Ágora sic Divulgación
VOLUMEN 36 · SEPTIEMBRE 2003

SUMARIO

@DAN: una plataforma para aplicaciones sobre PDAs que requieran firma digital y/o pago seguro

José Manuel López González
División de Consultoría y Proyectos
GyD Ibérica

La mejora de procesos de la empresa así como la oferta de medios de pago a menudo se ven frenadas por limitaciones técnicas o legales o ambas. Con el proyecto @DAN –iniciativa cofinanciada por la Comunidad Europea y acometida en calidad de socios por siete entidades–, se da respuesta a estas necesidades explorando los conceptos de ubicuidad, seguridad y pago actuales, uniéndolos en una única plataforma. Esto permite el desarrollo rápido (mínimo 'time to market') y con garantías legales de aplicaciones de firma digital y pago seguro en dispositivos móviles (PDAs.) Todo ello se basa en la tecnología de tarjeta inteligente con capacidades criptográficas y, adicionalmente, financieras.

@DAN: una plataforma para aplicaciones sobre PDAs que requieran firma digital y/o pago seguro

LOS CONCEPTOS

El estudio de la interrelación de los conceptos de pago, ubicuidad y seguridad en el mundo electrónico aporta el conocimiento necesario para descubrir y solucionar las deficiencias de las tecnologías actuales frente a las necesidades de la sociedad y de las empresas.

Pago

Cuando los servicios se convierten en electrónicos, el pago también debe hacerlo. La máxima expresión de pago electrónico es un Sistema de Pago basado en Internet (*Internet Payment System* - IPS) y, yendo más allá, un Sistema de Pago Móvil (*Mobile Payment System* - MPS.) Un MPS se debe entender como una extensión de un IPS, nunca como un sustituto.

Existen diferentes actores en el mercado que pueden dictar los requisitos de un MPS, como pueden ser los bancos, las operadoras, proveedores de medios de pago o administraciones públicas **[1]**. La lucha entre algunos de estos actores para determinar quién asume el rol financiero es una de las razones por las que es tan difícil introducir estos sistemas. Desde el punto de vista de las compañías, los MPS's pueden estar basados en bancos, en operadoras, ser independientes o una mezcla de todos estos enfoques.

En cualquier caso, los factores críticos de éxito de un MPS son los siguientes (los actuales MPS y ninguno de los sistemas actuales lo cumple):

– Ser transfronterizo: comerciantes y consumidores pueden ser de cualquier país.

– No ligado a ningún banco ni operador móvil.

– Independencia de bancos de comerciante y consumidor: los bancos de ambos pueden ser diferentes.

– Facilidad de uso: los consumidores están acostumbrados a utilizar tarjetas de crédito en el mundo físico y no están dispuestos a aceptar medios de pago más complicados.

– Debe sustituir con medios técnicos, de procedimientos y legales la seguridad que ofrece una autenticación cara a cara.

El diseño de un MPS debe cumplir estos requisitos:

@DAN ha seleccionado el IPS/MPS que representa los estándares de compra segura de Visa y Mastercard **[2]** (*Verified by* Visa y Mastercard *Secure Code*.) Este IPS está basado en el modelo Visa 3D - Mastercard SPA/UCAF, que cumple los requisitos anteriores para los bancos adheridos a Visa o Mastercard y además está bien posicionado (establecido).

Seleccionando y adaptando este IPS, @DAN extiende un medio de pago **universal**.

Ubicuidad

Se ha generalizado la visión de ejecutivos comprando en bolsa en teléfonos móviles de altas prestaciones, o navegando por Internet desde un coche. Esto ha llevado a pensar que la ubicuidad es sólo útil para aplicaciones elitistas, provocando un sentimiento de escepticismo sobre el futuro de la ubicuidad. Las expectativas sobre el tráfico inalámbrico de datos se han basado en percepciones imprecisas, como tratar de imaginar servicios de datos sobre los móviles actuales o pensar que el único uso de Internet es el correo-e y la navegación web.

En términos generales, la evolución del concepto de ubicuidad puede verse como sigue:

– *Etapa inicial*, con el desarrollo de Internet y correo-e. Se trata de la era de la ubicuidad en el almacenamiento de datos (los datos se almacenan en multitud de centros.) Se podían recuperar los datos almacenados en cualquier lugar pero no desde cualquier lugar, es decir, no había ubicuidad de acceso a datos.

– *Etapa del teléfono móvil.* Con el rápido crecimiento del mercado de telefonía móvil vino el comienzo de la ubicuidad de acceso a datos. Este acceso era muy limitado debido a las restricciones de los propios teléfonos (pequeña pantalla e incómoda entrada de datos), el escaso ancho de banda y la tarificación basada en tiempo de conexión en vez de en tráfico. Esto condujo a un mercado pequeño y, por lo tanto, a pocos proveedores de servicios y una pobre percepción de la necesidad de ubicuidad en acceso a datos, sólo necesaria para aplicaciones específicas y perfiles profesionales muy definidos.

– *Etapa de equipos de altas prestaciones*, con GPRS, mó-

viles J2ME, PDAs conectadas a Internet y los venideros dispositivos UMTS. Esta mejora de la tecnología aporta un ensanchamiento del mercado. La gente ya no sólo piensa en ejecutivos consultando y comprando en bolsa. ¿Por qué no buscar qué puedo ver en los alrededores de la catedral que estoy visitando?¿Por qué no echar una partida con un contrincante anónimo mientras viajo en tren?¿Por qué el revisor de la instalación de gas no realiza el informe y lo firma en línea? Las nuevas tecnologías permiten todas esta aplicaciones, junto a las de fuerza de ventas, los repartidores, los servicios técnicos a domicilio y cualquier otro trabajador cuyo día a día implique intrínsecamente ubicuidad.

Las soluciones de ubicuidad se están convirtiendo en una necesidad de mercado a todos los niveles y @DAN facilita el acceso a ella.

Seguridad

Seguridad significa ausencia de duda o miedo: confianza. Para obtener esta confianza la seguridad se basa tanto en medios técnicos y procedimientos como en acuerdos y normativas legales, por lo que no sólo nuevos conceptos o desarrollos técnicos pueden mejorar la seguridad actual.

Confianza en Internet significa proveer de los bien conocidos cuatro servicios de seguridad: privacidad, autenticidad, integridad y 'no repudio', servicios éstos que se pueden garantizar con el buen uso de una PKI y un diseño adecuado de las aplicaciones.

La tarjeta inteligente, reconocida como uno de los elementos de seguridad más fiables debido a la altísima carga normativa que soporta, provee a una persona de su identidad digital, independientemente del servicio, el dispositivo o la red. Es posible entonces utilizarla como elemento identificador en soluciones de *Single Sign On*, con un único certificado para diferentes aplicaciones, de diferente naturaleza y en diferentes entornos como nuestro banco, nuestra compañía o la e-administración.

Por todo ello, la seguridad en @DAN está respaldada por la **tarjeta inteligente** y por el concepto de **PKI**.

El escenario completo

Estos conceptos, tomados de dos en dos, aportan las siguientes ventajas:

Pago + Ubicuidad = Potencia los negocios

Pago + Seguridad = Minimiza el fraude

Ubicuidad + Seguridad = Permite la descentralización de la sociedad

Figura 1.- Evolución del concepto de negocio

Uniendo estos tres conceptos se obtiene la plataforma @DAN y su tesis: SC-Business (*Smart Card Business*), como elección de enfoque de negocio centrado en la tarjeta inteligente.

La idea que subyace bajo la plataforma @DAN se puede resumir con la siguiente declaración: utilizar la misma tarjeta inteligente para autenticar a personas en aplicaciones corporativas o de la administración o para pagar tanto en mercados reales como virtuales, así como utilizar la infraestructura de cajeros existente. En la **figura 2** se puede apreciar de forma gráfica a qué conceptos da respuesta @DAN.

EL PROYECTO

Planteamiento

Los objetivos del proyecto @DAN son: la creación de una plataforma para el desarrollo de aplicaciones seguras y pago seguro sobre dispositivos móviles, el desarrollo de dos prototipos de aplicación sobre esta plataforma y la realización de una valoración de la misma a través de los prototipos. Inicialmente la plataforma se basaba sobre los tres pilares tecnológicos que más desea fomentar la Unión Europea (EU), que son UMTS, tarjetas inteligentes y certificados digitales (PKI). Este enfoque está alineado con los objetivos de la EU, concretamente con el programa '*IST 2001-V.1.5 CPA5: Smart Cards*' y con la descentralización de los cúmulos de generación de negocio de las grandes ciudades y otras aportaciones a la sociedad de la información **[3]**.

Ante la carencia de prototipos de terminales UMTS se optó por el uso de PDAs y conexión WiFi o GPRS. Esta alternativa ya se ha utilizado en otros proyectos **[4]** y hoy en día es un verdadero caso de negocio.

Los socios

La plataforma @Dan es el fruto del trabajo de siete socios pertenecientes a cinco países europeos, trabajando bajo el quinto programa marco de la IST. Los participantes se agrupan en tres roles que son: desarrollador de la plataforma, desarrollador de prototipo sobre la plataforma para probar la viabilidad técnica de la misma, evaluadores de la plataforma en el mercado.

El primer grupo está compuesto por:

– **Giesecke&Devrient**, empresa alemana con más de 150 años de historia, dedicada a la fabricación de papel moneda, máquinas procesadoras de billetes, tarjeta inteligente y proyectos de seguridad TIC. La filial española, GyD Ibérica, desarrolló todas las funcionalidades criptográficas del dispositivo cliente y del servidor.

– **Caixa Catalunya**, caja de ahorro puntera en el mercado español y comprometida con la aplicación de las tecnologías más innovadores en sus servicios. Se encargó de adaptar el Terminal Punto de Venta virtual (TPV virtual) para los dispositivos cliente así como de la autenticación del titular de la tarjeta vía certificado digital.

El segundo grupo lo componen:

– **Universitat Pompeu Fabra (UPF)**, universidad pública catalana creada en 1990 con la intención de desarrollar su propio modelo de enseñanza basado en la eficacia y jugar un importante rol en el área de la investigación. Basado en su intranet, *CampusGlobal* (http://campusglobal.upf.es), dedicada a soportar la innovación en la enseñanza, desarrolla el primer prototipo aplicando firma digital a los asuntos administrativos y pago seguro sobre la contratación de cursos de postgrado.

Figura 2.- Marco conceptual de @DAN y posibles aplicaciones

– **Universitat Politécnica de Catalunya**, ofrece carreras en diferentes ramas de la ingeniería y la arquitectura. Concretamente el grupo de investigación Técnicas Cuantitativas de Gestión del departamento de Estadística e Investigación Operacional desarrolla el segundo prototipo sobre su aplicación de provisión de servicios de previsión mediante series temporales. Adicionalmente aporta una dilatada experiencia en proyectos europeos como VL-CATS (IST-1999-10971), FORCE-4 (ESPRIT IV num 20704 and TIC96-1310-CE) y TESS (ESPRIT num 29741).

El tercer grupo está formado por:

– **VSN International**, dedicada a la provisión de produc-

tos para cálculos estadísticos de alta calidad y de servicios para que los usuarios finales puedan explotar las nuevas técnicas de computación y métodos estadísticos, elabora la metodología de evaluación y la lleva a cabo junto con los otros dos socios 'testeadores'.

– **Fundación IECS**, es una organización privada sin ánimo de lucro cuyo objetivo principal es la promoción e impartición de cursos de postgrado y 'Masters' en el ámbito de la gestión empresarial en la *IECS Graduate School of Management*, una facultad afiliada a la *Robert Schuman University of Strasbourg*. Lleva a cabo dentro del proyecto tareas de test desde el punto de vista de 'usabilidad' para el usuario final como del grado de satisfacción que la plataforma @DAN ofrece a las necesidades del mercado.

– **Contiforme**, empresa portuguesa dedicada a la fabricación de papel moneda, tarjetas de crédito y soluciones basadas en tarjeta inteligente, realiza los tests de usuario final.

LA SOLUCIÓN

El cliente

La solución cliente se basa de una tarjeta inteligente Java más la PDA, con los periféricos necesarios para leer la tarjeta y conectarse de manera inalámbrica.

La elección de una **tarjeta** Java está motivada, entre otras razones, por la necesidad de multiaplicación, uno de los requisitos del proyecto, como se puede ver en el apartado de conceptos. Esta tarjeta lleva cargados un *applet* EMV **[5]**, que permite utilizarla como una tarjeta de crédito de nueva generación en cajeros y comercios físicos y un *applet* criptográfico que la dota de los requisitos técnicos necesarios para generar firmas digitales de forma segura. Del mismo modo, el uso de una tarjeta Java independiza los desarrollos de los *applets* del proveedor de tarjetas. Tanto las tarjetas como los *applets* para el proyecto los proporciona Giesecke&Devrient a través de su filial española.

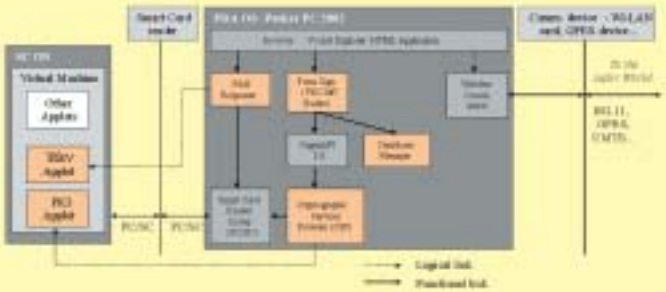


Figura 3.- Arquitectura cliente

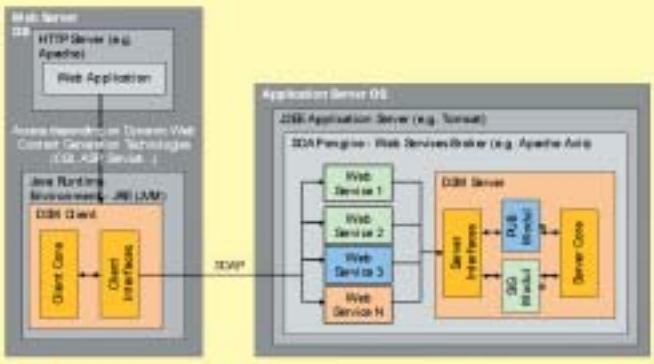


Figura 4.- Posible integración con aplicación web

La **PDA** utiliza sistema operativo (SO) Microsoft. Esta decisión está basada en el número de fabricantes de PDAs que utilizan este SO, la cuota de mercado creciente del mismo en el sector de las PDAs y la disponibilidad de herramientas y de soporte. De todas formas, el enfoque modular de la plataforma, que independiza totalmente el cliente del servidor, asegura que migrar a un nuevo SO de PDA no resulte traumático.

Es necesario dotar a la PDA de una camisa de expansión en la que se insertan el lector de tarjeta inteligente y el hardware de comunicaciones (tarjeta WiFi o GPRS). Este hardware se obtiene de proveedores externos al proyecto. En el proyecto se desarrollan los siguientes módulos de software que se ejecutan en la PDA:

– **FormSign:** se responsabiliza de firmar formularios web. Se itera a lo largo de los elementos del formulario y se va construyendo la cadena a firmar. Algunos elementos que no aportan información, como botones p.e., no se incluyen.

– **Certificate Manager:** módulo encargado de gestionar los certificados en la PDA. Permite extraer certificados de la tarjeta inteligente e instalarlos en el registro de la PDA y relacionarlos con sus respectivas claves privadas, bajo autorización del titular del certificado. También presenta una ventana al usuario que le permite seleccionar qué certificado utilizar cuando una aplicación requiere el uso de certificado.

– **PKCS#7 Builder: [6]** este módulo, siguiendo el estándar PKCS#7, genera los mensajes criptográficos requeridos por las aplicaciones y que en su caso serán validados por el sevidor. Actualmente implementa los *contentType Data* y *SignedData* del estándar y se está trabajando en la implementación del resto de *contentType*.

– **Cryptographic Service Provider (siguiendo la especificación de Microsoft): [7]** Pieza básica en la arquitectura criptográfica se encarga de proveer a las aplicaciones de servicios criptográficos que éstas necesitan, tales como cifrado, descifrado, firma digital... En el caso @DAN delega esta responsabilidad en la tarjeta inteligente, por lo que actúa como *token interface*. Se accede a él a través de la CryptoAPI 2.0 implementada en Pocket PC2002.

– **PAN Requester:** este módulo se invoca desde servidor y su propósito es obtener la información del número de tarjeta de crédito (PAN - *Personal Account Number*) y fecha de caducidad de la misma. Esta información, que es pública, se encuentra en el *applet* EMV y se recupera para presentarla a las aplicaciones que la necesiten sin necesidad de que el usuario introduzca esta información.

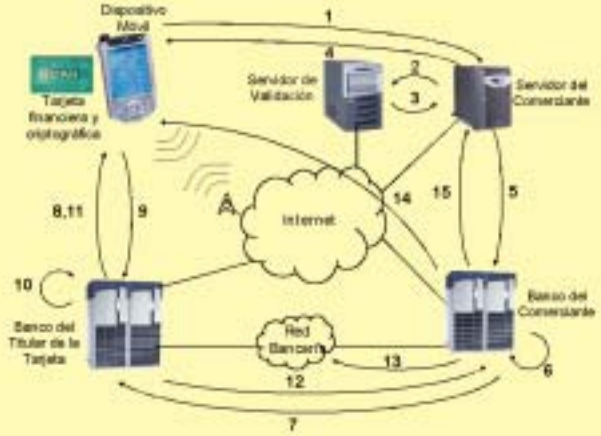
El servidor

La firma digital se enfrenta a ciertos problemas culturales. La mayoría de la gente desconoce qué es una firma digital y cuán segura es. Durante el proyecto hemos detectado que ciertos procesos pueden ayudar a la aceptación y entendimiento de lo que realmente es la firma digital. Es por este motivo que, aparte de ofrecer los servicios de **firma** y **verificación** (de integridad), basados en mensajes PKCS#7 *attached* o *detached*, y de **identificación** mediante el uso de certificados X.509v3 y la consulta del estado de los mismos vía CRLs, también se ofrece un servicio de **formateo** de los mensajes. Este servicio añade a los mensajes firmados ciertas marcas o identificadores que permitan al receptor saber quién, cuándo y cómo se ha firmado un mensaje. Estas marcas pueden ser firmas manuscritas escaneadas, códigos de barras bidimensionales o cualquier otro tipo de marca que se requiera.

El servidor puede reconocer certificados emitidos por una o más CAs y se puede desactivar la consulta a las CRLs. Desarrollado en JAVA para dotarlo de independencia de la plataforma, está orientado a integrarse con terceras aplicaciones (probada con éxito su integración con Siebel) por lo que ofrece interfaces para Java, C/C++, VB así como *Web Service* para recibir peticiones de servicio. Es un producto que puede instalarse en modo *stand-alone*, en un servidor dedicado o configuraciones intermedias.

@DSM (@DAN *Digital Signature Manager*) se basa en una arquitectura por capas, a saber:

– Capa de Módulos: define la agrupación de los servicios en módulos que representan los componentes que pueden



DESCRIPCIÓN

1. El repartidor entrega la PDA al cliente y éste introduce su tarjeta y los litros que desea en un formulario web. El comerciante (empresa que reparte el gas-oil) solicita que se firme el formulario. El cliente firma el formulario haciendo uso de las capacidades criptográficas de la tarjeta. El formulario firmado (mensaje PKCS#7) se envía al comerciante.
2. El comerciante envía el PKCS#7 recibido al Validador.
3. El Validador contesta con un informe (se asume que la respuesta es 'Ok').
4. El comerciante informa al cliente de que la firma es correcta, a través de una página web. El comerciante recupera el número de tarjeta y la fecha de caducidad de forma automática e informa de ello al cliente.
5. El comerciante se identifica frente al TPV virtual de su banco y le envía los datos de la compra (número de tarjeta, fecha de caducidad e importe.) El comerciante entrega a su banco el control de la sesión de Internet del cliente.
6. El banco realiza un conjunto de acciones entre las que se encuentra la verificación de que los datos de la tarjeta son correctos y qué banco ha emitido esa tarjeta (banco del titular de la tarjeta).
7. El banco del comerciante se comunica con el banco del titular para que éste autentique al cliente. Para ello le envía el número de tarjeta. El banco del comerciante le pasa el control de la sesión de Internet del cliente al banco del titular.
8. El banco del titular autentica a éste (es decir, se asegura que el cliente que está realizando la compra y el titular de la tarjeta son la misma persona) mediante la presentación de una web que requiere la presentación de certificado cliente para establecer una sesión SSL.
9. El cliente selecciona el certificado de la tarjeta y se lo envía su banco (el banco del titular).
10. El banco del titular realiza las operaciones pertinentes para asegurar la autenticidad y validez del certificado, autenticando así al cliente.
11. El banco del titular le muestra al cliente una ventana con los datos de la compra (litros, comerciante, importe, fecha y hora). La misma ventana informa al cliente que el certificado introducido para autenticarse es válido.
12. El banco del titular informa al del comerciante de que acepta el cargo en la tarjeta y le entrega el control de la sesión de Internet del cliente.
13. El banco del comerciante, a través de la red bancaria, carga el pago y hace una anotación para pagar posteriormente al comerciante.
14. El banco del comerciante muestra al cliente una ventana informándole de la comprar y de que su banco ha aceptado el cargo.
15. El banco del comerciante retorna el control de la sesión de Internet del cliente al comerciante.

Figura 5.- Caso de uso

instalarse separadamente. Actualmente, Módulos de Firma (SIG) y de Publicación (PUB).

– Capa de Servicios: servicios disponibles para terceras aplicaciones. Actualmente firma, verificación, identificación y formateo.

– Núcleo: librerías y servicios que no están disponibles para terceras aplicaciones (configuración, *log*, control de acceso y *PKI Core Library*).

Los servicios de pago

El concepto de pago de @DAN utiliza una tarjeta inteligente financiera como almacén de una clave privada (requisito) y del certificado asociado (recomendado por portabilidad.) El certificado se asocia unívocamente con el número de tarjeta de crédito que lo contiene, lo que implica un proceso de registro. Este certificado digital se utiliza en el proceso de pago para identificar la tarjeta (ya que está vinculado unívocamente a ella) y autenticar al titular.

Como ya se ha mencionado, los servicios de pago utilizados en @DAN se basan en los estándares de compra segura de Visa y Mastercard (*Verified by VISA* y *Mastercard Secure Code*) con modificaciones para adaptarlo a las restricciones de la PDA. Esta modificación es realmente importante pues implica que el servicio de pago seguro por Internet más extendido mundialmente está integrado en el concepto de movilidad de @DAN. También se ha modificado el servicio de pago para aceptar certificados digitales X.509v3 como medio de autenticar al titular de la tarjeta de crédito.

Los servicios de pago: Terminal Punto de Venta Virtual (TPV virtual)

El TPV virtual es el servicio que provee el banco del comerciante que ofrece sus productos o servicios en Internet para la gestión de las órdenes de compra, el procesado de las mismas en tiempo real (cargo en la tarjeta de crédito del comprador y abono en la cuenta del comerciante) y la respuesta tanto al comprador como al comerciante del resultado de la transacción.

Para que un comerciante pueda integrar un TPV virtual en su comercio web, en @DAN se han desarrollado y se entregan como parte de la plataforma, los siguientes elementos:

– Instrucciones técnicas para el comerciante.

– Simuladores de TPV virtual: tres programas que simulan las llamadas de un TPV virtual. Con estos simuladores el desarrollador del web del comerciante puede probar la ejecución de su TPV virtual desde el primer momento. Se provee también un ejemplo de cómo programar la llamada al TPV virtual.

– Conjunto de rutinas de algoritmos de *hash* sha-1. Estas rutinas se pueden utilizar desde diferentes entornos de programación (ASP, JSP, perl, php.) Una de estas rutinas es necesaria para firmar los mensajes intercambiados entre el comercio web y el servidor de TPV virtual.

El objetivo prioritario de esta parte del proyecto es hacer tan fácil como sea posible el desarrollo de comercios web que utilicen este TPV virtual.

UN CASO DE USO: REPARTO DE GAS-OIL

Se asumen los siguientes prerrequisitos:

– La asociación del certificado digital con la tarjeta (registro) ya se ha realizado.

– La tarjeta es de crédito/débito (*applet* EMV) y almacena certificado digital y clave privada asociada (*applet* criptográfico).

– El titular de la tarjeta y el cliente son dos roles diferentes, aunque deben coincidir en la misma persona física.

– Si no se menciona explícitamente, las comunicaciones son por Internet.

CONCLUSIÓN

Algunos procesos basados en papel no se podían migrar al mundo digital porque la tecnología no daba soporte a los requisitos de la empresa o legales. Esto implica que la optimización de estos procesos se veía frenada por las limitaciones que imponía el soporte físico de los mismos. @DAN, mediante las facilidades que ofrece para integrar la firma digital en PDAs, permite esta migración, es decir, habilita la mejora de procesos.

Las empresas como elemento diferenciador y la administración como herramienta de acercamiento al ciudadano, necesitan ofrecer nuevas vías de realizar pagos. Estas vías deben ofrecer ahorro de tiempo, facilidad de uso y confianza. @DAN extiende las vías existentes a nuevos dispositivos y ofrece mecanismo de seguridad a los entes implicados en un pago. ❖

José Manuel López González
Jefe de Proyectos, Secartis
División de Consultoría y Proyectos
GyD Ibérica
jmanuel.lopez@es.gi-de.com

REFERENCIAS

[1] Effectiveness Criteria for Internet Payment Systems. Tae Hwan Shon, Paula M.C. Swatman. Department of Information Systems. Monash University. Australia
[2] 3D Model: http://international.visa.com/fb/paytech/secure/main.jsp
[3] White Paper on growth, competitiveness, and employment: The challenges and ways forward into the 21st century. COM(93) 700 final
[4] GOTIC Project: http://dursi.gencat.es/generados/catala/societat_informacio/noticia/1020_12_4880.html
[5] EMV: <http://www.emvco.com/>
[6] PKCS standards: <http://www.rsasecurity.com/rsalabs/pkcs/index.html>
[7] CSP: http://msdn.microsoft.com/library/en-s/security/security/cryptographic_service_providers.asp <http://msdn.microsoft.com/library/en-us/security/security/cryptographic_service_providers.asp>