Unión Internacional de Telecomunicaciones

# UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

# Y.2725

(07/2014)

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

Redes de la próxima generación – Seguridad

## Soporte de OpenID en redes de la próxima generación

Recomendación UIT-T Y.2725

Unión Internacional de Telecomunicaciones

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 |
| Televisión IP sobre redes de próxima generación | Y.1900–Y.1999 |
| 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 la próxima generación | Y.2250–Y.2299 |
| Mejoras de las NGN | Y.2300–Y.2399 |
| Gestión de red | Y.2400–Y.2499 |
| Arquitecturas y protocolos de control de red | Y.2500–Y.2599 |
| Redes basadas en paquetes | Y.2600–Y.2699 |
| **Seguridad** | **Y.2700–Y.2799** |
| Movilidad generalizada | Y.2800–Y.2899 |
| Entorno abierto con calidad de operador | Y.2900–Y.2999 |
| REDES FUTURAS | Y.3000–Y.3499 |
| COMPUTACIÓN EN LA NUBE | Y.3500–Y.3999 |

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

# Recomendación UIT-T Y.2725

## Soporte de OpenID en redes de la próxima generación


### Resumen

En la Recomendación UIT-T Y.2725 se especifican mecanismos y procedimientos para el soporte y la utilización de OpenID cuando el proveedor NGN asume la función de proveedor OpenID.

En la Recomendación UIT-T Y.2724 se facilita el marco para el soporte y la utilización de OAuth y OpenID en las NGN. La Recomendación UIT-T Y.2725 se basa en la Recomendación UIT-T Y.2722 y la Recomendación UIT-T Y.2724 para definir los mecanismos específicos para dar soporte a OpenID.

NOTA – En la Recomendación UIT-T Y.2725 no se cambia ni modifica el protocolo OpenID, sino que se centra únicamente en el soporte y la utilización de OpenID en las NGN.



### Historia

| Edición | Recomendación | Aprobación | Comisión de Estudio | ID único* |
|---|---|---|---|---|
| 1.0 | ITU-T Y.2725 | 2014-07-18 | 13 | 11.1002/1000/12079 |


* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

## PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) 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 [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 en la dirección http://www.itu.int/ITU-T/ipr/.

## ÍNDICE

# Recomendación UIT-T Y.2725

## Soporte de OpenID en redes de la próxima generación

### 1 Alcance

En esta Recomendación se describen los mecanismos y procedimientos para el soporte de OpenID en las NGN. Los mecanismos y procedimientos descritos en esta Recomendación pueden emplearse para soportar servicios de aplicación en un entorno de proveedor multiservicios. En esta Recomendación se asume que el proveedor NGN es el proveedor OpenID.

### 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.

[UIT-T Y.2701] Recomendación UIT-T Y.2701 (2007), Requisitos de seguridad de la versión 1 de la red de próxima generación.

[UIT-T Y.2702] Recomendación UIT-T Y.2702 (2008), Requisitos de autentificación y autorización en las redes de próxima generación versión 1.

[UIT-T Y.2720] Recomendación UIT-T Y.2720 (2009), Marco general para la gestión de identidades en las redes de la próxima generación.

[UIT-T Y.2721] Recomendación UIT-T Y.2721 (2010), Requisitos de la gestión de identidades NGN y ejemplos de utilización.

[UIT-T Y.2724] Recomendación UIT-T Y.2724 (2013), Marco para el soporte de OAuth y OpenID en las redes de la próxima generación.

[OASIS XRI SYNTAX] Extensible Resource Identifier (XRI) Syntax V2.0.

### 3 Definiciones

#### 3.1 Términos definidos en otros documentos

En esta Recomendación se emplean los siguientes términos definidos en otros documentos:

**3.1.1 autentificación (de entidad) (*(entity) authentication*)** [b-UIT-T X.1252]: Proceso utilizado para obtener una confianza suficiente en la vinculación entre la entidad y la identidad presentada.

**3.1.2 autorización (*authorization*)** [b-UIT-T X.800]: Concesión de derechos y, sobre la base de esos derechos, concesión de acceso.

**3.1.3 concesión de autorización (*authorization grant*)** [b-IETF RFC 6749]: La concesión de autorización es una credencial que representa la autorización del propietario de los recursos (para acceder a sus recursos protegidos) utilizada por el cliente para obtener un testigo de acceso.

**3.1.4 servidor de autorización (*authorization server*)** [b-IETF RFC 6749]: Servidor que expide de los testigos de acceso al cliente tras autentificar con éxito al propietario de los recursos y obtener la autorización.

**3.1.5 cliente (*client*)** [b-IETF RFC 6749]: Aplicación que realiza peticiones de recursos protegidos en nombre del propietario de recursos y con su autorización. El término "cliente" no implica características de aplicación particulares (por ejemplo, si la aplicación se ejecuta en un servidor, un escritorio u otros dispositivos).

### 3.2 Términos definidos en esta Recomendación

Ninguno.

## 4 Abreviaturas y acrónimos

En la presente Recomendación se utilizan las siguientes siglas y acrónimos:

FE Entidad funcional (*functional entity)*

FRA Requisitos funcionales y arquitectura (*functional requirements and architecture*)

IdM Gestión de identidades (*identity management*)

IdP Proveedor de identidad (*identity provider*)

IETF Grupo Especial sobre Ingeniería de Internet (*Internet engineering task force*)

IP Protocolo Internet (*Internet protocol*)

OAuth Protocolo de autorización OAuth 2.0 (*authorization protocol oauth 2.0*)

OP Proveedor de OpenID (*OpenID provider*)

SAML Lenguaje de marcación de aserción de seguridad (*security assertion markuplanguage*)

URI Identificador uniforme de recursos (*uniform resource identifier*)

WS Servidor web (*web server*)

## 5 Convenios

La expresión "**se requiere**" indica que el requisito es absolutamente obligatorio y debe aplicarse sin excepción si se pretende declarar la conformidad con este documento.

La expresión "**se recomienda**" indica que se trata de un requisito recomendado y que, por ende, no es absolutamente obligatorio. Su cumplimiento no es indispensable para poder declarar la conformidad.

La expresión "**se prohíbe**" indica que el requisito está terminantemente prohibido y no se permite excepción alguna si se pretende declarar la conformidad con este documento.

La expresión "**se tiene la opción de**" indica que el requisito se permite, sin que ello signifique que se recomienda. No se pretende implicar que el fabricante deba ofrecer esta opción y que el operador de red/proveedor de servicio tenga la posibilidad de activarla. Significa, más bien, que el fabricante tiene la opción de proporcionar esta función sin que ello afecte a la conformidad con la presente especificación.

## 6 Soporte de OpenID en las NGN

En esta cláusula se describen los principales aspectos del soporte de OpenID en las NGN.

## 6.1 Modelo de referencia

De acuerdo con la especificación de OpenID [b-OpenID v.2], el servidor IdP OpenID participa en todo el flujo de autentificación. En la Recomendación [UIT-T Y.2724] se presenta el marco general de OAuth y OpenID.

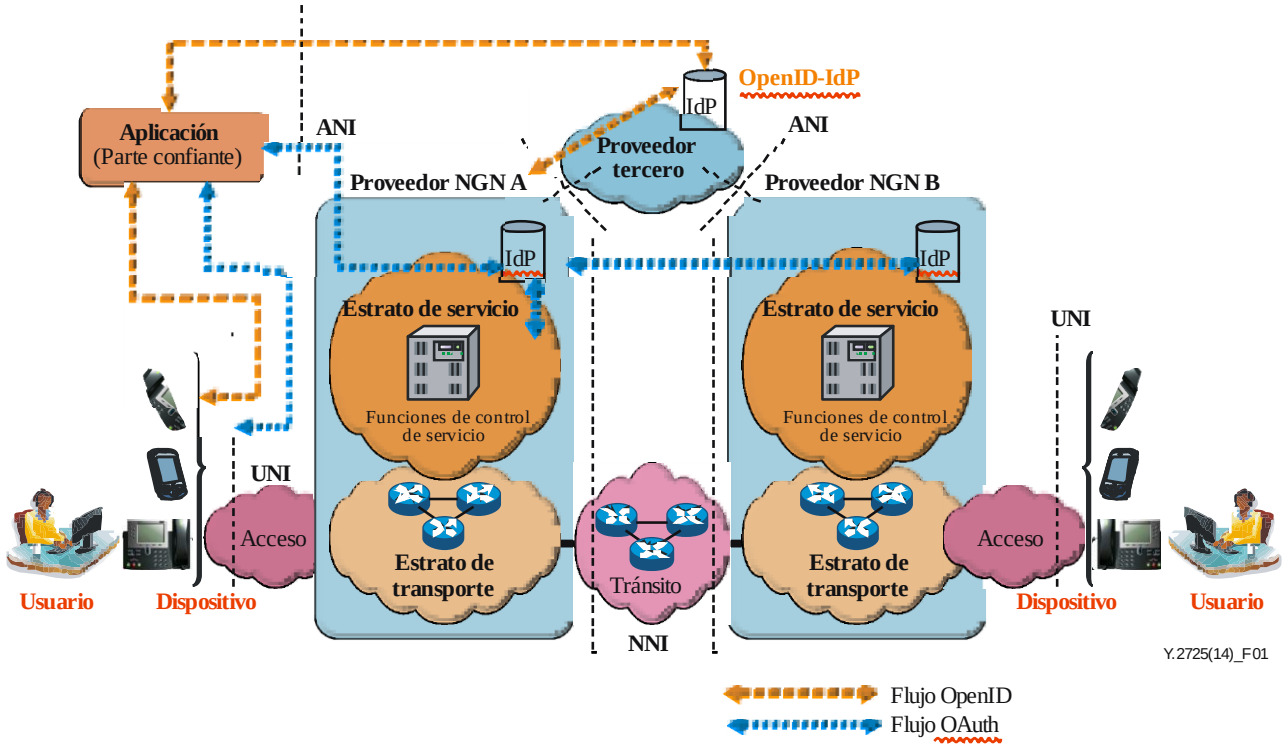


**Figura 1- Flujos OpenID y OAuth en las NGN**

## 6.2 Formatos de mensaje de protocolo en las NGN

[b-OpenID v.2] define dos tipos de formato de mensaje de protocolo:

- codificación de forma clave-valor;
- codificación HTTP.

En la sección 4.1.1 de [b-OpenID v.2] se explica que la "codificación de forma clave-valor se utiliza para el cálculo de firma y para la respuesta directa a partes confiantes".

En el caso de la codificación HTTP, en la sección 4.1.2 de [b-OpenID v.2] se indica que "este modelo se aplica a los mensajes procedentes del usuario-agente dirigidos tanto a la parte confiante como al OP, así como a los mensajes de la parte confiante al OP".

Se requiere que las entidades soportadas por las NGN cumplan los requisitos al enviar un mensaje de protocolo.

## 6.3 Tipos de comunicación

[b-OpenID v.2] define dos tipos de comunicación:

- comunicación directa;
- comunicación indirecta.

En la sección 5.1 de [b-OpenID v.2] se explica que la comunicación directa la inicia una parte confiante con un URL de punto extremo OP. Se utiliza para establecer asociaciones y verificar aserciones de autentificación.

En la sección 5.2 de [b-OpenID v.2] se explica que en la comunicación indirecta, los mensajes de comunicación pasan a través del usuario-agente. Esta comunicación puede estar iniciada por la parte confiante o por la OP. La comunicación indirecta se utiliza para las solicitudes de autentificación y las respuestas de autentificación.

Se requiere que las entidades soportadas por las NGN cumplan estos requisitos al iniciar el contexto de comunicación.

## 6.4 Generación de firmas

La autentificación OpenID soporta dos algoritmos de firma:

- HMAC-SHA1 – longitud de clave de 160 bits
- HMAC-SHA256 – longitud de clave de 256 bits.

En esta cláusula se recomienda la utilización de HMAC-SHA256. El procedimiento para generar firmas de mensaje en la sección 6.1 de [b-OpenID v.2] satisface los requisitos de seguridad de las NGN.

## 6.5 Procedimiento para la autentificación OpenID en las NGN

### 6.5.1 Requisitos de autentificación

En la sección 13 de [b-OpenID v.2] se dice que se recomienda que las partes confiantes utilicen el protocolo Yadis para publicar sus URL return_to válidos. Las partes confiantes pueden opcionalmente publicar esta información en cualquier URL, y se recomienda que la publiquen bajo el dominio para que los proveedores puedan verificar los URL return_to.

En esta Recomendación es obligatorio recomendar a las partes confiantes la utilización del protocolo Yadis para publicar sus URL return_to válidos en las NGN.

En la sección 9 de [b-OpenID v.2] se especifican las solicitudes de autentificación.

Los siguientes requisitos se aplican a la interacción entre la parte confiante y el usuario extremo. Se exige que la parte confiante:

- Inicie la autentificación OpenID
- Normalice un identificador facilitado por el usuario
- Descubra la información necesaria para iniciar las solicitudes.

#### 6.5.1.1 Inicio de la autentificación OpenID

En la sección 7.1 de [b-OpenID v.2] se formula la siguiente recomendación: "Para iniciar la autentificación OpenID se recomienda que la parte confiante presente al usuario extremo un formulario con un campo para la introducción de un identificador facilitado por el usuario".

Se recomienda que el atributo "name" del campo del formulario tenga el valor "openid_identifier" para que los usuarios-agentes puedan automáticamente determinar que se trata de un formulario OpenID. Es posible que las extensiones de navegador o software de otro tipo, que soporten la autentificación OpenID, no detecten el soporte de la parte confiante si este atributo no está definido adecuadamente.

En esta Recomendación se exige la inclusión del campo "openid_identifier" en el formulario que la entidad parte confiante presenta en las NGN.

#### 6.5.1.2 Normalización del identificador facilitado por el usuario

[b-OpenID v.2] define tres tipos de identificadores: el URI "http" o "https" (comúnmente denominado "URL" en este documento), o un identificador XRI [OASIS XRI SYNTAX 2.0].

Se requiere que la aportación del usuario extremo se normalice en un identificador. El procedimiento especificado en la sección 7.2 de [b-OpenID v.2] satisface los requisitos de normalización de las NGN.

#### 6.5.1.3 Descubrimiento de la información necesaria para el inicio de solicitudes

En [b-OpenID v.2] se explica que el descubrimiento es el "proceso mediante el cual la parte confiante utiliza el identificador para encontrar (descubrir) la información necesaria para iniciar solicitudes".

La autentificación OpenID tiene tres trayectos por los cuales efectuar el descubrimiento, como se especifica en la sección 7.3 de [b-OpenID v.2].

En [b-OpenID v.2] se definen dos métodos de descubrimiento:

- Descubrimiento XRDS
- Descubrimiento HTML.

Si se utiliza el descubrimiento XRI [b-OASIS XRI SYNTAX 2.0] o Yadis, el resultado será un documento XRDS. Se trata de un documento XML con entradas para los servicios relacionados con el identificador, como se especifica en la sección 7.3.2.1 de [b-OpenID v.2].

Se requiere que las partes confiantes soporten el descubrimiento HTML que sólo puede utilizarse para el descubrimiento de identificadores reclamados. Se requiere que los identificadores OP XRI [b-OASIS XRI SYNTAX 2.0] o URL soporten el descubrimiento XRDS. Para utilizar el descubrimiento HTML, se requiere que esté disponible en el URL del identificador reclamado un documento HTML, como se especifica en la sección 7.3.3 de [b-OpenID v.2].

En esta Recomendación se requiere obligatoriamente que la parte confiante cumpla los requisitos al realizar el descubrimiento, y se recomienda que el identificador se ajuste a los formatos XRI o URL.

### 6.5.2 Respuestas de autentificación

De acuerdo con la sección 10 de [b-OpenID v.2], cuando una solicitud de autentificación procede de un usuario-agente a través de una comunicación indirecta, se recomienda que la OP determine que un usuario extremo autorizado desea completar la autentificación. Si un usuario extremo autorizado desea completar la autentificación, se recomienda que la OP envíe una aserción positiva a la parte confiante.

En esta Recomendación se exige la inclusión del parámetro "return_to" en las solicitudes de autorización.

NOTA – Quedan fuera del alcance de la presente Recomendación los métodos de identificación de usuarios extremos autorizados y de obtención de aprobación para la devolución de una aserción de autentificación OpenID.

#### 6.5.2.1 Aserciones positivas

Las aserciones positivas son respuestas indirectas. En la sección 10.1 de [b-OpenID v.2] puede encontrarse información sobre los parámetros de respuesta.

De conformidad con [b-OpenID v.2] la OP, cuando esté en comunicación indirecta con una parte confiante a través de un usuario-agente, deberá:

- Verificar que el URL return_to coincide con uno de los puntos extremos de la parte confiante
- Determinar que un usuario extremo autorizado desea completar la autentificación
- Generar respuesta nonce

- Formar una respuesta positiva
- Enviar la aserción positiva a la parte confiante a través del usuario-agente.

#### 6.5.2.2 Aserciones negativas

Si la OP no puede identificar al usuario extremo, o el usuario extremo no aprueba o no puede aprobar la solicitud de autentificación, se recomienda que la OP envíe una aserción negativa a la parte confiante como respuesta indirecta. Véase también la sección 10.2 de [b-OpenID v.2].

Al recibir una aserción negativa en respuesta a una solicitud modo "checkid_immediate", se recomienda que las partes confiantes creen una nueva solicitud de autentificación empleando el modo "checkid_setup".

##### 6.5.2.2.1 Aserciones negativas en respuesta a solicitudes inmediatas

Si la solicitud era inmediata, no hay posibilidad alguna de que el usuario extremo interactúe con páginas en la OP para facilitar las credenciales de identificación o la aprobación de una solicitud. La aserción negativa de una solicitud inmediata adopta la forma especificada en la sección 10.2.1 de [b-OpenID v.2].

##### 6.5.2.2.2 Aserciones negativas en respuesta a solicitudes no inmediatas

Dado que la OP puede presentar páginas al usuario extremo y solicitarse credenciales, una respuesta negativa a una solicitud no inmediata es definitiva y adopta la forma especificada en la sección 10.2.2 de [b-OpenID v.2].

Si una parte confiante recibe la respuesta "cancel", la autentificación no se ha llevado a cabo y se requiere que la parte confiante considere que el usuario extremo no está autentificado.

### 6.5.3 Verificación de aserciones

De conformidad con [b-OpenID v.2], al recibir una aserción positiva, la parte confiante deberá:

- Verificar el URL de devolución
- Verificar la información descubierta
- Comprobar el nonce
- Verificar las firmas.

Si se verifica la aserción y ésta contiene un identificador reclamado, el usuario queda autentificado con ese identificador.

## 6.6 Consideraciones de seguridad

En la sección 15 (Consideraciones de seguridad) de OpenID 2.0 [b-OpenID v.2] se presentan directrices de seguridad para la prevención de ataques, usuarios-agentes, interfaces de usuario, identificadores URL HTTP y HTTPS URL, y variantes de protocolo. En este documento se recomienda el soporte de todas las consideraciones de seguridad en las NGN.

Las soluciones deberán también cumplir los requisitos de seguridad NGN e IdM especificados en [UIT-T Y.2701], [UIT-T Y.2720] y [UIT-T Y.2721].

# Bibliografía


[b-UIT-T X.800] Recomendación UIT-T X.800 (1991), *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT*.

[b-UIT-T X.1252] Recomendación UIT-T X.1252 (2010), *Términos y definiciones sobre gestión de identidad de referencia*.

[b-OpenIDv.2] OpenID Authentication 2.0
http://openid.net/specs/openid-authentication-2_0.html

[b-Yadis] Protocolo Yadis
http://infogrid.org/trac/wiki/Yadis

[b-IETF RFC 6749] IETF RFC 6749 (2012), *The OAuth 2.0 Authorization Framework*
http://tools.ietf.org/html/rfc6749

## SERIES DE RECOMENDACIONES DEL UIT-T

| | |
|---|---|
| Serie A | Organización del trabajo del UIT-T |
| 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 multimedia |
| Serie I | Red digital de servicios integrados |
| Serie J | Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia |
| Serie K | Protección contra las interferencias |
| Serie L | Construcción, instalación y protección de los cables y otros elementos de planta exterior |
| Serie M | Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes |
| Serie N | Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión |
| Serie O | Especificaciones de los aparatos de medida |
| Serie P | Terminales y métodos de evaluación subjetivos y objetivos |
| 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, comunicaciones de sistemas abiertos y seguridad |
| **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, 2015