerse disposiciones específicas para lograr el anonimato del usuario;
– la RGT deberá poder asociar con fiabilidad los datos comunicados con su origen;
– la RGT deberá poder proporcionar la integridad de extremo a extremo de los datos transmitidos en el interior o a través de las RGT;
– la RGT deberá proporcionar mecanismos de protección contra ataques de reproducción;
– la RGT deberá preservar la integridad de los datos de la red.

4.3.6 Requisitos de la auditoría de seguridad

Entre los requisitos básicos de la auditoría de seguridad figuran los siguientes:

– la RGT deberá proporcionar los medios para validar el funcionamiento correcto de los mecanismos de seguridad (por ejemplo, la activación del registro de seguridad);

– el registro de seguridad, el control de auditoría y otras funciones de seguridad incluidas en la RGT deberán continuar funcionando tras las reinicializaciones.

4.4 Servicios de seguridad

El método de seguridad para una aplicación concreta de la interfaz RGT-X debe incluir un perfil de seguridad. El perfil engloba el conjunto de requisitos considerados pertinentes y necesarios para contrarrestar las amenazas y minimizar los riesgos. Los servicios de seguridad vendrán determinados por los requisitos de aplicación de la forma siguiente:

Cuadro 3/M.3320 – Requisitos y servicios de seguridad

Requisito	Servicio de seguridad
Identificación y autenticación	Autenticación de usuario Autenticación de la entidad par Autenticación del origen de datos
Control de acceso y autenticación	Control de acceso Autenticación del origen de datos
Control de acceso y autenticación	Control de acceso
Integridad – Datos almacenados	Control de acceso Detección de servicio denegado
Integridad – Datos transferidos	Integridad Detección de servicio denegado
Confidencialidad – Datos almacenados	Control de acceso Reutilización de objeto[a)]
Confidencialidad – Datos transferidos	Confidencialidad Reutilización de objeto
No rechazo	No rechazo
(Todos)	Alarma de seguridad, pista de auditoría, recuperación

[a)] Esta expresión hace referencia a un servicio de seguridad que asegura que los medios de almacenamiento (memoria, disco, cinta, etc.) no conservan ningún resto de información después de haber sido utilizados.

4.4.1 Servicios de autenticación

La autenticación se refiere normalmente a la autenticación par-entidad en el instante de establecimiento de la asociación pero también pueden referirse a la autenticación de usuario y/u origen de datos. La autenticación de usuario proporciona únicamente una corroboración de la identidad del usuario que probablemente sea el iniciador de la asociación.

La autenticación par-entidad durante el establecimiento de la asociación puede ser unidireccional o bidireccional. La autenticación unidireccional señala únicamente la identidad del iniciador de la asociación y la autenticación bidireccional autentifica las identidades del iniciador de asociación y del receptor de la asociación.

El servicio de autenticación de origen de datos proporciona la confirmación de la fuente de una unidad de datos. El servicio no ofrece protección contra la duplicación o modificación de las unidades de datos.

4.4.2 Servicios de control de acceso

Este servicio proporciona protección contra el acceso, la utilización, la lectura, la escritura y la supresión de información no autorizada y la ejecución autorizada de un recurso de procesamiento o a todos los accesos a un recurso.

La utilización dependerá de los casos concretos identificados en los servicios de gestión RGT puesto que tanto la información como los recursos variarán según las funciones realizadas. Entre los mecanismos de control de acceso que pueden utilizarse cabe citar:

– Listas de control de acceso que indican los derechos de acceso de las entidades pares.
– Intercambio de información que identifica la información y recursos que pueden autorizarse.
– Intercambio de información de autenticación tales como contraseñas.
– Etiquetas de seguridad que indican los niveles de seguridad de los elementos de datos que pueden utilizarse para conceder o denegar el acceso, (a menudo es necesario incorporar la etiqueta de seguridad con los datos en tránsito).
– Registro del instante de acceso, la ruta de las tentativas de acceso, la duración del acceso y el seguimiento de la utilización de los recursos.

4.4.3 Servicios de confidencialidad

Entre las formas de servicio de confidencialidad existentes pueden emplearse dos de ellas para asegurar la privacidad de las transacciones de la interfaz X:

– La confidencialidad de la conexión proporcionará un cifrado total del tren de datos.
– La confidencialidad de los datos del mensaje, incluida la confidencialidad del campo selectivo, puede utilizarse para proteger la confidencialidad de los datos utilizados en las transacciones de la interfaz X.

La utilización de la confidencialidad debe considerarse opcional y sujeta al acuerdo bilateral y al cumplimiento de las políticas de seguridad.

4.4.4 Integridad de los datos

La integridad de los datos contrarresta las amenazas activas proporcionando integridad de todos los campos de datos seleccionados y detectando cualquier información, inserción, supresión o reproducción de cualquier dato dentro de toda la secuencia.

Los servicios de integridad de datos incluyen:

– *Integridad del campo selectivo*: Este servicio puede utilizarse en la capa de aplicación o en el propio proceso de aplicación puesto que es únicamente el propio proceso de aplicación el que puede discriminar entre campos.
– *Integridad de la conexión*: Puede proporcionarse en la capa de transporte, en la capa de aplicación o en el proceso de aplicación.
– *Integridad de la conexión sin recuperación*: Puede proporcionarse en la capa de red, en la capa de transporte, en la capa de aplicación o en el proceso de aplicación.

4.4.5 No rechazo

Proporciona al receptor de los datos una prueba del origen de los mismos y al remitente una prueba de la entrega de los mismos.

4.5 Gestión de seguridad

4.5.1 Requisitos de auditoría

Las RGT deben proporcionar las capacidades adecuadas para llevar a cabo las actividades de investigación, auditoría y detección y análisis en tiempo real de manera que puedan tomarse a tiempo las medidas correctivas adecuadas.

4.5.2 Pista de auditoría

La pista de auditoría de seguridad permite el registro de los sucesos relativos a la seguridad que pueden utilizarse en una auditoría de seguridad. La pista de auditoría de seguridad debe realizarse utilizando los registros de seguridad de la forma siguiente:

– Los registros de seguridad deberán generarse y mantenerse (por ejemplo, salvaguardándolos tras un fallo del sistema) dentro de la RGT.

– Los registros de seguridad deberán protegerse contra el acceso no autorizado y no se debe permitir su modificación.

– En los registros de seguridad se inscribirán al menos los siguientes sucesos: tentativas de autenticación de usuario no válidas, tentativas no autorizadas para acceder a los recursos de la RGT de cualquier tipo, modificación en los derechos de acceso de usuario, rearranque tras parada, supresiones en el registro, modificación de los atributos de seguridad asociados a un recurso de la RGT.

– Para cada suceso registrado, el registro de seguridad deberá incluir al menos los siguientes parámetros: fecha y hora del suceso en tiempo universal coordinado (UTC, *universal time coordinated*), ID de usuario incluida la dirección de la red (si ha lugar), tipo de suceso, nombres de los recursos RGT a los que se ha accedido, éxito o fallo del suceso.

– Registrar las aparentes violaciones de la seguridad así como los sucesos "normales", tales como la conexión. Para más información, véanse las Recomendaciones X.816, X.735, X.736 y X.740.

La Recomendación X.740 define un modelo para generar informes de pista de auditoría de seguridad. Los requisitos indicados a continuación son coherentes con la citada Recomendación.

4.5.3 Informe de alarmas

Las alarmas de seguridad son un tipo particular de informe de suceso que debe registrarse siempre. El informe de alarma de seguridad se utiliza para notificar a una entidad una violación o una posible violación de la seguridad. Deben aplicarse las siguientes Recomendaciones:

– Recomendación X.734 del CCITT (1992), *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Función de gestión de informes de eventos.*

– Recomendación X.736 del CCITT (1992), *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Función señaladora de alarmas de seguridad.*

La RGT deberá proporcionar un mecanismo para notificar (por ejemplo, alarma, informe en línea) al administrador en tiempo real, y en la medida de lo posible, si el registro de seguridad no ha podido registrar los sucesos que deben registrarse.

La RGT deberá ofrecer la capacidad de traspasar la información de auditoría a medios de almacenamiento para mantenerlos más tiempo; debe evitarse la sobreescritura.

4.5.4 Requisitos administrativos

Existe un cierto número de funciones administrativas que debe soportar la RGT de forma separada a otras funciones de usuario.

Como muchos incidentes de seguridad pueden implicar a varias RGT interconectadas, puede ser conveniente que la RGT intercambie la información relativa a estos sucesos. De no ser así, los requisitos indicados a continuación pueden referirse simplemente a la propia RGT en vez de estar limitados solamente a la interfaz RGT-X:

a) La RGT proporcionará un mecanismo para que el administrador de seguridad pueda indicar en cualquier instante todos los usuarios activos en ese momento.

b) La RGT proporcionará un mecanismo para que el administrador de seguridad pueda, de forma independiente y selectiva, examinar las acciones de cualquier usuario, incluidos los usuarios privilegiados, basándose en la identidad de usuario individual.

c) La RGT deberá proporcionar un mecanismo para que el administrador de seguridad bloquee un trayecto de comunicación específico controlando las entradas a un acceso y a los sistemas de retransmisión intermedios.

d) La RGT debe ofrecer controles de congestión automáticos y manuales para contrarrestar la negativa de los ataques al servicio; por ejemplo, ataques con desbordamiento intencionado que pueden impedir que la RGT realice acciones y dé respuestas en tiempo oportuno.

e) Si se produce un fallo de la seguridad, la RGT deberá poder mantener o restaurar oportunamente los servicios de red de funcionalidad OAM&P; por ejemplo, proporcionando la capacidad para recuperar y reinicializar el sistema.

f) La RGT proporcionará la capacidad necesaria para que el administrador de seguridad desactive los ID de usuario que no han sido utilizados durante un periodo específico de tiempo o por otras razones administrativas concretas.

g) La RGT proporcionará un mecanismo para que el administrador de seguridad reinicialice la información de autenticación a los usuarios o suprima las cuentas de usuario.

h) La RGT proporcionará la capacidad de generar alarmas para sucesos de seguridad concretos incluidas las violaciones de integridad (por ejemplo, reproducciones) y las violaciones físicas (por ejemplo, manipulación del cable y elementos de intrusión).

i) La RGT proporcionará al administrador de seguridad los instrumentos de análisis de auditoría posteriores que puedan producir informes de excepción, resúmenes de informes e informes detallados sobre usuarios y elementos de datos de red específicos.

j) La RGT también deberá proteger las herramientas de explotación contra el acceso no autorizado.

4.5.5 Gestión de la clave

La seguridad comienza con la disponibilidad y utilización del material de clave de cifrado de datos. La gestión de la clave se refiere a la generación, almacenamiento, distribución, supresión, archivo y aplicación del material de clave de acuerdo con la política de seguridad. Esta política puede definirse como el conjunto de criterios para la prestación de los servicios de seguridad. En consecuencia, la gestión de la clave representa un primer paso crítico para proporcionar y asegurar servicios de seguridad fiables.

La Recomendación Q.812, Protocolo de capa superior de la red de gestión de las telecomunicaciones, identifica los mecanismos del protocolo de seguridad específicos que deben aplicarse a la interfaz RGT-X. Sin embargo, esta Recomendación especifica únicamente los requisitos de gestión para el tratamiento del material de clave para la interfaz RGT-X. Además, esta Recomendación especifica los requisitos para utilizar la propia interfaz RGT-X de forma optativa para la distribución o intercambio del material de clave cifrado.

4.5.6 Requisitos

Las dos partes de la interfaz RGT-X deberán poder soportar la gestión de la clave debido a que se necesitarán claves de cifrado para implantar los diversos servicios de seguridad antes indicados. Los requisitos mínimos para la gestión del material de clave son:

– control del material de clave durante su vida útil para evitar su distribución no autorizada, modificación o sustitución;

– distribución del material de clave para permitir el interfuncionamiento entre equipos o facilidades criptográficas;

– asegurar la integridad del material de clave durante todas las fases de su vida útil, incluyéndose su generación, distribución, almacenamiento, inscripción, utilización y destrucción; y,

– recuperación en caso de fallo de los procesos de gestión de la clave cuando se cuestiona la integridad del material de clave.

La gestión de la clave puede realizarse de forma manual o automática. La gestión manual de la clave generalmente se refiere a la distribución del material de clave a los emplazamientos en que es necesario, utilizando algunos procedimientos manuales (correo registrado, correo depositado, cinta magnética, etc.). Por otro lado, la gestión automática de la clave permite la transmisión electrónica del material de clave a través de un canal de comunicaciones seguro, hasta los emplazamientos adecuados. Sin embargo, obsérvese que incluso cuando se ha acordado una gestión automática de la clave, sigue siendo necesario soportar los procedimientos manuales para que el esfuerzo "de cebado" establezca la primera conexión segura, que es la más importante.

La gestión de la clave también varía según el tipo de sistema de cifrado utilizado en una aplicación particular de la interfaz RGT-X. Hay dos tipos de sistemas de cifrado: clave privada y clave pública, como se describe a continuación.

4.5.7 Gestión de la clave privada

El primer tipo de gestión de clave es el soporte de los sistemas criptográficos de clave privada que utilizan una transformación secreta (clave) para cifrar datos enviados a través de un canal de comunicaciones. En la RGT de recepción se utiliza la misma clave para convertir los datos cifrados a su forma original. La clave de transformación se envía al receptor autorizado a través de un canal seguro y, por consiguiente, no está disponible a otras partes.

Los sistemas de clave privada dependen de la distribución del material de clave privada por un canal seguro que puede ser manual o automática. El canal puede ser o no una interfaz RGT-X. El método de sistema de clave privada permite limitar la seguridad a únicamente las dos RGT que intervienen en el intercambio de información, independientemente de la información intercambiada con otras RGT. Esta naturaleza bilateral de los sistemas de clave privada es interesante para aplicaciones en las que interviene el modelo de gestión cooperativa.

En el apéndice II aparece más información al respecto.

4.5.8 Gestión de la clave pública

El segundo tipo de cifrado supone la utilización de sistemas de criptografía de clave pública que emplean claves distintas en las situaciones de transmisión y recepción. Una de las claves se hace pública y la otra se mantiene como clave privada. Esta no puede obtenerse a partir de la clave pública. Cada RGT en una relación de pares o en un grupo deberá mantener su clave privada en secreto y publicar la otra. Estas claves pueden utilizarse entonces en diversas transformaciones de seguridad.

4.5.9 Sistemas de confianza

La interfaz X deberá ser capaz de soportar interacciones con terceros de confianza para la autenticación, certificación y distribución de las claves.

4.6 Criptografía de los datos

Los participantes en las interacciones de la interfaz X deben poder utilizar un registro criptográfico tal como el ISO 9979. En el apéndice III se considera un ejemplo de registro criptográfico.

APÉNDICE I

Información adicional sobre evaluación de los riesgos de seguridad

Para contrarrestar las amenazas contra la seguridad, los participantes en los servicios de interfaz X pueden llevar a cabo un análisis de riesgos contra la seguridad para:

– realizar una evaluación de las distintas amenazas;

– identificar los posibles riesgos de acuerdo con las amenazas contra la seguridad pertinentes;

– clasificar las categorías de riesgos que deben considerarse así como la frecuencia con que deben tenerse en cuenta; y

– redactar un informe de evaluación de los riesgos.

Este informe constituye la base para el posterior análisis de los riesgos contra la seguridad, en el que se estudia cada uno de los riesgos por separado para determinar:

– la probabilidad de detectar un fallo en el sistema de seguridad;

– el coste y esfuerzos que suponen la existencia de esos fallos;

– el posible beneficio obtenido por el intruso al explotar el fallo del sistema;

– el posible quebranto comercial para la compañía explotadora y para los abonados de la compañía.

El resultado del análisis de riesgos debe proporcionar información suficiente para que los planificadores de la interfaz RGT-X puedan desarrollar un método de seguridad para contrarrestar las amenazas y minimizar los riesgos. El método de seguridad debe incluir un perfil de seguridad para esa aplicación determinada de la interfaz RGT-X, teniendo en cuenta las consideraciones de la aplicación y la implementación indicadas anteriormente.

APÉNDICE II

Información adicional sobre gestión de clave privada

El presente apéndice ofrece un ejemplo ilustrativo de un posible conjunto de requisitos mínimos para proporcionar un sistema de gestión de clave privada que utiliza la interfaz de un RGT-X como canal seguro:

– Manualmente, una clave principal es compartida entre ambos administradores de la RGT y representa el primer paso en un proceso de tres etapas. La clave principal se denomina también clave de cifrado de claves o KEK.

– Esta clave principal se utiliza para cifrar el segundo nivel de material de clave conocido como claves de sesión o claves de cifrado de datos (DEK, *data encrypting keys*).

– Las claves de sesión están distribuidas electrónicamente por un canal de comunicación seguro tal como la interfaz RGT-X. Las claves pueden distribuirse utilizando uno de los servicios de comunicación de la interfaz RGT-X. Sin embargo, en la mayoría de los casos el intercambio será simplemente una transferencia de ficheros.

– Las DEK son utilizadas por ambas RGT para cifrar los campos selectivos o los mensajes de datos de acuerdo con los servicios de seguridad requeridos en esa aplicación concreta de la interfaz RGT-X.

– En algunas instalaciones, puede que exista la necesidad adicional de cifrar ficheros que contengan claves de sesión utilizando un tercer conjunto de claves denominado claves de facilidad. Sin embargo, si no existe un riesgo aparente cuando las DEK se almacenan en ordenadores en cada RGT, no es necesario emplear claves de facilidad para cifrar las DEK.

La utilización de una jerarquía de dos categorías para las claves de cifrado se denomina concepto de "jerarquía de claves". Adicionalmente, el "concepto de separación de clave" debe ser también soportado por los sistemas de gestión de clave privada. La separación de clave exige que el material de clave utilizado para la autenticación no se emplee en el control de acceso, la confidencialidad de los datos, etc. Por consiguiente, las claves para cada servicio de seguridad OSI necesario en una aplicación concreta de interfaz RGT-X deben tener procedimientos distintos para la creación, almacenamiento, distribución, utilización y supresión. Si se sigue rigurosamente este concepto, la parte de RGT puede recuperarse tras un fallo en la seguridad y se puede minimizar la influencia total sobre las diversas comunicaciones que pasan a través de la interfaz RGT-X.

Para transmitir grandes volúmenes de material de clave por la interfaz RGT-X, las propias claves deben organizarse en ficheros de clave de seguridad, lo que permitirá utilizar el servicio de transferencia de ficheros y los mecanismos de protocolo de seguridad indicados en la Recomendación Q.812. Ambas partes de la RGT deben proporcionar periódicamente un fichero de texto cifrado que contenga una lista de 1000 claves, lo que puede bastar para un año. A partir de dicho conjunto, el administrador de la RGT indicará qué miembro es la clave válida utilizada para la siguiente sesión en la interfaz RGT-X. La clave real se elegirá aleatoriamente y a intervalos aleatorios por una o ambas partes de la RGT. La iniciación de una nueva clave deberá hacerse en un instante determinado acordado por ambas partes.

Los ficheros de seguridad de reserva deben contener índices múltiplos de 10 000 a efectos de reserva. El convenio de denominación para los ficheros de la clave de seguridad de reserva es: keys.networkid.bk, donde networkid es el nombre de identificación de la red para la administración/empresa de explotación reconocida y bk es el número secuencial del fichero, empezando por 10 000. Los ficheros de reserva se utilizan cuando:

1) el fichero en curso se ha visto comprometido;

2) el fichero en curso ha utilizado todas las claves; o

3) el fichero en curso ha sufrido una alteración.

Una vez utilizado un fichero de reserva, el agente debe proporcionar un nuevo fichero de reserva con un nuevo conjunto de claves e índices de reserva. Los nuevos índices comenzarán en el siguiente múltiplo secuencial de 10 000.

APÉNDICE III

Información adicional sobre criptografía de datos

El Registro ISO para Técnicas Criptográficas proporcionará las bases para la utilización de la seguridad en aplicaciones internacionales. La elección o selección de un algoritmo criptográfico en particular cae fuera del ámbito de ésta y de otras Recomendaciones de la UIT relativas a la RGT; sin embargo, dos partes de la RGT pueden referirse al Registro ISO de Algoritmos Criptográficos y acordar cuál de ellos, en su caso, puede ser el adecuado para satisfacer sus mutuas necesidades.

ISO 9979 define los procedimientos para registrar la información asociada con los algoritmos criptográficos de la manera siguiente:

a) un nombre de registro ISO formal para el algoritmo;

b) el nombre (o nombres) propietarios dados al algoritmo por su creador o propietario;

c) la gama pretendida de aplicaciones para los algoritmos;

d) requisitos de la interfaz criptográfica;

e) un conjunto de palabras de prueba para verificar la funcionalidad básica;

f) la identidad de la organización que ha solicitado el registro del algoritmo;

g) las fechas del registro y de las modificaciones;

h) si el tema es una norma nacional;

i) información relativa a la restricción de licencias sobre patentes.

De manera opcional, el Registro ISO de Algoritmos Criptográficos puede también contener:

j) una lista de referencias a cualquier algoritmo asociado;

k) una descripción del algoritmo;

l) modos de funcionamiento;

m) otras informaciones.

En ISO 9979 aparecen más detalles al respecto.

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 Z	Lenguajes de programación