Protection of Personal Information in User-centric Converged Service Platforms

J. C. Yelmo, C. Martínez, J. M. del Álamo and M. A. Monjas

Abstract— **The so-called User-Generated Services (UGS) provide users with the means to create and share their own advanced services that better fit their needs or those of their communities. Platforms supporting UGS for non-technically skilled users are becoming popular, both in the Internet and the Telecommunications domains. They provide creators with the means to include consumers' personal data or contextual information in order to generate attractive value-added services and also to improve the user-experience. However, the use and release of personal identifiable information poses several privacy and data protection concerns. In this paper we analyze the foreseeable problems and propose a solution for the protection of personal information on a UGS platform.**

Keywords— **Service Mashups, Digital Identity, Service Delivery Platform, Privacy, User-Generated Services, Web 2.0.**

I. Introducción

FRUTO de la convergencia, la regulación de mercados y los procesos de apertura de las redes se ha introducido nueva competencia en la provisión de servicios de telecomunicación. Los nuevos competidores, muchos de ellos procedentes del mundo Web, comprometen los modelos de negocio tradicionales al ofrecer sus servicios directamente a los usuarios finales de los operadores.

Como respuesta, los operadores están evolucionando sus entornos de provisión de servicios con el fin de ofrecer una gama más amplia de nuevos productos, más rápidamente y de manera más rentable. En este sentido, las redes de siguiente generación permiten el despliegue de nuevos servicios convergentes que pueden ser accedidos a través de diferentes redes de acceso. Además, la evolución hacia enfoques de arquitecturas orientadas a servicios permite ofrecer los recursos de red a la colaboración con terceros proveedores de servicios, a través de habilitadores de servicios. Todo ello simplifica y acelera la creación y despliegue de nuevos servicios, utilizando un enfoque basado en componentes.

Sin embargo, es poco probable la aparición de una única aplicación estrella (*killer application*) que permita resolver todos los problemas de una vez y para siempre. Por contra, parece un mejor enfoque el desarrollar multitud de pequeñas y buenas ideas, muchas de las cuales pueden convertirse en éxitos puntuales que permitan aumentar los ingresos del operador. Esta es la base de un nuevo paradigma surgido en Internet que permite a usuarios no expertos crear y compartir sus propios contenidos y aplicaciones (*mashups*) a partir de la combinación de una serie de servicios distribuidos: las plataformas de servicios centrados en los usuarios.

Uno de los valores que los consumidores más valoran en estos servicios es el nivel de personalización que proporcionan. Por definición, para poder personalizar un servicio, se precisa el conocimiento de información personal (o de identidad) del usuario. Esta información no sólo se refiere al color favorito, nombre o lengua materna. Por el contrario, los atributos que pueden proporcionar un mayor valor para los consumidores son dinámicos por naturaleza y deben ser obtenidos por el análisis de su comportamiento, como la localización o el estado de presencia.

Debido a la naturaleza distribuida de los servicios centrados en el usuario, algunos atributos de identidad deberán ser compartidos con los proveedores de los servicios componentes. Recíprocamente, algunos proveedores ofrecerán recursos para la composición que incluyen información de identidad de los usuarios, como un medio de pago o información de crédito. Cabe señalar que los recursos proporcionados por terceros proveedores, normalmente estarán fuera de los límites de la plataforma, y por tanto en distintos dominios administrativos. La legislación de la mayoría de países (en especial la española y europea) respecto a la protección de la privacidad establece que los usuarios deben ser informados y dar su consentimiento sobre el uso de su información personal cuando ésta se comparte entre diferentes empresas [1].

Por consiguiente, es necesario que las plataformas de servicios centrados en el usuario proporcionen la infraestructura necesaria para el intercambio de información de identidad, a la vez que permiten a los usuarios la gestión de su privacidad. Sin embargo, este aspecto no ha sido abordado de forma adecuada en la literatura. Este artículo presenta las contribuciones de los autores en el contexto introducido. Para ello, primero se ofrece una visión general de las plataformas de servicios centrados en el usuario, revisando el estado del arte relacionado, prestando especial atención a los aspectos para la gestión de la identidad digital y la privacidad. Después, se describe la solución propuesta para la protección de la información personal, detallando

Juan Carlos Yelmo, Cristina Martínez y José María del Álamo realizan tareas de docencia e investigación en el Departamento de Ingeniería de Sistemas Telemáticos de la Universidad Politécnica de Madrid, Madrid, jcyelmo@dit.upm.es; cristinam@dit.upm.es; jmdela@dit.upm.es.

Miguel Ángel Monjas trabaja para *Ericsson España S.A.*, Madrid, miguel-angel.monjas@ericsson.com.

aspectos como la arquitectura y los mecanismos empleados. Además, se explica el escenario que ha permitido validar los desarrollos. El artículo termina con las conclusiones extraídas y presentación de líneas de trabajo futuro.

II. Plataformas de servicios centrados en los usuarios

Una de las tendencias que más está impactando en el mundo de las Tecnologías de la Información y las Comunicaciones (TIC) en los últimos tiempos es la "centralidad del usuario": los artefactos informáticos y de comunicaciones tienden a dirigirse y enfocarse principalmente a los usuarios y sus necesidades, tratando que sean ellos los protagonistas y diseñadores de su experiencia. Una plataforma de servicios centrados en el usuario se basa en este modelo, en el cual el usuario final, sin necesidad de ser un desarrollador profesional o un experto, es capaz de diseñar sus propios servicios convergentes totalmente personalizados [2][3][4].

En el mundo de Internet, ya existen distintos proveedores de servicios que ofrecen un conjunto de interfaces y servicios gratuitos permitiendo a sus usuarios crear y compartir sus propias aplicaciones y contenidos, combinando cajitas que representan servicios básicos de forma gráfica, como por ejemplo Yahoo! Pipes (http://pipes.yahoo.com/pipes/) y Microsoft Popfly (http://www.popfly.ms/). En el mundo telco hay operadores que recientemente han empezado a ofrecer interfaces para que desarrolladores profesionales accedan a servicios que ofrece la red de telecomunicaciones como Vodafone Betavine (http://www.betavine.net), Orange Partner (http://www.orangepartner.com) y Telefónica Open Móvil Forum (http://www.movilforum.com). Últimamente, ambos enfoques están convergiendo y han aparecido plataformas que permiten a usuarios no expertos crear servicios utilizando recursos proporcionados tanto por proveedores de servicios en Internet como por la infraestructura de red. Los ejemplos más relevantes son Microsoft Connected Services Sandbox (http://www.networkmashups.com/) y la plataforma OPUCE (Open Platform for User-centric service Creation and Execution) (http://www.opuce.eu/).

De todas estas iniciativas sólo OPUCE permite la utilización de información de identidad de los usuarios que consumen los servicios para facilitar una adaptación dinámica y automática al contexto de uso. Además, permite el uso de etiquetas de identidad a la hora de la creación del servicio que en tiempo de ejecución son sustituidas por los valores adecuados para cada consumidor, permitiendo así una perfecta personalización del servicio a la esfera personal del usuario. Sin embargo OPUCE no dispone de ningún mecanismo que garantice la privacidad del usuario en el uso de los servicios así creados. Estos servicios pueden hacer uso de componentes que provienen de distintos dominios administrativos, y por lo tanto es común que se intercambie información de identidad con ellos, lo cual está regulado por ley.

La plataforma sobre la que hemos trabajado se basa en el modelo propuesto por el proyecto OPUCE pero extiende su funcionalidad ya que permite el empleo de información de identidad en la composición de servicios a la vez que salvaguarda la privacidad de los consumidores. Además, nuestra solución incorpora un sistema de gestión de la privacidad que hace que mejore la experiencia de usuario al tener control en todo momento de qué información se está usando y por quién.

La siguiente sección explica de forma breve en qué consiste la gestión de la identidad digital y de la privacidad y qué herramientas existen para abordar el problema que enfrentamos.

III. Identidad digital y privacidad

La identidad digital se define como el conjunto de rasgos propios que caracterizan a un individuo o colectivo en un medio de transmisión digital. La información aislada carece de sentido y por ello es fundamental dar a conocer quién es o quién quiere ser en la red el individuo. Por su parte, la privacidad se puede definir como el derecho de los individuos para determinar por sí mismos cuándo, cómo y qué información de identidad se divulga.

A. Gestión de identidad digital

La gestión de identidad digital es la disciplina que trata sobre la gestión del acceso a recursos de identidad de los usuarios distribuidos en la red, en sus aspectos técnicos, legales y de negocio. A nivel técnico, la gestión de identidades tiene que ver con áreas como la seguridad en redes, la provisión de servicios, la gestión de clientes, el registro único de usuario y la prestación de Servicios Web [5].

Existen dos enfoques básicos para la gestión de identidad en servicios de red. El primero es el enfoque centralizado, donde una única entidad gestiona atributos y elementos de identificación de todos los usuarios de servicios de red y ofrece servicios de autenticación y de información de identidad en nombre de los proveedores de servicio.

El enfoque alternativo es el descentralizado o federado, en el que los proveedores de servicios federan sus sistemas de gestión de identidades para permitir que los usuarios naveguen entre servicios sin volverse a autenticar, aunque sin poner en riesgo la privacidad de sus datos o la seguridad en el acceso a los servicios. Además, permite la compartición segura de información de identidad entre las partes. La gestión de identidad digital toma un papel relevante en las plataformas de servicios centrados en los usuarios, ya que manejan gran cantidad de datos de identidad digital que se encuentran distribuidos en servicios ofrecidos por distintos proveedores.

B. Gestión de privacidad

Actualmente, hay una amplia gama de tecnologías que abordan distintos aspectos de la gestión de la identidad, pero sólo unas pocas tienen mecanismos de salvaguarda de la privacidad. La gestión de la privacidad, ofrece un medio que permite a las personas controlar la naturaleza y cantidad de información personal que se facilita sobre ellas, de modo que se refuerce su protección.

Hay que distinguir entre el concepto de seguridad y el de privacidad. Como seguridad se entiende que el usuario puede acceder a los recursos, porque tiene el privilegio de usarlos. En cambio, la privacidad permite al solicitante acceder a los recursos, sólo si no viola la intimidad de otro usuario.

La falta de confianza en la privacidad y seguridad es un obstáculo importante para el éxito de los negocios online en general y de las plataformas de servicios centrados en el usuario en particular. Para ganarse esa confianza, las organizaciones deben proveer a los clientes de sistemas para gestionar la privacidad, es decir, deben explicar las directrices (políticas) por las que se guían, representándolas en un lenguaje conveniente para que pueda ser fácilmente comprensible por los usuarios.

En el estado del arte, existen distintos tipos de lenguajes y herramientas para gestionar las políticas de privacidad. Algunos han sido diseñados para ayudar a las organizaciones a expresar sus políticas de privacidad y otros para ayudar a los usuarios a definir sus preferencias de privacidad.

En 1997, el Consorcio W3C (World Wide Web Consortium) desarrolló P3P (Platform for Privacy Preferences Project) [6] para expresar las políticas de privacidad de un sitio Web en un formato XML. W3C también desarrolló un Lenguaje de Intercambio de Preferencias P3P (A P3P Preference Exchange Language - APPEL) [7] para expresar las preferencias de privacidad de los usuarios. Otra especificación del W3C es WS-Policy (Web Services - Policy) [8], que permite definir políticas de seguridad, calidad de servicio, etc. y forma parte del conjunto de especificaciones WS-*. En el año 2000 surgió CPExchange [9] que facilita las relaciones de negocio entre empresas en lo relativo políticas de privacidad. Después, se necesitaban lenguajes para que las organizaciones expresaran sus propias políticas internas. Para esto mismo IBM diseñó EPAL (Enterprise Privacy Authorization Language) [10] en 2003. El lenguaje XACML (eXtensible Access Control Markup Language) [11] fue creado por un consorcio de organizaciones para expresar seguridad y privacidad.

Cada lenguaje tiene su propia sintaxis y mecanismos de implementación, ya que cada uno está enfocado a un contexto distinto, distinguiéndose entre aquellos orientados a entidades y los orientados a usuarios. Teniendo en cuenta el papel del usuario en las plataformas de servicios analizadas y después de un estudio sobre todos los lenguajes de privacidad citados anteriormente, se ha optado por utilizar los lenguajes P3P y APPEL.

P3P es un protocolo basado en XML que permite a los sitios Web expresar sus prácticas de privacidad en un formato estandarizado y procesable por dispositivos. Las políticas descritas en P3P pueden ser recuperadas de forma automática por los navegadores. Además los usuarios pueden encontrar dichas políticas en un formato fácil de entender para ellos ya que el formato XML puede ser fácilmente traducido a un formato comprensible por humanos.

Por su parte, el lenguaje APPEL permite describir preferencias de privacidad. Empleando este lenguaje, un usuario puede expresar sus preferencias a través de un conjunto de reglas, las cuales pueden ser utilizadas para tomar decisiones automáticas o semiautomáticas de acuerdo a la aceptación de las políticas de privacidad de los sitios Web, en función de lo que el usuario prefiera.

Finalmente, la combinación de ambos lenguajes nos puede ayudar a conocer si un servicio es compatible con las preferencias de un usuario, mediante la comparación de las políticas del servicio expresadas en P3P con las preferencias del usuario expresadas en APPEL.

IV. Propuesta

Esta sección describe nuestra propuesta de un sistema de gestión de la privacidad para plataformas de servicios convergentes centrados en el usuario. Nuestra propuesta se sustenta sobre una plataforma de servicios que dispone de varios módulos: un entorno de creación de servicios básicos, un entorno de creación de servicios compuestos, un sistema de suscripción a servicios, un sistema de gestión de ciclo de vida de los servicios y, por último, un entorno de ejecución. La arquitectura completa se muestra en la Fig. 1 en la que los subsistemas correspondientes a la gestión de la privacidad aparecen en color naranja.

A. Entorno de creación de servicios básicos

La plataforma dispone de un Entorno de Creación de Servicios Básicos que permite introducir servicios, existentes en Internet u ofrecidos por la infraestructura de red, para su uso en la plataforma.

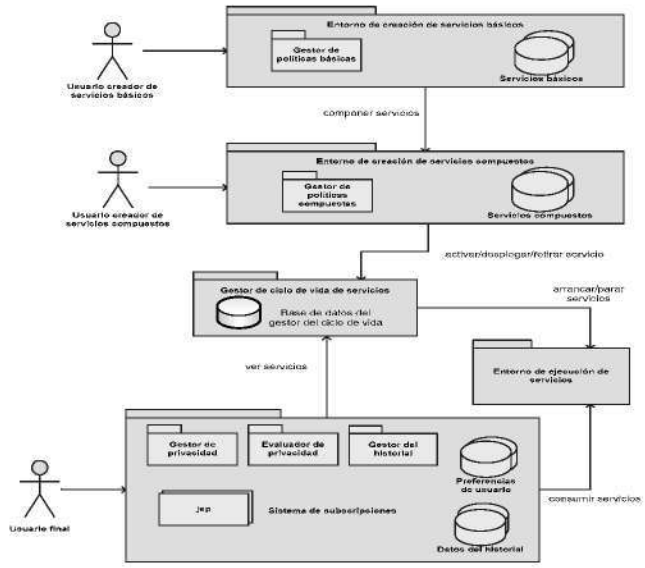

Figura 1. Arquitectura de la plataforma.

Una de las características claves que diferencia los servicios de los componentes software tradicionales es la de ser autodescriptivos, lo que separa la descripción del servicio de la implementación del mismo. Para conseguir una completa descripción de servicios, hay que caracterizar a los servicios atendiendo a algunos criterios específicos como son

su funcionalidad, lógica de ejecución y privacidad, entre otros. En este caso, la tecnología de Servicios Web usa el lenguaje de descripción de Servicios Web (WSDL) para describir las interfaces y los puntos de acceso al servicio.

La característica de privacidad ofrece un valor añadido a los servicios, ya que informa a los posibles consumidores de la información personal que el servicio precisa intercambiar, y las condiciones en las que lo hace. El entorno de creación de servicios básicos utiliza un editor de políticas P3P para incorporar políticas de privacidad a los servicios básicos.

En nuestro caso, las políticas P3P de un servicio recogen información sobre qué datos de información personal del usuario se requieren para el empleo de dicho servicio y además se indica para qué propósito se hace uso de los datos, el tiempo que se retienen y si se envían a terceras compañías o son sólo para uso propio.

B. Entorno de creación de servicios compuestos

En el entorno de Creación de Servicios Compuestos, el usuario tiene a su disposición una serie de servicios básicos introducidos gracias al subsistema explicado anteriormente. Con ayuda de un editor se permite combinarlos de forma gráfica, obteniendo como resultado un nuevo servicio más complejo y de valor añadido.

La composición debe realizarse a distintos niveles, como son a nivel de lógica, a nivel funcional, a nivel de privacidad, etc. A nivel de lógica se emplean lenguajes de orquestación tales como BPEL para describir la lógica de composición de servicios. Un proceso BPEL se crea de manera gráfica, combinando ciertas cajas de servicios Web básicos y dando como resultado un servicio Web compuesto.

Además, a este servicio compuesto se incorporan las políticas de privacidad en lenguaje P3P, generadas de forma automática por la plataforma a partir de las políticas de los servicios básicos y apoyándose en los ficheros que describen éstos. De esto se encarga el gestor de políticas compuestas.

Primero se analiza el código BPEL del servicio compuesto del cual se extraen todos los datos intercambiados (consumidos o enviados) con los servicios básicos. Se comprueba si estos datos son o no de identidad, y para ello, se examinan las políticas de privacidad de cada servicio básico. Si se detecta que un dato es de identidad, éste se incorpora automáticamente a la política de privacidad del servicio compuesto, junto con toda la información relevante asociada (servicio básico relacionado, condiciones de uso, etc.).

La Fig. 2 muestra un ejemplo simplificado del proceso que tiene lugar en el caso de un servicio compuesto llamado MapMe: este servicio permite solicitar a usuarios el envío de un mensaje multimedia con un mapa de sus alrededores.

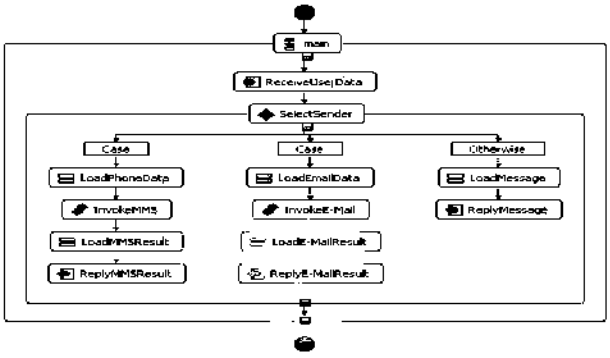

Figura 2. Diagrama de la lógica del servicio BPELMessageSender

Para ello el servicio intercambia información de identidad con dos servicios básicos: Geolocator y MMSSender. Geolocator ofrece la localización geográfica de un terminal, que es un dato de identidad. MMSSender envía mensajes multimedia utilizando el número de teléfono del destinatario, que también es un dato de identidad. Dado que ambos datos aparecen reflejados en las políticas de privacidad de cada servicio básico pasan a incluirse también en la política de privacidad del servicio compuesto.

C. Gestor de ciclo de vida de servicios

Es la parte encargada de comunicar el entorno de creación de servicios y el de ejecución. Sus tareas principales son gestionar de forma autónoma el ciclo de vida de los servicios y mantener información actualizada de éstos.

D. Sistema de subscripciones

El Sistema de Suscripción a Servicios es la parte encargada de presentar al usuario consumidor los servicios activos, permitir el acceso a los servicios creados y gestionar perfiles de usuario. Este sistema dispone de un módulo (Gestor de la privacidad) por el cual a partir de los deseos de los usuarios expresados mediante una interfaz gráfica se generan los ficheros de preferencias de privacidad. Otro módulo, llamado Evaluador de la Privacidad, se encarga de evaluar las preferencias del usuario a la hora de suscribir un servicio. Por último, el módulo llamado Gestor del Historial se encarga de generar un historial de uso de información de identidad para cada usuario.

Cuando un consumidor llega por primera vez a la plataforma, debe registrarse como nuevo usuario. Para ello, rellena un formulario en el que se le solicita información básica, como nombre de usuario y contraseña. A continuación, el usuario debe rellenar un formulario en el cuál se le pregunta cuáles son sus preferencias de privacidad sobre ciertos datos de identidad. Aquí el usuario puede elegir entre conceder permiso para el uso de cierto dato, denegarlo o que le pregunten en caso de uso y decidir en ese momento. También se permite ser más específicos a la hora de definir los permisos para cada uno de los datos de identidad, indicando para qué propósitos se permite su uso, el tiempo que pueden estar los datos retenidos en la plataforma y si esa información se puede enviar a terceras compañías o no.

Una vez completado el formulario el Gestor de la Privacidad genera un fichero en lenguaje APPEL. Adicionalmente, si un usuario dispone ya de un fichero en este lenguaje con sus preferencias definidas, existe la posibilidad de importarlo directamente.

Antes de pasar a ejecutar cualquier servicio, hay que comprobar que éste respeta las preferencias de privacidad del usuario, haciendo una comparación entre la política del servicio y las preferencias de usuario. De ello se encarga el Evaluador de la Privacidad del Sistema de Subscripciones.

El Evaluador de la Privacidad compara la política de un servicio con un conjunto de preferencias de usuario. Para la comparación se emplea la herramienta AppelEvaluator (http://p3p.jrc.it/). Tras la comparación, se devuelve el resultado de la evaluación, es decir: (a) se bloquea el servicio y una descripción de la causa del bloqueo; (b) se requiere intervención del usuario o; (c) se concede permiso para ejecutar el servicio con total normalidad.

Tras esta evaluación, los servicios podrán aparecen en diferentes colores. Un servicio que se muestre en rojo indica que hay un conflicto entre las preferencias del usuario y las políticas del servicio, por ejemplo, cuando el usuario no permite el uso de alguno de los datos de identidad que emplea el servicio, éste se bloquea mostrando la causa del bloqueo y no se permite su ejecución. Otro caso es que el servicio compuesto aparezca en color naranja, lo cual le hace saber al usuario que se puede pasar a ejecutar, pero que éste requiere de su consentimiento explícito, ya que hace uso de un dato de identidad que él ha pedido que sea avisado en el caso de que se utilice. Por último, si un servicio se presenta en color verde, indica que no existen conflictos y puede ser ejecutado sin restricciones.

Dentro del sistema de subscripciones también se encuentra el Gestor del Historial. Este gestor tiene dos partes, la primera se encarga de generar los eventos almacenados en dicho historial mientras que la segunda es la que permite a un usuario consumidor de servicios consultar el historial de uso de sus datos de identidad personal.

Al ejecutar con éxito cualquier servicio, se comprueba qué datos de identidad utiliza ese servicio. Esa información se obtiene de una base de datos en la que están almacenados los datos de identidad que usa cada servicio. La base de datos se actualiza cada vez que se activa un servicio compuesto en la plataforma. A continuación, se modifica el historial de usuario para indicar que se ha ejecutado un servicio que hace uso de información de identidad.

El historial que puede consultar un usuario dispone de tres secciones. En la primera se muestran gráficas generadas en Flash, una por cada dato de identidad personal que se emplee en alguno de los servicios compuestos. En estas gráficas el usuario puede obtener información de qué dato se ha empleado, qué servicio ha hecho uso de él y la fecha y la hora en qué tuvo lugar. En otra de las secciones, se muestra un gráfico indicando el porcentaje de uso de cada dato de identidad. Por último, también se dispone de una tabla resumen con un registro de eventos que se generan cuando se hace uso de un dato de identidad.

E. Entorno de ejecución de servicios

Es la parte encargada de arrancar o detener la ejecución de los servicios, y de gestionar los procesos involucrados durante el tiempo de vida de los mismos. Gracias al Evaluador de la Privacidad, los servicios sólo se ejecutan si no existen conflictos de privacidad.

V. Escenario de validación

Para realizar la validación de la plataforma se ha implementado el siguiente escenario. Primero, es necesario incorporar servicios básicos a la plataforma e incorporarles políticas de privacidad como ya se ha explicado en el apartado anterior. Después, el usuario creador de servicios compuestos, genera un mashup haciendo uso del plugin BPEL y pasa a activarlo para que se encuentre disponible a cualquier usuario. En el momento de activación del mashup, se genera su política de privacidad, que podrá ser consultada por los usuarios consumidores de servicios previamente a la suscripción. Una vez que existan mashups en la plataforma disponibles para ser ejecutados, el usuario consumidor de servicios podrá hacer uso de ellos. Cuando un usuario nuevo llega a la plataforma es necesario que realice el proceso de registro para crearse un perfil y declarar sus preferencias de privacidad. Después, ya como usuario dado de alta en la plataforma, decide visualizar los servicios disponibles en ese momento y pasar a ejecutar alguno de ellos. Por último después de un uso prolongado de servicios en la plataforma decide consultar el historial de uso de su información de identidad.

A. Generación de servicios compuestos en la plataforma

Suponemos en este punto que se dispone de varios servicios básicos ya introducidos en la plataforma como son un servicio de mensajería multimedia (MMSSender), servicio de localización de terminales (GeoLocator), servicio de generación de mapas (Mapper), servicio de correo electrónico y servicio de DNS (que traduce nombres de hosts a direcciones IP). Tomando como base estos servicios básicos, en este escenario vamos a manejar tres servicios compuestos: BPELMaps, BPELMessageSender y URLLocator.

El servicio BPELMaps es una evolución del servicio MapMe. Está formado por cuatro servicios básicos e incluye múltiples posibilidades de ejecución en función del resultado de invocación de los servicios. El servicio ha sido diseñado pensando que será el usuario que desea conocer su posición el que hará una solicitud al servicio desde su teléfono móvil. Accediendo al subsistema de suscripciones éste se encargará de proporcionar al servicio los datos necesarios (número de teléfono y dirección de correo) para que el usuario final obtenga el mapa con un mínimo de interacciones con la plataforma. Por lo tanto, este mashup hace uso de los siguientes datos de identidad: número de teléfono móvil, dirección de correo electrónico y localización del usuario. Esto se muestra en su política de privacidad.

Figura 3. Activación, despliegue y retirada de servicios (II)

El servicio BPELMessageSender permite enviar mensajes que pueden ser mensajes multimedia o correos electrónicos según la selección del usuario final. Para la implementación, utiliza el servicio básico de mensajería y el servicio de correo. Por ello, el usuario debe proporcionar el número de teléfono móvil y el correo electrónico.

Finalmente, el servicio URLLocator es un servicio de localización geográfica URL. Este servicio se ayuda del servicio básico de DNS y de un servicio de Internet de localización geográfica de direcciones IP. En cuanto a la privacidad, no hace uso de ningún dato de identidad del usuario.

B. Activación de un servicio en la plataforma

Una vez se han desarrollado los servicios compuestos, el usuario procede a la activación o despliegue en la plataforma de uno de ellos. Para ello se selecciona la opción activar servicio y el entorno muestra al usuario un cuadro de diálogo en el que se solicita toda la información necesaria para generar una descripción de servicio válida. Se requiere el nombre de usuario, una breve descripción del servicio y la fecha de desactivación. La Fig. 3 muestra el cuadro correspondiente a la activación de un servicio.

Gracias al gestor de políticas de servicios compuestos, en este paso se genera automáticamente la política de privacidad del servicio. Si el proceso termina con éxito se muestra un mensaje indicando que todo ha ido bien.

Ahora, el servicio compuesto ya dispone de su política de privacidad que puede ser consultada por cualquier usuario. La política se genera en formato XML para que pueda ser interpretada por navegadores u otros sistemas software, y también se genera una descripción textual comprensible por humanos.

C. Registro de un nuevo usuario

Cuando un usuario llega por primera vez a la plataforma, es necesario que complete un formulario de registro donde debe introducir nombre de usuario, contraseña, número de teléfono móvil y dirección de correo electrónico. Además, también debe definir sus preferencias rellenando el formulario que se observa en la Fig. 5.

En este formulario se le pregunta acerca de tres datos de identidad personal, que son el número de teléfono móvil, la dirección de correo electrónico y la localización del usuario. Sobre cada uno de estos datos, el usuario puede elegir entre varias opciones: permitir su uso siempre, preguntarle en caso de uso, no permitir nunca, o personalizar. Al seleccionar la opción de personalizar, aparecen más opciones en el formulario sobre las que elegir. Una de ellas es decir para qué propósitos se permite el uso de esos datos, otra es el tiempo que se permite retener los datos de información y por último si esos datos se pueden enviar a terceras compañías o sólo se permite para uso propio. Para facilitar esta tarea al usuario, existe una barra deslizante en la que se puede elegir entre un nivel bajo de privacidad, medio, alto, personalizado, o incluso se permite importar un fichero propio en lenguaje APPEL con las preferencias ya definidas.

En este escenario, el usuario decide conceder su permiso para el uso en cualquier momento de su dirección de correo electrónico. Sobre el número del teléfono móvil es más prudente y decide elegir la opción de ser preguntado en caso de uso. Por último, deniega su permiso para el empleo de su localización. Al completar este formulario, se genera automáticamente un fichero en lenguaje APPEL con sus preferencias y el usuario ya está por fin dado de alta en la plataforma. Por consiguiente, ya puede acceder a ella.

D. Empleo de la plataforma por un usuario final

El usuario accede a la plataforma introduciendo su nombre de usuario y contraseña. Cuando el usuario decide ver los servicios públicos le aparecerá una pantalla similar a la que se muestra en la Fig. 4.

Se observa que el primer servicio BPELMaps aparece en rojo, ya que el usuario no ha permitido el uso de alguno de los datos de identidad que emplea el servicio. En este caso, el servicio se ha bloqueado porque requiere el empleo de la localización y no se puede pasar a ejecutar el servicio.

El segundo servicio compuesto BPELMessageSender aparece en naranja, que indica que se puede pasar a ejecutar, pero requiere la intervención del usuario, ya que hace uso de un dato de identidad que el usuario ha pedido que sea avisado en el caso de que requiriera.

Por último, el servicio URLLocator se presenta en color verde, que indica que dispone de todos los permisos para ser ejecutado.

Si pasamos a ejecutar el servicio BPELMessageSender (que aparece en color naranja), se nos muestra un aviso indicando que el servicio requiere el uso del número del teléfono móvil del usuario, por ello se le pide permiso para hacer uso de él siempre (lo que implicaría una modificación de las preferencias del usuario) o sólo esta vez como caso puntual.

Service	Client	Policy	Behavior
BPELMaps (Active)	---	**View policy**	Blocked because localizacion is required
BPELMessageSender (Active)	**Try it!**	**View policy**	User's intervention is required
URLLocator (Active)	**Try it!**	**View policy**	No policy restricts access

Figura 4. Servicios públicos disponibles para ejecución

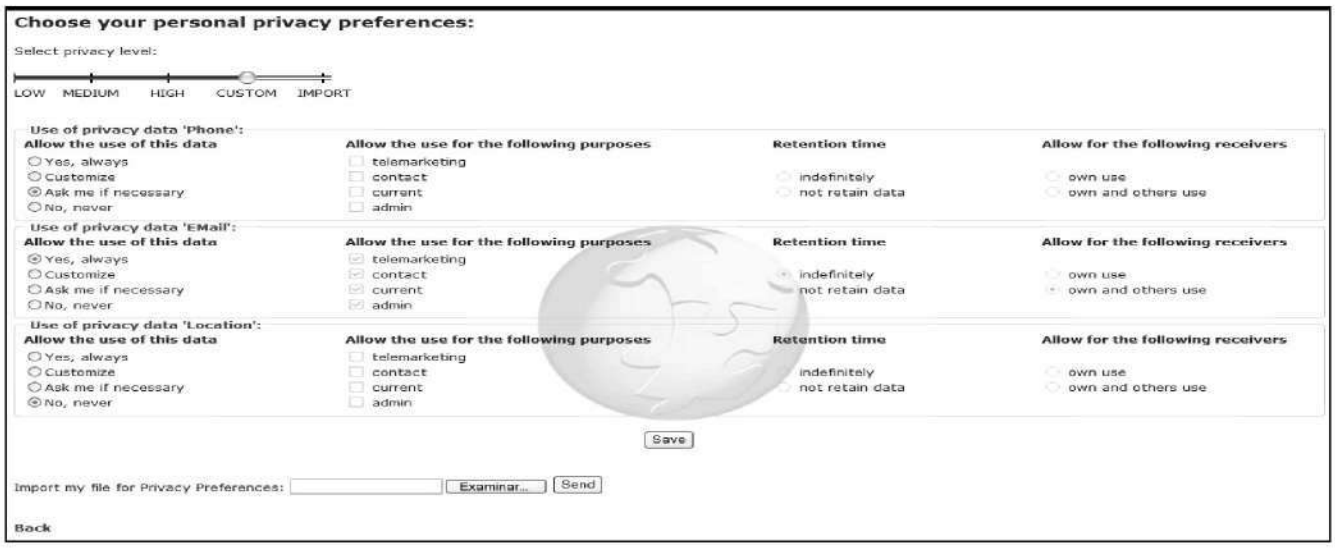

Figura 5. Formulario de preferencias de privacidad del usuario

Si el usuario desea ejecutar el servicio BPELMaps que aparecía en rojo, deberá modificar sus preferencias de usuario, volviendo a rellenar el formulario que se muestra en la Fig. 5.

Otra de las opciones del panel principal es editar el perfil. Ahí se pueden modificar las preferencias de privacidad y consultar el historial. El historial se divide en tres secciones. En la primera el usuario puede consultar un registro de todos los eventos ocurridos a lo largo de su trayectoria en la plataforma, incluyendo datos empleados, fecha y servicio que lo ha utilizado. El resto de secciones presentan esta información de forma gráfica, desglosando porcentajes de uso por atributo y servicio.

VI. Conclusiones

La plataforma que se ha descrito sitúa al usuario como protagonista de la creación de servicios convergentes, ofreciéndole la posibilidad de crear y desplegar servicios totalmente personalizados de forma rápida y sencilla. Así se abre un nuevo mundo de posibilidades a los operadores, dando lugar a un nuevo modelo de negocio, en el que los operadores puedan competir en mejores condiciones en un mercado cada vez más complicado.

Sin embargo, estos servicios manejan una gran cantidad de información personal de sus usuarios. Por ello, contar con un sistema de gestión de la privacidad se convierte en imprescindible para proporcionar un control sobre el tratamiento de esa información.

La solución que se propone en este artículo permite que los usuarios estén informados en todo momento del uso que se da a sus datos de información personal y disponen de un control que les permite conceder permiso sobre el empleo de identidad digital o denegarlo según deseen.

Para ello, se han incorporado políticas que describen el tratamiento de la información personal a todos los servicios básicos disponibles en la plataforma. Además, se ha creado un sistema para la generación automática de las políticas de privacidad de los servicios compuestos. Adicionalmente, se ha implementado un sistema para la recogida y almacenamiento de las preferencias de privacidad de los usuarios de la plataforma, que se evalúan dinámicamente frente a las políticas de privacidad de los servicios. Por último se ofrece un historial del uso de la información de identidad para cada usuario registrado.

Las futuras líneas de trabajo abordan la incorporación de un sistema de gestión de identidad. Además, se trabaja en crear un sistema más dinámico para que si un servicio básico incorpora un nuevo dato de identidad, automáticamente se incluya ese dato a la gestión de preferencias y se tenga en cuenta a la hora de generar el historial de uso.

Referencias

[1] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector*, Official Journal, L 201, Jul. 2002, pp. 37-47.

[2] R. Trapero, D. Suárez, J. M. del Álamo, A. León, Y. S. Martín, I. Ordás, Á. Martínez y J. C. Yelmo. "Next Generation Mashups. Cómo Crear mis Propios Servicios en un Mundo Convergente (*Next-Generation Mashups: How to Create my Own Services in a Convergent World*)", *XVIII Jornadas Telecom I+D*, Bilbao, España, oct. 2008.

[3] J. C. Yelmo, R. Trapero y J. M. Álamo, "Una plataforma para la creación y despliegue dinámico de servicios de telecomunicación centrados en el usuario (*A user-centric telecom-oriented service creation and delivery platform*)", *XVII Jornadas Telecom I+D*, Madrid, España, oct. 2007.

[4] A. Martínez, C. Baladrón, A. León, C. García, L. Calavia, J. Aguiar y J. Caetano. "Nuevos Modelos de Negocio: Servicios Generados por el Usuario (*New Business Models: User Generated Services*)", *XVIII Jornadas Telecom I+D*, Bilbao, España, oct. 2008.

[5] J. C. Yelmo, J. Ysart, R. Trapero y J. M. del Álamo, "Sistemas de pago en Internet móvil basados en Colaboración entre Círculos de Confianza Liberty (*Payment Methods for the Mobile Internet Supported by Liberty Circles of Trust*)", *IV Congreso Iberoamericano de Telemática*, CITA06, Monterrey, México, mayo 2006.

[6] R. Wenning and M. Schunter, "*The Platform for Privacy Preferences 1.1 (P3P1.1) Specification*", W3C Working Group, Nov. 2006.

[7] L. Cranor, M. Langheinrich and M. Marchiorio, "*A P3P Preference Exchange Language 1.0 (APPEL 1.0)*", W3C Working Group, Abr. 2002.

[8] A. S. Vedamuthu, D. Orchard, F. Hirsch, M. Hondo, P. Yendluri, T. Boubez and U. Yalçinalp, "*Web Services Policy 1.5 – Framework*", W3C Recommendation 4 Sep. 2007, Sep. 2007.

[9] K. Bohrer and B. Holland (Ed.), "*Customer Profile Exchange (CPExchange) Specification*", Oct. 2000, Version 1.0.

[10] P. Ashley, S. Hada, G. Karjoth, C. Powers, and M. Schunter, "*Enterprise Privacy Authorization Language (EPAL 1.2)*", Nov. 2003.

[11] S. Godik, and T. Moses, "*eXtensible Access Control Markup Language (XACML) Version 1.0*", OASIS SS TC, Feb. 2003.

Juan Carlos Yelmo es Ingeniero de Telecomunicación (Madrid, España, 1990) y Doctor Ingeniero de Telecomunicación (Madrid, España, 1996), ambos por la Universidad Politécnica de Madrid. Desde 1991 trabaja en el Departamento de Ingeniería de Sistemas Telemáticos de la misma universidad, donde actualmente es Profesor Titular de Universidad, impartiendo docencia de grado, postgrado y doctorado en el ámbito de la ingeniería del software de servicios de telecomunicación y aplicaciones distribuidas. Ha participado en numerosos proyectos de investigación de ámbito nacional e internacional. Sus áreas de interés actuales son los servicios avanzados en redes de siguiente generación, la identidad digital y los sistemas de gestión de identidades federadas, la usabilidad y accesibilidad en servicios telemáticos, las aplicaciones distribuidas y plataformas de intermediación y los temas avanzados de desarrollo de software en ingeniería telemática. El Prof. Yelmo es actualmente representante del DIT-UPM en el OMG y Liberty Alliance, miembro del grupo de trabajo español del European Security Research and Innovation Forum (ESRIF) y subdirector de Doctorado y Postgrado de la Escuela Técnica Superior de Ingenieros de Telecomunicación de la Universidad Politécnica de Madrid.

Cristina Martínez es Ingeniera de Telecomunicación (2009) por la Universidad Politécnica de Madrid (España). En 2008 comenzó a trabajar en el Departamento de Ingeniería de Sistemas Telemáticos de la Escuela Técnica Superior de Ingenieros de Telecomunicación de la Universidad Politécnica de Madrid, donde en la actualidad continúa con su carrera como Investigadora. Colabora en diversos proyectos relacionados con la gestión de identidad digital, la gestión de la privacidad, los servicios generados por el usuario, y las plataformas de servicios convergentes centrados en el usuario.

José María del Álamo es Ingeniero Técnico Industrial (2000), Ingeniero de Telecomunicación (2003) y Doctor Ingeniero de Telecomunicación (2009), todos ellos por la Universidad Politécnica de Madrid (España). En 2002 se incorporó al Departamento de Ingeniería de Sistemas Telemáticos de la Universidad Politécnica de Madrid, del que forma parte actualmente como Investigador. Anteriormente trabajó como Analista y Coordinador de Proyectos en INSA/IBM Global Services. Sus principales áreas de interés se centran en la gestión de identidad y privacidad, los sistemas de soporte a la operación, los servicios avanzados generados por el usuario, y las plataformas y servicios avanzados de telecomunicaciones sobre redes convergentes de nueva generación.

Miguel Ángel Monjas es ingeniero de Telecomunicación por la Universidad Politécnica de Madrid (1996). Comenzó su carrera en Goya Servicios Telemáticos, el primer ISP de España e ingresó en Ericsson en 1999. Vinculado a actividades de gestión de la identidad (investigación, arquitectura, estandarización, preventa, IPR...) desde hace seis años, trabaja desde hace dos en la organización de Tecnología e Innovación del centro de I+D de Ericsson España. Tiene tres patentes PCT concedidas y ocho solicitudes aún en proceso.