Cómo las administraciones públicas pueden beneficiarse de los estándares abiertos de mensajería instantánea y P2P

Jose Luis Hevia Oliver
Senior Software Architect
Alhambra-Eidos™
joseluis.hevia@a-e.es

José Carlos Díaz García
Business Manager Government Solutions
Alhambra-Eidos™
josecarlos.diaz@a-e.es

Prólogo

Durante mucho tiempo, la empresa ha sido el terreno donde maduraban la mayor parte de las tecnologías TI, que sólo después eran exportadas al mercado de consumo. Pero Internet está consiguiendo invertir el proceso en muchos casos, como es el de la mensajería instantánea (IM).
La Mensajería Instantánea es el canal de comunicación con el crecimiento más rápido nunca visto**.** Está creciendo más rápido que el uso del teléfono y el teléfono móvil, más rápido que el uso del e-mail. A pesar de que se tiende a asociar esta forma de comunicación con un uso adolescente, la mensajería instantánea está cada vez mejor establecida en el mundo de la empresa como una eficiente herramienta de colaboración y la realidad demuestra que usuarios online de todas las edades confían en ella como una tecnología de comunicación clave.
Para muchos trabajadores del conocimiento, la mensajería instantánea es ya una necesidad tan crítica como el acceso a un teléfono o al correo electrónico, con las ventajas que supone lo siguiente:

- Posibilidad de comunicarse a través de redes IP entre dispositivos tanto fijos como móviles.
- Comunicación basada en voz, video y datos
- Incorporación de los últimos estándares de seguridad, tanto en el cifrado de datos como la autenticación del usuario
- Permitir la comunicación a través de servidores públicos, privados o P2P dependiendo de cada solución de mensajería y el protocolo de IM empleado.
- Permitir mensajes offline, cuando los destinatarios están desconectados
- Posibilidad de habilitar un control de presencia de usuarios
- Capacidad de acceder a herramientas y servicios
- Capacidad de distribución de nuevos productos y servicios

De la misma manera que el despliegue del correo electrónico en las corporaciones a principios de la década de los 90 ha demostrado ser una de las contribuciones incuestionables a la mejora de las relaciones y los negocios entre las personas y entre las organizaciones, muchos analistas consideran que ya está ocurriendo un fenómeno similar con la mensajería instantánea.
Algunos analistas de Gartner[1] predicen que a finales de 2011, la mensajería instantánea se convertirá en la herramienta por excelencia para las comunicaciones de voz, vídeo y texto en tiempo real con fines de negocio. Según la consultora, las organizaciones que aún no la hayan incorporado a sus procesos críticos de negocio, deberían de comenzar a planteárselo.
Todo ello hará que, de cumplirse las previsiones de Gartner, en 2013 más del 95% de los trabajadores de las principales organizaciones globales utilicen IM como principal interfaz para las comunicaciones en tiempo real. En cuanto al valor del mercado mundial de IM empresarial, la firma estima que crecerá desde los 267 millones de dólares que generó en 2005 hasta los 688 millones de dólares en 2010.
Pioneros de este tipo de aplicaciones fueron el archiconocido protocolo IRC de internet, el revolucionario concepto de ICQ y el relevo de éste tomado por Microsoft Windows Messenger. Aplicaciones que en la actualidad han demostrado ser más utilizadas casi que el propio correo electrónico, visto que mantienen un nivel de interacción más efectivo que dichas herramientas.
Las tecnologías actuales y la oferta de productos comerciales de IM existente permiten ofrecer una gama de soluciones muy amplia a las necesidades de comunicación online y offline de organizaciones y personas.
Alhambra-Eidos™[11] tiene muchos años de experiencia, así como algunos productos propios, en el mercado de las plataformas de mensajería (e-mail, SMS, Fax, IM). En el caso particular de la mensajería instantánea ha desarrollado además una plataforma experimental basada en estándares abiertos que le ha permitido explorar a fondo uno de los protocolos de IM más extendidos en el mundo: Jabber®.
En este artículo, los autores desean exponer su visión sobre las tecnologías que rodean el concepto de mensajería instantánea así como sus posibles usos.

La IM en la Era de los Trabajadores del Conocimiento

En 1969, Peter Drucker[2], uno de los autores más importantes de la literatura moderna del "management", en su libro más conocido "La era de la discontinuidad", escribió una sección sobre "la Sociedad del Conocimiento", basándose en una serie de datos y proyecciones económicas de Fritz Machlup (uno de los primeros autores en acuñar la expresión "Sociedad de la Información"). Drucker se interesó siempre por la creciente importancia de los trabajadores que trabajaban con sus mentes más que con sus manos, lo que vendría a denominarse posteriormente Trabajadores del Conocimiento. A diferencia del trabajador manual, el Trabajador del Conocimiento es dueño de los medios de producción que son precisamente sus conocimientos.
Actualmente vivimos en la era de los Trabajadores del Conocimiento. Muchos de nosotros lo somos en las organizaciones para las que trabajamos, bien sean AA.PP. o empresas.
Trabajamos exclusivamente con información y para ello necesitamos emplear una amplia variedad de herramientas y sistemas de comunicaciones. Estos sistemas han ido evolucionando a medida que se han planteado nuevos retos de gestión en las organizaciones con la mejora de la competitividad y la productividad siempre presentes.
La IM es precisamente la herramienta de comunicación entre Trabajadores del Conocimiento que más se está extendiendo por sus bondades, que nos permiten intercambiar, compartir o distribuir información de forma fiable, inmediata y segura.

¿Qué es y cómo funciona la mensajería instantánea?

La mensajería instantánea es un sistema de comunicación que permite la transmisión de datos en tiempo real entre grupos cerrados de usuarios, incluso cuando el destinatario no está conectado.
La mensajería instantánea requiere el uso de un cliente informático que realiza el servicio de IM y que se diferencia del correo electrónico en que las conversaciones se realizan en tiempo real. Existe una gran variedad de clientes de IM (también llamados mensajeros instantáneos) en el mercado (gratuitos o de pago, como aplicación de escritorio o web). Los mensajeros instantáneos más utilizados son ICQ[3], Yahoo! Messenger[4], Windows Live Messenger[5], AIM (AOL Instant Messenger)[6] y Google Talk[7] (que usa el protocolo abierto Jabber®). Estos servicios han heredado algunas ideas del viejo, aunque aún popular, sistema de conversación IRC[8]. Cada uno de estos mensajeros permite enviar y recibir mensajes de otros usuarios usando los mismos software clientes, sin embargo, últimamente han aparecido algunos clientes de mensajerías que ofrecen la posibilidad de conectarse a varias redes al mismo tiempo (aunque necesitan registrar usuario distinto en cada una de ellas). También existen programas que ofrecen la posibilidad de conectarse a varias cuentas de usuario a la vez como MSN.
La mayoría de estos mensajeros usan las redes propietarias de las diferentes clases de software que ofrecen este servicio. Por otra parte, existen programas de mensajería instantánea que utilizan protocolos abiertos como Jabber®[9], con un conjunto descentralizado de servidores.

Usos empresariales de la mensajería instantánea

Citando nuevamente a Gartner, la mensajería instantánea está pasando de ser un "extra" utilizado por determinados grupos de empleados a convertirse en parte clave de la infraestructura de colaboración empresarial y está erigiéndose como una alternativa cada vez más robusta a las comunicaciones "ad hoc" tradicionales, como las llamadas telefónicas y correos electrónicos, para resolver determinados asuntos en los que la inmediatez de una interacción en tiempo real constituye un valor esencial. Constituye sobre todo una valiosa herramienta para compartir ideas y opiniones en encuentros virtuales y videoconferencias organizadas. La IM, debido a su riqueza digital posibilita establecer en una misma sesión intercambio de mensajes, voz, pizarras, control remoto… etc.
Las organizaciones que apuestan por introducir este tipo de plataformas de IM, tradicionalmente eligen soluciones de mensajería instantánea de nivel empresarial que ofrecen diferentes fabricantes, incluidos IBM y Microsoft. Pero la creciente aceptación de la mensajería instantánea en las empresas está llevando a muchos proveedores de IT a desarrollar aplicaciones IM capaces de satisfacer los requerimientos propios de estos entornos, más allá de las herramientas originariamente diseñadas para el segmento de consumo. Gartner también espera que el nivel de penetración de las herramientas de IM de clase empresarial aumente desde el 25% actual hasta casi el 100% a finales de la década.
Pero las aplicaciones de la IM en el mundo de la empresa van mucho más allá de la propia comunicación humana. Mediante la IM, es posible comunicar entre sí los sistemas de información, creando así un entorno convergente que en el que intercambiar cualquier tipo de información, en cualquier contexto y de la misma forma. La convergencia aportará niveles de colaboración excepcionales y nunca vistos en las relaciones humanas, empresariales e institucionales.

La importancia de los estándares abiertos: Jabber®

Si Internet se ha convertido en la revolución de los canales de comunicaciones mundiales, ha sido precisamente por su carácter abierto, estándar y accesible a las tecnologías. El no haber sido desarrollado con carácter propietario ha hecho que Internet evolucione como un ecosistema en el que hemos participado –y estemos participando- todos.
En el concepto de la IM ocurre lo mismo. Si un fabricante "A" construye un producto empleando la tecnología IM "A", se estará acotando el contexto a lo que el fabricante decida en un momento que le es beneficioso. Y esto siempre coartará las posibilidades de la plataforma. En cambio, empleando estándares abiertos, será la propia comunidad la que vaya incorporando nuevos contextos y posibilidades para que todo el mundo las aproveche. Lo que siempre redundará en sistemas de mejoras continuas e infinitas posibilidades.
Precisamente por la importancia que tiene la IM en el futuro –si no, presente- de las comunicaciones, es por lo que se ideó el protocolo Jabber®. Una definición estándar de protocolo basado en otro estándar abierto (EL estándar): XML.
Las tecnologías IM no son nuevas como concepto, pero sí es ahora cuando la tecnología está permitiendo su explotación, haciendo que cada vez más gente pueda acceder a ellas. De hecho, la especificación base de Jabber® (protocolo XMPP) fue inventada en 1998 por Jeremie Miller y tomada como protocolo por la comunidad open-source en 1999, donde ha ido creciendo y evolucionando hasta nuestros días.
El protocolo de mensajería y presencia XMPP[10] (Extensible Messaging and Presence Protocol) es una tecnología abierta basada en XML, para la comunicación en tiempo real, lo cual proporciona potencialmente un amplio rango de aplicaciones, incluyendo: mensajería instantánea, presencia, negociación de múltiples medios, pizarras compartidas, colaboración, middleware ligero, sindicación de contenidos, y enrutamiento XML genérico.
Es el proyecto más aceptado como la alternativa libre al sistema MSN Messenger de Microsoft, al AIM de AOL, al Yahoo Messenger y, por supuesto al ICQ. Y aunque todavía es un protocolo algo desconocido, está creciendo más cada día, gracias a los usuarios y, por supuesto, a Google, que ha creado un cliente de mensajería instantánea que utiliza Jabber®: Google Talk.
Jabber® está fundado sobre una serie de protocolos y tecnologías que permiten a dos entidades el intercambio de mensajes, información de presencia, y otros tipos de información estructurada casi en tiempo real (en este texto nos referiremos, en la práctica, a tiempo real). Las ventajas que aporta Jabber® son muchas:

- Abierto. Los protocolos en que se basa son libres, abiertos y públicos, están ampliamente documentados y disponen de múltiples implementaciones tanto para clientes, como para servidores, componentes y librerías.
- Estándar. El protocolo XMPP en el que se basa está aprobado por la Internet Engineering Task Force (IETF), y sus especificaciones han sido publicadas como RFC 3920 y RFC 3921.
- Probado. Desde que Jeremie Miller desarrollara Jabber® en 1998 ya existen productos muy estables y existen varios cientos de desarrolladores en la Comunidad Jabber®, así como importantes empresas que contribuyen a su Desarrollo. Actualmente se calculan en decenas de miles los servidores de IM compatibles con XMPP instalados en el mundo, ofreciendo soporte a 40 millones de usuarios.
- Descentralizado. La arquitectura de un red Jabber® es bastante similar al correo electrónico; como resultado, cualquiera puede instalar su propio servidor Jabber®, permitiendo así la implantación de redes privadas de IM.
- Seguro. Cualquier servidor Jabber® puede aislarse de la red pública de servidores Jabber® (p.e. en la intranet de una organización), así como incrementar su seguridad empleando SASL y TLS, tecnologías soportadas por las especificaciones XMPP. Incluso es posible extender la seguridad tal y como se explica en este artículo.
- Extensible. Empleando la potencia de los espacios de nombres XML, resulta sencillo añadir nuevas funcionalidades que encapsulen los protocolos de Jabber®. No obstante, la Jabber® Software Foundation se ocupa de regular las aportaciones públicas.
- Flexible. Los usos de Jabber®, como se detallará posteriormente, van más allá de la pura IM, podremos emplearlo para la gestión de red, sindicación de contenidos, herramientas de colaboración, compartir ficheros, juegos en red y monitorización remota de dispositivos.

XMPP es un protocolo basado en XML que se apoya en sistemas de streaming de datos para el intercambio de la información. El protocolo XMPP es extremadamente extensible, siendo necesario establecer nuevas especificaciones conforme se vayan añadiendo nuevas funcionalidades que extiendan sus capacidades originales. Esto ha llevado a la comunidad open-source a crear el proyecto Jabber® y establecer las siguientes RFC's:

- XMPP CORE. En el que se establece cuál es el núcleo más elemental del protocolo y lo mínimo que se le puede pedir a un sistema que lo implemente.
- XEP o XMPP Extensions. Que son especificaciones perfectamente documentadas que establecen la implementación de las extensiones que el protocolo soporta para implementar nuevas actualizaciones.
- XMPP Registrar, que son el conjunto de espacios de nombres que organizar todo el conjunto de clases, especificaciones y definiciones de los elementos que integran el protocolo.

XMPP tiene una estructura básica como la que se puede ver en la Ilustración 1.
En dicho bloque se puede ver que el protocolo se compone de las siguientes piezas:

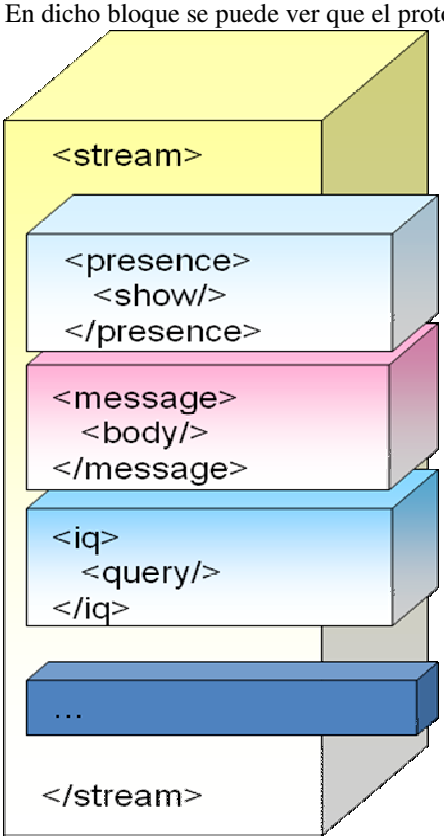


Ilustración 1. Estructura del núcleo de XMPP

- STREAM. En la unidad contenedora de una secuencia de mensajes XMPP. En un stream pueden venir una o varias stanzas XML o bloques de mensaje, que pueden ser de diferentes tipos.
- MESSAGE. Una stanza delimitada para el intercambio de mensajes de información, normalmente texto.
- IQ. Stanza especial de señalización de Jabber®, por el cual el protocolo ofrece un sistema de petición/respuesta para señalizar clientes/servidores y delimitar funcionalidades del protocolo.
- XEP. Son el conjunto de especificaciones que extienden los diferentes tipos de stanzas que el protocolo soporta. Por ejemplo, el bloque *<presence>* en un subconjunto de directivas IQ empleadas para el control de presencia. Dentro de las XEP es donde se definen las extensiones del protocolo tales como: seguridad, intercambio de ficheros, soporte de capacidades VoIP, presencia… etc.

Como se puede ver, la base del protocolo XMPP es muy elegante y aprovecha al máximo la potencia que ofrece XML como lenguaje descriptor de información abierto.

Puesto que el sistema de comunicaciones se basa en *streaming* de datos, la arquitectura es muy fluida y posibilita el envío de datos en *tiempo real*. Pero la arquitectura de Jabber® también permite los contextos offline, pues la infraestructura interna de los servidores de streaming, se basa en potentes gestores de colas que permiten almacenar la información temporalmente cuando al menos uno de los interlocutores no está disponible.
Todo esto, unido a la flexibilidad de la topología de redes y sus sistemas, convierte a Jabber® en una red robusta, fiable y totalmente escalable. De esto hay que decir que existen en la actualidad multitud de servidores Jabber® interconectados entre sí en Internet, lo que ofrece una infraestructura de acceso gratuita a todo ese mundo de servicios del que estamos hablando.

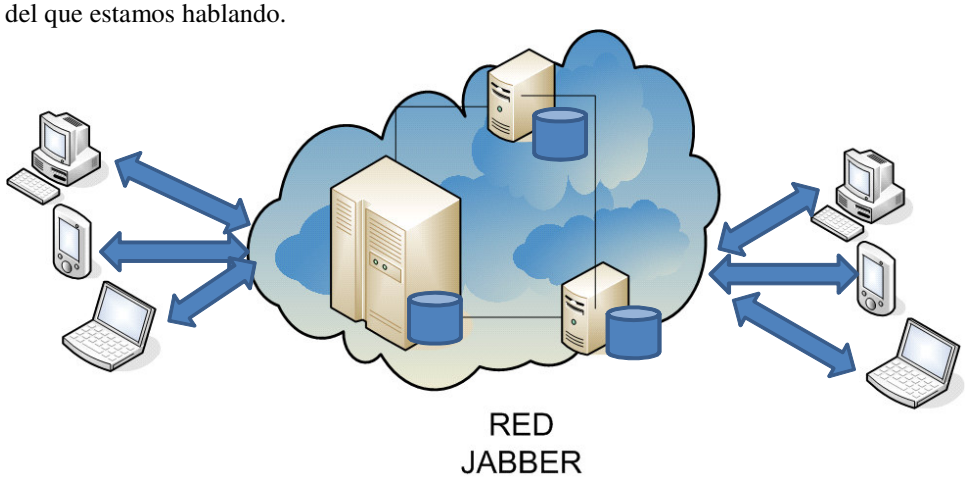


Ilustración 2. Esquema de alto nivel de la red Jabber®

Seguridad y privacidad

Puesto que los sistemas de IM requieren del intercambio de información, es necesario aplicar políticas de protección de los datos que se intercambian.
El protocolo Jabber® proporciona multitud de mecanismos para salvaguardar los accesos al sistema, pero todos ellos están centrados en la seguridad de acceso a los servicios de Jabber®: la autenticación. Estos mecanismos se centran

únicamente en proteger los accesos a las cuentas propietarias de los usuarios Jabber® y proteger que el canal de comunicaciones una vez establecido no es corruptible ni interceptable para evitar las impersonalizaciones y el acceso a información que por defecto siempre debe ser confidencial y privada. En cambio, para proteger la información que circula por la red, el único mecanismo de protección disponible es el empleo del estándar del protocolo SSL como sistema para cifrar todas las comunicaciones cliente/servidor – Servidor/servidor.
Dada esta la situación, los usuarios que desean un nivel más alto de privacidad y protección se van a encontrar con lo siguiente:

- Los mensajes que circulan por los gestores de colas se almacenan tal cual se envían. Esto puede provocar que un posible ataque dirigido hacia dichos sistemas, deje expuesto el mensaje intercambiado.
- Pueden no establecerse canales seguros en todos los puntos de la red Jabber®, pues eso depende los valores de conexión y la configuración y las habilidades de los productos empleados. Es decir, que un cliente puede estar empleando una conexión abierta en un punto, y blindada con SSL en otro. Con lo que no hay garantías de protección de los mensajes intercambiados.

Conscientes de estas limitaciones, la comunidad de desarrolladores de Jabber® está trabajando en nuevas especificaciones del protocolo que refuercen estos aspectos. Mientras tanto, podemos optar por extensiones *hechas a medida* que a nivel de aplicación proporcionen un intercambio de mensajes seguro, sin tocar la base del protocolo (lo que en un futuro, serviría de refuerzo a lo que Jabber® implemente como parte del estándar). Esta última alternativa ha sido explorada por Alhambra-Eidos™ en diversas pruebas de concepto.
Una aproximación a la solución consiste en hacer que la capa de aplicación emplee algoritmos de cifrado para proteger la información intercambiada, y dejar que Jabber® se encargue del resto. Con esto se extremaría suficientemente la seguridad del canal: autenticación segura, canales SSL de protección de los canales de información de protocolo y cifrado para proteger la información sensible.
Por supuesto, todas las medidas anteriores se pueden complementar con otros sistemas de seguridad, como por ejemplo, con la implementación de certificados X.509 de de usuario. De ahí que una posibilidad podría ser la incorporación del DNI electrónico para la autenticación de los usuarios en el acceso a redes seguras de Jabber® de una manera transparente y sencilla.

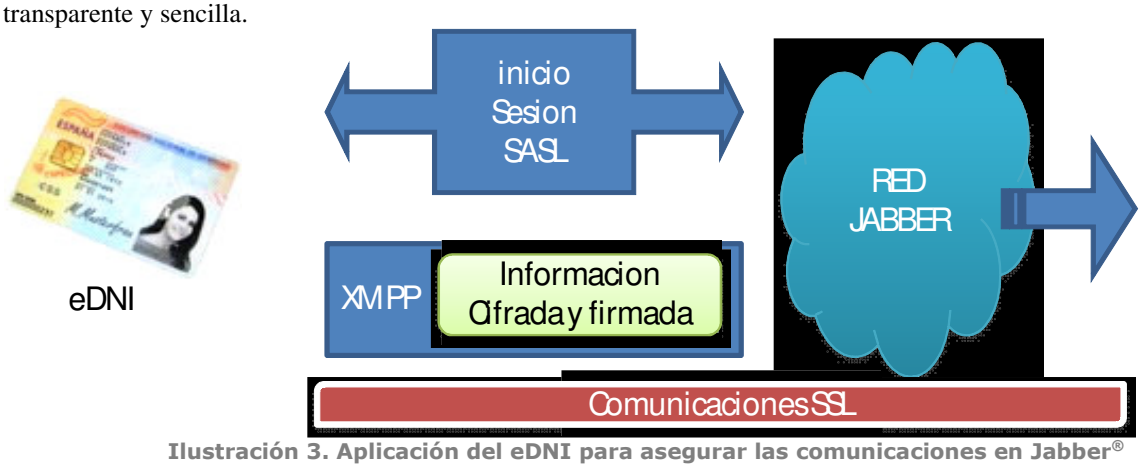


Ilustración 3. Aplicación del eDNI para asegurar las comunicaciones en Jabber®

Las aplicaciones de XMPP y Jabber®. Aplicativos y SDK.

Son muchas las posibilidades de aplicación de Jabber® en el mundo real. En la base de esta afirmación reside el hecho de que la IM proporciona un marco de envío de mensajes, y esto se puede aplicar a virtualmente cualquier contexto de comunicaciones, simplemente variando el contenido del mensaje. Por ejemplo:

- Comunicaciones entre capas de arquitecturas cliente/servidor alternativas a las existentes.
- Conexiones entre clientes ricos (*rich-clients*) para intercambiar cualquier tipo de contenido (texto, imágenes, ficheros de documentos, etc.)
- Comunicación mediante paso de mensajes entre aplicaciones distribuidas.
- Interconexión Business-to-Business o *B2B* (empleados-clientes, empleados-proveedores, etc.)

- Aplicaciones de atención al usuario/ciudadano por las cuales se puede atender en tiempo real a una persona y a través de los canales multimedia asistirle gráficamente, enviarles documentación, compartir recursos, etc.
- Implementación de sistemas de VoIP, Videoconferencia, intercambio de ficheros, acceso remoto… etc. Todo depende del uso que haga la aplicación cliente de la información que viaje encapsulada en la trama XMPP.

Todo ello en un marco en el que las comunicaciones pueden ser on-line, off-line y, mejor aún, compatibles con múltiples clientes de IM de otros fabricantes, pues otro de los grandes alicientes de la red Jabber® es su capacidad de adaptación a protocolos de terceros empleando los adaptadores. Esto hace factible conectar una red Jabber® con una red Google de forma transparente a la aplicación.

Ilustración 4. Implementación de alto nivel de una librería que complemente los mecanismos de seguridad de Jabber

Los SDK, o kits para el desarrollador, son vitales para complementar la potencia de la plataforma Jabber® pues la ventaja de poder emplear cajas negras que implementan los servicios de Jabber® como clases, objetos y acciones hace mucho más accesible esta tecnología.

Tal y como habíamos comentado, gracias que el protocolo Jabber® es completamiento abierto, cualquiera puede construirse una librería que encapsule el protocolo y construir aplicativos sobre esta base. En internet existen multitud de librerías en multitud de lenguajes, y existen clientes Jabber® de IM para múltiples sistemas operativos.

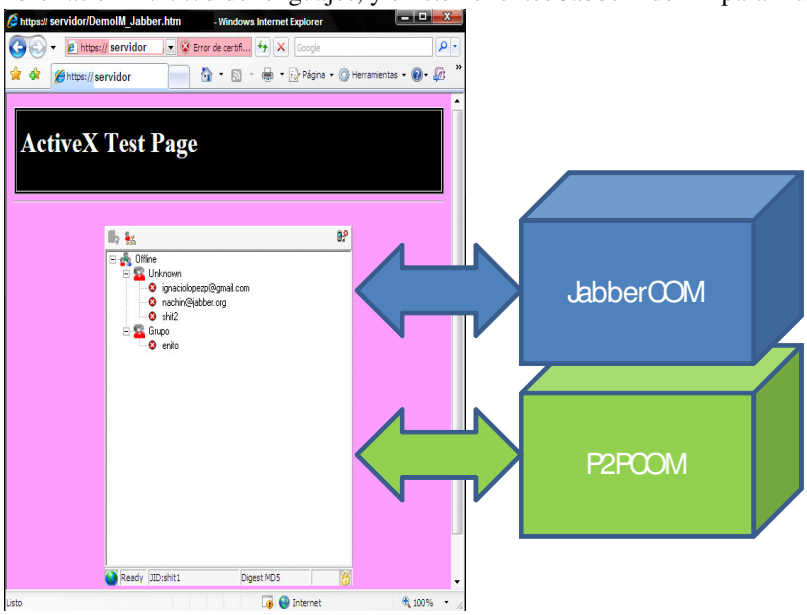


Ilustración 5. Arquitectura de la prueba de concepto

Alhambra-Eidos™ ha desarrollado ya varias pruebas de concepto en las que el objetivo fue construir una nueva librería Jabber® que ofreciera todas las funcionalidades del Jabber® CORE más un plus de seguridad que complementara las capacidades de las implementaciones actuales de Jabber® en este aspecto. Concretamente, dicho plus consistía en aumentar la seguridad y privacidad de las transmisiones de datos empleando algoritmos de cifrado, implementando además las más novedosas técnicas de inicio de sesión SASL disponibles. Las pruebas de concepto que se desarrollaron fueron completamente satisfactorias. Para ello se han seleccionaron las tecnologías de Microsoft Windows™ como base para su desarrollo de tal forma que se proporciona una DLL COM que a través de un API de muy alto nivel, es extremadamente sencillo iniciar una sesión Jabber®, intercambiar mensajes y desconectar. Dejando que sea ya la aplicación cliente la que decida que hace con la información que intercambia.

Es importante remarcar que las técnicas de cifrado no son el foco del protocolo Jabber®, con lo que se deja a libertad del desarrollador que construya el componente el seleccionar las técnicas y algoritmos de cifrado que considere oportunos para proteger los mensajes. De hecho, la librería JabberCOM de Alhambra-Eidos™, proporciona un marco de protocolo de aplicación que apoyado sobre el IM de Jabber® proporciona un nivel de diálogo de más alto nivel que se adecúa a la lógica de negocio del sistema de información en cuestión.

En las pruebas de concepto sobre Jabber® llevadas a cabo por Alhambra-Eidos™, uno de los productos construidos sobre este API fue un cliente ActiveX que posibilita las comunicaciones empleando la red Jabber® desde un explorador o aplicación compatible con esta tecnología, totalmente *Out-of-the-box* (es decir, que tal cual se pone en marcha, ya se puede establecer una sesión IM). Dicho ActiveX se puede incrustar en una página web o en un documento de Microsoft Office para permitir conversaciones entre usuarios de este sistema de IM. Las posibilidades son impresionantes.

Las implementaciones mencionadas anteriormente es posible aplicarlas tanto en su forma de cliente completo XMPP para su uso e integración en aplicativos compatibles COM como en su librería de bajo nivel para poder establecer la sesión Jabber® por código.

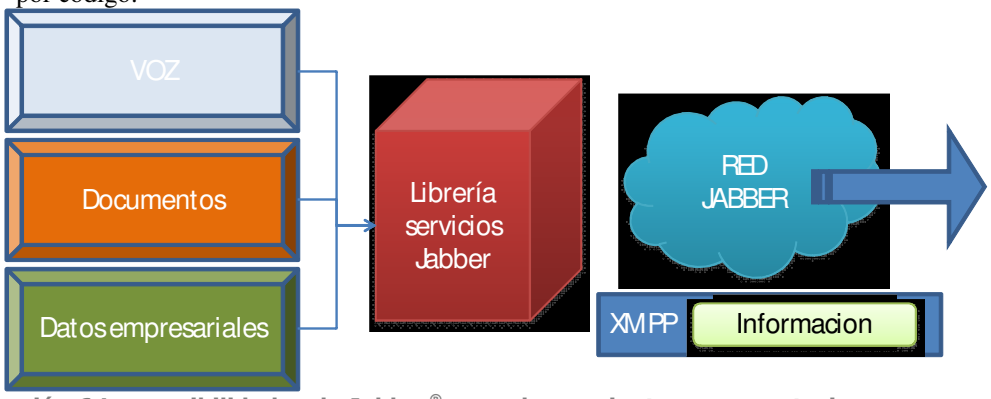


Ilustración 6 Las posibilidades de Jabber® como herramienta para construir nuevos servicios

En lo que respecta a compatibilidad entre implementaciones de clientes hay que tener en cuenta que para disfrutar de los mismos servicios entre los extremos, ambos deben implementar los mismos servicios. Cada fabricante es libre de implementar cuantas extensiones XEP quiera o de dotar a sus sistemas de capas adicionales de aplicación, que no tienen por qué afectar a Jabber® en su totalidad).

El marco P2P como apoyo a IM

Para finalizar, comentar que la IM no es específica de protocolos abiertos como Jabber®. Las tecnologías P2P basadas en canales de comunicaciones más básicos de comunicaciones, tales como los **sockets** también pueden ser utilizadas como medios para implementar sistemas de IM. Eso sí, tendríamos que renunciar a la estandarización del protocolo de comunicación, pues más allá del protocolo TCP/IP, el protocolo de IM sería de libre diseño de la persona que estableciera las reglas de las comunicaciones entre sistemas.
¿Por qué P2P como alternativa? La respuesta es que, a veces, nos encontramos con la necesidad de conectar directamente con el destinatario sin pasar por servidores centrales. Esto proporciona otros medios de conexión, y por tanto más posibles contextos a los ya de por sí extensos de los analizados hasta este momento. La mayor ventaja de P2P es la conexión directa y el control absoluto de los parámetros de la conexión. Una conexión directa proporciona como ventajas:

- los procesos de autenticación no son tan necesarios, pues la conexión se establece entre interlocutores conocidos,
- la conexión directa es más eficiente,
- se pueden desarrollar protocolos propietarios que cubran ciertas funcionalidades de formas más concretas.

Las desventajas de este modelo de conexión se pueden minimizar si se combinan redes Jabber® con clientes P2P. Alhambra-Eidos™, en sus pruebas de concepto con Jabber®, ha explorado también esta posibilidad, concluyendo que dicha combinación resulta mucho más efectiva y sencilla de lo que parece. La conclusión es que resulta interesante enriquecer un sistema de IM con esta característica P2P como opción de comunicación a las anteriormente comentadas que necesitan de al menos un servidor Jabber® público o privado. La idea consiste en montar un conjunto de diálogos de aplicación sobre un conjunto de protocolos de comunicaciones (bien Jabber®, bien un streaming de P2P), con lo que a nivel de aplicación la funcionalidad es la misma (salvando las limitaciones propias del propio P2P).

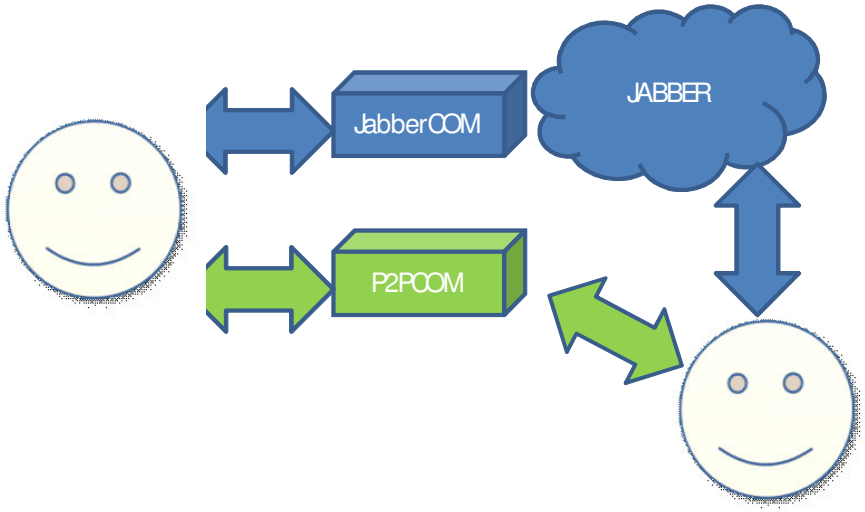
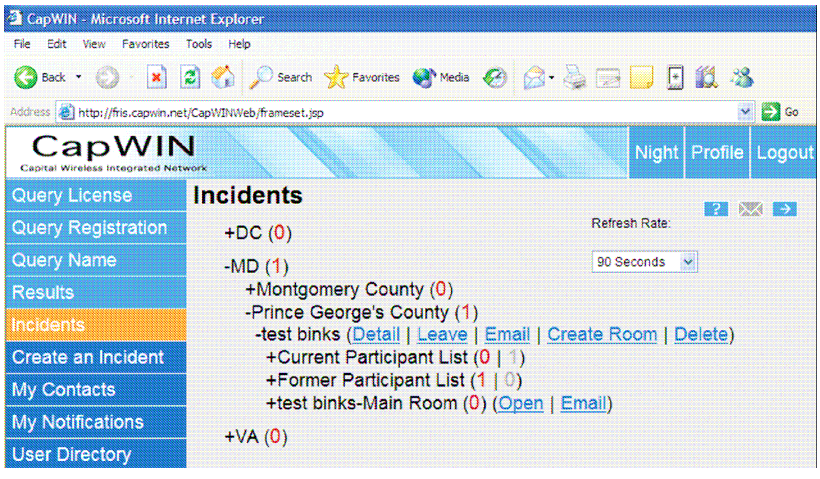


Ilustración 7 Arquitecturas P2P como refuerzo a las ventajas del IM de Jabber®

La cuestión final es que estamos trabajando con tecnologías complementarias que juntas proporcionan contextos más amplios y totalmente adaptados a las características del entorno, con un coste de desarrollo extremadamente pequeño. Alhambra-Eidos™ desarrolló un cliente ActiveX desarrollado sobre el binomio Jabber+P2P que proporcionaba una capa de interfaz de usuario o *UI* a las funcionalidades de los diferentes módulos. De esta forma, se logró un componente con funcionalidades totalmente *Out-of-the-box (OTB)* que permite elegir el modelo de comunicación de las conversaciones de sus usuarios.
Para finalizar, es conveniente recordar que la principal ventaja que proporcionan los SDK es la facilidad de poder crear un modelo de servicios adecuado. En el caso de querer ofrecer accesos a diversos sistemas, siempre será factible desarrollar capas de *middleware* que actúen de pasarelas con los aplicativos y/o dispositivos, centralizando y encapsulando los servicios y exponiendo casos de uso sencillos e integrables virtualmente con cualquier cosa. Por ejemplo, crear una pasarela de servicios web para permitir la IM en dispositivos móviles o aplicativos (clientes ligeros) de otras plataformas.

Aplicaciones en el mundo real

Actualmente, la IM está siendo empleada en el mundo en escenarios muy diversos: Defensa, Seguridad, Educación, Sanidad, Mercados bursátiles, etc.
Un ejemplo significativo de ello lo prueba que existan cada vez más aplicaciones militares y civiles de IM basada en XMPP.
Hechos como los atentados terroristas del 11 de Septiembre de 2001 pusieron en evidencia la falta de coordinación de los servicios de emergencia (policía, bomberos, servicios de evacuación y rescate de heridos). Un año después, en Washington D.C., se puso en marcha un proyecto denominado Capital Wireless Integrated Network (CapWIN) que contó con un presupuesto inicial de 20 millones de dólares. La red CapWIN se pensó como un sistema de coordinación basado en IM con XMPP que permitiera, a las decenas de agencias de seguridad y emergencias (más de 40 entidades de seguridad y emergencias entre policías, bomberos, asistencia sanitaria, y otros cuerpos), hacer tres cosas, fundamentalmente: comunicarse entre sí a través de una red segura de IM; realizar búsquedas en bases de datos de todo tipo; y permitir una mejor coordinación entre las diferentes agencias y efectivos sobre el terreno que atiendan una emergencia.



Por ejemplo, un oficial de policía que acaba de llegar a la escena de una emergencia, podría emplear la IM para obtener un informe resumen de la situación, así como enviar información exacta en tiempo real al centro de control de emergencias a la vez que otros efectivos procesan dicha información, realizando las pertinentes consultas en las bases de datos de cada una de las agencias coordinadas.
En realidad, el proyecto CapWIN comenzó a diseñarse mucho antes del 11 de Septiembre, fue en 1999 cuando un

hombre que amenazaba con saltar al río Potomac desde el puente de Woodrow Wilson que conecta los estados de Virginia y Maryland provocó un colapso de tráfico que duró 7 horas porque los oficiales de policía de ambos lados del puente no podían siquiera hablar directamente ya que utilizaban redes independientes e incompatibles. Eso, unido a la compleja división administrativa de Washington DC, con 3 jurisdicciones y además sede del gobierno federal, hizo que algunas autoridades se plantearan que había que hacer algo para que situaciones como esta que hemos comentado no volvieran a ocurrir.
Otro de los escenarios de uso de los protocolos de IM tiene que ver con las agencias y organismos vinculados a la defensa nacional y de seguridad interior. A este tipo de usuarios les resultan muy atractivas las posibilidades que brindan protocolos como XMPP, que permiten convergencia de las comunicaciones, movilidad y ubicuidad, unido a la capacidad de utilizar redes públicas o privadas, de emplear sistemas de cifrado estándares o propietarios, dado el carácter abierto del protocolo y lo sencillo que resulta implementar aplicaciones de servidor o clientes que puedan comunicarse entre sí o con clientes estándares de otras redes de IM como GoogleTalk.
A finales del año 2005, el Information Technology Standards Council (ITSC) del Departamento de Defensa de los Estados Unidos (US DoD) aprobó la inclusión del protocolo XMPP como un estándar obligatorio del DoD IT Standards Registry (DISR). Este hecho tiene especial relevancia porque XMPP es el único estándar de IM aprobado por el DISR. Desde entonces han sido decenas de agencias gubernamentales las que han adoptado XMPP como protocolo de IM.

Conclusiones

La contribución que los diferentes protocolos de IM (y más en concreto, XMPP) pueden aportar en el desarrollo de la administración electrónica de nuestro país es considerable. Pero será cada institución, cada organismo, quien determine en última instancia la necesidad de incorporarlos e integrarlos con las aplicaciones existentes. No obstante, la intención de los autores con este artículo no es otra que abrir las mentes de aquellos decisores tecnológicos que aún no han explorados las posibilidades y el impacto que la mensajería instantánea podría tener en el seno de sus organizaciones y de sus procesos.
XMPP y las redes de mensajería basadas en Jabber® nos brindan la oportunidad de implementar nuestras propias plataformas IM para comunicar instituciones entre sí, para intercambiar información, en sustitución incluso del correo electrónico, que no aporta el factor clave de la información de presencia, esencial para la toma de decisiones en tiempo real.
El nivel de privacidad de la información, determinará el nivel de seguridad de la plataforma IM. Así puede haber comunicaciones abiertas o bien comunicaciones cifradas para proteger información sensible. En el canal de comunicaciones podrán incorporarse varias personas, o bien establecer canales privados. E incluso en esta subdivisión, se podría utilizar la tecnología P2P para establecer canales directos y protegidos para el intercambio de información extremadamente sensible.
Gracias al intercambio multimedia, la riqueza de la información hará que los trámites y las comunicaciones sean más fluidos. Redundando en una mejor gestión de los recursos.
Como se puede deducir de todos los casos, la mayor ventaja pues de Jabber® y del protocolo XMPP es que todas sus especificaciones, implementaciones y servicios de terceros están ya disponibles.
Las administraciones públicas españolas pueden sacar mucho partido de la mensajería instantánea, mejorando el servicio y la comunicación con los ciudadanos y el resto de administraciones, adaptando la tecnología a nuestra vida cotidiana con unos innovadores servicios que harán que el futuro sea ya nuestro presente.

Bibliografía

Adams, DJ. Programming Jabber (Programming). OReilly, 2002.
Wright, William y Dana Moore. Jabber Developers Handbook (Developer's Library). Sams, 2003. IETF, 2004.
RFC 3920, *Extensible Messaging and Presence Protocol (XMPP): Core* which describes client-server messaging using two open ended XML streams. IETF, 2004.
RFC 3921, *Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence*. IETF, 2004.
RFC 3922, *Mapping the Extensible Messaging and Presence Protocol (XMPP) to Common Presence and Instant Messaging (CPIM)*. IETF, 2004.
RFC 3923, *End-to-End Signing and Object Encryption for the Extensible Messaging and Presence Protocol (XMPP).* IETF, 2004.
http://www.xmpp.org/extensions. XMPP Extension Protocols (XEPs). XMPP Standards Foundation.

Notas

[1] http://www.gartner.com
[2] http://www.peterdrucker.at
[3] http://www.icq.com
[4] http://es.messenger.yahoo.com
[7] http://www.google.com/talk
[8] RFC 1459. Internet Relay Chat Protocol. IETF, 1993
[9] http://www.jabber.org
[10] http://www.xmpp.org

[5] http://get.live.com/messenger/overview
[6] http://www.aim.com
[11] http://www.alhambra-eidos.es