Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1256

(03/2016)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Seguridad en el ciberespacio – Gestión de identidades

Directrices y marco para la compartición de los resultados de la autentificación de red con las aplicaciones de los servicios

Recomendación UIT-T X.1256

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	**X.1250–X.1279**
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
Recomendaciones relacionadas con la PKI	
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/eurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de eurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699

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

Recomendación UIT-T X.1256

Directrices y marco para la compartición de los resultados de la autentificación de red con las aplicaciones de los servicios

Resumen

Con la explosión de los dispositivos y las aplicaciones móviles que acceden a internet, la red y el entorno de servicio están adquiriendo una complejidad creciente. En consecuencia, existe una presión para simplificar el mecanismo de autentificación del usuario y así mejorar la experiencia del mismo y la calidad del servicio.

Varias organizaciones de normalización, incluida la UIT, han realizado muchas actividades de investigación sobre el mecanismo de autentificación unificado (por ejemplo, el inicio de sesión con registro único). Sin embargo, todo el trabajo actual se centra básicamente en la autentificación unificada entre las aplicaciones de los servicios, sin considerar la relación con la autentificación de red.

Desde el punto de vista del operador de red, los usuarios realizan alguna forma de autentificación de red cuando acceden a ella, aunque cuando vuelven a registrarse para solicitar un acceso a un servicio no se vuelve a reutilizar su autentificación inicial de red. Cuando se adopta un mecanismo de compartición de los resultados de la autentificación entre el servicio y la red, las aplicaciones del servicio pueden identificar un usuario utilizando los resultados de la autentificación de red. Un mecanismo de este tipo permite al usuario autentificarse una vez con la red y acceder directamente al servicio.

La Recomendación UIT-T X.1256 desarrolla las directrices para que los operadores de red y los proveedores de servicios compartan los resultados de la autentificación de red, y ofrece un marco para compartir los atributos mínimos entre múltiples servicios dentro de una relación establecida de confianza.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1256	2016-03-23	17	11.1002/1000/12605

Palabras clave

Autentificación, atributos de identidad, autentificación a nivel de red

* 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

Recomendación UIT-T X.1256

Directrices y marco para la compartición de los resultados de la autentificación de red con las aplicaciones de los servicios

1 Alcance

En esta Recomendación se desarrollan las directrices para que los operadores de red y los proveedores de servicios compartan los resultados de la autentificación de red, y ofrece un marco para compartir los atributos mínimos entre múltiples servicios dentro de una relación de confianza establecida.

Los métodos que utilizan los operadores de red para llevar a cabo, integrar o aplicar la autentificación a nivel de red quedan fuera del alcance de la presente Recomendación.

2 Referencias

Las siguientes Recomendaciones UIT-T y demás referencias contienen disposiciones que, por referencia a las mismas en este texto, constituyen disposiciones de esta Recomendación. En la fecha de publicación, las ediciones citadas estaban en vigor. Todas las Recomendaciones y demás referencias están sujetas a revisión, por lo que se alienta a los usuarios de esta Recomendación a que consideren la posibilidad de aplicar la edición más reciente de las Recomendaciones y demás referencias que se indican a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T vigentes. La referencia a un documento en el marco de esta Recomendación no confiere al mismo, como documento autónomo, el rango de Recomendación.

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

3 Definiciones

3.1 Términos definidos en otros documentos

Ninguno.

3.2 Términos definidos en esta Recomendación

Ninguno.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las abreviaturas y los acrónimos siguientes:

2G/3G Segunda/tercera generación

AC Controlador de acceso (*access controller*)

AKA Autentificación y acuerdo clave (*authentication and key agreement*)

AN Red de acceso (*access network*)

AP Punto de acceso (*access point*)

API Interfaz de programación de aplicaciones (*application programming interface*)

AUG Pasarela de autentificación (*authentication gateway*)

BRAS Servidor de acceso a distancia de banda ancha (*broadband remote access server*)

EAP-SIM Método de protocolo de autentificación extensible para módulos de identidad de abonados (GSM) (*extensible authentication protocol method for (GSM) subscriber identity modules*)

GGSN Nodo soporte pasarela de GPRS (*gateway GPRS support node*)

GPRS Servicio general de radiocomunicaciones por paquetes (*general packet radio service*)

HTTP Protocolo de transferencia de hipertexto (*hyper text transfer protocol*)

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

IMPU Identidad de usuario público de multimedios IP (*IP multimedia public user identity*)

IMS Subsistema de multimedios IP (*IP multimedia subsystem*)

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

IP Protocolo Internet (*internet protocol*)

LoA Nivel de garantía (*level of assurance*)

MSISDN Número RDS1/RTPC de abonado móvil internacional (*mobile subscriber international ISDN/PSTN number*)

RADIUS Servicio de usuario de marcación de autentificación a distancia (*remote authentication dial-in user service*)

RDSI Red digital de servicios integrados

RPTC Red telefónica pública conmutada

SGSN Nodo soporte de servicio de GPRS (*serving GPRS support node*)

SIM Módulo de identidad del abonado (*subscriber identity module*)

SIP Protocolo de iniciación de la sesión (*session initiation protocol*)

SNS Servicio de red social (*social network service*)

UE Equipo de usuario (*user equipment*)

USIM Módulo de identidad universal de abonado (*universal subscriber identity module*)

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

WAP Protocolo de aplicación inalámbrico (*wireless application protocol*)

WLAN Red de área local inalámbrica (*wireless local area network*)

5 Convenios

Ninguno.

6 Mecanismos de compartición de los atributos de autentificación

6.1 Marco

Cuando los usuarios acceden a la red de un operador, se exige que estén fuertemente autentificados por la red de acceso. Sin embargo, esta capacidad de autentificación no facilita por lo general los servicios. En la mayoría de los casos, los usuarios finales se autentifican en la red y en el sistema de servicio, respectivamente. Por ejemplo, los usuarios finales son autentificados por la red de tercera generación (3G) basada en la tarjeta del módulo de identidad universal de abonado (USIM) situadas dentro de sus teléfonos móviles (el que tengan) pero, cuando visitan un determinado servicio de red

social (SNS) tienen que ser autentificados de nuevo por el servidor web sobre la base del binomio (nombre de usuario, contraseña) registrado con anterioridad (el que conocen).

El concepto básico de la compartición de atributos de autentificación es permitir a los servicios utilizar los atributos de autentificación de red. En la Figura 6.1 se muestra el marco de compartición de los atributos de autentificación.

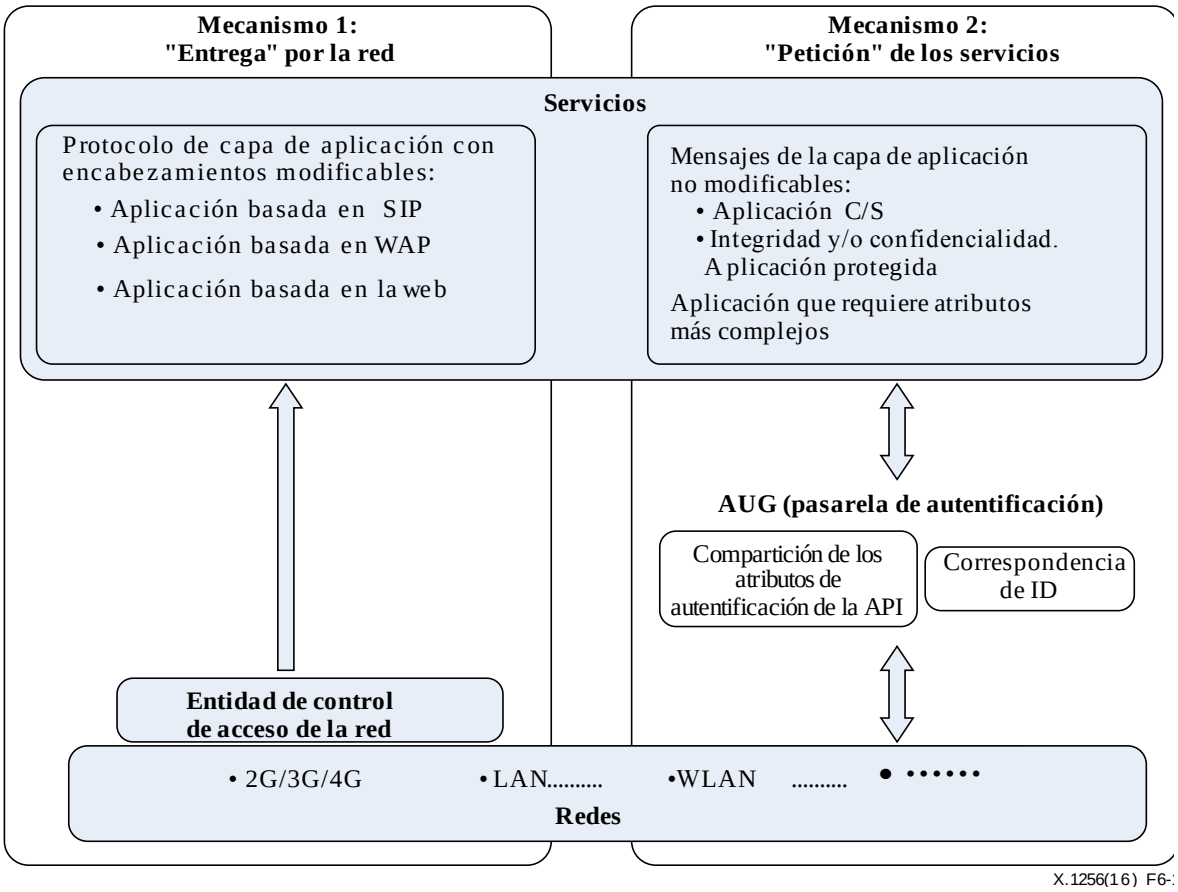

Figura 6.1 – Marco de compartición de los atributos de autentificación de la red con las aplicaciones de los servicios

En este marco, hay dos tipos de autentificación de los atributos de los mecanismos de compartición:

- Mecanismo 1 – Mecanismo controlado por la red: transfiere directamente los atributos de autentificación a las aplicaciones de los servicios

  Cuando la entidad de control de acceso de la red entiende el protocolo de la capa de aplicación del servicio (por ejemplo SIP, WAP, HTTP, etc.), le resulta posible insertar los atributos de autentificación de red en los mensajes de la capa de aplicación y transferirlos directamente a la plataforma del servicio. En este caso, no es necesario definir una interfaz de programación de aplicaciones (API) para que las aplicaciones de los servicios obtengan de manera activa los atributos de autentificación, ya que se limitan a recibir de manera pasiva tales parámetros, contenidos en los encabezamientos de los mensajes.

  Las aplicaciones de los servicios pueden decidir analizar y utilizar los encabezamientos insertados por la red, o simplemente ignorarlos. Si las aplicaciones de los servicios necesitan más atributos que los que se facilitan, deberán utilizar el mecanismo de petición del servicio.

  En el Apéndice I.1 se presenta un caso práctico.

- Mecanismo 2 – Mecanismo de petición del servicio: compartir los atributos de autentificación de red a través de la pasarela de autentificación (AUG).

  Si la entidad de control de acceso de la red no puede analizar o modificar los mensajes de la capa de aplicación de los servicios (por ejemplo, cuando el protocolo de la capa de aplicación está patentado, o cuando está protegida la integridad y/o confidencialidad de los mensajes de la capa de aplicación), es necesario introducir una AUG autónoma en la red para la compartición de los atributos de autentificación. La AUG aplica una API de red bien definida a la que pueden acudir las aplicaciones de los servicios para obtener los atributos de autentificación de red.

  Además, si las aplicaciones de servicio mencionadas en el caso del mecanismo por el que la red facilita atributos requieren más atributos que los que se les facilitan, también deberán utilizar el citado mecanismo de petición del servicio para obtener de la red atributos de autentificación adicionales.

  En el Apéndice I.2 se presenta un caso práctico.

6.2 Mecanismo de entrega por la red

6.2.1 Guía de aplicación

Cuando el usuario visita la red, la entidad de control de acceso de la red autentifica la identidad del usuario en la entrada. Entre los ejemplos típicos de entidad de control de acceso de la red figuran el dispositivo de control de acceso (AC) en una red de área local inalámbrica (WLAN), el nodo soporte de servicio GPRS (SGSN) o el nodo soporte pasarela GPRS (GGSN) en un servicio general de radiocomunicaciones por paquetes (GPRS), y el dispositivo servidor de acceso a distancia de banda ancha (BRAS) en una red fija. La entidad de control de acceso de la red conoce la identidad del usuario como resultado de la autentificación de red.

Si la entidad de control de acceso de la red conoce el protocolo de la capa de aplicación del servicio (por ejemplo SIP, WAP, HTTP, etc.) le resulta posible encapsular la identidad del usuario y alguna información adicional en los mensajes de solicitud de servicio y transferirlos a la plataforma de los servicios.

Si la plataforma de los servicios confía en la entidad de control de acceso de la red, puede extraer directamente la identidad del usuario de las solicitudes de servicios, y considerar que el usuario ya está autentificado.

En esta arquitectura, la plataforma de los servicios tiene que determinar si confía o no en los atributos de autentificación insertados por la entidad de control de acceso de la red. Para ello, el operador de red tendrá que alcanzar un acuerdo con el proveedor de servicios, y facilitar una lista de dispositivos de control de acceso fiables o un mecanismo (por ejemplo claves precompartidas o certificados digitales) para identificar los dispositivos de control de acceso fiables. La información de usuario transferida entre el dispositivo de control de acceso y la plataforma de servicios debe estar protegida. Los dispositivos de control de acceso de la red también deben mantener una lista blanca de plataformas de servicios contratadas. Los atributos de autentificación de red sólo deben transferirse a las plataformas de servicios de la lista blanca. Las directrices sobre la manera de lograr esta relación de confianza queda fuera del alcance de la presente Recomendación.

6.2.2 Descripción de la interfaz

Los atributos de autentificación de red están cargados en el encabezamiento del protocolo de aplicación (por ejemplo SIP o HTTP) de los mensajes de solicitud de servicios, y se transfieren desde la entidad de control de acceso de la red a la plataforma de servicios.

Deben incluirse los siguientes atributos:

1) Identidad del usuario:

   El contenido de este campo es la identidad de red del usuario (por ejemplo SIP URI, MSISDN, Nombre de usuario, etc.). La plataforma de servicios puede utilizarlo para identificar al usuario.

2) Método de autentificación con un nivel de garantía (LoA) (UIT-T X.1254]:

   El contenido de este campo es el identificador del método de autentificación (por ejemplo, 2G/3G/4G AKA, IMS AKA, HTTP/SIP Digest, EAP-SIM, etc.).

   El operador de red y los proveedores de servicios deben acordar una lista de identificadores de método de autentificación reconocibles y sus correspondientes LoA.

   Una determinada plataforma de servicios debe decidir si acepta o no los atributos de autentificación facilitados por la red sobre la base del LoA del método de autentificación y su propia política en materia de seguridad.

3) Otros atributos requeridos con arreglo al contrato entre el operador y el proveedor de servicios.

6.3 Mecanismo de petición de los servicios

6.3.1 Guía de aplicación

No es posible implementar el mecanismo controlado por la red si la entidad de control de acceso de la red no puede analizar o modificar los mensajes de la capa de aplicación del servicio, por ejemplo, cuando el protocolo de la capa de aplicación está patentado, o cuando los mensajes de servicio están encriptados o protegidos en términos de integridad. En tal caso, puede colocarse una AUG entre la red y la plataforma de los servicios, que actúa como mandatario (proxy) para que la plataforma de los servicios obtenga información adicional acerca de los atributos de autentificación de red.

Otra justificación para el modelo de petición del servicio es que los atributos incluidos en los mensajes facilitados por la red pueden no ser los adecuados para una solicitud de servicio específica. En este caso, puede que la plataforma de los servicios tenga que comunicarse activamente con la red para obtener información adicional acerca de los atributos de autentificación de red.

Para habilitar el modelo de petición del servicio, la AUG tiene que exponer un conjunto de API de la red a las que pueden recurrir las aplicaciones de servicio para obtener de la red informaciones diversas acerca de los resultados de la autentificación. La red y las plataformas de servicios pueden utilizar diferentes ID (identificadores) para identificar a los usuarios. Por lo tanto, la AUG debe incluir una función de correspondencia que establezca una correspondencia entre la ID de servicio de un usuario y su ID de red, y viceversa.

En esta arquitectura, la plataforma de servicios y la AUG tienen que confiar la una en la otra. Para ello, el operador de red debe alcanzar un acuerdo con el proveedor de servicios, y facilitar una lista de dispositivos AUG fiables o un mecanismo (por ejemplo claves precompartidas o certificados digitales) para identificar los dispositivos AUG fiables. La información de usuario transferida entre el dispositivo AUG y la plataforma de servicio debe estar protegida. Los dispositivos AUG deben ejecutar un mecanismo de autorización (por ejemplo, lista blanca) en relación con las API expuestas de modo que los atributos de autentificación de red sólo puedan ser compartidos con plataformas de servicios contratadas. Las directrices sobre la manera de lograr esta relación de confianza queda fuera del alcance de la presente Recomendación.

6.3.2 Descripción de la interfaz

La AUG aplica API de la red bien definidas a las que pueden recurrir las aplicaciones de servicio para obtener de la red los atributos de autentificación.

Los operadores de red pueden aplicar las API de distintas maneras con arreglo a sus preferencias. La definición de estas API queda fuera del alcance de la presente Recomendación.

Los atributos de autentificación que pueden compartirse de esta manera incluyen cualquier información relacionada con un usuario de red autentificado, tales como la ubicación del usuario, la información de suscripción del usuario, las estadísticas de utilización de la red por dicho usuario, etc.

7 Consideraciones en materia de seguridad

Al aplicar las soluciones técnicas pertenecientes al marco de la cláusula 6, deben tenerse en cuenta algunas consideraciones de seguridad:

- Es indispensable proteger los elementos de autentificación relativos a la red, y velar por la fiabilidad y seguridad de la capacidad de autentificación de red.
- Los sistemas de servicios deben establecer una relación de confianza con la red, de manera que los sistemas de servicios dependientes puedan fiarse de los atributos de autentificación transferidos desde la red. La plataforma de servicios sólo debe confiar en la información de identidad de usuario procedente de un servidor de autentificación conocido a fin de evitar la suplantación del servidor de autentificación.
- Resulta esencial que los atributos de autentificación se transfieran de manera segura a la plataforma de servicios. La confidencialidad e integridad de la información de identidad de usuario debe estar garantizada, y la transmisión de la misma protegerse frente a ataques de reproducción y falsificación.
- Al facilitar los resultados de la autentificación y otra información de usuario a la plataforma de servicios, la red debe respetar estrictamente la legislación y reglamentación en materia de protección de la vida privada de la jurisdicción donde se presta el servicio.
- La plataforma de servicio debe manejar adecuadamente la información de autentificación obtenida a partir de la red, por ejemplo, almacenarla de manera segura para su utilización, y destruirla rápidamente una vez que se ha utilizado. Deben evitarse los abusos y las filtraciones de la información de usuario.

Apéndice I

Ejemplos de utilización

(El presente apéndice no forma parte integrante de esta Recomendación.)

I.1 Caso de utilización del mecanismo controlado por la red

I.1.1 Red 2G/3G/4G a servicio WAP

El protocolo de aplicación inalámbrico (WAP) es un servicio móvil de datos conocido al que los usuarios pueden acceder a través de redes 2G/3G/4G. Tras el acoplamiento a la red y la autentificación, la pasarela WAP GW puede insertar el número RDS1/RTPC de abonado móvil internacional (MSISDN) del usuario en las siguientes solicitudes WAP. El servidor WAP puede extraer el MSISDN de las solicitudes e identificar al usuario directamente mediante su MSISDN, o establecer una correspondencia entre el MSISDN y la ID de un usuario registrado.

Un ejemplo típico de estas aplicaciones basadas en WAP es la que la gente utiliza para contratar un taxi. Un usuario anónimo puede visitar ese sitio WAP desde su teléfono móvil sin exponer su verdadero nombre. El servidor WAP puede utilizar el MSISDN para identificar al usuario y gestionar su(s) pedido(s). Si el conductor del taxi necesita comunicarse con el usuario, puede devolver la llamada al MSISDN correspondiente.

El servidor WAP también requiere previamente que los usuarios se registren, especifiquen una ID de usuario y la liguen a uno o varios MSISDN. En este caso, antes de tramitar la solicitud el servidor WAP necesita mapear MSISDN facilitado desde la red a una ID de usuario registrado.

El procedimiento técnico detallado se presenta a continuación (véase la Figura I.1):

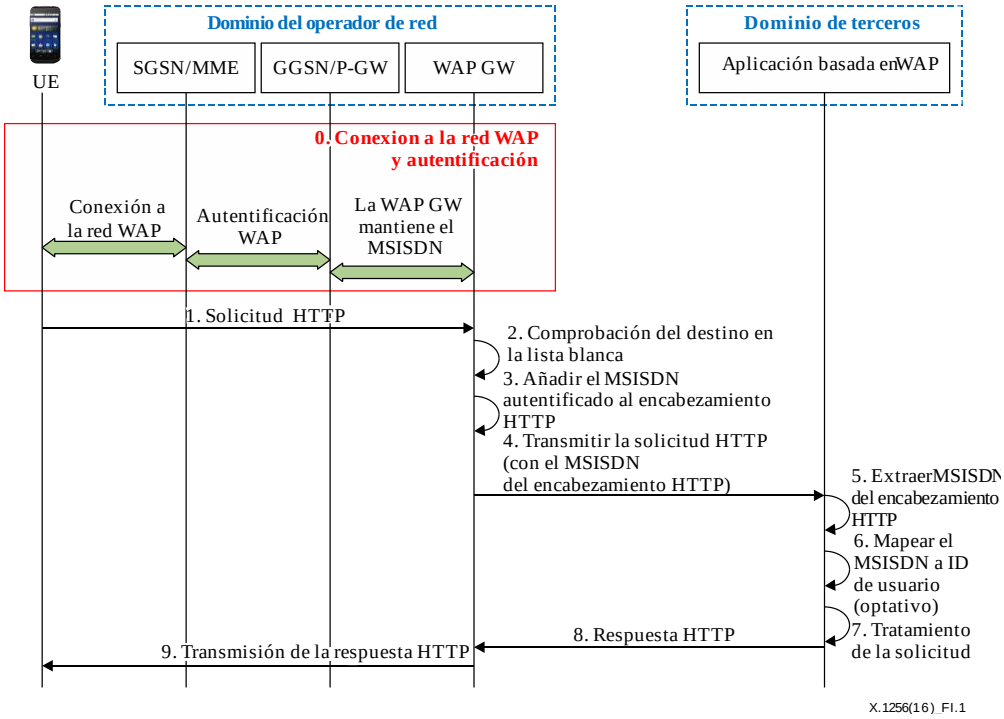

Figura I.1 – Compartición de la autentificación para un servicio WAP a través de una red 2G/3G/4G

0 El equipo de usuario (UE) se conecta a la red 2G/3G/4G. La pasarela WAP mantiene el MSISDN de cada usuario autentificado.

1 El UE inicia una solicitud mediante el protocolo de transferencia de hipertexto (HTTP) para acceder a un servicio WAP.

2 La pasarela WAP recibe la solicitud, y comprueba si el destino del servicio figura en la lista blanca.

3 Si la dirección de destino figura en la lista blanca, la pasarela WAP inserta un nuevo campo de encabezamiento HTTP (por ejemplo, «x-up-carlinga-line-id») en la solicitud, que incluye el MSISDN del usuario.

4 La pasarela WAP transfiere la solicitud HTTP modificada al servidor WAP.

5 El servidor WAP extrae el MSISDN del usuario del encabezamiento HTTP.

6 De manera optativa, el servidor WAP mapea el MSISDN a una ID de usuario registrado.

7 El servidor WAP procesa la solicitud con arreglo al MSISDN o la ID de usuario mapeada a partir del MSISDN.

8 El servidor WAP envía la respuesta HTTP a la pasarela WAP.

9 La pasarela WAP transfiere la respuesta HTTP al UE.

I.2 Caso de utilización del mecanismo de petición de los servicios

I.2.1 Servicio de Internet que utiliza atributos de localización de red 2G/3G/4G

Hay muchos servicios basados en la localización disponibles en Internet y la Internet móvil. Por ejemplo, un usuario puede visitar un servicio WAP desde su teléfono móvil y buscar un banco, hotel, restaurante o centro comercial a proximidad. Si el teléfono está equipado con un GPS, pueden enviar los parámetros de localización del usuario al servidor WAP como parte de la solicitud de búsqueda. Sin embargo, si no hay GPS o el GPS no funciona en ese momento (por ejemplo en un entorno cerrado), el servidor WAP puede necesitar la ayuda de la red medular 2G/3G/4G para localizar al usuario.

El procedimiento técnico detallado de servicio de Internet que utiliza los resultados de localización de la red 2G/3G/4G se define como sigue (véase Figura I.2):

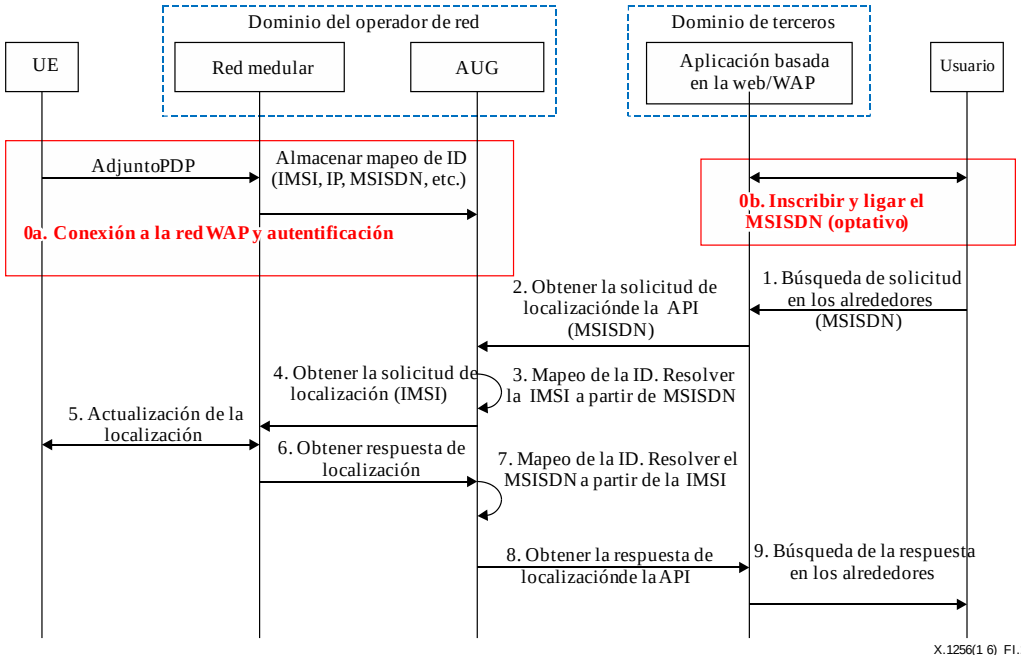

Figura I.2 – Servicio de Internet que utiliza los resultados de localización de la red 2G/3G/4G

0a El UE se conecta a la red 2G/3G/4G. GGSN/P-GW envía la relación de mapeo entre la identidad de abonado móvil internacional (IMSI) del usuario, el MSISDN y la dirección IP a la AUG utilizando el protocolo del servicio de usuario de marcación de autentificación a distancia (RADIUS).

0b Optativamente, el usuario de inscribe en el servidor de aplicaciones basado en la Web/WAP y liga su ID de usuario a uno o más MSISDN.

1 El usuario inicia una solicitud de búsqueda en los alrededores incluyendo su MSISDN como uno de los parámetros. El MSISDN puede ser insertado por la pasarela WAP según se describe en el Apéndice I.1.1, o ser introducido por el propio usuario y ser verificado por el servidor de una manera que queda fuera del alcance de la presente Recomendación.

2 El servidor WAP/Web analiza el MSISDN de la solicitud y recurre a la API para obtener la localización a fin de enviar a la AUG una solicitud con el MSISDN especificado.

3 La AUG mapea el MSISDN (ID de servicio) a la IMSI (ID de red).

4 La AUG pregunta a la red medular acerca de la localización actual correspondiente a la IMSI.

5 La red medular se comunica con el UE correspondiente a la IMSI y finaliza la actualización de la localización.

6 La red medular responde a la solicitud de localización de la AUG.

7 La AUG resuelve el MSISDN a partir de la IMSI.

8 El AUG responde a la llamada API de localización del servidor WAP/Web.

9 El servidor WAP/Web trata la solicitud en los alrededores del usuario utilizando la información de localización devuelta por la red y muestra al usuario los resultados de la búsqueda.

Bibliografía

[IETF RFC 3261] IETF RFC 3261 (2002), *SIP: Session Initiation Protocol*.

[IETF RFC 4186] IETF RFC 4186 (2006), *Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM).*

[3GPP TS 33.328] 3GPP TS 33.328 V12.6.0 (2014), *IP Multimedia Subsystem (IMS) media plane security (Release 12).*

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
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	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás 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	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
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, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2017