Tecnologías y soluciones para seguridad de la identidad: Valoración de su estado actual

Jose E. López, Carlos Plaza, Álvaro Armenteros, Pedro Luis Muñoz

jelg@tid.es, cplaza@tid.es, aap@tid.es, plm@tid.es

Telefónica Investigación y Desarrollo S.A.U

Ponencia

***Abstract* — Durante los últimos tres años, nuestros laboratorios del área de Seguridad en Redes y Servicios han venido identificando a la seguridad de la identidad digital y su gestión, como un factor clave para el éxito de los servicios y negocios en Internet, y en los propios procesos internos de las organizaciones. Este interés se ha materializado en la dedicación de una parte de del esfuerzo investigador de sus grupos de trabajo, a la evaluación de una serie de tecnologías y soluciones orientadas a proporcionar una mayor confianza en el uso de la identidad digital; ya sea por el usuario o por el servicio al que accede. Este breve artículo pretende presentar las principales experiencias llevadas a cabo, así como algunas de las conclusiones más interesantes que se han derivado de ellas.**

I. INTRODUCCIÓN

La creciente utilización de Internet por parte de empresas y usuarios como medio para la realización de negocios, ha hecho que todo lo que rodea a la seguridad de la identidad digital pase a convertirse en una preocupación de primer orden tanto para empresas, como para usuarios y organismos reguladores (Prueba de ello es la creación por parte de ITU-T del "*Focus Group on identity management*" para el seguimiento de estas tecnologías [1]). Las tecnologías para la gestión de la identidad, junto con las de garantía de la identidad en los procesos de autenticación, se presentan como las herramientas más adecuadas para dar soporte a esta búsqueda de seguridad en el uso de la identidad digital. Asimismo, la explosión de lo "*wireless*", junto a la naturaleza promiscua de este medio, hace que las medidas de seguridad habitualmente usadas en este tipo de accesos a redes sean insuficientes y empiece a notarse cierta preocupación al respecto [2].

Ante este escenario, nuestros laboratorios han llevado a cabo una serie de experiencias donde se ha evaluado las potencialidades que ofrecen iniciativas como Liberty Alliance, OpenID y CardSpace, en el campo de la gestión de la identidad; el nuevo eDNI y la biometría, en el área de autenticación de identidades; y las soluciones de localización en interiores, en el campo de la securización de accesos inalámbricos.

II. TECNOLOGÍAS DE GESTIÓN DE LA IDENTIDAD DIGITAL

A. Federación de identidades con Liberty Alliance

A grandes rasgos, la federación de identidades es un concepto mediante el cual se ofrece al usuario de un dominio de seguridad, la funcionalidad de *Single-Sign-On* entre diferentes dominios ("*cross-domain SSO*"), a la vez que habilita el acceso, la portabilidad y el intercambio de información de identidad a través de estos. Uno de sus máximos exponentes es la iniciativa Liberty Alliance [3]: un consorcio de más de 150 empresas de todo tipo y tamaño creado en 2001 con el objetivo de elaborar estándares abiertos y recomendaciones para la gestión de la identidad federada, con una focalización en las soluciones interoperables, la prevención del robo de identidad y la garantía de privacidad y confidencialidad del usuario.

Las experiencias que hemos llevado a cabo con "soluciones Liberty Alliance" han estado enfocadas en comprobar la disponibilidad de sus dos principales funcionalidades: El *cross-domain SSO*, que permite que el usuario pueda autenticarse una sola vez para acceder a diferentes servicios y propagar (y hacer accesible) su identidad en ellos; y el desarrollo de webservices basados en identidad, que permiten pasar de un servicio X ofrecido a todos los usuarios por igual (el concepto básico de webservice), a tener un servicio X personalizado para el usuario Y. Todo ello, a través de protocolos basados en *SAML2.0* de OASIS (el estándar "de facto" para el intercambio de información de seguridad entre entidades), que garantiza la seguridad y la privacidad de la información de identidad transmitida.

Estas nuevas funcionalidades suponen un vuelco importante en la oferta de soluciones tecnológicas para gestión de identidad y justifican su estudio, ya que las soluciones "clásicas" (metadirectorios o consolidación de repositorios, por ejemplo) no dan una respuesta satisfactoria al problema de la gestión de identidad entre dominios de seguridad diferentes (escenario presente habitualmente en Internet) al estar orientadas a tratar con la identidad en marcos con un solo dominio de seguridad (típico en escenarios de intranets o servicios de una organización)

Así, aunque las soluciones de gestión de identidad "clásicas" abordan y pueden solucionar temas como el robo de identidad, las violaciones de la privacidad, las acciones repetitivas de autenticación, una mala experiencia de usuario en el

acceso a un servicio, información de usuarios inconsistente o información de usuarios repetida (todas ellas cuestiones habituales en gestión de identidad); sin embargo, no sirven cuando el escenario planteado rebasa los límites de una organización para incluir a terceras partes totalmente independientes; es decir, con sus propios dominios de seguridad. La razón para ello es que en este tipo de soluciones "clásicas" todos los actores de un servicio "pertenecen" de alguna forma a una misma entidad (empleados o clientes de una empresa), por lo que es perfectamente factible implementar un único punto central autorizado y reconocido para tomar las decisiones sobre seguridad y privacidad. ¿Pero qué ocurre cuando los actores pertenecen a distintas entidades (un usuario reconocido en una organización trata de hacer uso de un servicio de otra organización con la que no tienen una relación previa); como típicamente se encuentra en Internet o en las relaciones inter-empresa? En este último escenario existen impedimentos legales (privacidad), tecnológicos (infraestructuras diferentes), y prácticos (costoso llegar a acuerdos entre organizaciones), que suponen un importante (y casi definitivo) obstáculo para las soluciones de gestión de identidad que hemos llamado "clásicas".

Actualmente existen en el mercado un amplio abanico de soluciones que incorporan el estándar Liberty, generalmente como parte de "suites" de software que tratan de cubrir todo el espectro de necesidades en torno a la gestión de la identidad. Prácticamente todas las grandes compañías de software cuentan con este tipo de productos, además de otros proveedores más pequeños y soluciones open-source. El grupo de trabajo ha desplegado varias de estas soluciones (openSSO, Lasso, Zxid y Software comercial) para recrear casos de usos que ilustren la potencialidad de esta tecnología: desde el SSO y la federación de múltiples cuentas, a la mejora de la experiencia de usuario a través de la personalización de servicios en base a sus datos, pasando por el intercambio de atributos de forma privada y segura entre servicios.

1) Escenarios

Como caso más sencillo se ha habilitado el Single-Sign-On del usuario en varios portales web a priori independientes: Mediante la inclusión de un proveedor de identidad y la federación de sus diferentes cuentas en dichos portales, el usuario puede acceder a cualquiera de ellos con un solo paso de login en el proveedor de identidad, siendo después su identidad reconocida en todos los portales asociados a ese proveedor sin necesidad de introducir más credenciales. Esto supone una mejora notable de la experiencia de usuario en la navegación. Este caso de negocio fue uno de los precursores de la actividad de Liberty y otras iniciativas relacionadas con la identidad, al identificarse la demanda de los usuarios de sitios .online. Es, por tanto, uno de los primeros que tuvo una solución estandarizada y probada, y consecuentemente es uno de los casos más maduros en la actualidad.

Avanzando en las potencialidades del estándar, se ha desplegado también un caso de uso donde se explota la información privada del usuario para personalizar su servicio: El usuario accede a un portal, autenticándose en el proveedor de identidad, y éste, de forma transparente, detecta si tiene contratado o no un servicio concreto que ofrece el portal a sus clientes gracias a información privada consignada durante la autenticación. Según la información obtenida, el portal presenta al usuario una oferta personalizada sobre dicho servicio. La identidad real del usuario no revelada al portal en ningún momento.

El siguiente caso de uso que se ha implementado utiliza algunos de los servicios estandarizados en Liberty: mediante el *Personal Profile* se permite compartir atributos de un proveedor de servicios en otro, y gracias al *Interaction Service* se puede pedir la autorización del usuario a la hora de compartir dichos atributos. El escenario presenta dos servicios web pertenecientes a compañías diferentes. El usuario es cliente de ambas, o puede serlo solo de una de ellas, pero en ambos casos, cuando acceder a uno de los servicios, éste puede solicitar información del usuario almacenada en el otro servicio para mejorar la oferta del suyo propio. Como siempre, los protocolos de Liberty garantizan que la identidad del usuario en uno de los servicios no es conocida en el otro. Además, el usuario es consciente de esta captura de atributos al serle solicitada autorización.

Como caso de uso más avanzado, se ha trabajado en el campo de los servicios web, tan en boga en los últimos tiempos con la eclosión de las arquitecturas SOA. Para ello se ha explorado la potencialidad de los servicios web basados en identidad, donde el usuario no utiliza un servicio genérico, sino que dispone de su propia instancia asociada. En nuestro escenario, el usuario dispone de un servicio de envío de mensajes, de forma que desde otro servicio web no relacionado con la compañía que ofrecía dicho envío, se puede utilizar su número móvil sin necesidad de que este trascendiera, preservando la privacidad de sus datos personales, pero consiguiendo toda la funcionalidad, gracias a los protocolos transparentes al usuario que "transportan" su identidad en las peticiones de servicios.

Por último, se ha podido comprobar de forma experimental la factibilidad de la incorporación de técnicas de autenticación fuerte basadas en biometría, eDNI y One Time Password, en sistemas de gestión de identidad basados en Liberty Alliance; lo que permite cerrar el círculo de la seguridad y la privacidad en el uso de la identidad digital del usuario. Así, se ha desplegado una tienda online que permite hacer el pago mediante un servicio de un tercero (con cargo a una cuenta personal sin relación con ninguno de ellos). Al ser una operación más sensible, se establece que no basta con la autenticación inicial con usuario y contraseña, y se exige una autenticación más fuerte, dándose a elegir al usuario como alternativas el uso de claves OTP o del eDNI. La autenticación toma lugar en el proveedor de identidad de acuerdo con la opción elegida. En ambos casos, si la autenticación es exitosa, como en el caso descrito del envío de mensajes, se utiliza un servicio web basado en identidad que proporciona la pasarela de pago.

2) Conclusiones

Si bien los escenarios se lograron implementar en todos los casos, y así se ha constatado el vuelco que supone en la forma de gestionar la identidad, hasta el punto de permitir la creación de nuevos servicios que de otra forma no serían abordables; también se ha comprobado la dificultad que entraña desplegar estos sistemas, donde casi para cualquier tarea hace falta personal altamente especializado con un profundo conocimiento de la especificación Liberty y conocimientos consolidados en un importante abanico de tecnologías: SAML (Cada servicio diseñado es necesario plantearlo a través de las posibilidades que ofrecen los servicios de Liberty y hay que saber interpretar los "metadata" a intercambiar en SAML); Servidores de aplicaciones y programación HTML (Es necesario configurar los servidores para habilitar ciertas funcionalidades necesarias, así como incluir peticiones dentro de formularios en el código de las páginas de las aplicaciones web); Firma digital (Los protocolos utilizados hacen uso extensivo de certificados para establecer canales seguros https); y JAVA (La mayoría de las implementaciones utilizadas usan este lenguaje, y en muchos casos es necesario añadir ciertas piezas de código para conseguir la funcionalidad deseada).

Así, aunque la seguridad de las soluciones está garantizada por el uso de SAML, y la madurez tecnológica de las diferentes implementaciones es considerable tras un par de años de evolución (también del propio estándar), la capacidad de integración de estos productos se ve mermada por el conocimiento necesario para ello, y la usabilidad tampoco es la más deseable, pues se requiere de un gran esfuerzo en el interfaz de usuario para conseguir que éste interprete correctamente lo que significan los distintos conceptos y facilidades que encierra Liberty, extremadamente técnicos. Además, los sistemas comerciales están enfocados a grandes proveedores (se ha decidido trabajar con software abierto para solucionar este problema.) Aunque a día de hoy se están mejorando estos aspectos, continúan existiendo ciertas carencias que dificulta su expansión masiva en entornos de producción, donde existe un parque amplio de servicios ya desplegados y en funcionamiento (la integración no es inocua).

No obstante, dado que estas tecnologías son capaces de resolver el problema de las múltiples identidades en Internet, consiguiendo a su vez desplegar servicios basados en identidad que de otra forma no serían abordables, tanto su potencial demanda, como su "expectativa de vida", son altas.

B. Gestión de identidad con soluciones "user-centric": OpenID y CardSpace

Los sistemas de gestión de identidad centrada en el usuario (*user-centric*) proponen ofrecer al usuario la máxima libertad posible para elegir su identidad en un servicio, y hacerle claramente consciente de la información personal que se va a utilizar y permitirle el control directo sobre la misma. Los trabajos realizados por nosotros permiten concluir que, entre los sistemas que responden a este concepto, son dos los que parecen tener mayor impulso: OpenID y CardSpace

1) OpenID

El identificador del usuario es una "URL" suministrada por un proveedor de identidad elegido por el usuario (Ej.: http://www.miIdP.com/maria). Es una iniciativa que nació y que crece en el mundo del software abierto, siendo el desarrollo de sus especificaciones un proceso colaborativo soportado en Internet [4]. La experiencia desplegada ha conseguir crear un proveedor de identidad basado en librerías de software abierto y se ha probado con servicios reales de Internet que admiten OpenID (blogs, redes sociales, wikis). En cuanto a la usabilidad, el usuario debe teclear en cada servicio su URL; aunque este aspecto se está mejorando con la introducción de *widgets* que permiten seleccionar de una lista los proveedores más populares y así evitar tener que recordar la URL completa.

La sencillez de despliegue es lo más destacado, al no requerir el establecimiento previo de relaciones de confianza entre servicios y el proveedor de identidad que sí exige SAML 2.0, así como la facilidad de integración con aplicaciones web ya existentes o sistemas de almacenamiento de datos (LDAP o bases de datos relacionales) gracias a los desarrollos disponibles en software abierto. Se ha usado la versión 1.2 de OpenID por disponerse de un servidor completo que se despliega rápidamente, aunque ya está disponible la versión 2.0 en forma de librerías, que introduce mejoras de seguridad. Así, esta nueva versión, más las mejoras en usabilidad, la introducción de autenticación fuerte en los proveedores de identidad y los trabajos de integración que se están desarrollando con los otros sistemas citados en este artículo, van a ayudar a alcanzar una mayor madurez en este sistema de gestión de identidad, así como promover su difusión.

Sin embargo, presenta una serie de problemas que disuaden de su aplicación en situaciones con información confidencial o valiosa: ausencia de "círculos de confianza" (que permite que cualquiera pueda crear un proveedor de identidad o de servicio malicioso para capturar credenciales de usuario), el servicio no tiene conocimiento del tipo de autenticación en el proveedor de identidad, aunque se resuelve en la versión 2, o el riesgo de trazabilidad al tener que presentar en todos los servicios el mismo identificador (al contrario que en SAML 2.0, donde los identificadores de un usuario dados a conocer al servicio no pueden ser relacionados unos con otros). Estos problemas, que no están impidiendo la expansión de OpenID, sí están limitando a los grandes actores de Internet a ser proveedores de identidad pero sin admitir en sus servicios identificadores OpenID de terceros.

2) CardSpace

CardSpace [5] es un sistema propuesto por Microsoft basado en estándares de la familia de protocolos WS-*. Existen iniciativas compatibles para otras plataformas, como Higgins u OpenInfoCard.

Se basa en el manejo de “tarjetas de información”: Un proveedor de identidad proporciona una “tarjeta” que el usuario gestiona en su equipo mediante un componente denominado “selector de identidad”. La tarjeta contiene información firmada sobre el emisor, métodos de autenticación asociados, o datos de usuario que puede proporcionar el emisor. A su vez, los servicios indican los requisitos que debe cumplir la tarjeta que permite acceder al usuario y el selector presenta visualmente al usuario las tarjetas válidas. El usuario podrá revisar los datos que el servicio solicita y, una vez que escoge una, se autentica en el proveedor de identidad, que suministrará la corroboración de la identidad y los datos.

En la experiencia realizada, se han desplegado un proveedor de servicios que simula ser una tienda online y que admite tarjetas de identidad. Se ha usado distintas combinaciones de emisores de tokens de seguridad o STS (proveedores de identidad) como Xmldap.org y Microsoft; navegadores (Internet Explorer 7, que incorpora el tratamiento de tarjetas, y Firefox instalando un plugin); selectores de identidad (el propio de Microsoft Windows y “Digital Me” del proyecto “Bandit”) y proveedores de servicio mezclando distintos productos que implementan los protocolos de este sistema (código en Visual Basic para entorno Windows, módulo para Apache de SourceId y Xmldap.org). Algunas de las opciones fueron descartadas por la imposibilidad de ponerlas en funcionamiento, y los selectores han dado muestras de inestabilidad, de tal manera que al tiempo de funcionamiento quedaban inoperativos, lo que indica que hay un recorrido importante hasta lograr la madurez de esta tecnología. En cuanto a su integración con otros sistemas, como se ha señalado en el apartado anterior, están realizándose diversas pruebas de interoperabilidad para transportar identificadores openID en tarjetas de información, o asociar un tarjeta como método de autenticación a OpenID, así como el uso de tarjetas en entornos Liberty (en el ámbito del proyecto Concordia: projectconcordia.org)

Como conclusión de la experiencia en nuestros laboratorios, se considera que es un sistema prometedor, sobre todo por el novedoso concepto del “selector de identidad”, que aporta un símil con el mundo real de las tarjetas de identidad en posesión de una persona, que permite un uso intuitivo por parte del usuario (algo clave para el éxito de estas iniciativas). Actualmente están en marcha escenarios de interoperabilidad entre proveedores SAML 2.0 y proveedores de tarjetas de información, pero es un sistema menos maduro que los otros tratados en este artículo, y su expansión estará supeditada al éxito de Windows Vista, donde viene incluido, y a la existencia de kits para los diversos entornos más sencillos de instalar. Asimismo, también es necesario plantear mejoras en diversos aspectos como la portabilidad de tarjetas entre equipos o una mayor flexibilidad en el tratamiento de los datos de usuario que se pueden manejar.

III. TECNOLOGÍAS PARA LA AUTENTICACIÓN Y GARANTÍA DE LA IDENTIDAD DIGITAL

De los principios básicos de la seguridad electrónica (autenticación, autorización, integridad, confidencialidad y no repudio) la autenticación, definida como el proceso mediante el cual se confirma la identidad presentada por un usuario, es la pieza fundamental en la que se basa el intercambio de información confidencial. En este sentido, nuestras experiencias han estado centradas en explorar las características prácticas, potencialidades y problemáticas relacionadas con el uso de las tecnologías comúnmente asociadas a la llamada “autenticación fuerte” (basada en factores de autenticación con altos niveles de confianza o en la mezcla de varios de ellos para obtener sinergias en la confianza de la autenticación resultante); para lo cual se ha seleccionando soluciones representativas de este tipo de soluciones: Las técnicas biométricas (autenticación basada en el factor “lo que soy”), el DNI electrónico o eDNI (autenticación basada en “lo que tengo” más “lo que se”) y las contraseñas de un solo uso (que no comentaremos aquí por ser sobradamente conocidas y estar disponibles ya en numerosos servicios).

A. Biometría

La biometría consiste en la identificación automática de manera única de personas mediante sus características fisiológicas o de comportamiento (huellas dactilares, el mapa de su iris, la geometría de la mano, etc.) Esta tecnología siempre ha sido considerada como la solución definitiva que garantiza la identidad de una persona[6], pero los estudios realizados aconsejan ser menos optimistas en este aspecto[6]. Así, presentan aún cierta falta de practicidad y capacidad de integración en terceros procesos que las desaconsejan para entornos de negocio donde el precio de la tecnología que se repercute al usuario, la usabilidad, la escalabilidad o la seguridad son factores principales que deciden la adopción o no de una tecnología

En nuestros laboratorios se trabajó con diversas soluciones comerciales de reconocimiento de huella digital, facial y del iris, así como del mapa de venas de la mano y otras modalidades menos comunes (encefalograma). Se articularon dos escenarios objetivo: Por un lado; el acceso físico a un lugar (por ejemplo, a un PC), y por otro, la identificación del usuario como parte del proceso de autenticación de un servicio web; el más interesante para asegurar la identidad del usuario que accede remotamente.

En todos los casos fue necesario realizar una integración “ad-hoc” de los dispositivos en el escenario de prueba (base de datos particular, interfaces de usuario diferentes, etc.), y si bien se podía seguir el estándar BioAPI para el tratamiento de la información biométrica una vez realizada la extracción de la característica, lo cierto es que el seguimiento del estándar en sí mismo tampoco era del 100%, lo que en la práctica requería retocar también parte del código encargado de tratar los patrones.

Adicionalmente, las técnicas no intrusivas (como el iris o el reconocimiento de la cara) denotaron cierta necesidad de colaboración voluntaria por parte del usuario que, en principio, no ayudan a la usabilidad de este tipo de soluciones, así como condiciones especiales de contexto (luz ambiente) que aunque son factibles para el control de acceso físico, no son controlables en una autenticación remota como la requerida para el acceso a un servicio web. Es en este escenario de acceso remoto donde las soluciones biométricas presentan más problemáticas, al necesitar tener un dispositivo en "casa" del usuario y, por tanto, fuera del control del que ofrece el servicio, así como costear una licencia del software de captura que bien podría ser un lastre económico para la aceptación de estas soluciones por parte del usuario.

Por último, en muestras de entre 40 y 60 personas (dependiendo de la técnica), los ratios de acierto en algunas de las soluciones eran muy bajos, dependiendo mucho de la calidad del registro que se hubiese hecho. Esto, para una técnica que se supone de "autenticación fuerte", supone un problema.

No obstante, hay que destacar que la huella digital ha presentado resultados bastante aceptables, habiendo conseguido desarrollar prototipos para autenticar remotamente desde web y utilizando la huella digital, a usuarios en servicios web; así como para integrar este tipo de autenticación en soluciones de gestión de identidad basadas en Webservices (como Liberty Alliance). Adicionalmente, se ha contemplado el uso de la biometría como factor adicional para proteger un certificado almacenado en una tarjeta inteligente (tarjetas biométricas), de forma que la comparación del patrón biométrico se realiza dentro de la tarjeta, impidiendo su manipulación directa; así como un estudio teórico relativo a las "claves biométricas", basadas en técnicas híbridas que unen biometría y criptografía, que aunque aún está en fase de concepto, resulta prometedora para generar una encriptación "personalizada" que solo el usuario será capaz de descifrar a través de la presentación de su huella digital, por ejemplo.

B. eDNI

En España, la adopción del eDNI puede suponer un punto y a parte en la autenticación de usuarios en servicios web. Su carácter institucional y el estar basado en una tecnología madura y ampliamente aceptada, lo hace un claro candidato a convertirse en el estándar de autenticación "de facto" a corto/medio plazo[7]. Por esta razón, se ha considerado el estudio de las características de esta solución, así como las posibilidades de uso que presenta, como parte de las experiencias llevadas a cabo.

El escenario planteado para su estudio ha consistido, básicamente, en el análisis de sus partes "hardware" y en la experimentación con API de acceso desde aplicaciones. En los servicios web simulados, se detectaba cuándo estos requerían una autenticación más fiable que la simple "usuario/contraseña" y se procedía a solicitar por interfaz web la inserción de un DNIe válido. Una vez introducido en un lector de tarjetas del PC, se trataba de acceder al certificado de autenticación y posteriormente se validaba éste por OCSP contra los servidores habilitados para ello por la autoridad certificadora. La experiencia en sí misma trataba de validar el uso del DNIe en sí mismo, ya que las tecnologías envueltas en él ya eran sobradamente conocidas y utilizadas.

Así, se ha comprobado que es posible configurar el acceso a una aplicación web de forma que la autenticación se realice mediante el nuevo eDNI, lo que acarrea una serie de ventajas directas sobre otro tipo de soluciones de autenticación: Es cómodo y fácil de usar para el usuario; y se trata de un documento que siempre porta el usuario (ya que es su DNI), por lo que es de esperar que le preste unas atenciones que no siempre dispensa otro tipo de credenciales: Aviso de sustracción o pérdida, mantener el PIN en secreto y ser menos susceptible al olvido. No obstante, el eDNI también presenta algunos problemas de usabilidad para el personal no técnico. Así, todo acceso con HTTPS requiere confirmación de PIN, lo que puede hacer pensar al usuario que el servicio al que accede le está solicitando datos personales, cuando no es así, y decidir no acceder. De igual forma, cualquier acceso a un servicio protegido por eDNI requerirá el PIN dos veces (para leer el certificado, y para firmar)

IV. SOLUCIONES DE LOCALIZACIÓN EN INTERIORES APLICADAS AL CONTROL DE ACCESO

A. Concepto básico

Convencionalmente, en el proceso de identificación y autenticación de un usuario suele utilizarse hasta tres factores de autenticación (lo que el usuario conoce, lo que tiene y lo que es). Sin embargo, el creciente uso de las tecnologías de localización y posicionamiento, así como de los servicios de valor añadido basados en localización ha llevado a proponer recientemente el uso de ésta en el área de la seguridad y la gestión de de identidad [8], añadiendo un factor extra ("dónde está el usuario") a los tres típicamente utilizados.

Gran parte de los nuevos servicios basados en localización se centran en el uso de tecnologías para entornos de exteriores y amplias coberturas [9]. Ejemplos son las basadas en sistemas satelitales (ej. navegación), o los que utilizan información de la red GSM (ej. tarificación según localización). Para complementar a las tecnologías de localización que ofrecen servicio sólo en zonas abiertas (como GPS) o que no ofrecen una gran precisión (como técnicas convencionales basadas en ID de celda en GSM), se encuentran las tecnologías de localización en interiores (o ILS, *Indoor Location System*) [10]. Éstas permiten

localizar a un usuario con mayor precisión, así como en entornos cerrados como edificios u hogares, lo que abre posibilidades a ofrecer servicios diferenciados. Existen diversas tecnologías ILS, siendo éste un campo de creciente interés en el mundo de la I+D+i.

Los usos ya propuestos de la información de localización se centran principalmente en ofrecer servicios de entretenimiento, información dinámica basada en la localización, etc. Incluso se ha considerado la localización como información adicional para ofrecer servicios personalizados una vez que el usuario ha sido identificado en servicios de gestión de identidad como Liberty [11]. A pesar de este creciente interés, la localización apenas ha sido utilizada para mejorar la seguridad y el proceso de identificación, autenticación y autorización de usuario. Sin embargo, su interés en esta área es claro, y ya ha sido mencionado como un aspecto a tener seriamente en cuenta en la gestión de identidad [12]. Un primer paso supone utilizar la localización como factor para autorizar/denegar el acceso a recursos o servicios, siendo esta una solución ya utilizada (por ejemplo en escenarios de banca online, en los que puede no permitirse realizar ciertas operaciones sensibles desde el extranjero). Sin embargo, una localización más fina o precisa permite llegar un paso más allá, en el que se combine identidad y localización para mejorar la seguridad, o en el que se pueda relacionar una identidad con localizaciones esperadas o vinculadas a dicha identidad. Algunos de los escenarios donde la localización combinada con la identidad permite añadir un grado más en la seguridad o autenticación son:

· gestión de acceso selectivo según la localización de usuario: se trata de realizar un control de acceso a recursos de red o servicios dinámico, que permita/deniegue el acceso teniendo en cuenta no sólo quién accede, sino también desde dónde accede. Por ejemplo, en un escenario de oficinas se puede proteger el acceso a recursos privados desde zonas comunes (salas de reuniones, zonas de descanso...) permitiendo el acceso desde dichas zonas sólo para ciertos perfiles de usuario. De este modo se mejora la seguridad de los recursos accesibles en red.

· realización de comprobaciones de consistencia de localización para asegurar una identidad: mediante el control de la ubicación del usuario, ya sea en cada intento de acceso o bien periódicamente, se puede comprobar si hay inconsistencias en la localización (intentos de acceso desde sitios muy alejados en cortos periodos de tiempo) de un cierto usuario que dice tener cierta identidad, reduciendo así el riesgo de suplantación.

· autenticación por proximidad de usuario: múltiples soluciones permiten realizar la identificación de usuario mediante tecnologías de comunicación por proximidad o corto alcance (RFID, NFC, Bluetooth etc). De este modo se comprueba no sólo la identidad del usuario, sino también que éste se encuentra en cierta ubicación, y se simplifica el proceso de identificación y autenticación de usuario.

Hay que hacer notar que, salvo casos marginales, únicamente la información de localización de un usuario no permite realizar una autenticación fiable de por sí, por lo que se debe utilizar en combinación con uno o varios métodos de autenticación convencionales.

Como ejemplo de aplicación de los conceptos anteriores, en el laboratorio hemos llevado a cabo una prueba de concepto de un sistema de control dinámico de acceso a recursos a través de la red Wi-Fi que combina información de identidad y de localización obtenida a través de la propia señal de red para autorizar o rechazar el acceso a recursos de red. A continuación se presenta el esquema general implementado, y se resumen las principales pruebas realizadas.

B. Solución específica: sistema dinámico de control de acceso a recursos Wi-Fi basado en localización e identidad.

Un escenario donde la localización permite incrementar la seguridad en el control de acceso a recursos es el del acceso Wi-Fi en un edificio corporativo, o escenario tipo “oficinas”. Con el objetivo de cubrir dicho escenario, se ha desarrollado un sistema que realiza un control de acceso dinámico a recursos compartidos en la red corporativa. Para llevar a cabo el control de acceso, se tiene en cuenta no sólo la localización del usuario que accede a los recursos, sino también la identidad del mismo. Así, un usuario invitado que se encuentra en una sala de reuniones tendrá permisos para acceder a Internet y así poder consultar su correo, pero se le denegará el acceso a la intranet corporativa u otros recursos privados (repositorios, bases de datos, etc), protegiendo así dichos recursos privados y a la vez ofreciendo conectividad hacia el exterior al invitado. Un usuario que sea personal de la empresa, en la misma sala de reuniones sí podrá acceder a ciertos recursos privados (como acceso a la intranet corporativa o a su repositorio en red), facilitando así su trabajo. Sin embargo, a este mismo usuario se le podrá denegar el acceso a recursos privilegiados cuando se encuentre en zonas comunes o áreas de descanso (zona de entrada de edificio, etc…), para proteger la información privada de un eventual robo de identidad.

El sistema implementado consta de varios módulos, que se muestran esquemáticamente en la figura 1. La solución está basada en separar la red de acceso Wi-Fi de la red donde se encuentran los recursos a proteger, mediante un módulo de control de acceso o *firewall* adaptativo, diseñado específicamente para este caso. Las reglas de filtrado de dicho firewall cambian en tiempo de operación, para adecuarse a cambios en la localización de los usuarios activos y para considerar nuevos usuario que se identifican. A continuación se describe de forma general cada uno de los módulos que conforman la solución. Una descripción detallada de los mismos queda fuera de los objetivos de este artículo.

· **módulo de autenticación y base de datos**: es el módulo encargado de recibir las peticiones de conexión a la red Wi-Fi por parte de los usuarios, y de gestionar el proceso de autenticación. La información de autenticación (ID y clave) se registra previamente una base de datos, consultada por el módulo de autenticación durante dicho proceso. Además, este módulo se encarga de actualizar la información de usuarios en la base de datos, una vez que la autenticación ha sido realizada con éxito.

Para las pruebas realizadas, la autenticación se ha basado en un sencillo mecanismo de usuario/contraseña. Para evitar problemas de robo de identidad y suplantación, se ha utilizado un protocolo seguro de intercambio de credenciales, en concreto el especificado en el estándar 802.1x basado en WPA2 y EAP-MSCHAPv2, que utiliza un servidor de tipo RADIUS para realizar la autenticación. Además, con este método se asegura la confidencialidad de la información intercambiada gracias al uso de una clave dinámica para cifrar los datos. Estos protocolos se encuentran estandarizados y son típicamente utilizados en redes Wi-Fi con cierto nivel de seguridad (como las empresariales). La base de datos contiene también información sobre las políticas del sistema, los posibles permisos y los perfiles de usuario y de zonas del sistema, así como otros datos necesarios para el funcionamiento del sistema, como el tipo de localización asignada a un usuario.

· **módulo de localización**: cumple la doble función de estimar la localización de los usuarios activos en el sistema y ofrecer dicha información al módulo de gestión de acceso cuando sea necesario. La información de localización se ofrece en tiempo real, entendiendo por ello que se requieren sólo unos pocos segundos para actualizar dicha información. De este modo, se pueden tomar las decisiones de permitir o denegar el acceso dinámicamente, respondiendo a los cambios de localización de los usuarios en cada momento. La localización se puede estimar utilizando diversos sistemas, siendo los de localización en interiores (ILS) muy adecuados para este escenario de oficina. El sistema fue implementado de modo que permitiese el uso simultáneo de múltiples servidores de localización, mediante la inclusión de un submódulo de gestión de la localización. En concreto, las pruebas realizadas se han basado en dos métodos: localización basada en la propia señal Wi-Fi y localización basada en RFID (Radio Frequency Identification) activo.

· **Módulo de gestión de acceso**: es el módulo central del sistema, donde se toman las decisiones sobre permitir o rechazar el acceso a los recursos por parte de los usuarios. Como entradas toma en cuenta la información de autenticación y la de localización. La información de autenticación es actualizada por el módulo de autenticación cada vez que un usuario se conecta a la red Wi-Fi, incluyendo dicha información en la base de datos, que es consultada por el módulo de gestión de acceso. La información de localización es obtenida por el módulo de gestión de acceso a través del submódulo de gestión de localización, que se encarga de hacer las peticiones de localización de usuarios periódicamente. Como resultado, el módulo de gestión de acceso envía las decisiones sobre los permisos a aplicar para cada usuario, siempre que haya un cambio en dichos permisos (si hay un usuario nuevo en el sistema, si hay un cambio de zona de un usuario, etc…).

· **Módulo de control de acceso adaptativo**: es el módulo que lleva a cabo el control efectivo de las transferencias de información o acceso a recursos. Se ha implementado como un cortafuegos cuyas reglas de filtrado cambian dinámicamente, en función de las órdenes enviadas por el módulo de gestión de acceso. Los recursos accesibles para cada usuario se especifican con su dirección IP, mientras que los paquetes procedentes de cada usuario se identifican en función de la MAC del equipo de usuario.

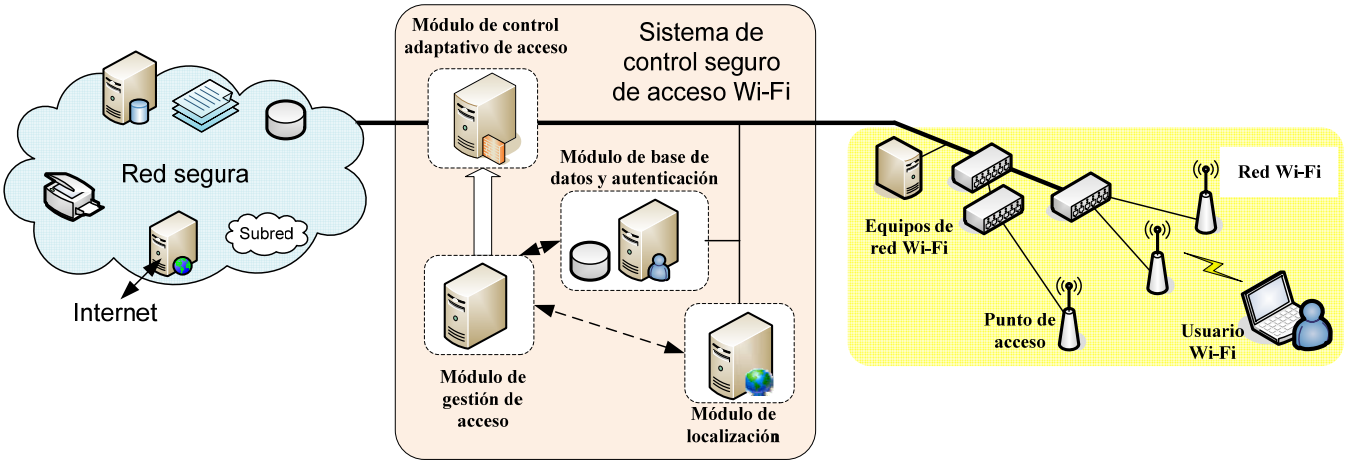

Fig. 1. Arquitectura general del sistema de control de acceso Wi-Fi implementado para evaluar el uso de la localización como factor extra en la seguridad e identidad.

El funcionamiento general del sistema se puede resumir como sigue: cuando un usuario intenta conectarse a la red Wi-Fi, el módulo de autenticación le pregunta sus credenciales (ID y clave de acceso), y comprueba dicha información en la base de datos. En caso de ser correcta, se indica en el repositorio que dicho usuario está autenticado, y se incluyen otros datos necesarios sobre su conexión (MAC, perfil de usuario). A partir de ese momento, el módulo de localización estima la ubicación del usuario periódicamente. El módulo de gestión de acceso comprueba periódicamente qué usuario están autenticados en el sistema, si están activos y dónde se encuentran, y toma una decisión sobre los permisos asignados, en función de la política de acceso definida en el sistema. En concreto, las políticas especifican los recursos disponibles en función del tipo de usuario (perfil de usuario) y el tipo de localización (perfil de zona), y son definidas por el administrador en una etapa previa de configuración. Finalmente, el módulo de control de acceso adaptativo aplica los permisos asignados filtrando los datos de los usuarios. Este proceso se repite periódicamente, de forma que cuando la localización de un usuario

cambia, el módulo de gestión de acceso observa la nueva localización de usuario a través del servidor de localización correspondiente, y cambia los permisos del usuario provocando un cambio en las reglas de filtrado.

C. Pruebas y evaluación

Para evaluar las mejoras obtenidas con el sistema propuesto de control dinámico de acceso seguro a través de Wi-Fi, se llevó a cabo una campaña de medidas y pruebas. Se seleccionó un entorno de oficinas, en concreto se consideró una planta de un edificio de Telefónica I+D, donde se encuentra varios tipos de zonas. En concreto se consideraron tres tipos de zonas: área general (bajo nivel de confianza), salas de reuniones (nivel medio de confianza) y oficinas privadas (nivel alto de confianza). También se consideraron varios perfiles de usuarios (invitado y empleado). Se definieron unas políticas de acceso, considerando como recursos a acceder el Proxy de Internet (acceso a Internet, con bajo nivel de seguridad) y el portal de la Intranet (recurso con mayor nivel de seguridad). Se realizaron pruebas funcionales con varios usuarios y ubicaciones, mostrando el correcto funcionamiento tanto en situaciones estáticas (ubicación fija) como dinámicas (cambio de ubicación mientras se accede a un recurso), y demostrando que el sistema permite mejorar la seguridad evitando accesos indeseados. Además, se realizó un análisis de precisión en localización para dicho entorno con la solución ILS basada en medida de señal Wi-Fi, obteniéndose un error promedio de 1.6m, que demostró ser suficiente para este tipo de entornos de oficina. También se realizó un estudio de vulnerabilidades del sistema, que se omite aquí por razones de espacio, pero del que una de las principales conclusiones fue que la solución es muy sensible a las vulnerabilidades del sistema de localización utilizado, y que se debe prestar atención a evitar que el usuario falsee su localización. Como ejemplo, se comprobó que para determinadas localizaciones, un usuario fuera de una zona puede falsear su localización en el sistema ILS basado en medidas de potencia de señal Wi-Fi utilizando una antena directiva, problema que se reduce significativamente teniendo en cuenta cálculos de probabilidad de error en la estimación de localización, para detectar la falsificación de ubicación.

VII. CONCLUSIÓN

Los trabajos llevados a cabo en nuestros laboratorios han permitido conocer el alcance potencial de las actuales tecnologías para la seguridad de la identidad. Los resultados obtenidos sugieren que estas tecnologías son una realidad en su mayoría, y que representan la mejor herramienta para dotar de confianza al uso de la identidad, pero su adopción por los diversos actores interesados resulta lenta debido a ciertos aspectos no cerrados de su desarrollo. No obstante, es previsible que en los próximos años estas tecnologías, u otras basadas en ellas, terminen por implantarse para dar respuesta a la demanda de seguridad que empezará a pedir el usuario y los servicios que se le ofrecen. Por su parte, la utilización de la localización en la autorización de accesos inalámbricos, se presenta como una buena solución para tratar de responder a la creciente demanda de securización de estos, pero aún no puede decirse que se trate de una solución final.

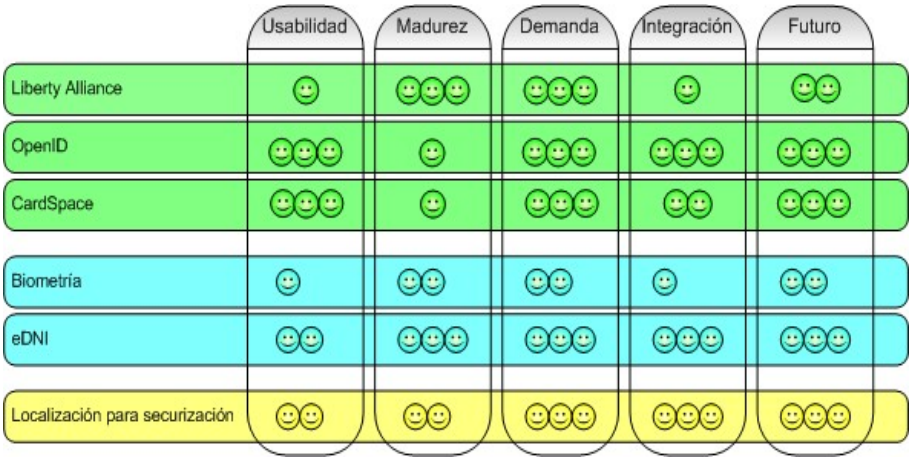

Fig. 2. Valoración de la usabilidad, madurez alcanzada, demanda de su funcionalidad, capacidad de integración en terceros sistemas y sus perspectivas de futuro, de las tecnologías trabajadas.

REFERENCIAS

[1] ITU-T Focus Group on Identity Management (http://www.itu.int/ITU-T/studygroups/com17/fgidm/index.html)
[2] B. Fryson para Associatedcontent: “Study: Passwords Alone Not Enough to Keep Wireless Networks Secure”, Agosto 2007 (http://www.associatedcontent.com/article/355815/study_passwords_alone_not_enough_to.html).
[3] Liberty Alliance project (http://www.projectliberty.org)
[4] OpenID.net, “Especificaciones OpenID” (http://openid.net/developers/specs/)
[5] Microsoft, “What is Windows CardSpace?” (http://netfx3.com/content/WindowsCardspaceHome.aspx)
[6] Peter Gutmann, “Why biometrics is not a Panacea” (http://www.cs.auckland.ac.nz/~pgut001/pubs/biometrics.pdf)
[7] J. L. Díez Aguado, “DNIe. La nueva identidad del ciudadano” (http://www.revista-ays.com/DocsNum16/SeguridadEstado/Diez.pdf)

[8] Mark Willoughby, “No agreement on Oath authentication”, Computer World versión digital, 2005.
[9] Berg Insight, “LBS Temperature Meter 2008” technical report, 11 March 2008.
[10] Hui Liu, H. Darabi, P. Banerjee, Jing Liu, “Survey of Wireless Indoor Positioning Techniques and Systems,” , IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, vol. 37, no 6, pp. 1067 – 1080, Nov. 2007.
[11] “Liberty Alliance ID-SIS Geo-Location”, Web Services Applications Brief, disponible en www.projectliberty.org.
[12] A. Antonopoulos, “Location and Presence Take Identity Management to Next Level,” Network World, 10th May 2004.