UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T Y.140.1

(03/2004)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE Y: INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN, ASPECTOS DEL PROTOCOLO INTERNET Y REDES DE LA PRÓXIMA GENERACIÓN

Infraestructura mundial de la información – Generalidades

Guía de atributos y requisitos para la interconexión entre operadores de redes públicas de telecomunicaciones y proveedores de servicio que intervienen en la prestación de servicios de telecomunicaciones

Recomendación UIT-T Y.140.1

RECOMENDACIONES UIT-T DE LA SERIE Y

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN, ASPECTOS DEL PROTOCOLO INTERNET Y REDES DE LA PRÓXIMA GENERACIÓN

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN	
Generalidades	**Y.100–Y.199**
Servicios, aplicaciones y programas intermedios	Y.200–Y.299
Aspectos de red	Y.300–Y.399
Interfaces y protocolos	Y.400–Y.499
Numeración, direccionamiento y denominación	Y.500–Y.599
Operaciones, administración y mantenimiento	Y.600–Y.699
Seguridad	Y.700–Y.799
Características	Y.800–Y.899
ASPECTOS DEL PROTOCOLO INTERNET	
Generalidades	Y.1000–Y.1099
Servicios y aplicaciones	Y.1100–Y.1199
Arquitectura, acceso, capacidades de red y gestión de recursos	Y.1200–Y.1299
Transporte	Y.1300–Y.1399
Interfuncionamiento	Y.1400–Y.1499
Calidad de servicio y características de red	Y.1500–Y.1599
Señalización	Y.1600–Y.1699
Operaciones, administración y mantenimiento	Y.1700–Y.1799
Tasación	Y.1800–Y.1899
REDES DE LA PRÓXIMA GENERACIÓN	
Marcos y modelos arquitecturales funcionales	Y.2000–Y.2099
Calidad de servicio y calidad de funcionamiento	Y.2100–Y.2199
Aspectos relativos a los servicios: capacidades y arquitectura de servicios	Y.2200–Y.2249
Aspectos relativos a los servicios: interoperabilidad de servicios y redes en las redes de próxima generación	Y.2250–Y.2299
Numeración, denominación y direccionamiento	Y.2300–Y.2399
Gestión de red	Y.2400–Y.2499
Arquitecturas y protocolos de control de red	Y.2500–Y.2599
Seguridad	Y.2700–Y.2799
Movilidad generalizada	Y.2800–Y.2899

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

Recomendación UIT-T Y.140.1

Guía de atributos y requisitos para la interconexión entre operadores de redes públicas de telecomunicaciones y proveedores de servicio que intervienen en la prestación de servicios de telecomunicaciones

Resumen

Dentro del marco establecido en la Rec. UIT-T Y.140, la presente Recomendación se concentra en uno de los escenarios de interconexión pertinentes a la infraestructura mundial de la información (GII), la interconexión entre operadores de redes públicas de telecomunicaciones (PTNO) y proveedores de servicio (SP). Tras examinar la situación antes de la transición hacia una implementación completa del denominado modelo de empresa, y en el curso de dicha transición, los atributos de los puntos de referencia para la interconexión entre PTNO y SP se tratan con cierta profundidad. En distintas cláusulas se examinan los diversos aspectos de estos atributos, en particular los relativos a la seguridad, la interacción del servicio, la tarificación/facturación, la disponibilidad del servicio, el acceso a las direcciones de red y la gestión de éstas. Las partes interesadas en la implementación del concepto GII dentro de una red de la próxima generación deberán considerar el contenido de esta Recomendación como una directriz.

Orígenes

La Recomendación UIT-T Y.140.1 fue aprobada el 29 de marzo de 2004 por la Comisión de Estudio 13 (2001-2004) del UIT-T por el procedimiento de la Recomendación UIT-T A.8.

Palabras clave

Infraestructura mundial de la información, interconexión, interfaces de interconexión, política pública, puntos de referencia para interconexión, requisitos esenciales para la prestación del servicio.

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 Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), 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 1 de la AMNT.

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.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

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.

© UIT 2004

Reservados todos los derechos. Ninguna parte de esta publicación puede reproducirse por ningún procedimiento sin previa autorización escrita por parte de la UIT.

ÍNDICE

Introducción

Esta Recomendación tiene por objetivo estudiar un aspecto de la Rec. UIT-T Y.140, trabajar sobre el mismo, y complementarlo. El lector debe tener en cuenta el contenido de la Rec. UIT-T Y.140 y las consideraciones que en ella se hacen.

La Rec. UIT-T Y.140 describe los puntos de referencia para la interconexión técnica entre diversas entidades que intervienen en la prestación de servicios de telecomunicaciones. Uno de los sectores en los que, según la Rec. UIT-T Y.140, se requiere la interconexión técnica es "para el acceso y/o interconexión de un proveedor de servicio a productos de un operador de red pública" (véase el inciso b de la cláusula 8/Y.140).

La presente Recomendación (Rec. UIT-T Y.140.1) examina con mayor detalle la relación entre el proveedor de servicio y el operador de red, así como los elementos de la interfaz de interconexión resultantes de esta relación.

Es preciso reconocer desde el principio que los elementos de la interconexión técnica entre estas dos entidades, el operador de red y el proveedor de servicio, tienen su origen no solamente en las necesidades de estas dos entidades. Fuerzas externas influyen también en la determinación de los elementos de interconexión que existirán entre estas dos entidades. Por ejemplo, las necesidades de los abonados al servicio también influirán en la naturaleza de la interconexión entre el operador de red y el proveedor de servicio. Asimismo, las autoridades gubernamentales encargadas de establecer los reglamentos pueden imponer ciertos requisitos relativos a la naturaleza de la interconexión entre las dos partes. (Dicho sea de paso, puede existir una relación inversa en cuanto a la medida en que el operador de red y el proveedor de servicio tienen en cuenta voluntariamente las necesidades de los abonados al servicio, y la necesidad de que la reglamentación gubernamental, como cuestión de política pública, exija que estas dos entidades así lo hagan. Si el operador de red y el proveedor de servicio actúan voluntariamente de una manera que satisfaga la política pública, la necesidad de una reglamentación gubernamental puede reducirse. Esta relación se conoce también por correglamentación.)

Además, la naturaleza de la interconexión técnica convenida entre las dos partes tendrá que ser plasmada en un acuerdo contractual entre las mismas.

La figura 1 representa estas relaciones en forma de diagrama. Esta Recomendación está centrada en los aspectos técnicos de la interconexión entre el operador de red y el área de servicio (superficie rectangular sombreada). No obstante, se reconoce que los intereses de otras partes (que en este diagrama están situadas fuera de la superficie sombreada) pueden influir en esta relación. Por tanto, si bien la Recomendación sólo trata el sector representado por la superficie sombreada, en la misma se hace referencia a aquellos casos en que conviene identificar lugares en los esas fuerzas externas pueden influir en estos puntos de referencia. Los acuerdos contractuales también están fuera del ámbito de la presente Recomendación; asimismo, en algunos lugares, la Recomendación identifica puntos de referencia en los que pueden influir acuerdos contractuales externos.

En la bibliografía adjunta puede encontrarse más información general sobre la forma en que el entorno de reglamentación, en evolución, puede influir en los aspectos técnicos de estos puntos de referencia.

Recomendación UIT-T Y.140.1

Guía de atributos y requisitos para la interconexión entre operadores de redes públicas de telecomunicaciones y proveedores de servicio que intervienen en la prestación de servicios de telecomunicaciones

1 Alcance y finalidad

Esta Recomendación trata la interconexión de proveedores de servicio y redes (públicas) (en adelante, este tipo de interconexión se designará brevemente por acceso a proveedor de servicio). Las partes que intervienen no deberán considerar esta Recomendación como una disposición obligatoria, sino como directrices que ayudan a reconocer y aplicar, de una manera voluntaria, los atributos y/o requisitos esenciales adecuados y facilitan la consecución de los objetivos de la política pública.

Por esta razón se han considerado dos aspectos, o puntos de vista:

a) requisitos de los proveedores de servicio que habrán de ser observados por los operadores de red para la prestación de servicios de telecomunicaciones, y

b) requisitos de los operadores de red para la prestación de acceso al proveedor de servicio.

En la figura 1/Y.140, se muestra un conjunto de posibles puntos de referencia para interconexión (RPI, *reference points for interconnection*). En la cláusula 8/Y.140 se señala que pudiera haber una pareja de atributos y/o requisitos esenciales relativos a diferentes clases de interfaces de interconexión. Los de la clase b se relacionan con la interconexión de proveedores de servicio a (productos de) operadores de redes públicas. En esta Recomendación se propone una descripción de atributos/requisitos para las interfaces de interconexión de clase b.

El acceso a proveedor de servicio (SPA, *service provider access*) indirecto, es decir, el que se obtiene a través de redes intermedias, no se trata en la presente Recomendación.

En la figura 1 se presenta un ejemplo de un posible escenario. Se muestra un entorno de participantes en el que se desempeñan muchos papeles y existen muchas relaciones diferentes. La presente Recomendación sólo trata el área representada por la superficie sombreada.

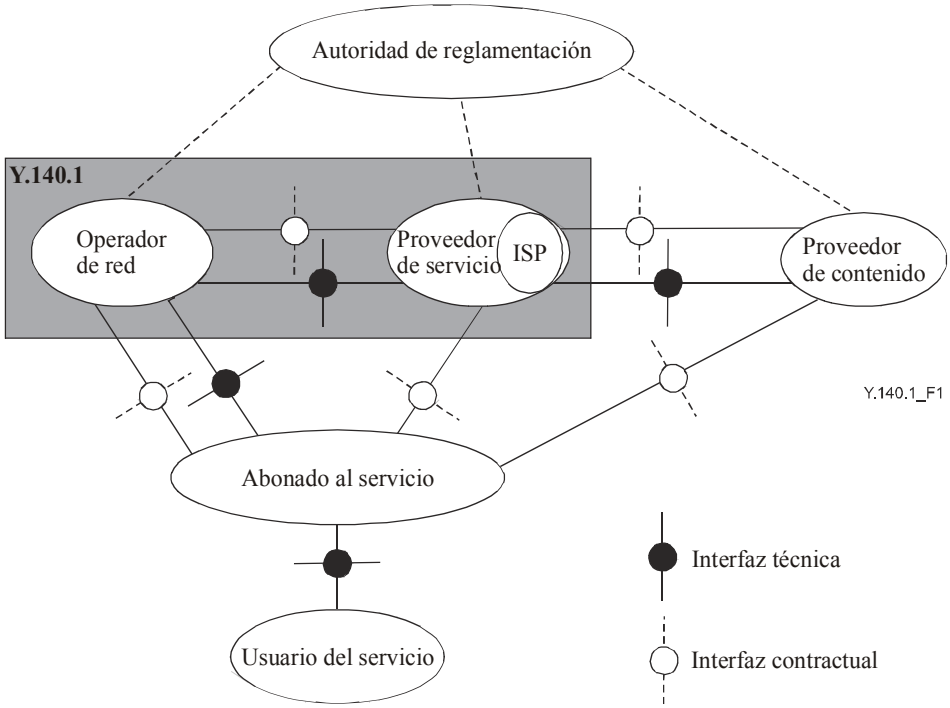

Figura 1/Y.140.1 – Ejemplo de relaciones entre participantes

Esta Recomendación tiene por finalidad describir requisitos funcionales genéricos relativos al acceso a proveedor de servicio. La prioridad de cada requisito se basa en la necesidad percibida desde el punto de vista del proveedor de servicio a o del operador de red (pública) b. Para cumplir estos requisitos puede ser necesario elevar el nivel de protocolos existentes, o crear protocolos adecuados, teniendo particularmente en cuenta la integridad de la red.

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. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

[1] Recomendación UIT-T F.115 (1995), *Objetivos de servicio y principios para los futuros sistemas públicos de telecomunicaciones móviles terrestres*.

[2] Recomendación UIT-T H.235 (2003), *Seguridad y criptado para terminales multimedios de la serie H (basados en las Recomendaciones UIT-T H.323 y H.245)*.

[3] Recomendación UIT-T J.93 (1998), *Requisitos del acceso condicional en la distribución secundaria de televisión digital por sistemas de televisión por cable*.

[4] Recomendación UIT-T J.95 (1999), *Sistema de protección de la propiedad intelectual contra la copia de contenidos transmitidos a través de sistemas de televisión por cable*.

[5] Recomendación UIT-T Q.1290 (1998), *Glosario de términos utilizados en la definición de redes inteligentes*.

[6] Recomendación UIT-T X.800 (1991) | ISO/CEI 7498-2:1989, *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT*.

[7] Recomendación UIT-T Y.140 (2000), *Infrastructura mundial de la información: Puntos de referencia para el marco de interconexión*.

[8] ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*.

[9] ETSI ES 201671 V2.1.1 (2001), *Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic*.

[10] ETSI TS 101 331 V1.1.1 (2001), *Telecommunications security; Lawful Interception (LI); Requirements of Law Enforcement Agencies*.

[11] ETSI ETR 232 ed.1 (1995), *Glossary of security terminology*.

[12] ETSI EG 201 722 V1.2.1 (2000), *Intelligent Network (IN); Service provider access requirements; Enhanced telephony services*.

[13] ETSI EG 201 781 V1.1.1 (2000), *Intelligent Network (IN); Lawful interception*.

[14] ETSI EG 201 807 V1.1.1 (2000), *Network operators' requirements for the delivery of service provider access*.

[15] ETSI EG 201 897 V1.2.1 (2002), *Service Provider Access Requirements in a Fixed and Mobile Environment*.

[16] ETSI EG 201 899 V1.1.1 (2001), *Modelling Service Provider Access Requirements using an API Approach*.

[17] ETSI EG 201 916 V1.1.1 (2001), *Development of standards to support Open Inter-Network Interfaces and Service Provider Access*.

[18] ETSI EG 201 965 V1.1.1 (2001), *Service Provider Access Management Requirements for Open Network Access*.

3 Términos y definiciones

A los efectos de esta Recomendación, el término "servicio" se utiliza en un sentido amplio y no debe entenderse en el sentido limitado del término definido por la CE 2 del UIT-T como "servicio de telecomunicación" completamente especificado.

A los efectos de esta Recomendación se aplican las definiciones siguientes.

3.1 autenticación: Proceso que permite comprobar con certeza la identidad de un participante en una comunicación. La autenticación generalmente sigue a la identificación, estableciendo la validez de la identidad reclamada, en previsión de acciones fraudulentas.

3.2 disponibilidad[1]: Propiedad de ser accesible y de poder ser utilizado, a petición, por una entidad autorizada. [8], [6]

3.3 confidencialidad[1]: Propiedad en virtud de la cual la información no se pone a disposición de personas, entidades, o procesos no autorizados, ni se revela a esas personas, entidades o procesos. [8], [5]

[1] Las definiciones de los términos "seguridad", "disponibilidad", "integridad" y "confidencialidad" están estrechamente relacionadas entre sí y deben utilizarse unas en el contexto de las otras.

3.4 fraude (protección contra el)

3.4.1 fraude: Acto mediante el cual se consigue una ventaja pecuniaria por medio de una representación falsa o una acción no autorizada.

3.4.2 participante fraudulento: Participante que comete un fraude.

3.4.3 fraude mediante equipo: Uso fraudulento de la red de telecomunicaciones, que implica el uso indebido de un equipo terminal, por ejemplo un teléfono de previo pago.

3.4.4 fraude mediante la red: Uso fraudulento de la infraestructura de la red de telecomunicaciones, que implica el uso indebido de dispositivos técnicos de la red, acompañado a veces del uso de un equipo terminal.

3.4.5 fraude en el servicio: Uso fraudulento de servicios de telecomunicaciones, a veces acompañado de la interacción esperada o inesperada de dos o más servicios.

3.4.6 fraude en el abono: Uso fraudulento de la red de telecomunicaciones por un participante que no tiene la intención de pagar el precio correspondiente.

3.4.7 fraude en las telecomunicaciones: Fraude cometido directamente contra la red de telecomunicaciones o sus abonados.

3.5 integridad[1]:

a) Propiedad en virtud de la cual los datos no han sido alterados ni destruidos de una manera no autorizada [8], [6], [5]).

b) Propiedad en virtud de la cual una función no permite ser tomada y aplicada a un uso no autorizado, ni modificada para que produzca resultados no autorizados [3], [4].

3.6 intercepción legal: Acción (basada en la ley), ejecutada por un operador de red/proveedor de acceso/proveedor de servicio, en virtud de la cual se proporciona cierta información y se pone a disposición de un dispositivo de monitorización con miras a la aplicación de la ley. [13]

3.7 privacidad:

– Modo de comunicación según el cual sólo los participantes explícitamente habilitados pueden interpretar la comunicación. Esto puede conseguirse, por ejemplo, utilizando criptado y claves compartidas para el texto cifrado [2].

– Derecho de las personas a controlar o ejercer influencia en cuanto a qué información relacionada con ellas puede ser recogida y almacenada, quién o quiénes ejecutan esta acción y a quién o quiénes se puede revelar esta información.

NOTA – Como este término está relacionado con los derechos de personas, no puede ser muy preciso y se debe evitar su uso, salvo como un motivo para exigir seguridad [6], [1].

3.8 política pública: En el contexto de las telecomunicaciones, por política pública ha de entenderse la política que los encargados de la reglamentación aplican cuando determinan el bien público, y que pueden aplicar mediante reglamentos que se imponen a las entidades de telecomunicaciones.

3.9 seguridad[1]: Protección de la disponibilidad, integridad y confidencialidad de la información [10].

---

[1] Las definiciones de los términos "seguridad", "disponibilidad", "integridad" y "confidencialidad" están estrechamente relacionadas entre sí y deben utilizarse unas en el contexto de las otras.

4 Abreviaturas

En esta Recomendación se utilizan las siguientes siglas.

NNI Interfaz red-red (*network-network interface*)

PTNO Operador de red pública de telecomunicaciones (*public telecommunication network operator*)

RTP Red pública de telecomunicaciones

SLA Acuerdo de nivel de servicio (*service level agreement*)

SP Proveedor de servicio (*service provider*)

SPA Acceso a proveedor de servicio (*service provider access*)

SPAI Interfaz de acceso a proveedor de servicio (*service provider access interface*)

SPAR Requisito(s) de acceso a proveedor de servicio (*service provider access requirement*)

NOTA – El término "Servicio" (con S mayúscula) no se utiliza en la versión española de esta Recomendación (en la versión inglesa se evita su uso, pues es un término "utilizado exclusivamente" por la CE 2).

5 Seguridad

En la presente Recomendación, las cuestiones relacionadas con la seguridad se tratan en la cláusula 7 "Atributos de puntos de referencia para la interconexión entre PTNO y SP", en particular en 7.1 "Aspectos de seguridad". En esa cláusula, los aspectos de seguridad se tratan en relación con los puntos de vista de usuarios de extremo, por un lado, y de SP y PTNO, por otro lado. Además, se tratan los aspectos de integridad (7.1.1), autenticación (7.1.2) y confidencialidad (7.1.3), términos que están estrechamente relacionados con la seguridad. Dado que la Recomendación debe considerarse fundamentalmente como un conjunto de directrices, los aspectos que se consideran son, esencialmente, los de naturaleza general. Esto se refleja también en la cláusula 2 "Referencias (informativas)" donde, por ejemplo, la mayor parte de los documentos ETSI enumerados son guías.

6 Situación antes y durante la transición a una implementación completa del modelo de empresa

Actualmente, el modelo de empresa descrito en la Rec. UIT-T Y.110 no está implementado completamente. En el pasado, las redes se diseñaban fundamentalmente para aquellos servicios que los propios operadores de red querían ofrecer a sus clientes. En esa situación, en la mayoría de los casos bastaba con diseñar redes de tal manera que pudieran generar y prestar los servicios "propios" de los operadores de las redes. En consecuencia, era suficiente proporcionar soporte técnico, con fines domésticos solamente, con respecto a acceso, facturación, señalización, integridad, gestión, etc. Incluso si esos servicios se prestaban a través de más de una red (por ejemplo, a través de países o de operadores de red en competencia comercial), no existía un requisito real que exigiera el soporte del acceso de terceros a funciones internas de la red. Con las decisiones, basadas en la política a seguir, de confiar en las fuerzas del mercado y de abrir el mercado, se produjeron cambios fundamentales en el entorno de la reglamentación de las telecomunicaciones.

En primer lugar, para estimular la competencia, los operadores de red en ejercicio eran obligados por los encargados de la reglamentación a conceder a terceros acceso a sus redes o a partes de las mismas.

Con la creciente liberalización y las nuevas tecnologías en evolución, el diseño de las redes de telecomunicaciones ha cambiado. Esos cambios importantes con respecto a la filosofía y la arquitectura se describen, por ejemplo, en las Recomendaciones UIT-T Y.110 e Y.140.

Como consecuencia de este nuevo "enfoque", la industria de las telecomunicaciones está siendo reconfigurada por cambios fundamentales en los derechos de propiedad sobre la misma, en la estructura de los mercados y en los avances tecnológicos, lo que ha venido acompañado de un gran número de desafíos. Para hacer frente a esta nueva situación hay que garantizar la acomodación de los diferentes y a veces divergentes intereses de al menos tres categorías de participantes (los usuarios de extremo, los operadores de red y los proveedores de servicio a terceros).

Uno de los requisitos más importantes es el de asegurar la integridad de la red, del servicio, y de los datos. Si bien en el pasado la totalidad de la gestión, incluida la generación del servicio, la efectuaba un solo participante (el operador de red), actualmente existe la exigencia de abrir, al menos, partes de la gestión de red para ayudar a la prestación del servicio, por ejemplo para señalización, reserva de ancho de banda, facturación y tarificación, etc. Un proveedor de servicio puede tener interés en obtener un acceso más o menos directo a la red. Si no se toman medidas adicionales, esto puede afectar a la red (de transporte) original de una manera tal, que otros servicios y/o datos de otros usuarios pierdan su integridad y/o privacidad. Además, el operador de red original puede ser afectado por un tercero de una manera tal, que quede imposibilitado de garantizar un esquema de seguridad para comunicaciones de urgencia.

Otro ejemplo puede ser el de un proveedor de servicio que desee tener acceso a la información sobre capacidades de terminal para ofrecer un servicio personalizado o para "modificar" las capacidades, comportamiento, funcionalidades y condiciones de un terminal. Estos requisitos afectarían los derechos de al menos un usuario, si se cumplieran sin la aprobación explícita e individual del usuario. Por tanto, es necesario tener, en el terminal, en la red de transporte y en la prestación del servicio, un mecanismo que permita soportar y respetar el interés y los derechos de los participantes.

Estos escenarios pueden tomarse como un ejemplo de los requisitos/atributos que podrían necesitarse para implementar el modelo de empresa descrito en la Rec. UIT-T Y.110 y para responder a las exigencias de un mercado de telecomunicaciones plenamente competitivo.

La presente Recomendación examina varias propiedades/atributos (no exhaustivos) de los puntos de referencia para interconexión (RPI) y debe ayudar a desarrollar interfaces que respeten en la mayor medida posible los intereses de los participantes.

7 Atributos de puntos de referencia para la interconexión entre PTNO y SP

NOTA – El contenido de esta cláusula se basa en las ETSI Guides [12] a [18].

Las relaciones mutuas entre PTNO y SP se establecen generalmente en acuerdos de nivel del servicio (SLA, *service level agreement*). Estos acuerdos contienen detalles sobre la información que habrá de intercambiarse entre el SP y el PTNO, y el mecanismo que se utilizará con este fin.

7.1 Aspectos de seguridad

NOTA – En el sitio web de la UIT [B-7] se da una información real, y regularmente actualizada, sobre temas relacionados con la seguridad.

Los usuarios de extremo, SP y PTNO tienen distintos objetivos y requisitos comerciales relativos a la prestación de servicios de telecomunicaciones a través de las redes públicas de telecomunicaciones. Cierto número de esos objetivos se han identificado. Para satisfacerlos es necesario considerar con sumo cuidado los aspectos de seguridad en un nuevo entorno que comprende una gran cantidad de interconexiones y configuraciones de acceso para los SP.

Los requisitos de los usuarios de extremo y de otros participantes en la prestación de servicios pueden competir unos con otros. Por ejemplo, un usuario de extremo puede desear visitar sitios web anónimamente, en tanto que el Ministerio Fiscal puede estar interesado en rastrear las actividades de los navegantes en Internet.

Entre los riesgos generales de seguridad están: la piratería en perjuicio de los usuarios (suplantación ilícita de la identidad, ataques por reproducción de identidad; diversión y hurto de servicio, etc.), integridad de los datos (los datos tienen que ser, exactamente, los mismos datos que han sido enviados, sin que se pueda añadir, modificar ni suprimir nada), protección contra el espionaje (escucha, copia de datos), privacidad de los datos y de los servicios (los participantes en la comunicación pueden estar seguros de que su comunicación es privada y continúa siendo privada), confianza de las partes cuando se produce el acceso a datos o el tránsito de datos, no repudiación (prueba irrefutable de que un participante ha recibido los datos que fueron enviados, retenidos y generados por una fuente de confianza), y protección contra ataques por denegación de servicio.

Si bien algunas de estas cuestiones se resuelven mediante suma de control, autenticación, y criptado, el no repudio y la protección contra los ataques por denegación de servicio no tienen soluciones directas basadas en el servicio. Es necesario diseñar redes y protocolos capaces de contornear parcialmente estos problemas. Otros aspectos del fraude (tales como negarse al pago, robos, etc.) incumben a la policía. Las redes requerirán dispositivos de contabilidad fiables y securizados, así como la trazabilidad para la protección contra el robo de servicio y la diversión del uso de recursos.

Desde el punto de vista de los usuarios de extremo, los requisitos esenciales son:

– disponibilidad de los servicios;
– facturación correcta;
– protección contra el fraude;
– confidencialidad;
– (a veces) anonimato; y
– privacidad.

Desde el punto de vista de los SP y PTNO, los requisitos esenciales son:

– disponibilidad de la red, los servicios, y el mantenimiento;
– tarificación correcta;
– capacidad de rastrear cada llamada;
– protección contra la intrusión en los datos relacionados con los abonados; y
– eliminación del uso fraudulento del equipo de los PTNO y SP.

Las violaciones de la seguridad pueden tener una importante repercusión comercial negativa, tanto para los SP como para los PTNO, por ejemplo, pérdida de ingresos, de reputación y de participación en el mercado.

En particular, la integridad de la red es una cuestión primordial cuando se establecen relaciones basadas en el funcionamiento combinado de redes entre PTNO y SP.

En cuanto al acceso a proveedor de servicio (SPA), se puede necesitar un conjunto básico de dispositivos para securizar las interfaces entre los PTNO y SP. En ETSI TR 101 365 se presenta un análisis de las amenazas que afectan a las interconexiones basadas en red inteligente, y en ETSI TR 101 664 se dan algunas directrices sobre medidas de seguridad importantes.

Se utilizan funciones de cribado y de establecimiento de correspondencia lógica para controlar y securizar acuerdos bilaterales sobre las interfaces entre las redes públicas de telecomunicaciones (RTP). En la actualidad, los PTNO tienen dispositivos de cribado y establecimiento de correspondencia en algunas de las NNI de interconexión, como son las conexiones de parte usuario de la RDSI del sistema de señalización N.° 7. Estos dispositivos y funciones deben ser ampliados gradualmente de manera que abarquen todas las interfaces entre los PTNO y SP.

Otros aspectos de seguridad relacionados con las redes móviles, la de Internet, y las de banda ancha incluyen la transferencia de información sobre la identidad de los terminales y las personas [por

ejemplo, la identidad de abonado móvil internacional (IMSI, *international mobile subscriber identity*), firma electrónica, etc.] entre el entorno del usuario y el proveedor de servicio, o el soporte de una transmisión de extremo a extremo securizada entre el terminal de usuario y la aplicación del proveedor de servicio (por ejemplo, capa de zócalo securizado y tecnologías de cifrado).

7.1.1 Aspectos de integridad

NOTA – Para información sobre las responsabilidades que conlleva asegurar el mantenimiento de la integridad de la red en un entorno interconectado, véase [B-6].

La integridad de la red es una cuestión que concierne a la gestión de red y a la aptitud de la red para mantener ciertas características con respecto a la calidad de funcionamiento y la fiabilidad.

La integridad de la red es un aspecto esencial cuando se establece una relación de red entre la RTP y el SP. La apertura de las redes de los PTNO al SP implica el ensanchamiento del acceso a datos/información almacenados. Los datos deberán protegerse adecuadamente mediante la utilización de contraseñas y particiones, de manera que la integridad y la privacidad no queden comprometidas.

La integridad de la red implica también asegurar la integridad de los elementos de red y proporcionar un nivel de servicio aceptable. Una integridad de sistema que se vea afectada por vulnerabilidades puede tener por consecuencia denegaciones o interrupciones del servicio, o una modificación no autorizada de la información de usuario o red, y de los servicios de la red.

La evolución de las redes de los PTNO necesarias para el soporte de los servicios realzados de los SP crea la necesidad de planificar el crecimiento de la capacidad de conmutación en tiempo real en consonancia con la emergencia de este nuevo servicio de acceso. Para hacer frente a esta situación los PTNO y SP deben negociar los aspectos de ingeniería de tráfico para asegurarse de que se dispone de una capacidad de red adecuada. Si los PTNO y SP no planifican adecuadamente la capacidad de crecimiento, la red pública podrá verse expuesta a problemas de interrupción y de denegación del servicio.

Deben considerarse los siguientes aspectos:

– Una función de pasarela entre la RTP y el SP, especialmente para los mensajes de tarificación/facturación y sus parámetros.
– El mecanismo de protección para asegurar que los SP no influyan negativamente en los servicios proporcionados en la RTP.
– Los mecanismos de autenticación/cifrado para proteger la RTP contra las vulnerabilidades debidas al SPA.
– Por otro lado, a fin de mantener la integridad de la red, deben cumplirse los siguientes requisitos:
    - Deben aplicarse medidas de compatibilidad para asegurarse de que las redes y los SP con diferentes niveles de calidad funcionan correctamente cuando se combinan unas con otros.
    - Deben existir mecanismos que permitan aplicar procedimientos de pruebas de conformidad con el fin de verificar la interoperabilidad de RTP y SP.
    - El SPA aumenta las posibilidades de que aparezcan vulnerabilidades relacionadas con problemas de interfuncionamiento de características cuando el nivel de pericia técnica no sea suficiente para hacer frente a este problema. La interacción de características podría perturbar un servicio necesario o ser atacada por piratas informáticos. Se deben tomar medidas adecuadas para evitar este tipo de riesgos.

Es probable que la gama de servicios ofrecida por los SP conduzca a la utilización de diferentes tipos de interfaces para el SPA. Estos diferentes tipos de interfaces pueden requerir diferentes conjuntos de funcionalidades dentro de la pasarela en la demarcación de la red.

En futuras implementaciones habrá que tomar en consideración, en particular, los puntos de vista de los PTNO, SP y usuarios/abonados/clientes.

7.1.2 Aspectos de autenticación

En el marco de "¿Quién tiene que autenticarse ante quién?" hay que considerar ciertos aspectos de segundo orden:

– el usuario ante un SP y/o PTNO (por ejemplo, en el caso de acceso),

– el SP ante el PTNO,

– un PTNO ante otro PTNO (por ejemplo, cuando intervienen redes basadas en paquetes, en las que entran en juego conexiones virtuales que incluyen tunelización, y también

– un SP ante otro SP (autenticación mutua) si utilizan niveles diferentes ("semiproductos") de la cadena de valor añadido.

Además, existe también una especie de "autenticación pasada de extremo a extremo", basada en derechos de prioridad (por ejemplo, en caso de comunicaciones de urgencia). En general, se debe distinguir entre el proceso de verificación propiamente dicho y el mecanismo de paso de extremo a extremo, es decir entre quién verifica y cómo debe darse a conocer el resultado de la verificación entre los participantes en la "cadena de autenticación".

Son medios típicos de autenticación los números de identificación personal (PIN) y las tarjetas de identificación de abonado (SIM) o firmas digitales (por ejemplo, en el contexto de las comunicaciones móviles).

En futuras implementaciones habrá que tomar en consideración, en particular, los puntos de vista de los PTNO, SP y usuarios/abonados/clientes.

7.1.3 Confidencialidad

La confidencialidad es un requisito esencial en el mundo comercial. Mantener la confidencialidad en el caso de reuniones personales directas en las que sólo intervienen las personas directamente interesadas es relativamente fácil. En cambio, este no es necesariamente el caso cuando se trata de una telecomunicación pública a través de terceros como PTNO y SP (o dispositivos de terceros). Pueden distinguirse varios niveles de mantenimiento de la confidencialidad, los cuales, enumerados en orden ascendente del grado de dificultad, podrían ser los siguientes:

Nivel 1: Se intercambian contratos por correo ordinario o, por ejemplo, por facsímil. En el primer caso, el 'secreto de la correspondencia', y en el segundo caso el 'secreto de las telecomunicaciones' garantizan un cierto grado de confidencialidad.

Nivel 2: Se intercambian contratos a través de Internet (por ejemplo, mediante correo electrónico).

Nivel 3: También se llevan a cabo negociaciones sobre contratos a través de redes de comunicaciones.

Si intervienen telecomunicaciones hay que distinguir entre la utilización de redes públicas y la utilización de redes de compañías (grupos cerrados de usuarios).

Un ejemplo particularmente importante en el que la confidencialidad desempeña un papel de primer orden es el comercio electrónico (brevemente, comercio E).

Un conocido medio de garantizar la confidencialidad es la firma electrónica.

7.1.3.1 Punto de vista del operador de red pública de telecomunicaciones

Un PTNO puede contribuir al mantenimiento de la confidencialidad cuidando de que sólo las personas autorizadas puedan extraer información de dispositivos de telecomunicaciones (véase Intercepción legal).

7.1.3.2 Punto de vista del proveedor de servicio

Un dominio típico, quizás el más importante, ejemplo de una acción donde SP desempeña un papel primordial en la confidencialidad es el comercio E.

7.1.3.3 Punto de vista del usuario/abonado/cliente

El usuario/abonado/cliente tiene interés en una confidencialidad absoluta.

Cuanto mayor es el grado de confidencialidad que se le ofrece, tanto más alto es el precio que el usuario/abonado/cliente está dispuesto a pagar por ella.

7.1.4 Protección contra el fraude

La protección contra el fraude es un aspecto esencial del comercio E, porque:

i) mucho depende de esta protección, y

ii) existen muchos puntos de ataque posibles.

7.1.4.1 Punto de vista del operador de red pública de telecomunicaciones

Un PTNO tiene interés en recibir una remuneración adecuada si alguien utiliza "sus" dispositivos de red. Fuentes de fraude pueden ser usuarios/abonados/clientes, SP, así como otros PTNO que intervienen en la totalidad del proceso de comunicación.

7.1.4.2 Punto de vista del proveedor de servicio

Un SP desea que los servicios que ofrece sólo sean utilizados por personas autorizadas, es decir, únicamente por las que hayan suscrito el correspondiente contrato.

Un SP tiene interés en que se le remunere efectivamente por cada servicio ofrecido contra el pago de un precio.

7.1.4.3 Punto de vista del usuario/abonado/cliente

Un usuario/abonado/cliente tiene interés en evitar situaciones en las que cualquier otra persona utilice un servicio a sus expensas, por ejemplo usando el número de identificación personal (PIN) del abonado.

7.1.5 Intercepción legal

La intercepción legal (LI, *lawful interception*) no incumbe a la UIT en la medida en no existe una autoridad gubernamental que la introduzca en un mandato a nivel de las Naciones Unidas (Mandato de la UIT).

Sin embargo, los puntos de referencia para interconexión y sus correspondientes interfaces (véase la Rec. UIT-T Y.140) deben diseñarse de tal manera que se tengan en cuenta los requisitos nacionales relativos a la intercepción legal, y no deben impedir (excluir) por sí mismos la implementación de medidas nacionales conexas, si existen.

Por razones económicas, los **SP** y **PTNO** tienen interés en que no se les obligue a realizar esfuerzos innecesarios en posibles realizaciones.

Los **usuarios** no quieren verse demasiado afectados por medidas necesarias para implementar la intercepción legal.

Una cierta guía sobre los requisitos de la intercepción legal y posibles soluciones para la intercepción legal pueden encontrarse en las publicaciones ETSI [10] y [9].

7.2 Aspectos de interacción de servicios

En un entorno en que el usuario de extremo está abonado a una gama de servicios proporcionados por más de un proveedor, pueden producirse interacciones adversas entre servicios y características

de servicios. Esto implica la necesidad de disponer de una funcionalidad adicional para gestionar los aspectos de interacción con el fin de hacer posible una prestación integrada y coherente de los servicios.

Se necesita un estudio más profundo sobre los aspectos de la interacción de servicios, incluidas las interacciones adversas que pueden producirse entre el equipo de los PTNO y el de los SP, cuando se requiera que más de uno de los participantes en la llamada tengan capacidad para controlarla.

Un buen ejemplo de tales cuestiones de interacción de servicios lo proporciona la combinación de los requisitos relativos a la portabilidad del número y el acceso a proveedores de servicio. Por ejemplo, en varios requisitos se indica que una acción relacionada con el SP se puede iniciar sobre la base de una llamada con la identificación de la línea llamante de la parte llamante en una determinada gama de numeración. Debido al mecanismo de portabilidad de número, la detección de tal gama de numeración no garantiza que la llamada habrá de ser procesada por el SP al que se le asignó inicialmente esa gama de numeración.

7.3 Aspectos de tarificación/facturación

Los mecanismos de tarificación estándar permiten la tarificación de una llamada exitosa, por ejemplo entre la respuesta de la parte llamada y la liberación de la llamada. Algunos requisitos de los proveedores de servicio implican la utilización de la red del PTNO fuera de este caso estándar, por lo que la implementación de un mecanismo de tarificación conexo entre el PTNO y el SP es necesaria para abarcar esa utilización. Este es el caso, por ejemplo, de los siguientes requisitos de los SP:

– petición de la apertura de un trayecto de mensaje dentro de banda en sentido de retorno hacia la parte llamante original tan pronto como se recibe una confirmación del establecimiento de la llamada, sin devolver una señal de "respuesta";
– transmisión de una indicación de una llamada fracasada, desde la RTP de terminación, es decir, cuando se devuelve a la parte llamante una indicación que no sea la "señal de llamada", o cuando se produce la situación de "ausencia de respuesta";
– suministro de información de destino de la llamada y de encaminamiento de la llamada para controlar el destino y el encaminamiento de la llamada;
– interacción con el usuario del servicio antes de que comience cualquier tarificación por el uso del servicio;
– envío de datos a la RTP del usuario del servicio y recepción de datos desde dicha red sin una señal de aviso, como la señal de llamada;
– los aspectos de tarificación y facturación de la llamada, vistos desde la perspectiva de los PTNO, se consideran en ETSI EG 201 807.

En caso de que la tarificación del usuario sea suspendida, demorada, alterada o, por cualquier otra causa, sea diferente de la producida por el mecanismo estándar de tarificación de las llamadas, hay que crear los eventos apropiados para el posible registro cronológico, por ejemplo, proporcionando así los datos necesarios para la contabilidad correcta entre el SP y el PTNO.

Por ejemplo, en el mercado está surgiendo una demanda de:

– facturación basada en abono para el acceso a Internet;
– minutos incluidos en un abono prepagado para el servicio fijo y el móvil; y
– pago según la utilización, sin abono.

En todos estos casos se necesita una contabilidad en tiempo real (facturación en vivo) a través de una interfaz de datos securizada.

Es necesario tener en cuenta las leyes y reglamentos nacionales y europeos, cuando proceda, a la hora de diseñar e implementar mecanismos de tarificación, por ejemplo para transmitir al usuario del servicio un aviso sobre la cantidad que se le debita por la tarificación.

7.3.1 Punto de vista del operador de la red pública de telecomunicaciones

– Herramientas de señalización para facturación y tarificación (en tiempo real), señales de información de tráfico avanzadas.
– Transmisión de información de tarificación (en tiempo real) a través de las redes.
– Las redes y los proveedores de servicio requieren el rastreo de la información de facturación en tiempo real, y la seguridad de no-repudio en cuanto a que la factura se recibió, y que estaba correcta, con la integridad de datos que implica que es exacta y que no ha sido alterada.
– Hay que prestar especial atención a la precisión del reloj de red propiamente dicho y a la exactitud de su transmisión, sobre todo si intervienen más de una RTP.

7.3.2 Punto de vista del proveedor de servicio

– Generación y presentación de información de tarificación (en tiempo real) para el cliente.

7.3.3 Punto de vista del usuario

– Recepción de información de tarificación/facturación (en tiempo real).
– Los usuarios/clientes requieren la trazabilidad de lo que se les va a facturar y de que el servicio se estaba utilizando efectivamente en el tiempo que se reclama (comprobante de servicio, aviso de tarificación, desglose de la facturación son soluciones potenciales).
– Son aspectos de particular importancia para el usuario la exactitud de la factura y una "cuantificación" razonable de los intervalos en que se basa la facturación (cuanto más cortos sean, tanto mejor).

7.4 Disponibilidad del servicio

La disponibilidad del servicio es una cuestión de política, que depende de la relación de usuario a proveedor de servicio y de proveedor de servicio a operador de red, y de lo que éstos convengan en lo que respecta a la oferta de servicio.

Un punto esencial en este aspecto es el "esquema de preferencia".

7.5 Acceso a una dirección de red

NOTA – Aunque no se muestra en la figura 1, las relaciones entre diferentes participantes implican aspectos de denominación y direccionamiento. Estos aspectos pueden o no estar comprendidos en la esfera de competencia de una autoridad de reglamentación.

Son aplicaciones típicas en las que un SP puede necesitar acceso a una dirección de red los servicios de información sobre números de abonado, solicitudes de información en línea, servicios de reenvío, etc.

El acceso a redes, servicios de red y aplicaciones requiere que se proporcionen números y gamas de numeración adecuados para todos los servicios de comunicaciones electrónicas disponibles públicamente, y que éstos se puedan asignar de una manera objetiva, transparente y no discriminatoria.

7.6 Aspectos de gestión

La figura 2 ilustra una arquitectura de referencia que muestra los RPI entre SP y PTNO. Puede utilizarse para obtener los requisitos que deben cumplir ambas partes en lo que respecta al intercambio de información de gestión a través de las interfaces que corresponden a los RPI.

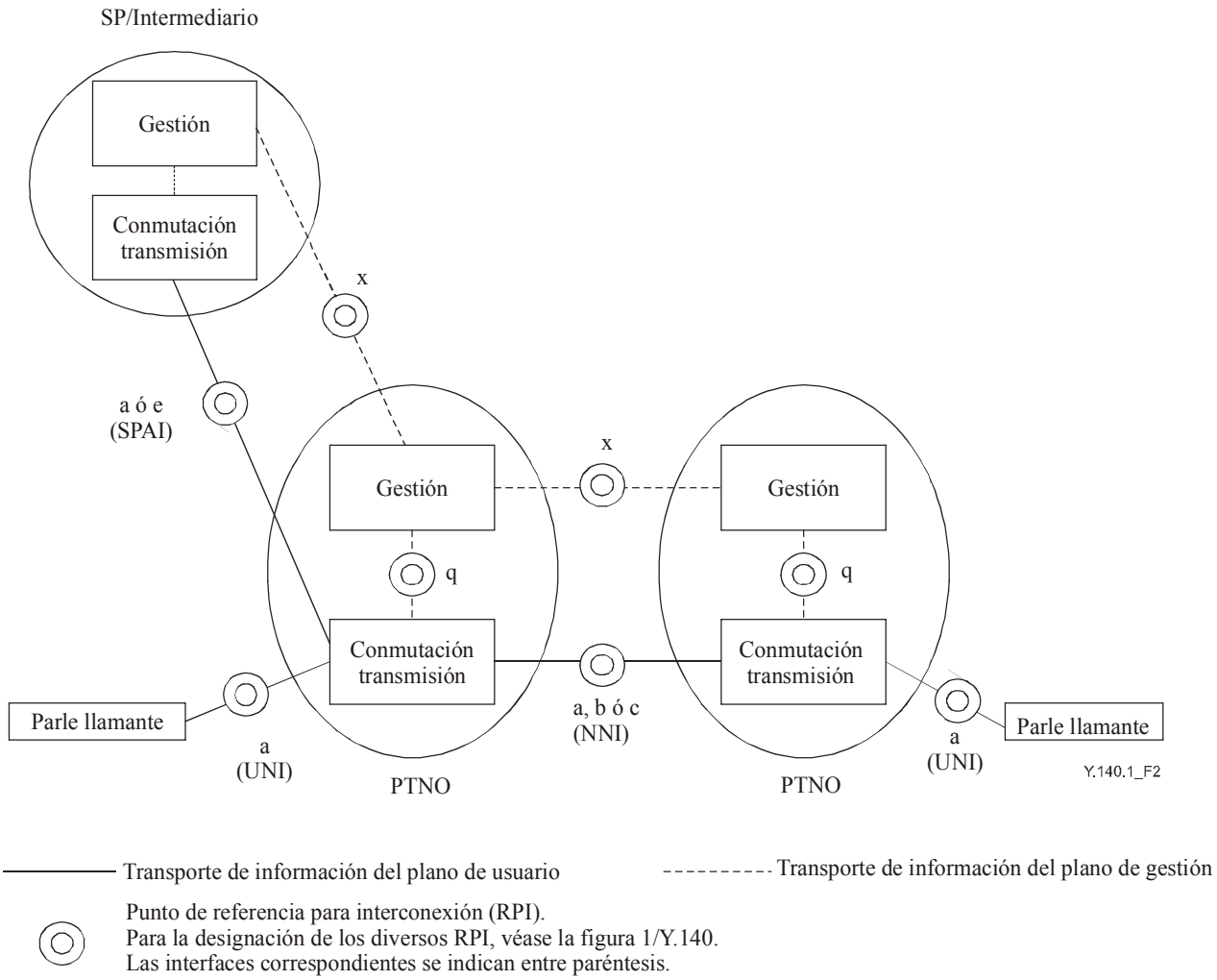

Figura 2/Y.140.1 – Arquitectura de referencia para los requisitos de gestión de SP-PTNO

En [18] puede encontrarse un análisis detallado de la situación. Se trata la interfaz del plano de gestión entre el equipo de proveedor de servicio y el equipo de operador de red de telecomunicaciones públicas. Cada requisito se basa en los estudios de los requisitos de acceso a proveedor de servicio (SPAR, *service provider access requirements*) publicados en [12] a [15]. [18] determina si cada SPAR tiene una implicación de gestión. Para cumplir estos requisitos de gestión se requerirán protocolos apropiados, basados en los flujos de información descritos en [18]. Cuando no estén disponibles protocolos apropiados, será necesario elevar el nivel de los protocolos existentes o crear nuevos protocolos.

Los requisitos de gestión tratados en [18] pueden dividirse en:

– Capacidades relacionadas con el tráfico (por ejemplo, establecimiento de activadores de conmutadores, relleno de datos, etc.), necesarios para permitir, desde una perspectiva operacional, uno o más de los requisitos de acceso a proveedor de servicio (SPAR).

– Capacidades de gestión de la calidad de funcionamiento, por ejemplo supervisión de la calidad de funcionamiento de enlaces SP/RTP, reconfiguración del enlace, etc.

– vinculación/ordenación electrónicas.

8 Requisitos y sus prioridades en los RPI

Cuadro 1/Y.140.1 – Requisitos y sus prioridades en los RPI

Atributos	Punto de vista del			Observa-ciones
	Operador de red pública de teleco-municaciones	Proveedor de servicio	Cliente Abonado Usuario de extremo	
Disponibilidad del servicio		Alta	Alta	
Facturación correcta	Alta	Alta		
Tarificación correcta			Alta	
Integridad de la red	Alta			
Integridad del servicio		Alta		
Acceso a dirección de red				
Requisito relativo a la gestión	Alta	Alta		

NOTA – El contenido de este cuadro no es exhaustivo y es susceptible de revisión.

BIBLIOGRAFÍA

[B-1] Publicación de la Secretaría de la UIT, *Tendencias en las reformas de telecomunicaciones 2000-2001 – Reglamentación de la interconexión*.

[B-2] WTO Telecommunications Services Reference Paper (24 April 1996) http://www.wto.org/english/tratop_e/serv_e/telecom_e/tel23_e.htm.

[B-3] APEC Principles of interconnection (Annex 3 to [B-1]).

[B-4] CITEL Guidelines and practices for interconnection regulation (Annex 4 to [B-1]).

[B-5] Directive 97/33/EC "Interconnection in Telecommunications with regard to ensuring universal service and interoperability through application of the principles of Open Network Provision (ONP)" of the European Parliament and of the Council of 30 June 1997.

[B-6] CEPT/ECTRA Recommendation (98)01, *Set of Guidelines on Responsibilities for ensuring maintenance of Network Integrity (NI) in an interconnected environment*.

[B-7] http://www.itu.int/osg/spu/ni/security/links/news.html and http://www.itu.int/osg/spu/ni/security/links/misc.html.

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	Redes de cable y transmisión de programas radiofónicos y televisivos, 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, aspectos del protocolo Internet y Redes de la próxima generación**
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2004