Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1258

(09/2016)

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

Seguridad en el ciberespacio – Gestión de identidades

Autentificación de entidad mejorada sobre la base de atributos agregados

Recomendación UIT-T X.1258

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	X.1340–X.1349

Recomendación UIT-T X.1258

Autentificación de entidad mejorada sobre la base de atributos agregados

Resumen

La agregación de atributos con origen en múltiples autoridades de atributos puede ser necesaria a fin de permitir que una parte confiante refuerce su confianza en la identidad de una parte. La agregación puede considerarse como el hecho de tener que tratar con un conjunto de identificadores globalmente únicos, algo que es común en todas las autoridades responsables de atributos. En la práctica, las entidades no disponen de un identificador global sino que tienen distintos identificadores de entidad y atributos asignados por sus diversos proveedores de servicios de identidad (IdSP).

Para abordar la cuestión de la agregación de atributos en este escenario, se utiliza el concepto de federación de identidad. Por ejemplo, si una tienda de libros electrónicos prevé una venta para personas mayores, debe facilitarse a la tienda un conjunto agregado de atributos (tarjeta de crédito y el tramo de edad) de dos IdSP, pero sin que ninguno de ellos tenga conocimiento de la implicación del otro IdSP. En la gestión normal de una identidad federada, una entidad sólo puede proporcionar atributos de una identidad, pero esta transacción requiere atributos de dos de ellas. Hay varios métodos de federación de identidad: lenguaje de marcación de aserción de seguridad (SAML), Shibboleth, la identidad abierta (OpenID) y la autentificación abierta (OAuth) entre otros.

La Recomendación UIT-T X.1258 introduce el concepto de agregación de atributos para permitir a una entidad agregar atributos de varios IdSP. La agregación de atributos es el mecanismo que permite recopilar atributos de una entidad obtenidos de múltiples IdSP. La agregación de atributos es necesaria para agregar los atributos de manera dinámica según la demanda. El IdSP puede realizar la solicitud de agregación cuando una entidad desea obtener un servicio. Además, también podría aplicarse en la autentificación la agregación de atributos centrada en la entidad a fin de mitigar la filtración de datos privados.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1258	2016-09-07	17	11.1002/1000/12850

Palabras clave

Agregación de atributos, gestión de identidad federada

* 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 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.1258

Autentificación de entidad mejorada sobre la base de atributos agregados

1 Alcance

La presente Recomendación proporciona una autentificación mejorada sobre la base de la agregación de atributos de una entidad entre dominios. La Recomendación abarca los siguientes asuntos:

– métodos destinados a agregar atributos de múltiples proveedores de servicios de identidad (IdSP); y

– autentificación mejorada sobre la base de atributos agregados.

2 Referencias

Ninguna.

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 atributo [UIT-T X.1252]: información relacionada con una entidad que especifica una característica de la entidad.

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 círculo de confianza [b-UIT-T X.1251]: conjunto de criterios fijados para que una organización pueda ingresar en una federación a fin de que cada una de ellas tenga acceso fiable a los recursos de las demás. Cabe señalar que un círculo de confianza es también el resultado final de la suma de organizaciones en una federación.

3.1.4 federación [b-UIT-T X.1252]: asociación de usuarios, proveedores de servicios y proveedores de servicios de identidad.

3.1.5 identidad [b-UIT-T X.1252]: representación de una entidad bajo la forma de uno o varios atributos que permiten distinguir suficientemente a la entidad o entidades dentro del contexto. A los efectos de la gestión de identidad (IdM), se entiende que este término constituye una identidad contextual (subconjunto de atributos), es decir que la diversidad de atributos está limitada por un marco con fronteras definidas (el contexto) en el cual existe e interactúa la entidad.

NOTA − Cada entidad está representada por una identidad holística que comprende todos los posibles elementos de información que caracterizan a dicha entidad (atributos). Sin embargo, la identidad holística es una cuestión teórica y elude cualquier descripción y utilización práctica, dado que el número de todos los atributos posibles es indefinido.

3.1.6 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.

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 agregación de atributos: mecanismo para recopilar atributos obtenidos de varios proveedores de servicios de identidad (IdSP).

NOTA – Una vez recolectados los atributos, deben ser agregados y confirmados para su autentificación y autorización.

3.2.2 dominio: esfera de gestión de un solo proveedor de servicios de identidad (IdSP).

3.2.3 proveedor de servicios (SP): entidad que presta servicios a clientes o a otros proveedores de servicios.

4 Siglas y acrónimos

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

CoT	Círculo de confianza (*circle of trust)*
DB	Base de datos (*database)*
ID	Identidad
IdM	Gestión de identidad (*identity management)*
IdSP	Proveedor de servicio de identidad (*identity service provider)*
LS	Servicio de enlace (*linking service)*
OAuth	Autentificación abierta (*open authentication)*
OpenID	Identidad abierta (*open identity)*
PKI	Infraestructura de clave pública (*public key infrastructure)*
SAML	Lenguaje de marcas de asertos de seguridad (*security assertion markup language)*
SP	Proveedor de servicios (*service provider)*
SSO	Inicio de sesión unificado (*single sign-on)*
VC	Colaboración virtual (*virtual collaboration)*

5 Convenios

Ninguno.

6 General

Por lo general, la gestión de identidad (IdM) electrónica abarca la gestión de cualquier tipo de identidad digital. El desarrollo de directorios, como por ejemplo el de la Recomendación [b-UIT-T X.500], puede ser considerado como el origen de la IdM. La Recomendación [b-UIT-T X.509] define certificados que contienen atributos de identidad. Los certificados que figuran en [b-UIT-T X.509] y los sistemas de infraestructura de clave pública (PKI) funcionan para validar la "identidad" en línea de un sujeto. Por consiguiente, la IdM puede ser considerada como gestión de información.

La identidad de una entidad puede estar compuesta por atributos que caracterizan dicha identidad en diferentes contextos. Se pueden necesitar diferentes identidades, según el contexto y la situación. Un sistema de IdM proporciona herramientas para la gestión de dichas identidades en un mundo digital. La IdM es un conjunto de funciones y capacidades, como la creación o supresión de la identidad, el descubrimiento y el intercambio de información. En el mundo real, la persona decide qué información desea compartir con los demás, teniendo en cuenta el contexto y la sensibilidad de la información. En cambio, en el mundo digital, esa tarea la lleva a cabo el sistema de IdM.

Sobre la base de las tecnologías y normas relativas a la IdM, los métodos del sistema de IdM se clasifican en: convencional, centralizado y federado. En el método convencional un proveedor de servicios (SP) gestiona identidades y está ubicado junto al proveedor de servicios de identidad (IdSP). Una entidad crea su identidad digital (ID) para cada uno de los SP de los que demanda la prestación de un servicio. Generalmente, las ID de las entidades no se comparten entre los distintos SP, enfoque que por lo general tiende a ser más costoso para la entidad y para los SP. Cada SP puede necesitar repetidas veces su propio conjunto de atributos para conformar la identidad digital de la entidad.

El método centralizado ha sido elaborado como una respuesta a la inflexibilidad del método convencional y comparte identidades entre los SP; se basa en el concepto de autentificación única o inicio de sesión unificado (SSO). Este método intenta evitar las inconsistencias y redundancias del método convencional, brindando a las entidades la capacidad de interactuar con varios SP sin necesidad de llevar a cabo una autentificación redundante.

Todos los SP que mantienen relaciones de confianza con un IdSP pueden estar completamente seguros de las autentificaciones de entidad facilitadas por dicho IdSP. El IdSP tiene la responsabilidad de autentificar una entidad y brindar a los SP la información de atributos de la entidad en el marco de un dominio que puede representar, por ejemplo, a una empresa o universidad, entre otros, y que se compone de entidades, varios SP y un único IdSP. El SSO es muy conveniente para las entidades, ya que sólo deben realizar el proceso de autentificación una única vez. A partir de ahí, las entidades pueden utilizar las credenciales obtenidas en todos los SP a los que desean acceder. Sin embargo, el punto débil del método centralizado reside en que el IdSP tiene un control absoluto sobre la información de sus entidades y puede utilizar su información de la forma que desee. Esta es la principal razón por la cual el método centralizado no ha sido ampliamente adoptado.

Para resolver los problemas derivados del método centralizado, se introdujo el método de identidad federada que se basa en la distribución de la labor de autentificación entre varios IdSP. Estos IdSP pertenecen a distintos dominios. El concepto de identidad federada reside en las relaciones de confianza establecidas entre múltiples IdSP y los dominios correspondientes. Para conectar entre un IdSP y un SP la información de identidad distribuida debe existir una relación de confianza entre ambas partes. Esta relación de confianza se denomina círculo de confianza (CoT) y puede estar constituido por uno o más IdSP y SP. Si un usuario es autentificado por un IdSP en un CoT, se permite el acceso a los SP dentro del CoT sin proceder a más autentificaciones. Así, el usuario únicamente debe autentificarse una sola vez en un CoT [UIT-T X.1251].

La IdM federada es un enfoque ideado para resolver el riesgo de que sólo exista un IdSP y reducir el intercambio de información con el IdSP durante la autentificación. Los acuerdos entre los IdSP garantizan que las identidades emitidas en un dominio son reconocidas por los SP en otros dominios y que puede aplicarse el concepto de SSO aun cuando participen diferentes dominios.

La ventaja para los SP de la identidad federada es que pueden manejar un volumen más reducido de información sobre entidades. La Iniciativa Kantara [b-Kantara], Shibboleth [b-Shibboleth] y Higgins [b-Higgins] utilizan el método de IdM federada. En este tipo de métodos de identidad, las identidades se distribuyen entre los diferentes IdSP, y la información sobre entidades se encuentra disponible para todas las terceras partes (IdSP) de la federación.

7 Arquitecturas y flujos para métodos de agregación de atributos

En los primeros estudios destinados a fusionar atributos de múltiples autoridades de atributos se asumía que la entidad debía tener un único identificador global, común a todas las autoridades de atributos. En realidad, las entidades no tienen identificadores globales, sino que cuentan con diferentes identificadores de entidad y atributos asignados por sus distintos IdSP.

La Liberty Alliance [b-Liberty], luego sustituida por la Iniciativa Kantara, fue el primer grupo en ocuparse del problema de agregación de atributos a través de su concepto de federación de identidad [b-Chadwick]. Sin embargo, uno de los problemas que queda por resolver es la falta de un

planteamiento normalizado de agregación de atributos de la entidad, reconocidos por múltiples autoridades a fin de que un SP pueda utilizarlos en sus decisiones sobre el control de acceso.

A continuación, se presentan dos casos de uso que ayudan a justificar la necesidad de la agregación de atributos:

– Si una tienda de libros electrónicos prevé una venta dirigida a personas mayores, la tienda debe recibir el conjunto agregado de atributos (información de la tarjeta de crédito y prueba de mayoría de edad) de varios IdSP. En este ejemplo, una entidad debe proporcionar atributos a partir de dos identidades.

– Si un investigador desea comprar una computadora utilizando una cuenta de banco federada en una tienda en línea que ofrece descuentos al sector educativo, el investigador debe probar que es miembro de una organización educativa y que posee una cuenta en su banco. Deben recopilarse atributos almacenados asociados a varias identidades y el resultado debe ser transmitido a un SP en un proceso conocido como agregación de atributos [b-Klingenstein].

La utilización compartida y coordinada de recursos dentro de comunidades dinámicas y multiinstitucionales es fundamental para un número creciente de aplicaciones informáticas, desde colaboraciones científicas hasta la atención sanitaria. Es necesario que ese intercambio de información sea estrictamente controlado. Los proveedores de recursos y los consumidores deben definir clara y cuidadosamente qué es lo que se ha de compartir, quién tiene permiso para compartir, y cuáles son las condiciones del intercambio. El conjunto de individuos o instituciones definido por esas reglas de intercambio forman lo que se denomina una colaboración virtual (VC). No resulta sencillo proporcionar habilidades de autogestión para que las VC puedan crear y gestionar fácilmente las membresías y las funciones de sus propios grupos, así como los controles de acceso a sus propios recursos, sobre todo cuando los recursos compartidos se alojan en varias instituciones. En un caso de VC, el IdSP federado generalmente no puede facilitar todos los atributos relevantes para los SP participantes. Estos atributos relacionados con la VC, como la condición de miembro, la lista de difusión de miembros, etc. deben ser agregados a partir de otras fuentes. En la gestión de atributos de los usuarios deben participar diversas autoridades de atributos [b-Hulsebosch].

Existen varios métodos de federación de identidad: el lenguaje de marcación de aserción de seguridad (SAML), Shibboleth [b-Shibboleth], la federación de servicios Web [b-WS-Federation], la iniciativa Kantara [b-Kantara], la identidad abierta (OpenID), la autentificación abierta (OAuth), CardSpace [b-CardSpace], el proyecto Higgins [b-Higgins], entre otros. Según quién se encargue de la mediación en todo el proceso, el método de agregación de atributos puede ser clasificado en tres categorías: métodos con mediación a cargo del IdSP, métodos con mediación a cargo del SP y métodos con mediación a cargo de la entidad.

7.1 Métodos con mediación a cargo del proveedor de servicios de identidad

7.1.1 Identidad por enlace

El método, creado en el marco de la Liberty Alliance, ha sido uno de los primeros en abordar el problema de la agregación de atributos a través del concepto de federación de identidad, véase la Figura 1[b-Liberty]. En dicha figura, los IdSP permiten que la entidad cree un enlace entre pares (CoT3) entre dos IdSP. Cuando una entidad cambia de servicio, el primer IdSP (IdSP1 en la Figura 1) pregunta a la entidad si desea federar ese IdSP (IdSP1) con otro IdSP (IdSP2). A partir de entonces, ambos IdSP interactuarán entre sí para crear un indicador de enlace. Al acceder a los servicios de un SP, el IdSP proporciona ese indicador de enlace al SP junto con las aserciones que contienen atributos. El SP puede utilizar el indicador para recuperar de otro IdSP otras aserciones con atributos. Al combinar los atributos procedentes de ambos IdSP, el SP puede determinar si la entidad puede acceder a un servicio.

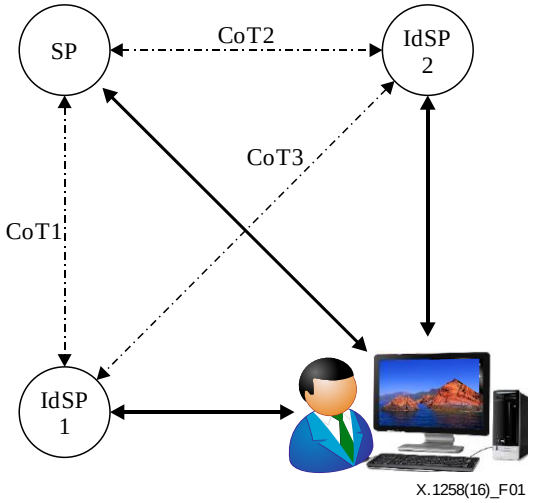

Figura 1 – Arquitectura del método de identidad por enlace

La Figura 2 muestra un flujo de control conceptual de la agregación de atributos mediante el método de identidad por enlace:

1) La entidad envía una solicitud de servicio al SP.

2) Cuando el SP necesita un permiso de servicio de la entidad, envía una solicitud de autentificación y de aserción de autentificación.

3) La entidad es redirigida al IdSP 1 para autentificación.

4) El IdSP 1 autentifica la entidad y solicita más atributos.

5) El IdSP 1 devuelve la aserción de autentificación.

6) La entidad presenta la aserción de autentificación al SP.

7) El SP solicita más atributos relacionados con la entidad al IdSP2.

8) El IdSP2 proporciona los atributos adicionales.

9) El SP verifica las aserciones y permite a la entidad el acceso al servicio.

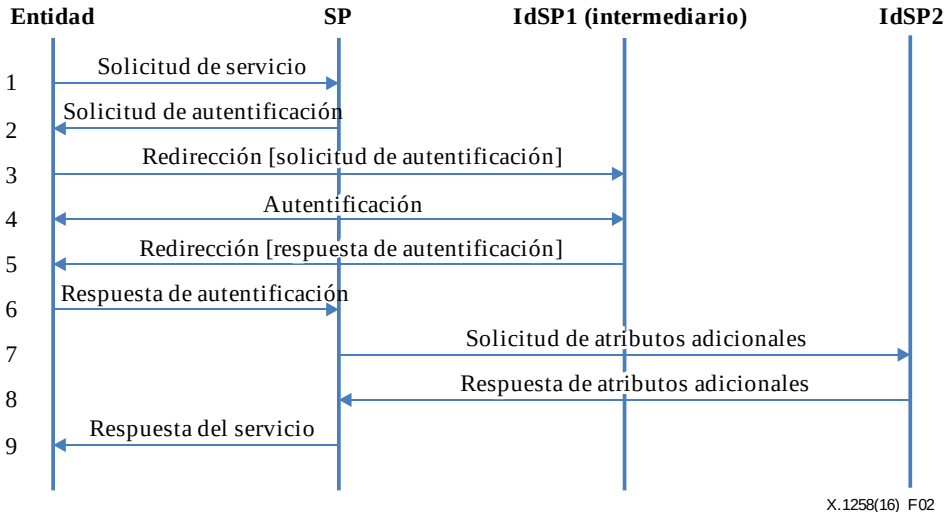

Figura 2 – Flujo de agregación de atributos por el método de identidad por enlace

7.1.2 Identidad por intermediación

Existe un IdSP que actúa como intermediario con el que un SP tiene una conexión que es plenamente digna de su confianza; otros IdSP desconocen al SP y solamente mantienen una relación de confianza

con el IdSP intermediario (IdSP1), véase la Figura 3 [b-Klingenstein]. Si la entidad desea agregar atributos a partir de varios IdSP, en primer lugar la entidad es redirigida al IdSP intermediario (IdSP1 en la Figura 3), y el IdSP intermediario la redirige nuevamente hacia otros IdSP. Una vez que cada IdSP autentifica a la entidad, la entidad devuelve una aserción al IdSP intermediario. Tras ello, el IdSP intermediario verifica cada aserción, recupera atributos de los IdSP y agrega todos esos atributos. El IdSP intermediario puede completar el conjunto agregado con sus propios atributos de la entidad y reafirmar las aserciones. Luego, el IdSP intermediario envía todas las aserciones de atributos reafirmadas al SP. De esta manera, el SP determina si la entidad puede acceder al servicio en base a los atributos agregados. Puesto que el SP no conoce la existencia de los demás IdSP, pues sólo tiene relación con el IdSP intermediario, supone que todos los atributos provienen del IdSP intermediario.

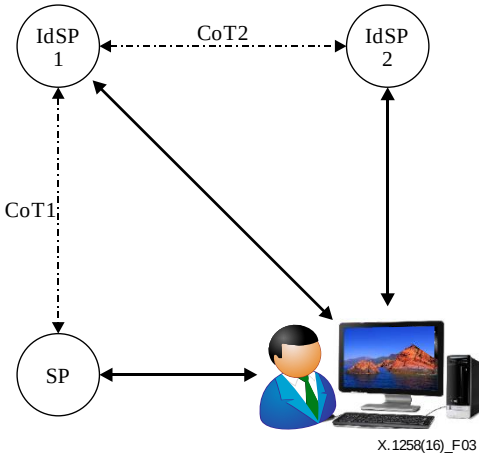

Figura 3 – Arquitectura del método de identidad por intermediación

La Figura 4 muestra un flujo de control conceptual de la agregación de atributos mediante el método identidad por intermediación:

1) La entidad envía una solicitud de servicio al SP.
2) Cuando el SP necesita un permiso de servicio de la entidad, envía una solicitud de autentificación y de aserción de autentificación.
3) La entidad es redirigida al IdSP 1 (que actúa como intermediario) para autentificación.
4) El IdSP 1 redirige a la entidad hacia el IdSP 2.
5) El IdSP 2 recibe una solicitud de autentificación y de atributos.
6) El IdSP 2 autentifica la entidad.
7) El IdSP 2 devuelve los resultados de la autentificación y las aserciones de atributos.
8) La entidad reenvía los resultados de la autentificación y las aserciones de atributos al IdSP 1.
9) El IdSP 1 añade atributos adicionales, firma las aserciones y las devuelve a la entidad.
10) La entidad presenta las aserciones al SP.
11) El SP verifica las aserciones y permite a la entidad el acceso al servicio.

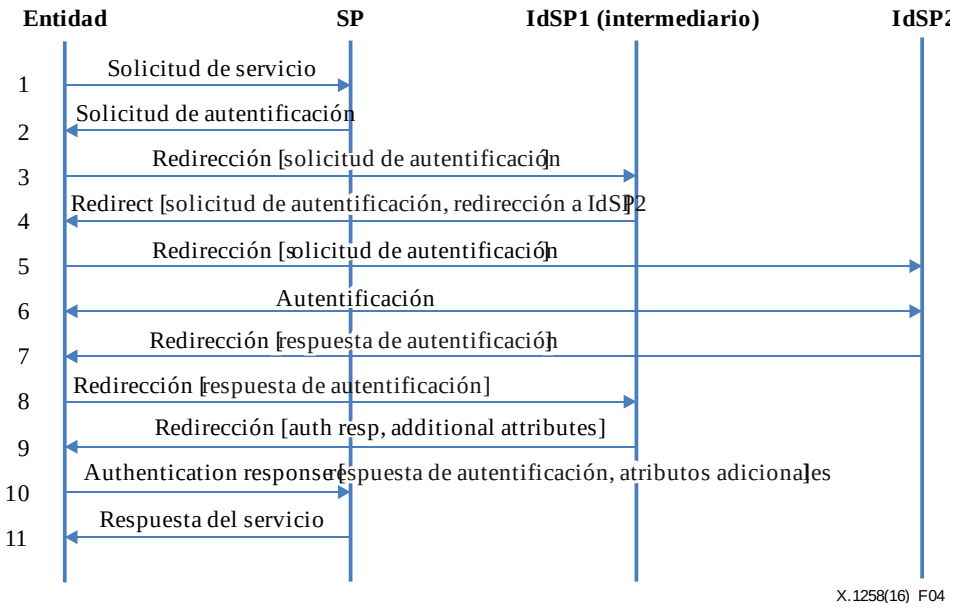

Figura 4 – Flujo de agregación de atributos por el método de identidad por intermediación

7.1.3 Identidad por sustitución

El método de identidad por sustitución es similar al método por intermediación, pero sin que se necesite un sólido vínculo de confianza entre el SP y un IdSP intermediario. Aunque el método por intermediación exige que el SP confíe plenamente en el IdSP, en realidad esta total confianza entre el SP y el IdSP intermediario puede ser imposible. En el método de identidad por sustitución, un IdSP con funciones de mediación (o IdSP sustituto), (IdSP1 en la Figura 5) puede actuar como un IdSP intermediario. A partir de ahí, el flujo es similar al del método por intermediación, en primer lugar, se redirige a la entidad hacia el IdSP sustituto, y éste luego redirige a la entidad hacia otros IdSP. Una vez que la entidad es autentificada individualmente por cada IdSP, la entidad devuelve una aserción al IdSP sustituto. Entonces, el IdSP sustituto combina todas las aserciones en una única aserción y las envía al SP. La diferencia entre ambos métodos reside en la firma de las aserciones de atributos. En el método de identidad por sustitución, el IdSP sustituto no firma las aserciones de atributos. Simplemente transmite las aserciones firmadas por el IdSP de origen. Así, el SP recibe las aserciones de atributos encriptadas desde los IdSP y el IdSP sustituto, y determina si la entidad puede acceder al servicio en base a los atributos agregados. Este método requiere una relación de confianza entre los IdSP y el SP.

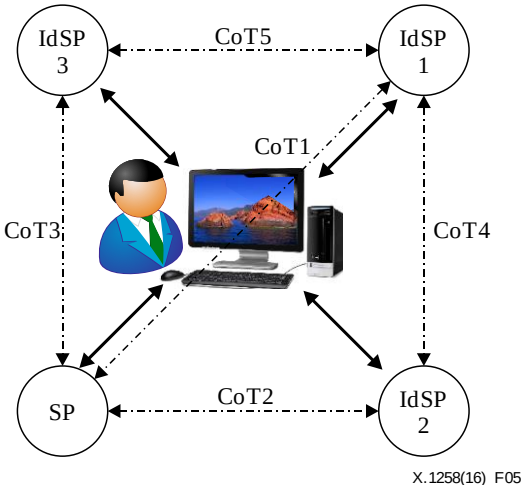

Figura 5 – Arquitectura del método de identidad por sustitución

La Figura 6 muestra un flujo de control conceptual de la agregación de atributos mediante el método identidad por sustitución:

1) La entidad envía una solicitud de servicio al SP.

2) Cuando el SP necesita un permiso de servicio de la entidad, éste envía una solicitud de autentificación y de aserción de autentificación.

3) La entidad es redirigida al IdSP 1 (que actúa como sustituto) para autentificación.

4) El IdSP 1 redirige a la entidad hacia el IdSP 2.

5) El IdSP 2 recibe la solicitud de autentificación y de atributo.

6) El IdSP 2 autentifica la entidad.

7) El IdSP 2 devuelve los resultados de la autentificación y las aserciones de atributos.

8) La entidad reenvía los resultados de la autentificación y las aserciones de atributos al IdSP 1.

9) El IdSP 1 añade atributos adicionales, firma las aserciones y las devuelve a la entidad.

10) La entidad presenta las aserciones al SP.

11) El SP verifica las aserciones y permite a la entidad el acceso al servicio.

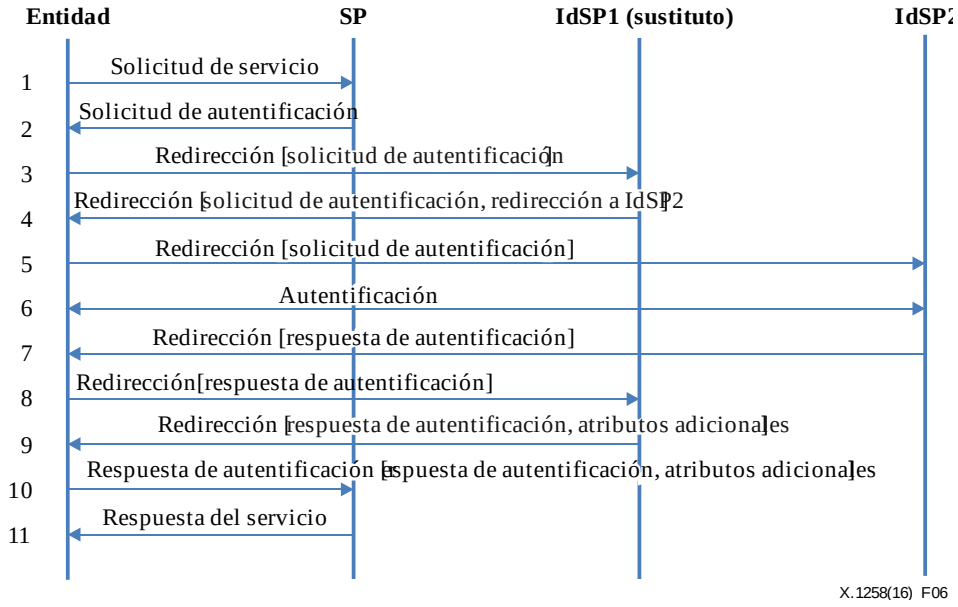

Figura 6 – Flujo de agregación de atributos por el método de identidad por sustitución

7.2 Métodos con mediación a cargo del proveedor de servicios

7.2.1 Base de datos de aplicación

El método de base de datos (DB) de aplicación es el más sencillo de los métodos de agregación de atributos, véase la Figura 7 [b-Hulsebosch]. El SP mantiene atributos adicionales de la entidad, como sobrenombres, preferencias de la entidad para un servicio en particular y pertenencia a determinados grupos, entre otras cosas, además de atributos proporcionados por el IdSP. El SP gestiona los atributos añadidos para las diferentes aplicaciones. Además, dichos atributos de su DB pueden ser recuperados posteriormente por el SP para determinar si la entidad puede acceder a un servicio en particular.

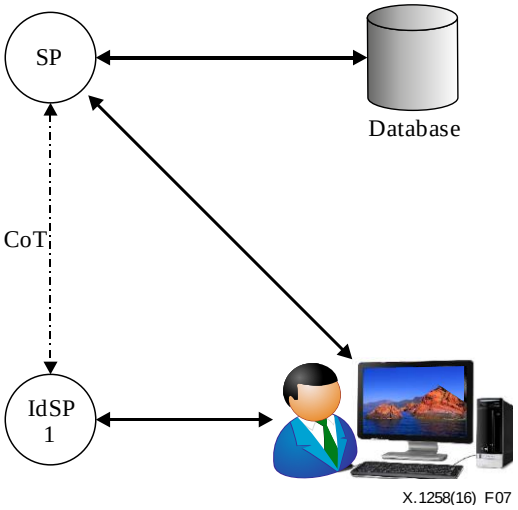

Figura 7 – Arquitectura del método de base de datos de aplicación

La Figura 8 muestra un flujo de control conceptual de la agregación de atributos mediante la base de datos de aplicación:

1) La entidad envía una solicitud de servicio al SP.

2) Cuando el SP necesita el permiso de servicio de la entidad, envía una solicitud de autentificación y de aserción de autentificación.

3) La entidad es redirigida al IdSP 1 para autentificación.

4) El IdSP 1 autentifica la entidad.

5) Una vez realizada la autentificación, el IdSP 1 devuelve el resultado de autentificación y la aserción.

6) La entidad presenta la aserción de autentificación al SP.

7) El SP recupera de su DB atributos adicionales de la entidad, de ser necesario.

8) El SP verifica la aserción o aserciones y permite a la entidad el acceso al servicio.

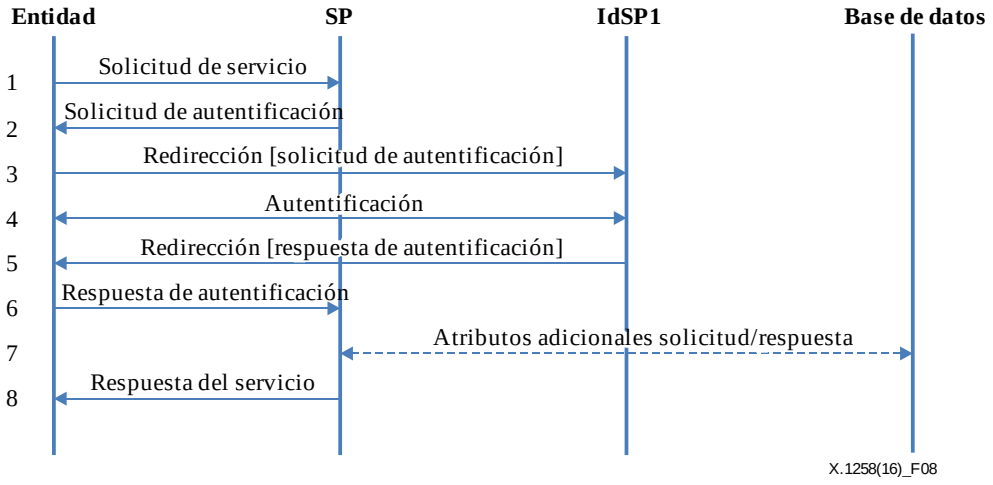

Figura 8 – Flujo de agregación de atributos por el método de base de datos de aplicación

7.2.2 Proveedor de servicios

El método del proveedor de servicios (SP) permite que la entidad agregue atributos a partir de múltiples IdSP en una única sesión, véase la Figura 9 [b- Hulsebosch]. La entidad es redirigida a diferentes IdSP, uno tras otro, donde la entidad es autentificada, y que devuelven una aserción de

atributos al SP. El SP agrega las aserciones de atributos de los IdSP y determina si la entidad puede acceder a un determinado servicio.

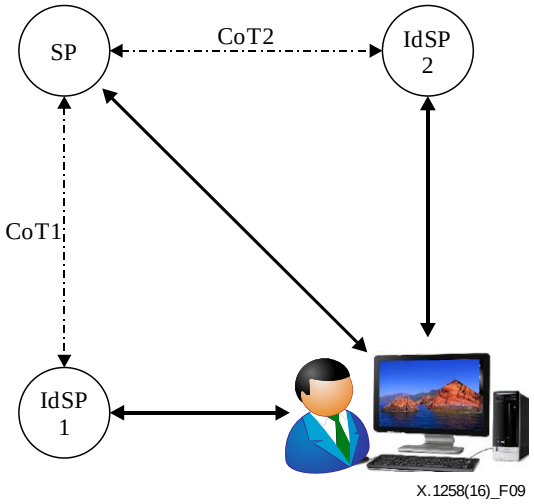

Figura 9 – Arquitectura del método del SP

La Figura 10 muestra un flujo de control conceptual de la agregación de atributos mediante el método del SP.

1) La entidad envía una solicitud de servicio al SP.
2) Cuando el SP necesita el permiso de servicio de la entidad, éste envía una solicitud de autentificación y de aserción de autentificación.
3) La entidad es redirigida al IdSP 1 para autentificación.
4) El IdSP 1 autentifica la entidad.
5) El IdSP 1 devuelve el resultado de la autentificación y la aserción.
6) La entidad presenta una aserción de autentificación al SP.
7) El SP solicita a la entidad más atributos relacionados con la entidad.
8) La entidad envía más solicitudes de atributos al IdSP 2.
9) El IdSP 2 autentifica la entidad.
10) El IdSP 2 proporciona los atributos adicionales.
11) La entidad presenta las aserciones de autentificación al SP.
12) El SP verifica las aserciones y permite a la entidad el acceso al servicio.

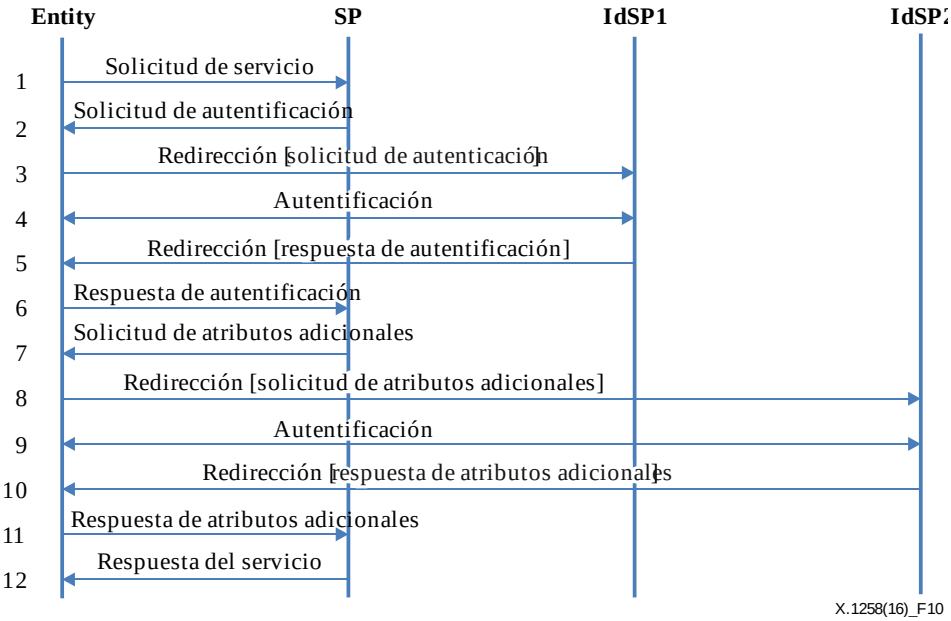

Figura 10 – Flujo de agregación de atributos por el método del SP

7.2.3 Servicio de enlace

El método de servicio de enlace (LS) es una combinación del método de identidad por enlace y del método de identidad por sustitución. El LS es un tipo especial de SP, véase la Figura 11, utilizado por una entidad que utilice un identificador proporcionado por un LS [b-Chadwick], [b-Hulsebosch]. El identificador proporcionado por el LS se utiliza para conectar diferentes IdSP a través de identificadores invariables proporcionados por el IdSP y específicos del LS, en la denominada tabla de enlaces. Si una entidad desea acceder a un servicio, contacta con un SP y es redirigida al primer IdSP (IdSP1 en la Figura 11). El IdSP1 autentifica la entidad, y a continuación devuelve al SP a través de la entidad una aserción con atributos de la entidad y el identificador para el LS. El SP reenvía el identificador al LS para obtener más atributos. En ese momento, existen dos posibilidades: el LS puede recuperar la lista de los IdSP conectados para ese identificador invariable mediante la tabla de enlaces y recuperar los atributos de cada uno de ellos, que se combinan en el LS y se devuelven al SP, o bien, el LS puede mandar de vuelta la lista de los IdSP conectados al SP. Luego, el SP recupera los atributos de cada IdSP. Finalmente, el SP determina si la entidad puede acceder el servicio en base a los atributos agregados.

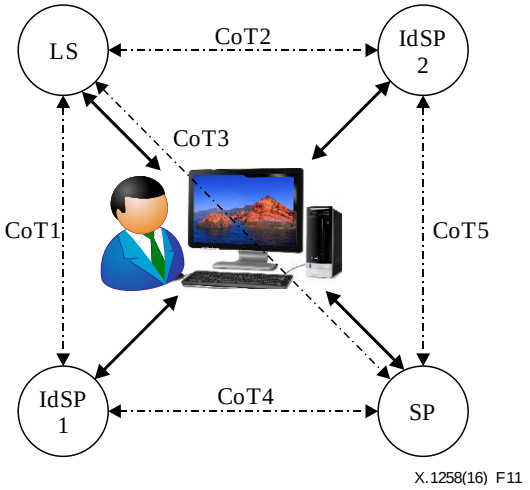

Figura 11 – Arquitectura del método de servicio de enlace (LS)

La Figura 12 muestra un flujo de control conceptual de agregación de atributos mediante el LS:

1) La entidad envía una solicitud de servicio al SP.

2) Cuando el SP necesita el permiso de servicio de la entidad, éste envía una solicitud de autentificación y de aserción de autentificación.

3) La entidad es redirigida al IdSP 1.

4) El IdSP 1 autentifica la entidad.

5) El IdSP 1 devuelve una aserción de autentificación y el identificador para el LS.

6) La entidad envía al SP la aserción y el identificador para el LS.

7) El SP envía nuevas solicitudes de atributos a la entidad.

8) La entidad es redirigida al LS.

9) El LS solicita atributos al IdSP 2.

10) El IdSP 2 proporciona los atributos.

11) Se devuelven los atributos a la entidad.

12) La entidad presenta la aserción o aserciones de autentificación al SP.

13) El SP verifica las aserciones y permite a la entidad el acceso al servicio.

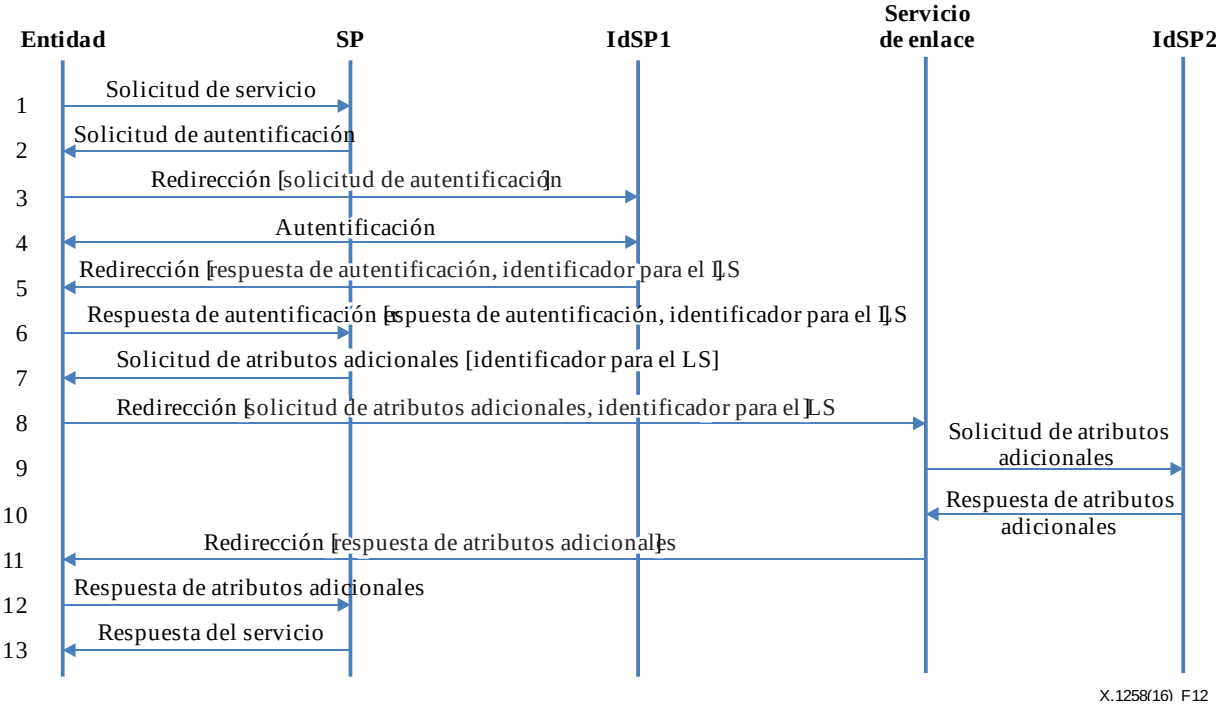

Figura 12 – Flujo de agregación de atributos por el método LS

7.3 Método con mediación a cargo de la entidad

El método de mediación a cargo de la entidad utiliza un cliente (entidad agente o aplicación) que tiene la capacidad de agregar atributos de diferentes IdSP, véase la Figura 13 [b-Klingenstein], y [b-Hulsebosch]. El SP informa al cliente sobre la lista de IdSP dignos de confianza. El cliente redirige a la entidad a cada uno de estos IdSP. Tras la respectiva autentificación de cada IdSP, el cliente recibe aserciones de todos los IdSP y presenta el conjunto combinado de aserciones al SP. El SP verifica cada aserción, recupera todos los atributos y finalmente determina si la entidad puede acceder al servicio.

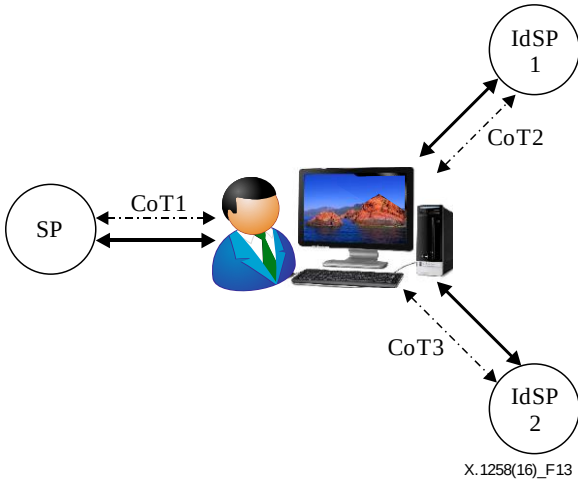

Figura 13 – Arquitectura del método basado en el cliente

La Figura 14 muestra un flujo de control conceptual de agregación de atributos mediante el método basado en el cliente:

1) La entidad envía una solicitud de servicio al SP.

2) Cuando el SP necesita el permiso de servicio de la entidad, envía una solicitud de autentificación y de aserción de autentificación.

3) El IdSP 1 autentifica la entidad.

4) El IdSP 1 devuelve la aserción de autentificación.

5) La entidad es redirigida al IdSP 2 para más aserciones de atributos.

6) El IdSP 2 autentifica la entidad.

7) El IdSP 2 devuelve las aserciones de atributos.

8) La entidad envía la aserción o aserciones de autentificación al SP.

9) El SP verifica las aserciones y permite a la entidad el acceso al servicio.

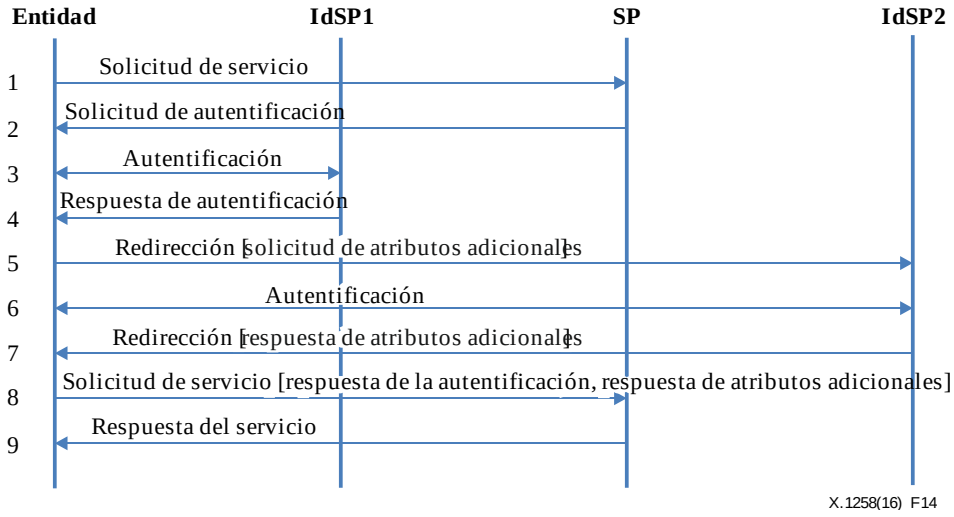

Figura 14 – Flujo de agregación de atributos por el método basado en el cliente

8 Comparación de los métodos de autentificación sobre la base de atributos agregados

Los siete métodos mencionados en la cláusula 7 son nuevas versiones del tradicional sistema de gestión de identidad (IdM) federada. Cada uno de estos métodos posee entidades o interacciones adicionales. Sobre la base de estas modificaciones, se analizan y comparan los siete métodos teniendo en cuenta diversos factores a fin de seleccionar un método de agregación apropiado. El diseñador y el desarrollador deben tener en cuenta cuestiones tales como: quién media, agrega o verifica los atributos, la dificultad de aplicación o la adición de nuevos elementos.

La cláusula 7 presenta varios métodos basados en SAML para la agregación de atributos. Estos métodos pueden ser interoperables habida cuenta de cómo se expresan en SAML.

Los métodos de agregación se analizan con respecto a la mediación para la agregación, la ejecución de la agregación y el elemento adicional. En el Cuadro 1 se comparan los métodos de agregación de atributos.

En dicho cuadro, el símbolo "✓" en las celdas intersección de columnas y filas indica que el método de agregación de la fila posee la capacidad de la columna. Más precisamente, la aplicación del método marcado debe soportar la capacidad marcada.

Cuadro 1 – Comparación de métodos de agregación

Método de agregación	**Capacidad**						
	Mediación a cargo	**Mediación a cargo**	**Mediación a cargo**	**Agregación a cargo**	**Agregación a cargo**	**Agregación a cargo**	**Elemento adicional**
Identidad por enlace	✓				✓		
Identidad por intermediación	✓			✓			
Identidad por sustitución	✓			✓			
Base de datos de aplicación		✓			✓		DB
Proveedor de servicios		✓			✓		
Servicio de enlace		✓			✓		LS
Cliente			✓			✓	cliente

En relación con el método de identidad por enlace, la mediación de la agregación está a cargo del IdSP y se ejecuta en el SP. Esto significa que el protocolo de agregación de atributos debe ser implementado en el IdSP y el SP. Sin embargo, en otros casos, la mediación y la ejecución de la agregación pueden quedar a cargo del mismo proveedor. Podría ser más fácil para el proveedor realizar la agregación de atributos que aplicar el método de identidad por enlace. Respecto a los elementos adicionales para la agregación de atributos, el método de la base de datos (DB) de aplicación precisa su propia DB; el método del servicio de enlace necesita un servicio de enlace (LS) como un tipo especial de SP; el método de mediación a cargo de la entidad, necesita un cliente como agente. Sobre la base de estos criterios, el método de mediación por intermediario y el método de identidad por sustitución son los métodos recomendados en el marco de la mediación a cargo del IdSP, y el método del SP es el recomendado en el marco de la mediación a cargo del SP.

Bibliografía

[b-UIT-T X.500] Recomendación UIT-T X.500 (2016) | ISO/CEI 9594-1:2017, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Visión de conjunto de conceptos, modelos y servicios.*

[b-UIT-T X.509] Recomendación UIT-T X.509 (2016) | ISO/CEI 9594-8:2017, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos.*

[b-UIT-T X.1251] Recomendación UIT-T X.1251 (2009), *Marco para el control de la identidad digital por el usuario.*

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

[b-CardSpace] *Introducing windows cardspace*. Artículos técnicos de MSDN, Microsoft Corporation. Disponible (constatado el 19-12-2016) en: http://msdn.microsoft.com/en-us/library/aa480189.aspx

[b-Chadwick] Chadwick, D.W. e Inman, G. (mayo de 2009), Attribute aggregation in federated identity management, *IEEE on Computer*, Vol. 42, No.5, págs. 33-40. <http://doi.ieeecomputersociety.org/10.1109/MC.2009.143>

[b-Higgins] *Proyecto Higgins Disponible* (constatado el 05-12-2016) en: http://www.eclipse.org/higgins/

[b-Hulsebosch] Hulsebosch, Bob, Wegdam, Maarten, Zoetekouw, Bas, van Dijk, Niels, van Wijnen, Poortinga Remco (2012), *Virtual collaboration attribute management*. 41 pp. Disponible (constatado el 05-12-2016) en: https://www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2012/EDS+11-06+Attribute+Management+v1.0.pdf

[b-Kantara] *Iniciativa Kantara*. Disponible (constatado el 19-12-2016) en: https://kantarainitiative.org/reports-recommendations/

[b-Klingenstein] Klingenstein, N. (2007), Attribute Aggregation and Federated Identity, *International Symposium on Applications and the Internet, SAINT Workshops*, p. 26.

[b-Liberty] Especificaciones de la Liberty Alliance, ID-FF 1.2 http://www.projectliberty.org/liberty/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications

[b-OAuth] OAuth. Disponible (constatado el 19-12-2016) en: http://oauth.net/documentation/getting-started/

[b-OpenID] OpenID authentication 2.0. Disponible (constatado el 19-12-2016) en: http://openid.net/specs/openid-authentication-2_0.html

[b-Shibboleth] *Shibboleth, Open Source Project*, Disponible (constatado el 05-12-2016) en: https://shibboleth.net/

[b-WS-Federation] Web Services Federation Language (WS-Federation) Versión 1.2. Disponible (constatado el 19-12-2016) en: http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html

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

Impreso en Suiza
Ginebra,