movilidad con seguridad

La propuesta de Sun Microsystems

Por José Manuel Estrada
Business Development Manager Java y Nuevas Tecnologías de Sun Microsystems

El primer pensamiento al empezar a escribir sobre movilidad y seguridad es: ¡Vaya dos palabras tan manoseadas cuando se habla de tecnología o de servicios! Me apoyo en el respaldo y tomo un poco de distancia del monitor, veo la *SmartCard* que me permite autenticarme y acceder de forma segura a la Red Privada Virtual de la empresa y acceder a toda la información de la que, posiblemente, es la organización que más tecnología y soluciones está aportando para hacer la movilidad más segura, hasta el punto de convertirla en uno de nuestros tres pilares estratégicos.

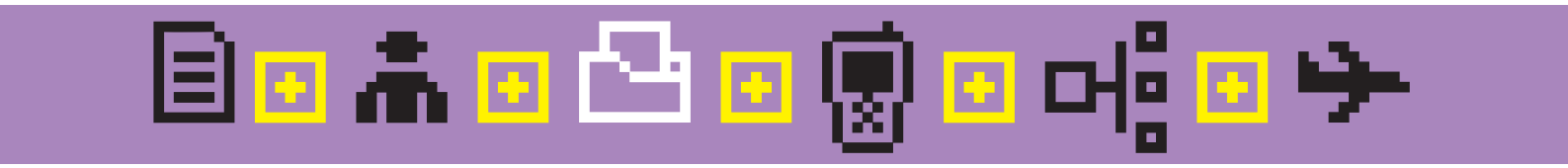
Esta visión del monitor, la *JavaCard*, el cable de red y el acceso que me dan a todos los proyectos e iniciativas de Sun Microsystems en estas áreas me sitúan en una posición cómoda para hablar un poco de estos dos términos tantas veces incompatibles.

Toda esta estrategia se basa en permitir que nuestros clientes proporcionen a ciudadanos, clientes o empleados toda la información y todos los servicios necesarios en cualquier momento, en cualquier lugar y con independencia del dispositivo que utilicen y de una manera segura y utilizable.

A principios de los ochenta Sun Microsystems salía al mercado con un lema rompedor y para muchos incomprensible: La red es el ordenador (*The Network is the Computer*). Hoy su significado está claro para todos nosotros. La red ha ido evolucionando de una pequeña red de ordenadores a una gran red a la que se conectan redes, red a la que se conectan dispositivos y aparatos con ordenadores embebidos, red a la que empezamos a conectar cosas: AutoID, sensores, ... Cualquier cosa acabará teniendo conectividad y una dirección IP.

El panorama es excitante si pensamos en todo lo que podemos y podremos hacer en la red, pero también puede ser preocupante desde el punto de vista de la seguridad o de la privacidad.

A pesar de la percepción generalizada de inseguridad en la red hoy disponemos de tecnología, productos, metodología y procedimientos para hacer



En telefonía móvil los operadores llevan años utilizando JavaCard como base de sus tarjetas SIM, inicialmente usada como mecanismo de autenticación y cada vez más como plataforma en la que descargar de forma dinámica nuevas aplicaciones y servicios

cualquier actividad en la red segura y además sin trabas y barreras que la hagan incómoda o sencillamente inutilizable.

Si empezamos por la plataforma donde se generan y residen los servicios y no la basamos en un sistema operativo sólido, robusto, seguro y con capacidad de escalar a miles, millones de usuarios estaremos condenando desde los cimientos toda edificación posterior. Hace escasas horas se presentaba públicamente Solaris 10, la mayor puesta al día de un sistema que ha contribuido más que ningún otro al nacimiento y evolución de la red. Con Solaris 10 se han dado varios pasos importantes y que van a marcar de forma notable los próximos años en la red. Mencionando sólo dos: su disponibilidad en plataformas hardware más asequibles que van a permitir llevar a todos lo que hasta ahora estaban en grandes sistemas, y la incorporación de *Trusted Solaris* en Solaris 10. *Trusted Solaris* ha sido durante años la referencia en comunidades con unas altas exigencias de seguridad. El sistema operativo que ha pasado todas las certificaciones de seguridad de las administraciones de inteligencia y militares. Si podemos disponer del sistema más seguro y lo podemos poner en los grandes sistemas o en los más asequibles servidores (basados en procesadores x86) en situaciones de poca carga o al borde de la red, nada podrá excusarnos nunca de las inseguridades de nuestra plataforma de servicios.

Sentados los cimientos seguiremos seleccionando materiales, y aparece Java. Algo menos de diez años han bastado para que Java se convierta en la mayor fuerza en la industria de software. Un ecosistema de cientos de compañías evolucionando y definiendo las nuevas funcionalidades y áreas de aplicación en *Java Community Process*, cuatro millones de programadores, la base de la enseñanza de programación en la mayoría de universidades de todo el mundo, las grandes empresas de *software* (con una sola excepción) basan en Java su estrategia, decenas de herramientas de programación compitiendo en beneficio del usuario y, finalmente, centenares de millones de plataformas en las que desplegar servicios: de servidores a teléfonos, de vehículos a tarjetas inteligentes, de ordenadores personales a "*gadgets*" multimedia.

750 millones de tarjetas inteligentes con tecnología *JavaCard* emitidas la convierten en la plataforma de autenticación segura más extendida. Su infraestructura de seguridad, capacidad multiplicación, interoperabilidad, capacidad de instalar aplicaciones y servicios una vez emitida y su disponibilidad por parte de decenas de fabricantes la están llevando a nuevos usos y escenarios. Frente a las debilidades y agujeros del mecanismo tradicional de usuario/contraseña la tarjeta nos permite de forma fácil y cómoda implementar mecanismos de autenticación multifactor: lo que tengo (la tarjeta), más lo que sé (el PIN), más otros posibles datos biométricos almacenados en la propia tarjeta.

En telefonía móvil los operadores llevan años utilizando *JavaCard* como base de sus tarjetas SIM, inicialmente usada como mecanismo de autenticación y cada vez más como plataforma en la que descargar de forma dinámica nuevas aplicaciones y servicios. La compatibilidad que *JavaCard* proporciona entre tarjetas de distintos fabricantes y el ahorro logístico de distribuir nuevas tarjetas con cada nuevo servicio al poder ser descargadas por la red inalámbrica, les supone a los operadores un gran ahorro de costes y una gran ventaja competitiva al poder desplegar nuevos servicios de manera instantánea. La apertura de la tarjeta SIM (y USIM en redes 3G) a servicios de terceros está posibilitando la aparición de servicios seguros en el móvil de la mano de administraciones públicas y de empresas privadas que explotan el potencial de la plataforma segura *JavaCard*.

En el mundo financiero los primeros despliegues de tarjetas inteligentes

con un volumen significativo de la mano de emisores como *American Express*, *Visa* o *MasterCard* con tecnología *JavaCard*, han abierto la vía a lo que en breve será la sustitución masiva de tarjetas de banda magnética por tarjetas inteligentes basadas en *JavaCard*.

Cada día son más las los gobiernos y administraciones públicas que están desplegando *JavaCards* como tarjetas de identidad de ciudadanos y para uso interno de acceso a sistemas y acceso a dependencias para sus funcionarios y empleados. Una de las referencias punteras es el sistema de acceso a dependencias y a sistemas por parte del Departamento de defensa de los Estados Unidos para su personal. Después de una larga evaluación de distintas tecnologías se decantaron por *JavaCard*, seguridad, potencia y flexibilidad para nuevos servicios eran requerimientos tan importantes como el resto de la infraestructura: provisión de certificados y servicios, gestión, administración, emisión,... Tanto *Sun Microsystems* como sus socios tecnológicos se emplearon a fondo en un proyecto de una complejidad no imaginable viendo el resultado en los escasos centímetros cuadrados de una tarjeta. De uso interno, como en el de Departamento de Defensa y varias decenas más de organismos en todo el mundo, *JavaCard* ha ido pasando a su uso en tarjetas de ciudadano, de su uso en sistemas sanitarios está pasando a su uso en DNIs, países como Taiwán, Tailandia o Bélgica han elegido JavaCard para sus documentos de identidad.

Uno de los delitos en la red que más preocupa a administraciones públicas y empresas es el robo de identidad, aunque no siempre denunciado y pocas veces publicado. La utilización de distintas técnicas como ataques a servidores, phising, trojanos, ingeniería social para obtener información y suplantar la identidad empieza a tener un coste comparable al de uso fraudulento de tarjetas de crédito. A partir de la experiencia con el Departamento de Defensa, aunque allí el acceso a red era sólo una parte de la solución, y de varios proyectos similares hemos trabajado en varios frentes.

Por una parte empezamos a elaborar, conjuntamente con otras empresas que compartían la misma preocupación por el problema de la identidad en la red, lo que hoy se ha convertido en un estándar de identidad en la red: *Liberty Alliance*. El objetivo de *Liberty* es crear unas especificaciones tecnológicas abiertas, documentos y guías de utilización en distintos sectores, controles de privacidad, *best practices* de seguridad y privacidad y finalmente certificaciones de interoperatividad entre distintas implementaciones. En lugar de crear un repositorio único de la información de identidad, con los riesgos de punto único de fallo y punto único de control, la propuesta de *Liberty* se basa en poder federar círculos de confianza. Un círculo de confianza puede ser un proveedor de servicios y sus usuarios, un operador con empresas que den servicios en su red y sus clientes, un organismo de la administración y los ciudadanos a los que da servicios, etc. Los mecanismos de federación de *Liberty* permiten pasar identificado de un servicio a otro, en definitiva permite un single sign-on en la red. Puesto que el valor y la criticidad de los servicios no es la misma, *Liberty* contempla y permite implementar el concepto de niveles de confianza. Si un usuario pasa de un proveedor de información a un banco para realizar una transferencia, este último puede y debe reforzar la autenticación con un mecanismo más exigente, cuando al revés podría ser suficiente. Finalmente *Liberty* da al usuario mecanismos de control de privacidad: qué información puede pasar un proveedor de identidad a un proveedor de servicios, a quién y cómo (siempre, por transacción, con autorización expresa, ...). Finalmente mencionar el cumplimiento por parte de *Liberty* de las distintas legislaciones sobre privacidad. Un vistazo a la web *www.projectliberty.org*, especificaciones, documentos de trabajo, escenarios de

Cada día son más las los gobiernos y administraciones públicas que están desplegando JavaCards como tarjetas de identidad de ciudadanos y para uso interno de acceso a sistemas y acceso a dependencias para sus funcionarios y empleados

uso, productos compatibles y finalmente la lista de miembros -empresas y organismos públicos- nos pueden dar una idea clara del potencial habilitador de servicios en red que *Liberty* empieza a aportar.

Otro importante frente de trabajo en *Sun Microsystems* ha sido desarrollar un sistema que recogiendo la experiencia de muchos proyectos ad-hoc permita a pequeñas empresas o grandes organizaciones desplegar un sistema robusto de autenticación multifactor basado en *JavaCard* sin los inconvenientes habituales en este tipo de proyectos: alto esfuerzo de integración de tecnologías heterogéneas, costes y tiempos no siempre controlados. *JavaCard Enterprise Software* nos permite desplegar una solución segura de identidad digital, autenticación y autorización con muy poco esfuerzo y con coste y plazos conocidos.

En las redes de telefonía móvil el negocio de las descargas de tonos musicales, más de quince mil millones de dólares según los analistas, superan en muchos países la venta de CDs musicales, y convierten en ridículas las cifras de negocio de descarga por Internet, a pesar de iniciativas relativamente exitosas como iTunes de Apple. ¿Por qué? Tal vez las razones haya que buscarlas en que son redes seguras, con un mecanismo robusto de autenticación (las SIM, basadas mayoritariamente en *JavaCard*), con un mecanismo fácil y amistoso de compra con cargo a la cuenta de abonado o a la tarjeta de prepago. Estamos viendo día a día la evolución de una red de un servicio espacializado a una red de servicios genéricos, la evolución de un teléfono a un dispositivo de acceso a la red y una plataforma de ejecución de aplicaciones. Pero esa red sigue manteniendo una característica básica: es segura.

Una de las claves de la conversión de una plataforma cerrada en una plataforma de ejecución de aplicaciones -con el riesgo añadido de ser en su mayoría aplicaciones descargadas- está en Java.

Desde la aparición de los primeros teléfonos con J2ME (Java 2 Micro Edition) en Extremo Oriente, apenas han pasado cuatro años, pero el fenómeno se ha extendido como la pólvora: más de 500 millones de terminales con J2ME en el mercado, más de cien operadores dando servicios basados en Java, más de treinta fabricantes de terminales incluyendo esta tecnología en sus terminales -desde las gamas más baratas a sus más sofisticados *smart phones* o PDA-comunicadores, con más de trescientos modelos donde elegir. Cifras de negocio de venta y descarga de aplicaciones que superan los dos mil millones de dólares al año (previsiones de unos 15.000 millones en 2007/2008 según el analista de mercado ARC Group), cada vez más empresas dando acceso a sus sistemas desde aplicaciones Java en móviles o PDAs a sus empleados o clientes en situaciones de movilidad.

Algunas de las razones del éxito de Java

- compatibilidad y capacidad multiplataforma, no importa qué procesador, no importa qué sistema operativo, si hay Java puede funcionar la misma aplicación. En pocos entornos hay tanta diversidad de plataformas hardware y sistemas operativos como en éste.

- Capacidad de usar servicios bajo demanda: descargar y usar aquello que necesito cuando lo necesito

- Apertura

- Independencia de proveedores.

- No intrusión en los modelos de negocio de operadores, fabricantes y proveedores de aplicaciones y servicios.

- Y por encima de todo: seguridad. Java nace en la red y con la red en mente, se diseña pensando que va a usar aplicaciones que están en la red, en sitios desconocidos y no necesariamente fiables. El modelo de seguridad de Java (SandBox) ha demostrado su validez a lo largo de estos años con un record inigualable: cero virus.

Sun Microsystems ha tenido desde su creación una presencia notable en universidades y en general en el mundo de la educación, y desde aquí estamos liderando interesantes iniciativas con organismos de educación para acceder al segmento de mercado que más servicios (distintos a la voz) consume en telefonía móvil: los adolescentes. Ninguna otra vía puede ser tan eficaz para la administración pública para dirigirse a este importante sector de ciudadanos y darle servicios a través de la red.

En los últimos años hemos visto proliferar dispositivos personales, PDAs que, siguiendo el modelo impuesto por *Windows* de *fat client*, entran y salen cada día con gigabytes de información sin el menor control y sin los más elementales elementos de seguridad y con total exposición a robos y pérdidas. Auditorías recientes de seguridad y protección de información en empresas y organismos públicos nos muestran la paradoja de inversiones multimillonarias en protección de sistemas y procedimientos ante ataques a través de la red, especialmente externos, conviviendo con graves deficiencias en la gestión de la seguridad en la red interna y en la gestión de identidad y un total descontrol de dispositivos (portátiles, PDAs, discos externos de bolsillo, memorias USB, reproductores MP3). En lugar de movilidad deberíamos llamarlo "inseguridad con patas" o "invitación al desastre".

Movilidad es más que telefonía móvil, dispositivos, tarjetas inteligentes, son también equipos de sobremesa, es trabajo remoto, son quioscos de información, son máquinas expendedoras, son sistemas de aparcamientos públicos, son sistemas de televisión digital, son AutoID ... tal vez algún día cada bombilla tenga una dirección IP, si es así, allí estará Java. Movilidad es llevar la información allí donde sea necesaria, de manera fiable, utilizable y segura y para ello deberá ser administrada y gestionada de manera profesional y segura en el centro de datos.