Aplicación de mecanismos de colaboración entre círculos de confianza Liberty a escenarios de comercio electrónico en la Internet móvil

Juan C. Yelmo[1], Rubén Trapero[1], Jorge Ysart[1], Alejandro Bascuñana[2]

[1]Departamento de Ingeniería de Sistemas Telemáticos, Universidad Politécnica de Madrid.
ETSI de Telecomunicación. Ciudad Universitaria S/N 28040 – Madrid
Telf: 91 336 6830 Fax: 91 336 7333
{jcyelmo, rubentb, coquey}@dit.upm.es

[2] Ericsson España S.A,
Vía del los poblados 13. 28033 Madrid, Spain.
Telf: 91 339 1897 Fax: 91 339 2958
alejandro.bascunana@ericsson.com

Resumen

La identidad se ha convertido en elemento esencial en la relación que existe entre una compañía y sus empleados, clientes o socios. Esto, unido a la tendencia de los operadores a abrir sus redes a otras compañías hace que estén introduciendo tecnologías de gestión de identidades, como Liberty Alliance, en sus plataformas de servicios y ofrecer así unos niveles de privacidad, confianza y seguridad adecuados a sus clientes. Este artículo describe como se ha extendido el protocolo de acceso a recursos de usuarios de Liberty que permite únicamente consulta de atributos, con la incorporación de un nuevo protocolo orientado a acción (Liberty Action Oriented Protocol) que permite desencadenar acciones en otro proveedor donde se encuentra almacenado un perfil de usuario. Éste se ha aplicado a un escenario de comercio electrónico que hace uso de mecanismos de colaboración entre distintos operadores y compañías.

1. Introducción

Los nuevos servicios de Internet móvil están atrayendo cada vez más el interés de las operadoras de telefonía móvil que han visto en ellos una manera de incrementar la facturación media por usuario en un mercado en el que el crecimiento de los ingresos por suscripción de nuevos abonados se ha estancado.

Al desarrollo de estos servicios contribuye un proceso de convergencia tecnológica alrededor del protocolo IP como tecnología de interconexión (ver Fig 1) que está dando lugar a las denominadas redes de siguiente generación. Se trata de una tecnología barata, fácil de gestionar y que favorece la aparición de nuevos modelos de negocio que surgen gracias a la apertura de las redes a terceros proveedores, otros operadores y compañías para ofrecer nuevos y avanzados servicios, así como desarrollar servicios más complejos gracias a la composición de servicios, esto es que un servicio interaccione con otro servicio externo para ofrecer al usuario, de forma transparente, una funcionalidad avanzada o una personalización del servicio [1].

Para llegar a conseguir estos nuevos servicios de valor añadido, los proveedores de servicio deberán acceder a recursos de identidad de los usuarios, que muchas veces pueden estar almacenados fuera del dominio al que pertenece el proveedor. Y es ahí donde surge la necesidad de mantener la seguridad y privacidad de la identidad de los usuarios y donde la gestión de identidades juega un papel esencial para aumentar la confianza de los clientes en estos nuevos servicios.

Este artículo describe cómo se ha extendido una plataforma para la gestión de identidades basada en las especificaciones de *Liberty Alliance*, con un protocolo orientado a acción para poder desencadenar acciones sobre recursos de identidad de usuarios que están almacenados en proveedores de servicios que pertenezcan o no su mismo dominio de confianza. Para demostrar esto se ha creado un escenario, que además hace uso de los modelos de colaboración entre dominios de confianza desarrollados en un trabajo anterior [2], y que permite demostrar cómo se puede construir un servicio de comercio electrónico componiendo servicios presentes en distintos dominios y que hacen uso de este nuevo protocolo para desencadenar transacciones sobre recursos de banca de usuarios.

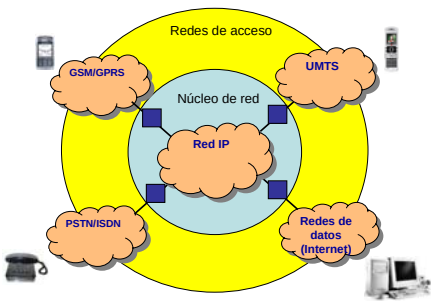

Fig 1 Redes de siguiente generación

La siguiente sección introduce la gestión de identidades mientras que la aplicación de esta a los servicios Web móviles se muestra en el tercer apartado. El apartado 4 describe la problemática del acceso a recursos de identidad y cómo se ha extendido *Liberty Alliance* para poder realizar acciones sobre estos recursos. Todo esto se ha aplicado a un escenario de validación que se describe en el apartado 5.

2. Gestión de identidades

La identidad se ha convertido en el núcleo de la relación de una empresa con sus clientes, empleados y socios. La gestión segura de esas identidades es crítica, y además incrementa la eficiencia en las actividades de la empresa, aumenta la seguridad y supone una apertura a nuevas fuentes de ingresos. Ésta es la razón por la que la gestión de identidades se está convirtiendo en un problema crítico al permitir el acceso a recursos presentes en múltiples dominios de seguridad. De los múltiples aspectos que tiene la identidad, aquí nos referimos a la identidad de red, entendida esta como un conjunto de datos a cerca de un sujeto, y que consta de atributos y preferencias de usuario en todas las cuentas que éste puede tener abiertas en la red. Hoy en día, es típico tener estas colecciones de datos repartidas en múltiples sitios de Internet, donde se ofrecen servicios sin cohesión entre entidades y preferencias de usuarios. Esto se traduce en una mala experiencia del usuario y reduce la confianza en los servicios telemáticos.

Se entiende por gestión de identidades la disciplina que trata de la gestión del acceso y gestión de usuarios a recursos de identidad de red distribuidos en sus aspectos técnicos, legales y de negocio. A nivel técnico, la gestión de identidades está relacionada con la seguridad en la red, provisión de servicios, gestión de clientes, acceso y salida transparente de los usuarios usando registro único de entrada y salida (normalmente conocidos como *Single Sign-On* y *Single Logout* respectivamente), vinculación de recursos de identidad distribuidos (federación de identidad) y provisión de servicios Web.

Existen varios estándares y plataformas que soportan esto, siendo el más el importante el *Security Assertion Markup Language* (*SAML*) [3], *Liberty Alliance [4]*, *Shibboleth* [5], y *WS-Federation* [6]. *SAML* es un estándar basado en *XML* definido por *OASIS* y que permite el intercambio de datos de autenticación y autorización entre dominios de seguridad. Tanto *Shibboleth* como *Liberty* tienen sus orígenes en anteriores versiones de SAML y han contribuido a la nueva especificación. Es más que probable que ambas tecnologías converjan en SAML v2. *Shibboleth* está desarrollado y pensado para entornos educativos, de la que hay disponible una plataforma de código abierto que cumple con sus especificaciones, mientras que *Liberty* son simplemente especificaciones pero que están soportadas por una gran parte de la industria de las telecomunicaciones. Existen no obstante, implementaciones de código abierto de algunas de las partes de *Liberty* [7], pero por el momento, no directamente ofrecidas por el consorcio. Por otro lado, *WS-Federation* está apoyado únicamente por IBM y por otras cuatro compañías de software.

Desde el punto de vista de escalabilidad, *Shibboleth* está pensado para gestionar pocas federaciones, mientras que *Liberty* está pensado para trabajar en un entorno de cientos de miles de usuarios, por tanto, es más adecuado para la industria de las telecomunicaciones en general, y para los servicios móviles en particular. Además, está apoyada por más de 170 compañías, organizaciones sin ánimo de lucro, y organizaciones gubernamentales, siendo la especificación de facto para los principales operadores móviles.

En el enfoque propuesto por *Liberty*, los proveedores de servicios se asocian en dominios de confianza llamados *Círculos de Confianza* (CoT) (ver Fig 2) que están soportados por la tecnología *Liberty* y por acuerdos de negocio en los que se definen relaciones de confianza y políticas comunes entre proveedores. Dentro de un círculo de confianza los usuarios pueden vincular (federar) sus cuentas aisladas en diferentes proveedores de servicios (SP). A esos proveedores de servicios que están especialmente preparados para identificar y autenticar a los usuarios y gestionar sus federaciones con otros proveedores de servicios se les llama Proveedores de Identidad (IdP). Un ejemplo típico es el de una compañía aérea que hace de IdP y las diferentes compañías (SPs) asociadas a su programa de fidelización.

Liberty propone el diseño de un conjunto de arquitecturas y protocolos distribuidos en tres fases:

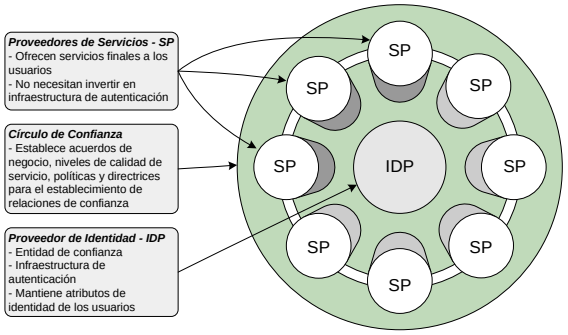

Fig 2 Círculo de confianza Liberty

- Fase 1 – *Identity Federation Framework* (*ID-FF*). Se definen protocolos para la federación de cuentas de usuarios, para realizar *Single Sign On* y *Single Logout*, y para realizar cambios en los pseudónimos establecimos en una federación (*Name Registration*).

- Fase 2 – *Identity Web Services Framework* (*ID-WSF*). Una plataforma basada en Web Services para desarrollar servicios de identidad, como descripción y descubrimiento de servicios, autenticación, acceso a atributos compartidos, interacción con el usuario para obtener permisos de acceso a recursos etc.

- Fase 3 – *Identity Services Interface Spefications* (*ID-SIS*). Se definen servicios específicos basados en identidad que hacen uso de la plataforma definida en *ID-WSF*. Algunos de los perfiles ya definidos son un perfil personal, perfil de empleado, agenda de contactos, perfil de presencia, localización …

3. Servicios Web móviles basados en Identidad

Una de las consecuencias del proceso de convergencia tecnológica introducido antes es que los operadores están ofreciendo interfaces abiertos a terceros proveedores para intentar así conseguir más oportunidades de negocio. El ofrecer productos tanto fijos como móviles ayuda a unificar los dominios, permitiendo a los usuarios acceder a servicios desde cualquier red o dispositivo. Esta es una de las razones por la que los operadores están implementando soluciones de gestión de identidades, no solo para ofrecer a los usuarios una experiencia de usuario mejorada, sino también para incrementar la seguridad y privacidad de los servicios.

El uso de tecnologías de gestión de identidades como *Liberty Alliance* beneficia no solo a los usuarios, sino también a los operadores o a los desarrolladores:

- El acceso a servicios es automático gracias al *Single Sign-On*, el descubrimiento y la invocación de servicios y la autenticación, que permite acceso transparente a aplicaciones.

- Se pueden añadir fácilmente nuevos proveedores de servicio a la plataforma de servicios del operador.

- Con un enfoque orientado a servicio como el que tiene *Liberty*, los desarrolladores lo tienen fácil para crear nuevos servicios, gracias al uso de APIs estándar, lo cual reduce el coste de implementar intercambios de información de autenticación, de descubrimiento e invocaciones de servicios [8].

- La interoperabilidad entre operadores y dominios ayuda al desarrollo de servicios de valor añadido, generando así nuevas oportunidades para incrementar los ingresos [9].

Por tanto, parece que ésta es la solución a los problemas que tienen operadores móviles cuando pretenden abrir sus redes a terceros proveedores. Sin embargo, la apertura de sus interfaces a estos proveedores y el modo de integrar una solución basada en *Liberty* a este enfoque es distinta en función del tipo de integración o colaboración que haya. En [10] se analiza esto, y se distinguen tres enfoques para dicha integración (ver Fig 3):

- El primer enfoque es similar al modelo *semi walled-garden* [11], en el que un cliente puede tener acceso transparente a muchos servicios, ya sean estos ofrecidos por el propio operador desde su red privada, u ofrecido por terceros proveedores desde redes externas a las del operador. El problema aquí surge por que el entorno de provisión de servicios del operador es cerrado, así como los servicios de autenticación, los protocolos de seguridad etc. No en vano, los operadores son los que tienen la información acerca de la identidad de los usuarios. Extender la oferta de servicios del operador con servicios externos es por tanto caro, lento y demasiado complejo. A esto hay que añadir que los desarrolladores de servicios son reacios a incorporar los protocolos y requisitos de seguridad impuestos por los operadores. Sin embargo, el círculo de confianza propuesto por *Liberty* encuadra perfectamente en este enfoque, y permite solucionar los problemas expuestos antes. En este caso, el operador será el IdP, mientras que los SP serán tanto los servicios propios del operador como los de los terceros proveedores, sin distinciones entre ellos. La tecnología *Liberty* se encarga de posibilitar el acceso transparente de los usuarios a los servicios y de proteger la identidad de los mismos.

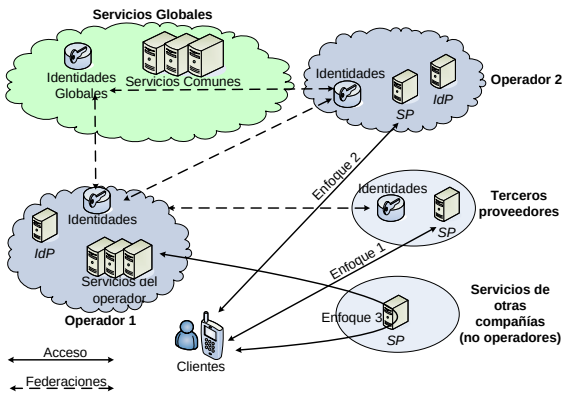

Fig 3 Distintos enfoques para la extensión de los operadores con nuevos servicios

- El segundo enfoque está basado en el anterior, salvo que este caso, el objetivo es ser capaz de ofrecer o tener disponibles servicios proporcionados no solo por terceros proveedores, sino por otros operadores móviles. Así por ejemplo, varios operadores pueden compartir infraestructuras y así reducir costes. Por ejemplo, un proveedor de ADSL se podría beneficiar de un servicio de localización proporcionado por un operador móvil para ofrecer servicios que dependan de la posición del usuario. Un caso especial es cuando los operadores están activos en más de un país. Esto crea nichos de identidades en cada país, lo que dificulta la implantación de servicios basados en identidad. Una solución aquí sería el tener un conjunto de servicios globales, disponibles para todos los usuarios de todos los países donde el operador está presente, y un conjunto de identidades federadas con las identidades presentes en cada país, de modo que la identidad principal se encuentre en el país origen.

- El último enfoque considera la colaboración entre operadores y otras compañías que pueden no ser necesariamente operadores, sino que pueden ser bancos, compañías eléctricas etc. El uso de *Liberty ID-WSF* ofrece seguridad, e integridad de la identidad de los usuarios, con independencia del dispositivo y método de acceso usado.

En nuestro caso, hemos utilizado una mezcla de los tres enfoques para demostrar cómo un servicio puede componerse de otros servicios ofrecidos en otros círculos de confianza, ya sean estos operadores (como el segundo enfoque anterior) o compañías (como en el tercer enfoque) que colaboran entre sí para ofrecer servicios de comercio electrónico en Internet móvil. Los mecanismos de colaboración utilizados son frutos de un trabajo anterior [2], en donde se establecieron las pautas para que los usuarios puedan acceder a servicios ofrecidos en círculos de confianza donde no tienen cuenta (por ejemplo, en situaciones de roaming) y cómo acceder a recursos de identidad presentes en otros círculos de confianza donde el usuario tiene disponible un recurso, en forma de perfil personal, perfil bancario etc.

4. Acceso a recursos de identidad

La apertura de las plataformas de servicios de los operadores a terceros proveedores o la creación de interfaces abiertas con otros operadores y compañías favorece la creación de servicios avanzados, que se componen y comunican entre sí para ofrecer una mejor experiencia de usuario, ofreciendo servicios de valor añadido imposibles de llevar a cabo sin esa colaboración.

Algunas de las características de estos servicios van desde la personalización del servicio adaptándolo a las preferencias personales del usuario o al dispositivo desde el que está accediendo hasta funcionalidades avanzadas, tales como envío automático de productos gracias a la consulta de la dirección del usuario, o compras directas contra la cuenta bancaria del cliente.

Es precisamente en la consulta de esta información donde la gestión de identidades cumple sus objetivos, permitiendo que un proveedor de servicio que, por ejemplo, necesite obtener la dirección postal de un usuario almacenada ésta en otro proveedor de servicio, no conozca verdaderamente quién es el usuario, únicamente la dirección a la que debe enviar el pedido.

En *Liberty*, si uno de los proveedores de servicio que pertenecen a un círculo de confianza de, por ejemplo un operador móvil tiene alguna información almacenada acerca de un usuario (por ejemplo, conoce la dirección postal) esta información puede ser compartida con otros proveedores de servicios, con el consentimiento del usuario naturalmente. Cuando un proveedor de servicio necesita acceder a un recurso determinado de un usuario se le llama *Consumidor de Servicios Web* (*Web Service Consumer, WSC*), mientras que a la entidad que gestiona el recurso se le llama *Proveedor de Servicios Web* (*Web Service Provider, WSP*). El acceso a estos recursos se lleva a cabo usando el protocolo definido en *Liberty ID-WSF* denominado *Data Service Template* (*DST*) [12]. Este protocolo permite no sólo consultar un dato de un usuario, sino también actualizar un perfil, que un WSC se suscriba a ciertos eventos en un WSP cuando ha variado un perfil de un usuario y enviar notificaciones cuando estos eventos ocurren. Sin embargo, este protocolo no está preparado para realizar tareas más complejas sobre un WSP, para, por ejemplo, desencadenar acciones. Es ahí precisamente donde se centra nuestra contribución.

4.1. Protocolo orientado a acción

En un entorno de servicios avanzados sobre redes convergentes, y sobre todo de servicios de Internet móvil, el simple acceso para consulta a recursos de identidad no basta. Por ejemplo, en un escenario de comercio electrónico es necesario desencadenar acciones en un proveedor de medios de pago que se encarga de hacer de intermediario o de interfaz con los sistemas de un banco para hacer efectivo el pago por la compra de un producto. El protocolo *Liberty Data Service Template* está basado en una simple consulta de información. Esto quiere decir que este dato puede ser solicitado o cambiado, pero no en todos los recursos esto es suficiente, y hay servicios donde supone una limitación, dado que puede haber recursos que necesiten de un cierto dato de entrada.

Un ejemplo de un recurso que no puede ser accedido simplemente con una consulta es una cuenta bancaria. Cuando se pretende acceder a una cuenta bancaria o a un servicio de monedero de un usuario, hay ciertos datos de entrada que son necesarios, como la cantidad de dinero que se va a usar o la cuenta destino a la que se va a mover el dinero.

Para solucionar esa carencia hemos creado el protocolo orientado a acción de *Liberty* (*Liberty Action Oriented Protocol, AOP*). En este protocolo se propone un conjunto de definiciones de esquemas de mensajes y reglas de procesamiento que permiten interacciones entre WSC y WSP y que requieren datos de entrada.

El esquema de los diálogos llevados a cabo por las entidades es el mismo que el seguido con el DST: Un SP que actúa como WSC y que necesita acceder a un recurso de un usuario accede al proveedor de servicios de descubrimiento para obtener credenciales e información de dónde y cómo se accede al recurso del usuario. Una vez obtenida esta información, el WSC usa el AOP para desencadenar determinadas acciones en el WSP. Otra característica del AOP es que está basado en la petición de varias acciones simples dentro de una única petición, pudiendo establecerse también precedencia y realizar transacciones.

Tal y como también ocurre con el DST, el AOP debe ser extendido con servicios específicos al igual que se definen perfiles en ID-SIS. Por tanto, es necesario extender el AOP con servicios específicos y definir mensajes adecuados para acceder a sus acciones. La Fig 4 muestra como puede usarse sobre el AOP un servicio de banca y un servicio de mensajería. También se muestra como el AOP se sitúa al mismo nivel que el DST, pero destinado a interaccionar con servicios distintos que los ya definidos en ID-SIS para el DST.

Internamente, el AOP se ha definido como un protocolo de petición-respuesta construido sobre SOAP y HTTP. Los mensajes de petición (*ActionRequest*) contienen un listado de acciones a llevar a cabo en el WSP, y pueden incluir una serie de datos de entrada. En la cabecera del mensaje SOAP que contiene el *ActionRequest* debe incluirse las credenciales necesarias para acceder al WSP, mientras que el cuerpo del mensaje SOAP contiene las peticiones de acción dentro de elementos *Action*. Cada una de ellas consta de un identificador (*ActionID*), un nombre, y opcionalmente, una precedencia en la ejecución a través de los atributos *executeAfter*, *executeAfterSuccess* y *executeAfterFailure* para indicar que dicha acción debe ejecutarse después, después del éxito o después del fallo de la acción cuyo *actionID* se corresponda con el valor de ese atributo.

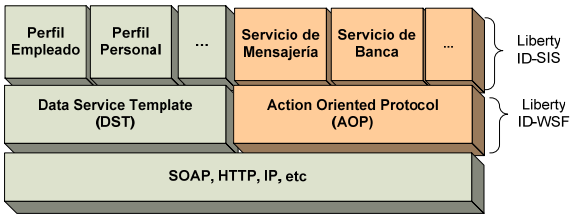

Fig 4 Servicios basados en identidad orientados a acción

Los mensajes de respuesta (*ActionResponse*) contienen el resultado y un mensaje de estado para cada una de las acciones enviadas por el WSC en la petición, así como una referencia al *actionID* que ha desencadenado dicha respuesta.

La Fig 5 muestra los esquemas de ambos mensajes.

5. Escenario de demostración

En esta sección se describe el escenario donde hemos aplicado los diseños y los modelos creados para mostrar cómo distintos operadores móviles y compañías pueden colaborar para ofrecer servicios avanzados a los usuarios y que además permiten desencadenar acciones en proveedores donde hay almacenados recursos de identidad de sus clientes. Además, el escenario está ideado de tal manera que se puede demostrar cómo es compatible con situaciones en las que el usuario no está accediendo desde su red origen, sino desde una red perteneciente a un operador que no conoce nada de él, pero que sin embargo puede usar su identidad de forma segura y privada para acceder a servicios tanto en su red origen como en la visitada.

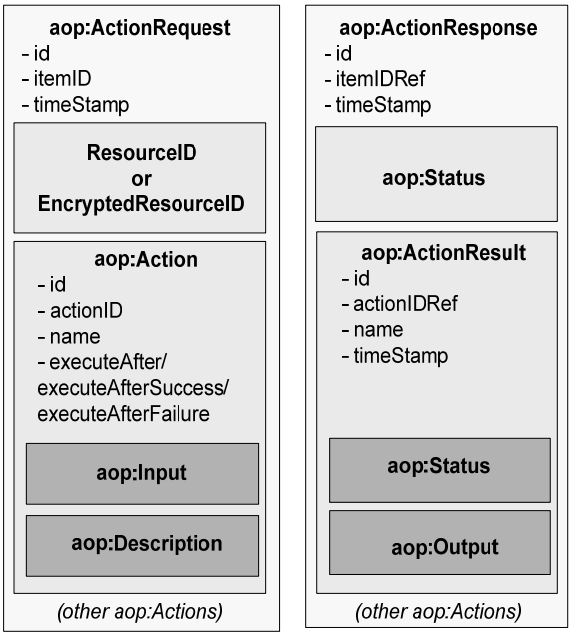

Fig 5 Mensajes del AOP: Petición de acción (izquierda) y respuesta a la petición (derecha)

En concreto, el escenario de simulación consta de tres dominios: *Bluemobile*, *Orangemobile* y *Oxenbank*.

- *Bluemobile* y *Orangemobile* son operadores móviles ficticios los cuales se supone que operan en España y Francia respectivamente

- *Oxenbank* es un banco ficticio que opera a nivel global por todos los países europeos.

Dentro de *Bluemobile* y *Orangemobile* hay una tienda online que proporciona un servicio de venta de entradas de cine para todo el país donde esté operando: *MySearch* es la tienda que pertenece a *Bluemobile* y *Marecherche* es la tienda que pertenece a *Orangemobile*. Estos proveedores de servicio pueden ser tanto servicios propios del operador como un servicio perteneciente a un tercer proveedor. Finalmente, dentro de *Oxenbank* hemos introducido un proveedor de medios de pago, donde los clientes del banco pueden registrar datos como números de tarjetas de crédito por ejemplo, para que puedan ser usados por terceros proveedores. La Fig 6 muestra este escenario.

5.1. Requisitos

El escenario debe de cumplir con varios requisitos previos. Por un lado es necesario suponer que las tres compañías que colaboran para ofrecer servicios de Internet móvil basados en identidad han acordado ciertas condiciones y formalizado sus relaciones. Desde el punto de vista técnico, es necesario que los proveedores de identidad de cada círculos de confianza se conozcan y confíen entre sí. Para ello se supone un intercambio previo de credenciales y otra información descriptiva de las entidades y sus actividades, en forma de ficheros de *metadatos* [13] que contengan perfiles soportados, puntos de acceso etc. En nuestro escenario, suponemos que todas estas condiciones se dan previamente. Por otro lado, se supone que el usuario pertenece a al menos uno de los operadores móviles y por tanto tiene una cuenta y una identidad en él. Además, el usuario es cliente del banco y por tanto tiene otra cuenta e identidad en su IdP. Así mismo, el usuario tendrá una cuenta y habrá registrado un perfil de banca en el proveedor de medios de pago del círculo de confianza del banco. Dicha identidad estará federada con la identidad que tiene en el IdP del banco.

El prototipo que hemos implementado usa una implementación compatible con las especificaciones ID-FF 1.2 y ID-WSF 2.0 proporcionada por Ericsson.

5.2. Implementación

El escenario de la Fig 6 permite representar un servicio de comercio electrónico en donde los usuarios pueden seleccionar entradas en alguna de las tiendas online presentes en los círculos de confianza de los operadores *Bluemobile* y *Orangemobile* y pagarlas usando el proveedor de medios de pago del círculo de confianza del banco. El escenario es aplicable a situaciones de roaming, en las cuales el usuario accede desde un círculo de confianza donde no es conocido. Un ejemplo puede ser la situación en la que un abonado de *Bluemobile* está accediendo desde la red de *Orangemobile* en Francia. Con este modelo, el usuario puede acceder al servicio de compra de entradas de cine online *Marecherche* mientras está en Francia, a pesar de ser un desconocido en la red del operador francés. Dado que hay acuerdos de colaboración entre ambos operadores, el IdP de *Orangemobile* puede reenviar la petición de acceso al IdP de *Bluemobile*, quien autenticará al usuario. Tras esto, *Orangemobile* creará una identidad anónima y temporal en su red, que federará con la identidad del usuario en su red origen.

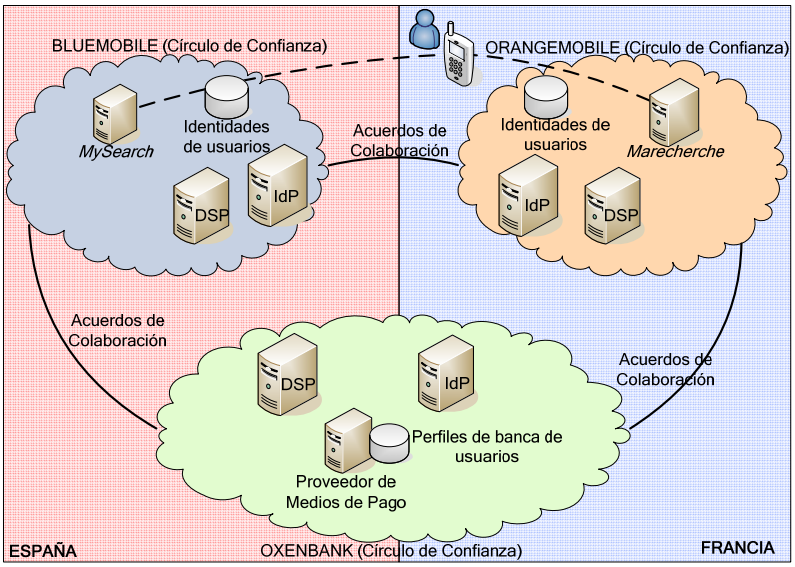

Fig 6 Escenario de demostración

Hasta aquí el usuario tiene acceso al servicio francés, pero además, y gracias no sólo al modelo de colaboración entre círculos de confianza, sino también al protocolo orientado a acción descrito en el apartado 4.1, puede realizar el pago por las entradas adquiridas desde la tienda francesa con su perfil de banca registrado en el proveedor de medios de pago del banco *Oxenbank*, donde el usuario es cliente. Para poder realizar ese pago, el proveedor de medios de pago y la tienda online usan el AOP, lo cual aporta ventajas tanto a ellos como al usuario:

- Permite que la tienda, actuando como *WSC*, pueda realizar varias acciones sobre un mismo perfil a la vez, así como tener control de qué hacer si alguna de estas acciones falla

- Simplifica las reglas de proceso del proveedor de medios de pago, ya que la propia petición ya incluye la información necesaria a cerca de los pasos a seguir en cada compra. Únicamente tiene que ser capaz de vincular las referencias que le llegan para acceder a un recurso con la cuenta bancaria o número de tarjeta de crédito del usuario para el que le llega la petición de pago. Para la transacción final el proveedor o el propio banco puede utilizar sus mecanismos o sus protocolos transaccionales habituales.

- El usuario puede estar tranquilo, ya que la tienda no va a conocer la identidad que tiene configurada en el proveedor de medios de pago y viceversa [14]. Lo único que va a saber es que ahí puede acceder al recurso bancario del sujeto que ha adquirido cierto producto y que puede usarlo para que pague por ello, sin conocer más detalles ni acerca de la identidad del usuario ni de los datos de la cuenta bancaria, número de tarjeta de crédito etc.

El procedimiento de pago se haría de la siguiente manera Fig 7:

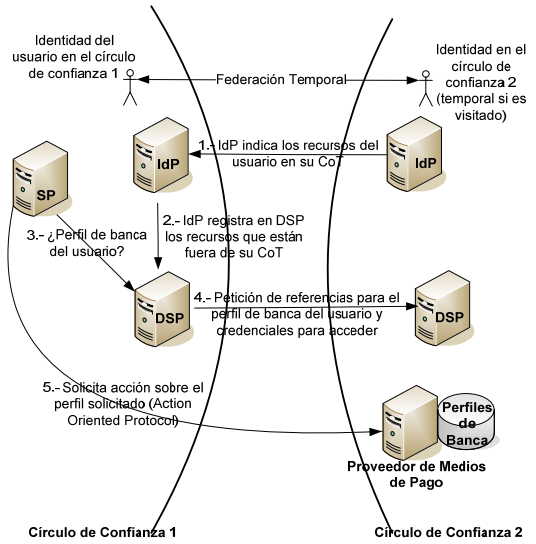

Fig 7 Dialogo completo para acceder a recursos del usuario

Cuando un proveedor de servicios, en este caso, la tienda en Francia, necesita acceder a un dato del usuario que está fuera del círculo de confianza al que pertenece, accede como es habitual en *Liberty* al servicio de descubrimiento [15]. Este servicio es usado en *Liberty* para obtener credenciales y devolver información de dónde se encuentran almacenados los recursos de los usuarios. Dado que en este caso, los recursos del usuario (perfil bancario) se encuentran almacenados fuera de su círculo de confianza, la petición es redirigida al servicio de descubrimiento del círculo de confianza donde se encuentran almacenados, esto es, *Oxenbank.*

Otros enfoques de este mecanismo [16] consideran que es el proveedor de servicio el que puede acceder directamente al servicio de descubrimiento del otro círculo de confianza, sin embargo, nosotros consideramos que no es la opción más adecuada. La entidad que proporciona el servicio de descubrimiento (*Discovery Service Provider*, DSP, en *Liberty*) es la que conoce dónde se encuentran los perfiles de los usuarios y es quien proporciona credenciales para acceder a ellos, por lo que consideramos que es una entidad que debería ser protegida por el operador o la compañía que gestiona el círculo de confianza en cuestión. En nuestro modelo, solo interactúan entre sí los *DSP* de ambos círculos de confianza, lo que es menos peligroso ya que entre ambos círculos de confianza existen acuerdos de colaboración.

Tras el encadenamiento entre ambos servicios de descubrimiento [2] el servicio de descubrimiento de *Orangemobile* ha obtenido referencias y credenciales para acceder al recurso bancario del usuario en *Oxenbank*. Esta información es redirigida a la tienda quien accede directamente al proveedor de medios de pago en *Oxenbank* para hacer efectivo el pago. En esa petición al proveedor de medios de pago se incluyen las credenciales obtenidas del servicio de descubrimiento y varias acciones a realizar en el destino, así como datos de entrada que puedan ser necesarios para realizar dichas acciones.

Finalmente, en la respuesta a la acción se incluyen los resultados y el estado para cada una de las acciones que se pidieron en la petición.

Un ejemplo de mensaje enviado de la tienda al proveedor de medios de pago sería el mostrado en la Tabla 1.

Tabla 1 Ejemplo de petición de acción usando AOP

```
<soap:Header>
...
</soap:Header>
<soap:Body>
   <ActionRequest xmlns="urn:liberty:id-sis-banking:2004-03" id="s31d351233d18as68d1sd">
       <ResourceID id="d4a6s8d42684d6a5s4d6s8z">
       http%3A%2F%2Fwww.bank.com%2Faccount0054821554878
       </ResourceID>
       <Action name="ChargingService" id="4d6s84dq684dzs68d4a6s8d46a8s4d"
                actionID="sa8d46824d6a8sd468as4a6w8">
              <Input>
                 <ChargingServiceRequest>
                     <Amount>30.00</Amount>
                     <Currency>euros</Currency>
                     <FinalAccount>0055-8878-4452-5689-7842-1515-2255</FinalAccount>
                 </ChargingServiceRequest>
              </Input>
              <Description>7 entradas para el cine</Description>
       </Action>
       <Action name="BalanceService"
                   id="44f54f68se4r68e4f6d84fd68d"
                    actionID="dsa4d84we84dz8sd64s84d6"
                    executeAfter="sa8d46824d6a8sd468as4a6w8">
        </Action>
      </ActionRequest>
   </soap:Body>
```

La cabecera del mensaje contendría en su interior las credenciales obtenidas del servicio de descubrimiento gracias a las cuales se podrá acceder al recurso de banca. Dentro del cuerpo del mensaje se indica la referencia al recurso al que se está accediendo (*ResourceID*), y un listado de acciones, cada una de ellas con un identificador distinto en el campo *actionID*. En este caso hay dos, la primera desencadena un pago de 30 euros por una serie de entradas de cine que serán transferidas a la cuenta bancaria que indica el elemento *FinalAccount*. Esta cuenta bancaria no es la del usuario, sino la de la tienda y donde se efectúa el pago. La segunda acción que se incluye en el mensaje es una petición adicional del usuario, para obtener el saldo de su cuenta corriente al acabar la operación. Esta acción contiene el campo *excuteAfter* para indicar que dicha acción debe realizarse después de aquella cuyo identificador se muestra como valor de ese campo, y que en este caso corresponde con el campo *actionID* de la acción de compra anterior.

Finalmente, la respuesta a la petición de acción anterior, enviada desde el proveedor de medios de pago a la tienda sería, omitiendo campos no relevantes, similar al contenido de la Tabla 2:

Aquí se ve como se hace referencia a las acciones que iban en la petición usando el campo *actionIDRef*.

Después de todo este proceso, el usuario ha podido comprar entradas para ir al cine en Francia, usando un proveedor de servicio asociado al círculo de confianza de un operador en donde no tiene una identidad, y pagándolas además usando su banco habitual, todo esto de forma sencilla, segura y manteniendo la privacidad y la confidencialidad de su identidad.

Tabla 2 Ejemplo de respuesta a acción usando AOP

```
<ActionResponse>
   …
   <Status>Ok</Status>

   <ActionResult name="ChargingService"
     actionIDRef="sa8d46824d6a8sd468as4a6w8"
     id="lsdkjfldglfdhgfdljgfg+65df+g5dfhh">
     <Status>Ok</Status>
   </ActionResult>

   <ActionResult name="BalanceService"
     actionIDRef="dsa4d84we84dz8sd64s84d6"
     id="lsdijslfihdskufhsdkufhsdkfh">
     <Status>Ok</Status>
     <Output>
      <BalanceServiceResponse>
        <Amount>75.25</Amount>
        <Currency>euros</Currency>
      </BalanceServiceResponse>
     </Output>
   </ActionResult>

</ActionResponse>
```

6. Conclusiones

En este artículo se ha presentado la aplicación de unos modelos de colaboración entre círculos de confianza *Liberty* a un escenario de comercio electrónico, soportado este por la creación de un nuevo protocolo orientado a acción que extiende el actual protocolo de *Liberty* para consultar datos de usuario que están distribuidos por distintos proveedores dentro de un círculo de confianza. La extensión de este protocolo, al que hemos llamado *Action Oriented Protocol*, permite desencadenar acciones que requieran de determinados datos de entrada y de prioridades a la hora de ejecutarlas en los proveedores de servicios Web. Además hemos aplicado este protocolo junto con los mecanismos de colaboración entre círculos de confianza para mostrar un escenario en el que un usuario accede a un servicio de tienda online, incluso si está accediendo en situación de itinerancia a través de un círculo de confianza donde no tiene una identidad, para comprar productos y pagarlos usando un proveedor de medios de pago presente en otro círculo de confianza gracias a este nuevo protocolo que permite desencadenar acciones.

La combinación de ambas soluciones permite crear escenarios atractivos para los operadores y los usuarios. Para los operadores permite ampliar su gama de servicios y obtener nuevas formas de ingresos gracias a las interacciones y acuerdos que puedan crearse entre operadores y compañías. Para los usuarios no sólo les permite acceder a servicios incluso cuando estos se encuentran desplegados en círculos de confianza donde no tienen cuenta, sino que además el uso de este nuevo protocolo orientado a acción les permite realizar transacciones avanzadas con proveedores donde tienen almacenados sus perfiles, por ejemplo, para realizar el pago por un producto utilizando este protocolo contra un perfil bancario almacenado en un proveedor de medios de pago dentro del círculo de confianza de un banco. Además, al igual con *Liberty*, todos estos mecanismos garantizan la seguridad de las transacciones y la privacidad de la identidad y perfiles de los usuarios, evitando que información privada pueda llegar a proveedores no autorizados, evitando así situaciones de spam o robos de identidad entre otros.

Agradecimientos

Los autores de este artículo desean expresar su agradecimiento a la Cátedra Ericsson de la ETSI Telecomunicación de la UPM por su apoyo y financiación a la línea de investigación

Referencias

[1] I. Jørstad and D. van Thanh, "Service personalisation in mobile heterogeneous environments," Proc. Int. Conf. on Telecomm. and Int. Conf. on Internet and Web Applications and Services, IEEE Press, 2006, p. 70.

[2] J. C. Yelmo, J. Ysart, R. Trapero, “Modelos de Colaboración y gestión de Círculos de Confianza Liberty en la provisión de servicios de Internet móvil”, Telecom I+D 2005, Noviembre 2005.

[3] S. Cantor et al, "Assertions and protocols for the OASIS Security Assertion Markup Language (SAML)," Standard v2.0, OASIS, 2005.

[4] Liberty Alliance project webpage. Disponible en: http://www.projectliberty.org

[5] Shibboleth Project webpage. Disponible en: http://shibboleth.internet2.edu

[6] S. Bajaj et al, "Web Services Federation Language (WS-Federation)". Draft v1.0, 2003. Disponible en : ftp://www6.software.ibm.com/software/developer/library/ws-fed.pdf

[7] SourceID Open Source Federated Identity Management. Disponible en: http://www.sourceid.org

[8] Hirsch, F., Kemp, J., Ilkka, J.: Mobile Web Services: Architecture and Implementation. J. Wiley & Sons, 2006.

[9] H. Vögel, B. Weyl, and S. Eichler, "Federation solutions for inter- and intradomain security in next-generation mobile service platforms," *Int. J. Electron. Commun. (AEÜ)*, vol. 60, issue 1, 2006, pp. 13-19.

[10] Nokia. “Identity Federation and Web services – technical use cases for mobile operators”. Disponible en: http://projectliberty.org/liberty/content/download/393/2738/file/

[11] G. Baker, V Megler, “The semi-walled-garden: Japan’s “i-mode phenomenon””. IBM pSeries Solutions Development, Octubre, 2001.

[12] Kellomäki, S., Kainulainen, J. “Liberty ID-WSF Data Services Template”. Version 2.1. Liberty Alliance Project. Disponible en http://www.projectliberty.org/resources/specifications.php

[13] Davis, P. Cantor, S. “Liberty Metadata Description and Discovery Specification”. Versión 2.0-02. Liberty Alliance Project. Disponible en http://projectliberty.org/liberty/content/download/1226/7980/file/draft-liberty-metadata-v2.0-02.pdf

[14] Yelmo, J. Ysart, J. Trapero, R. del Álamo, Jose M. “Sistemas de pago en Internet móvil basados en Colaboración entre Círculos de Confianza Liberty”. Congreso Iberoamericano de Telemática CITA2006.

[15] Beatty, J., Sergent, J., Hodges, J. Liberty ID-WSF Discovery Service Specification. Version 2.0. Liberty Alliance Project. Disponible en: http://www.projectliberty.org/resources/specifications.ph

[16] O. Jussila and M. Laukkanen, "FIDELITY – Federated Identity management based on Liberty, Fidelity Demokit" Disponible en: http://www.celtic-fidelity.org/fidelity, 2006.