Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Y.2724

(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

Marco para el soporte y utilización de OAuth y OpenID en las redes de la próxima generación

Recomendación UIT-T Y.2724

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.2724

Marco para el soporte y utilización de OAuth y OpenID en las redes de la próxima generación

Resumen

En esta Recomendación se especifica un marco para dar soporte y utilizar el protocolo de autorización abierta del IETF (*OAuth*) y del protocolo *Open ID* en las redes de la próxima generación. Ambos protocolos se han definido para su utilización general en la World Wide Web.

Los rigurosos requisitos de seguridad y gestión de identidades de las redes de la próxima generación (NGN) exigen que se restrinjan con tiento los protocolos mencionados. En esta Recomendación se expone la aplicabilidad de estos protocolos en las NGN y se facilitan directrices de alto nivel para su utilización.

En la Recomendación UIT-T Y.2723, Soporte de OAuth en las NGN, asociada se presenta una serie de perfiles NGN.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T Y.2724	2013-11-15	13	11.1002/1000/11914

* 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 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 3
5 Convenios 3
6 Marco para el soporte en las NGN de *OAuth* y *OpenID* 3
6.1 Modelo de referencia 4
6.2 Flujos *OAuth* y *OpenID* 4
Apéndice I – Caso de uso del servidor web 9
I.1 Ejemplo de utilización: servidor web 9
I.2 Ejemplo de utilización: credenciales de cliente 10
I.3 Ejemplo de utilización: aserción 11
Bibliografía 12

Recomendación UIT-T Y.2724

Marco para el soporte y utilización de OAuth y OpenID en las redes de la próxima generación

1 Alcance

En esta Recomendación se describe un marco para dar soporte y utilizar *OAuth* y *OpenID* en las redes de la próxima generación (NGN). El alcance de esta Recomendación comprende:

- El marco funcional para el soporte en las NGN de *OAuth* y *OpenID*.
- Los requisitos para el soporte en las NGN de *OAuth* y *OpenID*.
- Casos de uso de *OAuth* y *OpenID* (documentado en el Apéndice I).

NOTA – Los implementadores y operadores de las tecnologías descritas deberán ajustarse a las leyes, reglamentos y políticas nacionales y regionales aplicables.

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.2012] Recomendación UIT-T Y.2012 (2010), *Requisitos y arquitectura funcional de las redes de próxima generación*.

[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.2722] Recomendación UIT-T Y.2722 (2011), *Mecanismos de gestión de identidades en las NGN*.

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

3 Definiciones

3.1 Términos definidos en otros documentos

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

3.1.1 testigo de acceso [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. Los testigos dan acceso con un alcance y duración determinados. Los concede el propietario de los recursos y los aplican el servidor de recursos y el servidor de autorización.

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

NOTA – En el contexto de la gestión de identidad (IdM) se entiende que el término autentificación se refiere a la autentificación de una entidad.

3.1.3 autorización [b-UIT-T X.800]: Concesión de derechos y, sobre la base de esos derechos, concesión de acceso.

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

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

3.1.6 entidad [b-UIT-T X.1252]: Cualquier cosa que tenga una existencia autónoma y bien definida y pueda ser identificada en contexto.

NOTA – Una entidad puede ser una persona física, un animal, una persona jurídica, una organización, una cosa activa o pasiva, un dispositivo, una aplicación informática, un servicio, etc., o un grupo de estos elementos. En el contexto de las telecomunicaciones, como ejemplos de entidades cabe mencionar puntos de acceso, abonados, usuarios, elementos de red, redes, aplicaciones informáticas, servicios y dispositivos, interfaces, etc.

3.1.7 identificador [b-UIT-T X.1252]: Uno o más de los atributos utilizados para identificar a una entidad dentro de un contexto.

NOTA – En el contexto de las NGN, como se define en [b-UIT-T Y.2091], un identificador es una serie de dígitos, caracteres y símbolos, o cualquier otro tipo de datos, utilizada para identificar a los abonados, los usuarios, los elementos de red, las funciones, las entidades de red que ofrecen servicios/aplicaciones, o cualesquiera otras entidades (por ejemplo, objetos físicos o lógicos).

3.1.8 proveedor de identidad (IdP) [b-UIT-T X.1252]: Véase proveedor de servicio de identidad (IdSP).

3.1.9 proveedor de servicio de identidad (IdSP) [b-UIT-T X.1252]: Entidad que verifica, mantiene, gestiona y puede crear y asignar información de identidad de otras entidades.

3.1.10 testigo de refresco [IETF RFC 6749]: El servidor de autorización expide al cliente testigos de refresco, que se utilizan para obtener un nuevo testigo de acceso cuando el testigo de acceso original expira o deja de ser válido, o para obtener testigos de acceso adicionales con un alcance igual o menor (los testigos de acceso pueden tener una duración más corta o menos permisos que los autorizados por el propietario de los recursos). La expedición de testigos de refresco es optativa a discreción del servidor de autorización. Si el servidor de autorización expide un testigo de refresco, se incluye en la expedición de testigos de acceso.

3.1.11 propietario de los recursos [IETF RFC 6749]: Entidad capaz de conceder acceso a un recurso protegido. Cuando el propietario de los recursos es una persona, se le denomina usuario extremo.

3.1.12 servidor de recursos [IETF RFC 6749]: Servidor que alberga los recursos protegidos, capaz de aceptar las peticiones de los recursos protegidos, y de responder a ellas, utilizando testigos de acceso.

3.2 Términos definidos en esta Recomendación

Ninguno.

4 Siglas y acrónimos

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

AKA Acuerdo de autentificación y clave (*authentication and key agreement*)

ANI Interfaz aplicación-red (*application-to-network interface*)

FE Entidad funcional (*functional entity*)

GBA Arquitectura de inicialización genérica (*generic bootstrapping architecture*)

IdM Gestión de identidad (*identity management*)

IdP Proveedor de identidad (*identity provider*)

IdSP Proveedor de servicio de identidad (*identity service provider*)

IMPI Identidad privada de multimedios IP (*IP multimedia private identity*)

IMSI Identidad de abonado móvil internacional (*international mobile subscriber identity*)

NGN Redes de la próxima generación (*next generation networks*)

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

SNI Interfaz servicio-red (*service network interface*)

UNI Interfaz usuario-red (*user network interface*)

5 Convenios

En esta Recomendación se utilizan las siguientes expresiones con el significado que se indica a continuación:

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.

En el cuerpo de la presente Recomendación y en sus anexos aparecen algunas veces verbos que expresan *obligación*, *prohibición*, *recomendación* y *posibilidad*, en cuyo caso deben interpretarse en dicho sentido. Cuando estas expresiones o términos aparecen en apéndices o en partes incluidas explícitamente a *título informativo* no deben interpretarse en su sentido normativo.

6 Marco para el soporte en las NGN de *OAuth* y *OpenID*

Como se describe en [UIT-T Y.2720], las NGN están formadas por múltiples elementos funcionales que utilizan identificadores de entidades para realizar sus funciones a fin de dar soporte y facilitar servicios de autentificación abiertos a otros proveedores. Esas configuraciones pueden recurrir a *OpenID* y *OAuth*, como se muestra en la Figura 1, donde se ilustra la utilización de *OpenID* y *OAuth*.

De acuerdo con la especificación de *OpenID* [b-OpenID v.2], el servidor IdP *OpenID* participa en todo el flujo de autentificación y *OAuth* permite a la parte confiante enviar directamente el mensaje de autentificación al IdP NGN utilizando el protocolo *OAuth*.

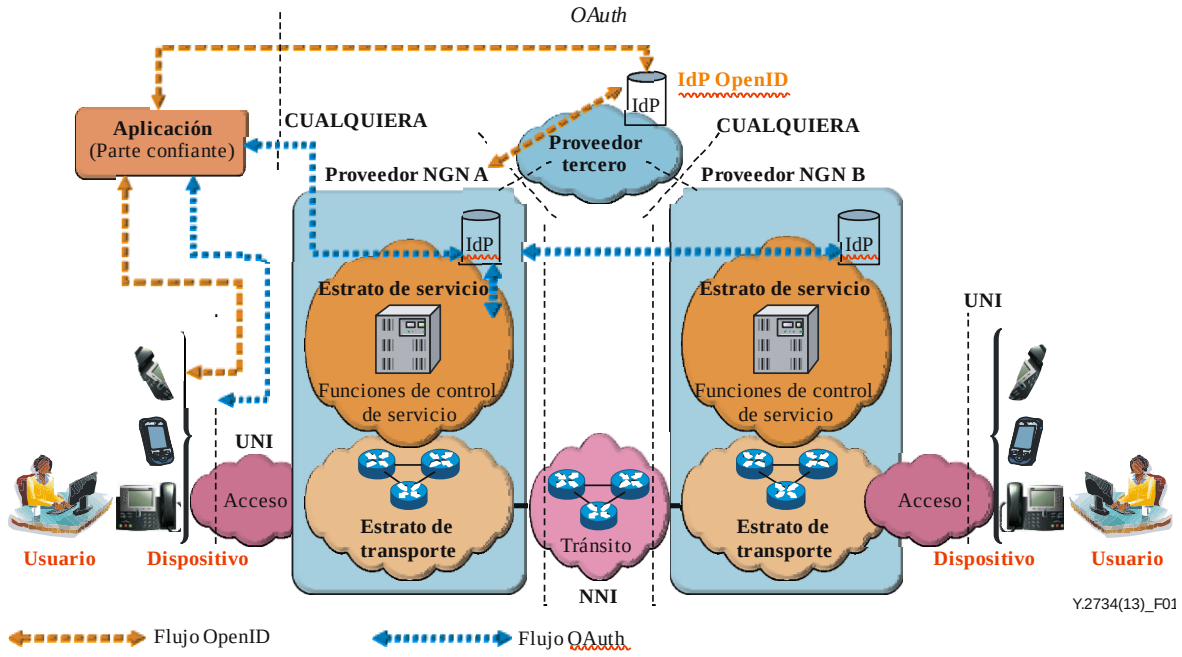

Figura 1 – Flujos *OpenID* y *OAuth* en las NGN

6.1 Modelo de referencia

En la Figura 1 se presenta una visión general del marco *OAuth* y *OpenID*.

En la Figura 2 se ilustra un modelo de referencia de la NGN que ofrece servicios de autorización *OAuth* y autentificación *OpenID*. Los proveedores NGN pueden utilizar *OpenID* y *OAuth* para ofrecer servicios IdSP y asociarse con proveedores de contenido y aplicación y/u otros proveedores de servicio.

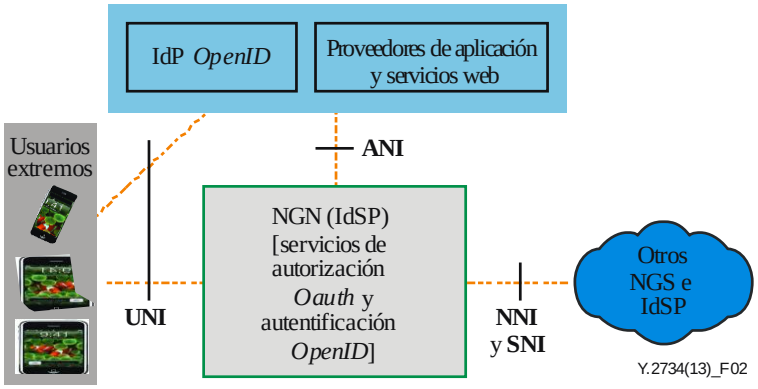

Figura 2 – Modelo de referencia

6.2 Flujos *OAuth* y *OpenID*

En esta cláusula se describen en términos generales los flujos de mensajes para *OAuth* y *OpenID* en las NGN.

6.2.1 Entidades participantes en los flujos de información

En esta cláusula se identifican las entidades (incluidas las entidades funcionales de [UIT-T Y.2012]) que participan en los flujos de información *OAuth* y *OpenID*.

6.2.2 Entidades comunes a los flujos *OAuth* y *OpenID*

Las entidades que participan tanto en los flujos *OAuth* como *OpenID* son las siguientes:

- Función de usuario extremo con capacidad de cliente web (por ejemplo, navegador).
- A-2: entidad funcional pasarela de aplicación (APL-GW-FE) [UIT-T Y.2012]. Esta entidad funcional debe ser capaz de soportar los protocolos *OAuth* y/u *OpenID*.

Como se define en [UIT-T Y.2012], *la APL-GW-FE* "sirve de entidad de interfuncionamiento entre las distintas funciones de las NGN y todos los servidores de aplicación externos y habilitadores de servicio". Eso hace que A-2 sea la opción lógica para ofrecer el soporte de *OAuth* y *OpenID*. Además, dada su conexión con la entidad funcional perfil de usuario de servicio-S-5 (SUP-FE) [UIT-T Y.2012], A-2 puede soportar la autentificación AKA, incluida la arquitectura de inicialización genérica (GBA) de los dispositivos de usuario. En [b-3GPP TS 33.220] se especifica un método de autentificación *OpenID* basado en GBA. Otro método de autentificación *OpenID* basado en AKA, semejante a GBA en algunos aspectos, puede encontrarse en la cláusula 6.2.8 de [UIT-T Y.2722]. Si tanto el servidor de autorización *OAuth* como el IdP *OpenID* [UIT-T Y.2722] utilizan la A-2, pueden utilizar la autentificación AKA mediante la interacción con S-5.

6.2.3 Entidades propias del flujo *OAuth*

Las entidades específicas de *OAuth* son las siguientes:

- Servidor de aplicación web que realiza un servicio para un usuario – un cliente *OAuth*. Es posible que el cliente no tenga que ejecutarse en una entidad NGN.
- Servidor de autorización aplicado como parte de A-2:

  En primer lugar, el servidor de autorización realiza la autentificación del usuario y luego procede a la autorización de la petición del cliente. Si ambos procedimientos se realizan satisfactoriamente, el intercambio *OAuth* resulta en que el servidor de autorización expide un testigo de acceso al cliente. Para soportar la autentificación AKA, el servidor de autorización debe poder interactuar con S-5.
- Servidor de recursos:

  El servidor de recursos accede a la petición del cliente cuando ésta va acompañada de un testigo de acceso válido. Se especifican dos tipos de procedimientos para acceder a un recurso utilizando testigos de acceso: los testigos de portador se especifican en [b-IETF RFC6750] y el IETF está trabajando en la especificación de testigos MAC. El servidor de recursos puede o no estar coubicado con el servidor de autorización en A-2.

A continuación se describen los flujos de información *OAuth* de alto nivel cuando se utiliza un servidor web (descrito en el Apéndice 1), como se ilustran en la Figura 3.

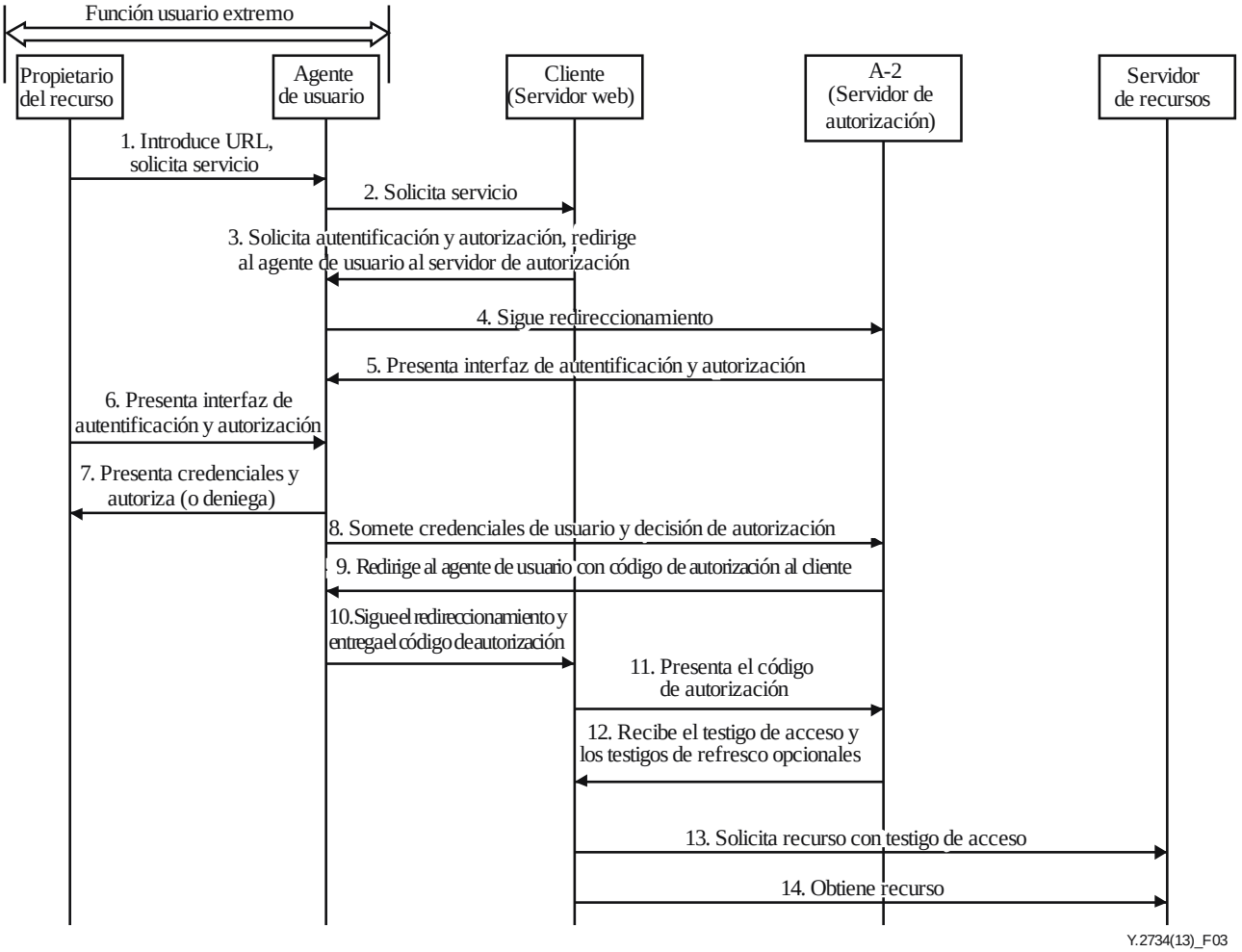

Figura 3 – Flujo *OAuth* con un servidor web

1. El usuario ordena al agente de usuario (por ejemplo, navegador) que solicite un servicio al cliente.
2. El agente de usuario somete la petición al cliente.
3. El cliente forma una respuesta y redirige al agente de usuario al servidor de autorización para autentificar al usuario y autorizar la petición del cliente.
4. El agente de usuario sigue el redireccionamiento.
5. El servidor de autorización responde al agente de usuario con una interfaz de autentificación y autorización.
6. El agente de usuario presenta la interfaz de autentificación y autorización al usuario (propietario del recurso).
7. El usuario facilita credenciales de autentificación e indica la decisión de autorización mediante el agente de usuario.
8. El agente de usuario envía los datos facilitados por el usuario al servidor de autorización.
9. El servidor de autorización, tras autentificar al usuario y asegurarse de que el usuario tiene la petición del cliente autorizado, redirige al agente de usuario de vuelta al cliente. La respuesta contiene el código de autorización.
10. El agente de usuario, tras el redireccionamiento, entrega el código de autorización al cliente.
11. El cliente envía el código de autorización al servidor de autorización.

12. El servidor de autorización responde con un testigo de acceso y testigos de refresco opcionales.
13. El cliente envía una petición al servidor de recursos y presenta el testigo de acceso.
14. El servidor de recursos facilita el recurso solicitado.

6.2.4 Entidades propias del flujo *OpenID*

Las entidades específicas de *OpenID* son las siguientes:

- Servidor de aplicación que confía en la autentificación realizada por el IdP *OpenID*.
- IdP *OpenID* como parte de A-2. A fin de soportar la autentificación AKA, esta entidad deberá poder interactuar con S-5.
- S-5, que participa en la autentificación *OpenID* si la NGN realiza la autentificación AKA de la función usuario extremo como se especifica en [UIT-T Y.2722].

A continuación se describen los flujos de información *OpenID* que se ilustran en la Figura 4. El texto y la figura describen el procedimiento *OpenID* cuando el IdP y el servidor de aplicación han establecido un secreto compartido. El secreto se utiliza para que el IdP firme un mensaje con el resultado de la autentificación y el servidor de aplicación lo verifique.

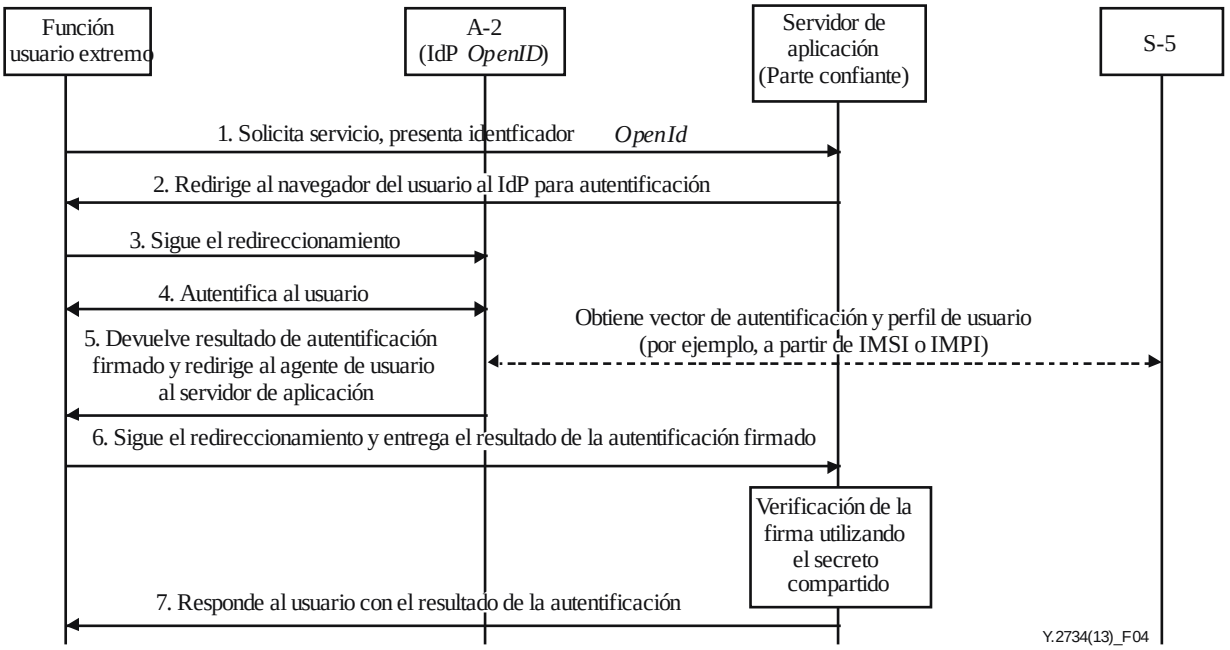

Figura 4 – Flujo *OpenID*

1. El navegador del usuario envía una petición de servicio a un servidor de aplicación. La petición contiene el identificador *OpenID* del usuario.
2. A partir del identificador *OpenID*, el servidor de aplicación descubre el IdP *OpenID* del usuario.
3. El navegador sigue la petición de redireccionamiento.
4. El IdP *OpenID* autentifica al usuario intercambiando información a través del navegador del usuario.
5. Si el IdP *OpenID* realiza una autentificación AKA (por ejemplo, como se describe en [UIT-T Y.2722]), debe interactuar con S-5. Estas interacciones se marcan con una línea discontinua.

6. El IdP *OpenID* redirecciona al navegador de usuario de vuelta al servidor de aplicación con una respuesta que contiene un mensaje firmado con el resultado de la autentificación.
7. El navegador sigue la petición de redireccionamiento y entrega el mensaje firmado al servidor de aplicación.
8. El servidor de aplicación, tras validar la firma y verificar el resultado de la autentificación, notifica al usuario si la autentificación se ha realizado con éxito. Los procedimientos de firma y validación se especifican en [b-OpenID v.2].

Apéndice I

Caso de uso del servidor web

(Este Apéndice no forma parte integrante de la presente Recomendación)

I.1 Ejemplo de utilización: servidor web

Descripción:

Alice accede a una aplicación que se ejecuta en un servidor web en www.X-printphotos.example y le indica que imprima sus fotografías, almacenadas en un servidor www.X-storephotos.example. Alice está abonada a un proveedor de servicios NGN que ejecuta el servidor de autorización *OAuth* en www.X-carrier.example. La aplicación en www.X-printphotos.example recibe la autorización de Alice para acceder a sus fotografías sin conocer sus credenciales de autentificación para www.X-storephotos.example o www.X-carrier.example.

Condiciones *a priori*:

- Alice se ha registrado en www.X-carrier.example para permitir la autentificación.
- La aplicación en www.X-printphotos.example ha establecido las credenciales de autentificación con el servidor de autorización en www.X-carrier.example.
- La aplicación en www.X-storephotos.example puede validar el testigo de acceso expedido por el servidor de autorización en www.X-carrier.example.

Condiciones *a posteriori*:

El éxito del procedimiento resulta en que la aplicación www.X-printphotos.example recibe un código de autorización de www.X-carrier.example. El código está ligado a la aplicación www.X-printphotos.example y a la URL de vuelta indicada en la solicitud. La aplicación en www.X-printphotos.example utiliza el código de autorización para obtener un testigo de acceso de www.X-carrier.example. La aplicación en www.X-carrier.example expide un testigo de acceso tras autentificar la aplicación en www.X-printphotos.example y validar el código de autorización que ha presentado. La aplicación en www.X-printphotos.example utiliza el testigo de acceso para obtener acceso a las fotografías de Alice en www.X-storephotos.example.

NOTA – Cuando expira el código de acceso, el servicio en www.X-printphotos.example necesita repetir el procedimiento *OAuth* para obtener de Alice la autorización para acceder a sus fotografías en www.X-storephotos.example. Por otra parte, si Alice quiere conceder a la aplicación un acceso duradero a sus recursos en www.X-storephotos.example, el servidor de autorización en www.X-carrier.example puede expedir testigos a largo plazo. Esos testigos pueden cambiarse por los testigos de acceso a corto plazo necesarios para acceder a www.X-storephotos.example.

Requisitos:

- El servidor www.X-printphotos.example, que alberga un cliente *OAuth*, debe ser capaz de expedir las peticiones de redireccionamiento HTTP para el agente del usuario Alice: un navegador.
- El servidor de autorización en www.X-carrier.example debe poder autentificar a Alice. El método de autentificación queda fuera del alcance de *OAuth*.
- La aplicación en www.X-carrier.example debe obtener la autorización de Alice para acceder a sus fotografías a través de www.X-printphotos.example.
- La aplicación en www.X-carrier.example puede desvelar a Alice el alcance del acceso que ha solicitado www.X-printphotos.example al pedirle su autorización.

- El servidor de autorización en www.X-carrier.example debe poder autentificar la aplicación en www.X-printphotos.example y validar el código de autorización antes de expedir un testigo de acceso. La aplicación en www.X-printphotos.example debe facilitar una URL de vuelta al servidor de autorización en www.X-carrier.example (NOTA: la URL ha de estar prerregistrada en www.X-carrier.example).
- El servidor de autorización en www.X-carrier.example debe mantener un registro que asocie el código de autorización con la aplicación en www.X-printphotos.example y la URL de vuelta facilitada por la aplicación.
- Los testigos de acceso son los testigos del portador (no están asociados con una aplicación específica como www.X-printphotos.example) y deben tener una duración corta.
- El servidor de autorización en www.X-carrier.example debe invalidar el código de autorización tras su primera utilización.
- La participación manual de Alice en el procedimiento de autorización *OAuth* (por ejemplo, introduciendo una URL o una contraseña) no debe ser obligatoria. (La autentificación de Alice ante www.X-carrier.example queda fuera del alcance de *OAuth*).

I.2 Ejemplo de utilización: credenciales de cliente

Descripción:

La empresa Good-X-Pay prepara las nóminas de los empleados de la empresa Good-X-Work. Para ello, la aplicación en www.Good-X-Pay.example obtiene acceso autentificado a los datos de presencia de los empleados almacenados en www.Good-X-Work.example. El servidor de autorización, que es parte de una NGN con URL www.X-carrier.example, realiza la autentificación.

Condiciones *a priori*:

- La aplicación en www.Good-X-Pay.example ha establecido mediante registro un identificador y un secreto compartido con el servidor de autorización de www.X-carrier.example.
- Se ha definido el alcance del acceso de la aplicación en www.Good-X-Pay.example a los datos almacenados en www.Good-X-Work.example.

Condiciones *a posteriori*:

La ejecución satisfactoria del procedimiento resulta en que la aplicación en www.Good-X-Pay.example recibe un testigo de acceso tras haberla autentificado el servidor de autorización en www.X-carrier.example. La aplicación en www.Good-X-Pay.example utiliza entonces el testigo de acceso para acceder a los datos de presencia de www.Good-X-Work.example.

Requisitos:

- Es obligatorio obtener la autentificación de la aplicación en www.Good-X-Pay.example del servidor de autorización en www.X-carrier.example.
- El método de autentificación debe basarse en un identificador y un secreto compartido, que la aplicación ejecutada en www.Good-X-Pay.example somete al servidor de autorización en www.X-carrier.example con la petición HTTP inicial.
- Dado que el procedimiento da como resultado el acceso a datos sensibles de Good-X-Work, ésta deberá establecer la confianza con Good-X-Pay y el servidor de autorización en www.X-carrier.example.

I.3 Ejemplo de utilización: aserción

Descripción:

La empresa Good-X-Pay prepara las nóminas de los empleados de la empresa Good-X-Work. Para ello, la aplicación en www.Good-X-Pay.example obtiene acceso autentificado a los datos de presencia de los empleados almacenados en www.Good-X-Work.example. El servidor www.Good-X-Work.example concede acceso a la aplicación en www.Good-X-Pay.example cuando recibe un testigo de acceso expedido por el servidor de autorización www.X-carrier.example. El servidor de autorización www.X-carrier.example autentifica la aplicación en www.Good-X-Pay.example validando la aserción presentada por www.Good-X-Pay.example.

Este caso es una solución alternativa a la expuesta en el caso de utilización de credenciales de cliente.

Condiciones *a priori*:

- La aplicación en www.Good-X-Pay.example obtiene una aserción de autentificación de una parte en la que el servidor de autorización www.X-carrier.example confía.
- Se ha definido el alcance del acceso de la aplicación en www.Good-X-Pay.example a los datos almacenados en www.Good-X-Work.example.
- El servidor de autorización www.X-carrier.example ha establecido una relación de confianza con la parte aseverante y puede validar sus aserciones.

Condiciones *a posteriori*:

La ejecución satisfactoria del procedimiento resulta en que la aplicación en www.Good-X-Pay.example recibe un testigo de acceso tras su autentificación por el servidor de autorización www.X-carrier.example mediante la presentación de una aserción (por ejemplo, aserción SAML). Obtiene acceso a los datos de presencia de los empleados utilizando el testigo de acceso.

Requisitos:

- Es obligatorio que el servidor de autorización www.X-carrier.example autentifique la aplicación en www.Good-X-Pay.example.
- El servidor de autorización www.X-carrier.example debe ser capaz de validar las aserciones expedidas por la parte aseverante y que le presenta la aplicación ejecutada en www.Good-X-Pay.example.
- Good-X-Work deberá establecer la confianza con Good-X-Pay y el servidor de autorización www.X-carrier.example.

Bibliografía

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

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

[b-ITU-T Y.2091] Recomendación UIT-T Y.2091 (2008), *Términos y definiciones para las redes de la próxima generación*.

[b-IETF RFC 6750] IETF RFC 6750, *The OAuth 2.0 Authorization Framework: Bearer Token Usage*.

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

[b-3GPP TS 33.220] 3GPP TS 33.220 (2013), *Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture, Release 12*.

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