Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Y.2723

(11/2013)

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 OAuth en las redes de la próxima generación

Recomendación UIT-T Y.2723

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.2723

Soporte de OAuth en las redes de la próxima generación

Resumen

En la Recomendación UIT-T Y.2723 se especifican los mecanismos y procedimientos para utilizar el "Marco de autorización OAuth 2.0 (*OAuth*)", definido por el Grupo Especial sobre Ingeniería de Internet, en aquellos casos en que un proveedor de red de la próxima generación (NGN) ejerce la función de servidor de autorización OAuth.

En la Recomendación UIT-T Y.2724, Marco para el soporte en las NGN de OAuth y OpenID, que complementa la presente, se describe el contexto, las consideraciones arquitectónicas y el marco de alto nivel para utilizar OAuth en las NGN.

En la presente Recomendación se especifican los requisitos para restringir la selección de opciones OAuth, así como otros requisitos que garantizan la coherencia de OAuth con los requisitos de seguridad y gestión de identidades en las NGN.

Historia

Edición	Recomendación	Aprobación	Comisión de estudios	
1.0	ITU-T Y.2723	2013-11-15	13	11.1002/1000/11913

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 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

Página

1 Alcance 1

2 Referencias 1

3 Definiciones 1

3.1 Términos definidos en otros documentos 1

3.2 Términos definidos en esta Recomendación 2

4 Siglas y acrónimos 2

5 Convenios 2

6 Soporte de OAuth en las NGN 3

6.1 Selección de tipos de cliente OAuth basada en los requisitos de seguridad NGN 3

6.2 Selección de tipos de concesión de autorización 3

6.3 Recomendaciones sobre las opciones OAuth para los clientes NGN 3

6.4 Autentificación del propietario de los recursos 5

6.5 Consideraciones de seguridad 5

Bibliografía 6

Introducción

En la Recomendación UIT-T Y.2723 se presenta el marco para dar soporte y utilizar OAuth y OpenID en las redes de la próxima generación (NGN). La presente Recomendación se basa en la Recomendación UIT-T Y.2724 para definir los métodos específicos para OAuth.

NOTA – Esta Recomendación no aporta cambios o modificaciones al protocolo OAuth, sino que se centra exclusivamente en cómo dar soporte y utilizar OAuth en las NGN.

Recomendación UIT-T Y.2723

Soporte de OAuth en las redes de la próxima generación

1 Alcance

En esta Recomendación se describen los mecanismos y procedimientos para dar soporte al protocolo de autorización OAuth 2.0 en las redes de la próxima generación (NGN). Los mecanismos y procedimientos descritos en esta Recomendación pueden emplearse para servicios de aplicación en un entorno de multiproveedor multiservicios. En esta Recomendación se parte del supuesto de que las NGN proporcionan el servicio de autorización OAuth.

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 X.1254] Recomendación UIT-T X.1254 (2012), *Marco de garantía de la autentificación de entidades*.

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

[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 gestión de identidad en las NGN y ejemplos de utilización*.

[UIT-T Y.2724] Proyecto de nueva Recomendación UIT-T Y.2724 (2013), *Marco para el soporte y utilización en las NGN de OpenID y OAuth*.

[IETF RFC 6749] IETF RFC 6749 (2012), *The OAuth 2.0 Authorization Framework*. <http://datatracker.ietf.org/doc/rfc6749/>

3 Definiciones

3.1 Términos definidos en otros documentos

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

3.1.1 testigo de acceso (*access token*) [IETF RFC 6749]: Credenciales utilizadas para acceder a recursos protegidos. Un testigo de acceso es una cadena que representa la autorización expedida al cliente. La cadena suele ser opaca para el cliente. El propietario de los recursos concede los testigos, que representan alcances y duraciones de acceso específicos, y el servidor de recursos y el servidor de autorización los ejecutan.

3.1.2 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.

3.1.3 autorización (*authorization*) [b-UIT-T X.800]: Concesión de derechos y, en función de esos derechos, concesión de acceso.

3.1.4 concesión de autorización (*authorization grant*) [IETF RFC 6749]: 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.

3.1.5 servidor de autorización (*authorization server*) [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.

3.1.6 cliente (*client*) [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).

3.1.7 clientes confidenciales (*confidential clients*) [IETF RFC 6749]: Clientes capaces de mantener la confidencialidad de sus credenciales (por ejemplo, cliente realizado en un servidor seguro con acceso restringido a sus credenciales de cliente) o capaz de autentificar al cliente de manera segura por otros medios.

3.1.8 clientes públicos (*public clients*) [IETF RFC 6749]: Clientes incapaces de mantener la confidencialidad de sus credenciales (por ejemplo, clientes ejecutados en el dispositivo del propietario de los recursos, como una aplicación nativa instalada o una aplicación de usuario-agente), e incapaz de autentificar al cliente de manera segura por otros medios.

3.1.9 propietario de recursos (*resource owner)* [IETF RFC 6749]: Entidad capaz de conceder acceso a un recurso protegido. Cuando el propietario de recursos es una persona, se denomina usuario extremo.

3.1.10 servidor de recursos (*resource server*) [IETF RFC 6749]: Servidor que aloja los recursos protegidos, capaz de aceptar y responder a las peticiones de recursos protegidos mediante testigos de acceso.

3.2 Términos definidos en esta Recomendación

Ninguno.

4 Siglas y acrónimos

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

IdM Gestión de identidad (*identity management*)

NGN Red de la próxima generación (*next generation network*)

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

SAML Lenguaje de marcaje de asertos de seguridad (*security assertion markup language*)

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

5 Convenios

Ninguno.

6 Soporte de OAuth en las NGN

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

6.1 Selección de tipos de cliente OAuth basada en los requisitos de seguridad NGN

En [IETF RFC 6749] se definen dos tipos de cliente OAuth: el cliente confidencial y el cliente público.

Los clientes públicos no cumplen los requisitos de autentificación de los proveedores de aplicación terceros NGN [UIT-T Y.2702], porque los clientes públicos no pueden ser autentificados por el proveedor NGN [UIT-T Y.2724]. Se recomienda aquí que las NGN sólo soporten clientes confidenciales. Los clientes han de cumplir los siguientes requisitos:

1) Debe ser posible autentificar al cliente OAuth NGN con un nivel de garantía específico [UIT-T Y.2702], [UIT-T X.1254].
2) El cliente OAuth NGN ha de registrarse en el servidor de autorización, como se especifica en la sección 2 de [IETF RFC 6749].

OAuth 2.0 [IETF RFC 6749] define los siguientes perfiles de cliente: aplicación web, aplicación de usuario-agente y aplicación nativa. La aplicación web es un perfil de cliente privado, mientras que los dos siguientes son perfiles de clientes públicos. En esta Recomendación sólo se describe el soporte en las NGN del perfil de cliente aplicación web.

6.2 Selección de tipos de concesión de autorización

En [IETF RFC 6749] se definen los siguientes tipos de concesión de autorización: código de autorización, implícita, credenciales contraseña del propietario de los recursos y credenciales de cliente. Además, el IETF está trabajando en definir una extensión, que especifique el tipo de concesión de aserto SAML 2.0 para OAuth 2.0.

En [IETF RFC 6749] se explica que, "cuando se expide un testigo de acceso durante el flujo de concesión implícita, el servidor de autorización no autentifica al cliente. En algunos casos, la identidad del cliente puede verificarse a través del URI de redireccionamiento utilizado para entregar el testigo de acceso al cliente. El testigo de acceso puede quedar expuesto al propietario de los recursos u otras aplicaciones con acceso al usuario-agente del propietario de los recursos".

Por consiguiente, el flujo OAuth que utiliza el tipo de concesión implícita no da como resultado una autentificación que cumple los requisitos de autentificación del proveedor de aplicación tercero NGN [UIT-T Y.2702].

Esta Recomendación se centra en describir el soporte en las NGN del cliente confidencial con perfil aplicación web utilizando las siguientes concesiones de autorización:

- código de autorización;
- credenciales contraseña del propietario de los recursos;
- credenciales de cliente;
- aserto SAML 2.0.

6.3 Recomendaciones sobre las opciones OAuth para los clientes NGN

Los flujos [IETF RFC 6749] están optimizados para diversos perfiles de cliente de los dos tipos de cliente. En la RFC se especifican las opciones de selección de tipos de concesión de autorización, parámetros y requisitos de seguridad.

En esta cláusula se formulan recomendaciones para el soporte de clientes confidenciales con perfil aplicación web. Esta cláusula se centra en los requisitos y parámetros opcionales cuya selección es fundamental para el soporte de OAuth en las NGN.

6.3.1 Registro de cliente

En la sección 2.2 de [IETF RFC 6749] se recomienda el registro de los URI de redireccionamiento del cliente en un servidor de autorización, porque los clientes con URI registrados ofrecen una mayor seguridad.

Esta Recomendación exige que los clientes soportados en las NGN registren sus URI de redireccionamiento en el servidor de autorización.

6.3.2 Confidencialidad de los mensajes al punto extremo de redireccionamiento cliente

En la sección 3.1.2.1 de [IETF RFC 6749] se recomienda lo siguiente: "el punto extremo de redireccionamiento DEBE exigir la utilización de TLS, como se describe en la sección 1.6, cuando el tipo de respuesta requerida es "código" o "testigo", o cuando la petición de redireccionamiento tendrá como resultado la transmisión de credenciales sensibles por una red abierta". La presente Recomendación exige que se utilice TLS para la transmisión de todo tipo de información sensible.

6.3.3 Autentificación de cliente

Los clientes definidos por el perfil aplicación web son clientes confidenciales, por lo que es necesario que un servidor de autentificación autentifique al cliente.

6.3.4 Procedimientos de autorización

Esta Recomendación atañe a los clientes confidenciales con perfil aplicación web que utilizan los procedimientos de autorización de los siguientes tipos de concesión de autorización:

- código de autorización;
- credencial contraseña del propietario de los recursos;
- credenciales de cliente;
- extensión SAML.

6.3.4.1 Código de autorización

El procedimiento de autorización para clientes confidenciales que utilizan el código de autorización se especifica en la sección 4.1 de [IETF RFC 6749]. Esta Recomendación exige la inclusión del parámetro *redirect_uri* en las peticiones de autorización.

Los siguientes requisitos se aplican a la interacción del servidor de autorización con los clientes con perfil aplicación web que utilizan el código de autorización. El servidor de autorización DEBERÁ:

- autentificar al cliente que expide la petición de autorización;
- garantizar que el valor del parámetro *redirect_uri* en la petición de autorización del cliente coincide con el valor registrado para ese cliente;
- expedir el código de autorización sólo a los clientes autentificados y autorizados;
- antes de expedir un testigo de acceso, garantizar que el código de autorización es válido.

6.3.4.2 Credenciales contraseña del propietario de los recursos

El procedimiento de autorización que utiliza este tipo de concesión está optimizado para los clientes que han establecido una relación fiable con el propietario de los recursos. El cliente utiliza las credenciales contraseña del propietario de los recursos para obtener un testigo de acceso del servidor de autorización. El procedimiento especificado en la sección 4.3 de [IETF RFC 6749] satisface los requisitos de seguridad de las NGN.

NOTA – [IETF RFC 6749] permite a los clientes públicos utilizar este procedimiento. La presente Recomendación sólo atañe a los clientes confidenciales, que han de ser autentificados por el servidor de autorización.

De acuerdo con [IETF RFC 6749], al interactuar con un cliente que utiliza el tipo de concesión credenciales contraseña del propietario de los recursos, el servidor de autorización DEBERÁ:

- autentificar al cliente;
- validar las credenciales contraseña del propietario de los recursos presentadas por el cliente;
- expedir un testigo de acceso si el cliente ha sido autentificado por el servidor de autorización y ha presentado las credenciales contraseña del propietario de los recursos válidas.

6.4 Autentificación del propietario de los recursos

La especificación de OAuth [IETF RFC 6749] no especifica la autentificación del propietario de los recursos (por ejemplo, el usuario extremo) por parte del servidor de autorización. En el entorno de las NGN, un mecanismo de autentificación del propietario de los recursos ha de cumplir los requisitos de [UIT-T Y.2702].

6.5 Consideraciones de seguridad

En la sección Consideraciones de seguridad de la especificación de OAuth 2.0 [IETF RFC 6749] se presentan las directrices de seguridad para todos los perfiles de cliente OAuth 2.0: aplicación web, aplicación de usuario-agente y aplicación nativa. En la presente se recomienda el soporte de los clientes aplicación web en las NGN. Por consiguiente, sólo son de aplicación en este contexto las consideraciones de seguridad de [IETF RFC 6749] relativas a los clientes aplicación web. Además, en [b-IETF RFC 6819] se presenta un modelo de seguridad OAuth global e información para el diseño del protocolo. Se habrá de tener en cuenta la información de [b-IETF RFC 6819] pertinente a los clientes aplicación web para la aplicación del soporte de OAuth en las NGN.

Toda solución deberá además cumplir con 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 de referencia para la gestión de la identidad*.

[b-IETF RFC 6819] IETF RFC 6819, *OAuth 2.0 Threat Model and Security Considerations.* http://datatracker.ietf.org/doc/rfc6819/

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, 2014