Medios de pago e identificación personal en la era digital

#InformeNae

nae_
doing ahead

Índice

Créditos

Dirección:
Ginés Alarcón

Autor:
Manuel Borrajo

Con la colaboración de:
José Miguel González

Publica:
Nae
www.nae.es
@nae_es

Segunda edición:
13.04.15

>1 Resumen ejecutivo

"La nueva generación de usuarios de servicios móviles ha nacido con internet (smartphones, aplicaciones, redes sociales, información en la nube, etc.), y su forma de relacionarse no se entiende sin estos medios tecnológicos."

"Las empresas privadas y los organismos públicos necesitan adoptar una transformación inmediata hacia estos entornos."

Sinopsis

En este documento se analiza la transformación de los sistemas de pago e identidad personal en la vanguardia de la digitalización y las áreas de negocio en las que impacta.

Para ello se describe la situación actual desde un punto de vista neutral, analizando los aspectos mas relevantes del entorno de negocio: cadena de valor, actores del ecosistema, tecnología, normativas, seguridad, oportunidades, y barreras.

Para concluir se describen los principales atributos que deben cumplir los servicios para garantizar la calidad, seguridad y usabilidad que demandan los clientes, y las recomendaciones para desarrollar un entorno de mercado abierto y competitivo.

Introducción

La nueva generación de usuarios digitales han nacido conectados (smartphones, aplicaciones, redes sociales, información en la nube, etc.), y su forma de relacionarse no se entiende sin estos medios tecnológicos, ya sea en el ámbito profesional o personal. Esto implica que los mercados, las empresas privadas y los organismos públicos necesitan adoptar una transformación inmediata hacia estos entornos.

Los avances tecnológicos están acelerando este proceso, proporcionando aplicaciones más sofisticadas y seguras, tanto en banca y pagos móviles como en identificación personal. Para 2017 se prevé que el valor de las transacciones móviles sea de 721.000 millones de dólares.

Claves para entender el nuevo entorno

- Aunque los usuarios ya están preparados y demandan esta transformación, los organismos públicos y privados, en general, no están listos para enfrentarse a este reto. Se han identificado razones como la inseguridad respecto a la evolución tecnológica y la incertidumbre de una modificación de la cadena de valor con la aparición de nuevos actores.

- En el ecosistema de los medios de pago móviles, a los actores que provienen del entorno natural (bancos, redes de medios de pago, comercios), se suman los que definirán su importancia próximamente (operadores móviles, compañías puntocom, fabricantes de móviles), y los organismos encargados de la regulación.

- Además de las tarjetas inteligentes con capacidad de comunicación sin contacto (*Contactless*; NFC), otros

avances tecnológicos que permiten ofrecer estos servicios son los smartphones y las redes GSM de tercera y cuarta generación. Otros servicios que estarán a disposición de los usuarios son: pago de billetes y abonos de transporte; tarjeta sanitaria, de seguros y fidelización; DNI y pasaporte digital; tarjetas de acceso físico a vehículos y edificios; claves de acceso a sistemas infomáticos y webs, entradas para espectáculos; y/o carteles inteligentes.

– Para alcanzar niveles de servicio óptimo existen aún muchos interrogantes pendientes de respuesta:

- ¿El Dispositivo Seguro debe ser una tarjeta SIM física en el teléfono móvil, o una tarjeta virtual mediante software en la red?
- ¿La seguridad de acceso a las credenciales y claves de usuario será suficiente para evitar el fraude y conseguir la confianza de los usuarios?
- ¿El DNI, pasaporte y otros títulos de identidad pública, podrán integrarse en este modelo junto con las iniciativas privadas?
- ¿Qué tecnología de proximidad será finalmente la utilizada, el modelo NFC utilizado por Samsung o el de Bluetooth de bajo consumo promovido por Apple?
- ¿Los clientes dispondrán de una atención común integrada o en caso incidencias deberán llamar a cada uno de los proveedores de los servicios? ¿Podrán gestionar múltiples tarjetas de diferentes proveedores?

Atributos de los Servicios

La estrategia para el desarrollo de estos nuevos servicios, tanto públicos como privados, debe plantearse desde la perspectiva de los clientes: asegurando los atributos mínimos que garanticen su aceptación con unos niveles de calidad y precio razonables:

- Seguridad
- Transparencia
- Confidencialidad
- Universalidad del servicio
- Portabilidad
- Simplicidad
- Consistencia
- Accesibilidad
- Fiabilidad
- Gratuidad del servicio básico universal
- Disponibilidad de servicios de valor añadido

"Las empresas de los sectores implicados corren el riesgo de centrarse en modelos protectores del status quo y bloquear las iniciativas abiertas y transversales, centradas en las necesidades de los clientes."

"El liderazgo en el desarrollo de los nuevos servicios puede servir de estímulo para la creación de nuevas iniciativas empresariales."

Conclusiones

- El crecimiento actual del negocio, superior al 30% anual, puede verse estancado o experimentar un crecimiento mayor si se orienta hacia un modelo sostenible centrado en las necesidades de los clientes y la viabilidad de las empresas.

- El modelo de los servicios móviles actual no ha conseguido aún implantar soluciones que cumplan los atributos mínimos de seguridad, simplicidad, universalidad, fiabilidad, precio, y disponibilidad que demandan los usuarios.

- Las empresas de los sectores implicados corren el riesgo de centrarse en modelos protectores del status quo y bloquear las iniciativas abiertas y transversales, centradas en las necesidades de los clientes. En un ecosistema tan fragmentado, es imprescindible que los organismos de regulación favorezcan un entorno colaborativo y competitivo.

- La Administración Pública tienen la oportunidad de liderar la definición de un modelo que facilite el desarrollo eficiente de servicios públicos: sanidad, transporte, seguridad e identificación.

- Aunque España ha sido un país líder indiscutible en la implantación de soluciones de banca y telecomunicaciones, no se visualiza ese liderazgo en la transformación digital. No debemos perder este posicionamiento que puede servir de estímulo para mejorar los servicios privados y públicos, disminuyendo a la vez los costes, y facilitando la creación de nuevas iniciativas empresariales y de empleo.

>2 Principales actores del ecosistema de medios de pago móviles

"Como líderes de la introducción de las TIC y tratándose de un ecosistema que se basa en la transacción financiera, las entidades bancarias adoptan un rol predominante, pero no único."

Clientes o usuarios de los servicios

Constituyen el objetivo principal del ecosistema. Es decir, analizamos el modelo centrado en el cliente o usuario de tal manera que los productos y servicios deben responder a las necesidades presentes o latentes.

Entidades proveedoras de los productos y servicios

Los proveedores de los servicios pueden ser, entre otros, entidades financieras que emiten tarjetas de pago, comercios que proporcionan tarjetas de fidelización, compañías de transporte que porporcionan títulos o abonos para sus usuarios, o entidades de salud y seguros que identifican a sus beneficiarios con tarjetas electónicas virtuales.

En el ecosistema intervienen también entidades proveedoras de servicios, que gestionan determinados procesos de la cadena de valor, subcontratadas por las empresas que prefieren externalizar una determinada función muy especializada o compleja. Por ejemplo: emisión física o virtual de las tarjetas, certificados y claves de usuario, atención al cliente, o gestión de los sistemas TIC correspondientes.

Entidades Bancarias

Como líderes de la introducción de las TIC y tratándose de un ecosistema que se basa en la transacción financiera adoptan un rol predominante, pero no único. Pueden producirse actividades que no requieran pagos, como en servicios de identificación, o en los que el pago se realice directamente entre usuarios.

Redes y sistemas de medios de pago

Los pagos electrónicos actuales se realizan mediante tarjetas de crédito y débito, emitidas por los bancos, que ofrecen su servicio tanto al comerciante (adquiere el pago) como al consumidor final (emite la tarjeta). Los sistemas informáticos y las redes de comunicación segura que permiten dichos pagos son operados por empresas especializadas proporcionadas por la marca correspondiente de las tarjetas.

Operadores de servicios móviles (*Mobile Network Operator, MNO*)

Son imprescindibles para acceder a los servicios. El acceso al sistema de medios de pago e identificación se realiza a

"Los sistemas de pagos bancarios y servicios de identificación requieren una presencia activa de la administración pública, tanto desde el punto de vista fiscal como de identificación en los servicios públicos (sanidad, transporte, etc.)."

través de los terminales móviles las aplicaciones y credenciales necesarias se almacenan principalmente en las tarjetas SIM.

Fabricantes de equipos

Aunque algunos servicios pueden ser accesibles desde teléfonos básicos mediante SMS (transferencia de mensajes de texto), el verdadero potencial del sistema solo es accesible a través de los smartphones que soporten aplicaciones específicas y comunicación con los Terminales del Punto de Venta (TPV, o en inglés *POS: Point of Sale*).

Proveedores de software

Permiten el desarrollo, integración y mantenimiento de aplicaciones no sólo para los usuarios y comercios, sino también para el resto de actores: bancos, redes de medios de pago y operadores.

Proveedores de tarjetas inteligentes

Responsables de la introducción de chips en las tarjetas SIM y bancarias, tienen un papel importante en la migración de la banda magnética a la funcionalidad inalámbrica NFC (*Contactless*).

Gestores de Servicios de Confianza (*TSM: Trusted Service Managers*)

Permiten la gestión de los servicios de provisión y posventa en el ecosistema de pagos móviles de una manera independiente y segura. Estos gestores de servicio neutrales pueden facilitar los acuerdos operativos entre los principales actores.

Regulación y normativa

Fomentan la calidad e integridad de los servicios, y aseguran la competitividad e interoperabilidad de un sistema universal.

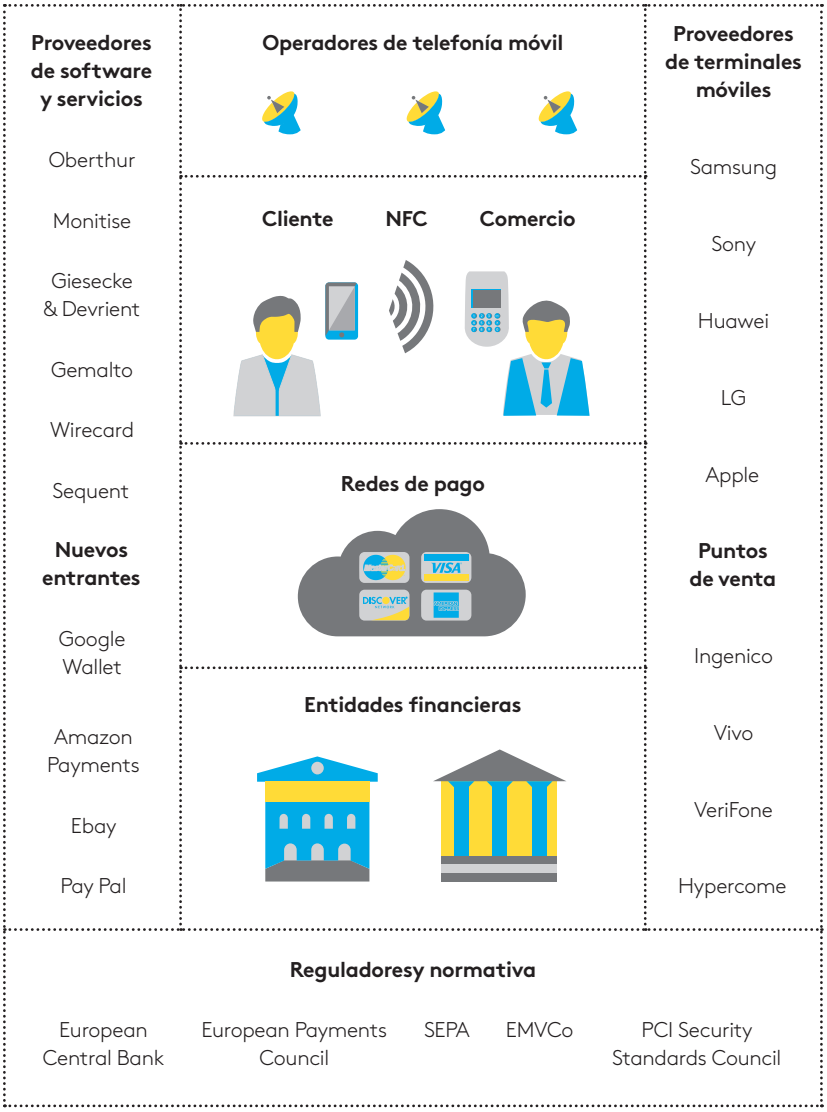
Organismos públicos

Los sistemas de pagos bancarios y servicios de identificación requieren una presencia activa de la administración pública, tanto desde el punto de vista fiscal como de identificación en los servicios públicos (sanidad, transporte, etc.).

Compañías de internet (puntocom)

El ecosistema de medios de pago móviles es un entorno natural para las compañías que han nacido o se han desarrollado con internet, como Google, Amazon, o Apple. Su dinamismo y flexibilidad en la orientación al cliente y su experiencia y capacidad de innovación las puede convertir en protagonistas de esta transformación. La integración con el comercio electrónico y los servicios de marketing relacional abren un abanico de oportunidades a estas compañías para captar nuevo negocio.

Diagrama del ecosistema de servicios de pago por móvil



>3 Entorno tecnológico

Terminales móviles inteligentes

Los smartphones actuales no tienen nada que envidiar a los ordenadores personales, tanto en capacidad de proceso como en memoria, almacenamiento, comunicaciones y resolución de la pantalla. No es extraño que nuestro móvil sea más potente en la mayoría de sus funciones que el ordenador personal que usamos, por lo que en lugar de teléfono móvil podríamos hablar de ordenador personal móvil.

El aspecto más relevante de las capacidades de un smartphone, y quizá el más necesario por su condición móvil, son las comunicaciones:

- WiFi 802.11 a/b/g/n/ac
- GPS / GLONASS
- NFC
- Bluetooth® 4.0
- Infra Rojos LED
- 3G y 4G

Especificaciones técnicas de un smartphone:

- Procesador: 1,9 GHz QuadCore
- Pantalla: 1980x1080 (441 ppi)
- Memoria RAM: 2 GBs
- Almacenamiento: 64 GB + Slot microSD 64 GB
- Cámara: 13 megapíxeles

Estas capacidades permiten que los smartphones puedan soportar las mismas aplicaciones que cualquier ordenador personal fijo, añadiendo funciones propias como GPS, acelerómetro, etc. El desarrollo de aplicaciones para las plataformas móviles más extendidas: Android de Google, iOS de Apple y Windows Phone de Microsoft, ha sido exponencial y se estima que existen mas de 1 millón de aplicaciones disponibles.

La penetración media de los smartphones a finales del 2012 en España superó el 66% del total de móviles[1], con un crecimiento del 15% respecto al año anterior. Esta cifra sitúa a España como líder de penetración en la Europa de los 5 (Alemania, Francia, Reino Unido, Italia y España), con una penetración media del 57%. Durante el 2012, 8 de cada 10 móviles vendidos fueron del tipo smartphone; adicionalmente se estima que el 70% de los usuarios de teléfonos inteligentes dispone también de tableta.

Tarjetas inteligentes y NFC (Contactless)

Las tarjetas inteligentes (*Smart Card o ICC: Integrated Circuit Card*) son actualmente el corazón de los medios de pago.

— 1
Comscore: Spain Digital Future in Focus, 2013.
http://goo.gl/wJnAoj

"Una tarjeta inteligente permite integrar, en un solo microchip, aplicaciones seguras de diferentes proveedores de servicios."

Estas tarjetas contienen un microchip con su correspondiente unidad de control (CPU), memoria de almacenamiento (RAM/ROM/EPROM) y sistema de entrada y salida. En su parte superior disponen de unas patillas para facilitar el contacto eléctrico, tanto para la alimentación del chip como para la transmisión de datos a los lectores de tarjetas.

Capacidades de las tarjetas inteligentes

Los microchips de las tarjeta actuales disponen de procesadores tipo RISC de 32 bits, alcanzando velocidades de 32 MHz y con capacidades de memoria RAM de 144 KB y memoria FLASH 1,2 MB. La seguridad en las tarjetas se realiza tanto a nivel físico (es necesario destruir la tarjeta para acceder a sus componentes), como a nivel lógico, con mecanismos de encriptación tipo 3DES, RSA y ECC.

Las capacidades de proceso y almacenamiento permiten proporcionar no solo servicios de identificación y autenticación segura, sino todo tipo de aplicaciones que requieran almacenamiento y proceso de datos.

Diferentes aplicaciones pueden incluso convivir en una misma tarjeta mediante mecanismos que facilitan entornos seguros completamente independientes. Esta funcionalidad de las tarjetas inteligentes permite integrar, en un solo microchip, aplicaciones seguras de diferentes proveedores de servicios, por ejemplo: modulo SIM del operador móvil, tarjetas de crédito bancarias, abonos de transporte, etc.

Aplicaciones de las tarjetas inteligentes

Las primeras experiencias con tarjetas inteligentes en servicios masivos nacieron en Francia en el sector de las telecomunicaciones (*Télécarte*: tarjetas prepago para utilización en cabinas telefónicas), y en el sector financiero (*Carte Bleue*: tarjetas con PIN de seguridad para transacciones en puntos de venta). Posteriormente se fueron introduciendo en otros sectores: expendedores, acceso a sistemas informáticos, televisión de pago, transporte, identidad, etc.

Los teléfonos móviles en las redes GSM adoptaron el uso de tarjetas inteligentes con la denominación SIM (*Suscriber Identification Module*). En estas tarjetas SIM se almacena la identificación del usuario y las claves (PIN) correspondientes para el acceso y comunicación segura al servicio. Las tarjetas SIM han evolucionado según el modelo UICC (*Universal Integrated Circuit Card*) que permite la convivencia de diferentes aplicaciones en la misma tarjeta y es una de las bases para el modelo de medios de pago por móvil.

Aunque las tarjetas inteligentes usadas en telefonía móvil y las tarjetas de crédito/débito del sector financiero utilizan básicamente el mismo concepto de microchip, existen diferencias menores en el tipo de encapsulado plástico y también en las especificaciones eléctricas.

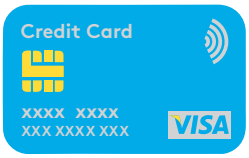
NFC - Contactless

Para facilitar la comunicación sin contacto entre las tarjetas inteligentes y los puntos de venta, se desarrolló el estándar NFC (*Near Field Communication*) cuando Nokia, Sony y Philips formaron el NFC Forum.

NFC se basa en la tecnología RFID (*Radio Frequency Identification*) y permite la comunicación bidireccional entre dispositivos a menos de 4 cm de distancia y a una velocidad máxima de 424 kbps.La alimentación eléctrica del microchip se proporciona sin necesidad de contacto, gracias a la inducción electromagnética proporcionada a través del dispositivo terminal NFC (cajero o punto de venta).

NFC define 3 modos de operación:

- Comunicación de igual a igual (P2P: Peer to Peer)
- Comunicación en modo lectura/escritura
- Emulación de Tarjeta NFC



Actualmente el modo más extendido de funcionamiento es el de emulación de tarjeta. Mediante este sistema, una tarjeta UICC-NFC en un teléfono móvil puede actuar emulando una tarjeta de crédito/débito del tipo NFC-*Contactless* de forma transparente para el Terminal de Punto de Venta con funciones NFC.

Aplicaciones NFC

NFC y otros estándares RFID no sólo facilitan las aplicaciones de medios de pago. También permiten otras múltiples aplicaciones basadas en la identificación personal: acceso

"Los servicios en la nube, o servicios en la red, permiten un acceso universal a los contenidos, independientemente del tipo de terminal (móvil, tablet, TV y PC) que el usuario requiera en cada momento."

físico a edificios, acceso lógico a sistemas informáticos, control de vehículos, estacionamiento, etc.

Otra de las aplicaciones más extendidas de esta tecnología es el intercambio de información, bien directamente entre usuarios de teléfonos móviles, o para facilitar la lectura de información de carteles en centros comerciales. En este último caso el cartel podría informar, por ejemplo, del estreno de una película, y a la vez permitir la compra online de la entrada correspondiente.

Servicios en la red (nube)

El desarrollo y abaratamiento de las plataformas de multiproceso virtual, tanto hardware como software, junto con el incremento de las capacidades en el acceso a las redes IP mediante la utilización de fibra óptica y banda ancha móvil, ha propiciado una transformación en el modelo de acceso a los contenidos y aplicaciones. Los servicios en la nube, o servicios en la red, permiten un acceso universal a los contenidos, independientemente del tipo de terminal (móvil, tablet, TV y PC) que el usuario requiera en cada momento. Además se asegura la disponibilidad de la información y el software, sin temor a la perdida o destrucción de los terminales de acceso.

Los servicios en la nube también pueden proporcionar la capacidad necesaria tanto en velocidad de acceso y proceso, como de seguridad para albergar las aplicaciones y credenciales de pago de los usuarios (ver apartado *Dispositivos Seguros*). De esta forma se consigue establecer un modelo independiente, tanto de los operadores móviles como de los fabricantes de terminales móviles.

Bluetooth y WiFi

La última especificación de Bluetooth versión 4.0, también denominada *Bluetooth Smart*, incluye las especificaciones del Bluetooth clásico: de alta velocidad (basado en WIFI), y de bajo consumo, utilizada en los dispositivos *iBeacon* (ver capítulo *Beneficios y oportunidades*).

El desarrollo de las capacidades de esta nueva versión en cuanto a velocidad (hasta 24 Mbits.), alcance (hasta 100 m.), seguridad, y bajo consumo, hace que Bluetooth sea particularmente atractivo en todo tipo de dispositivos de consumo tales como: teléfonos, impresoras, teclados, televisiones, equipos de música, mandos, relojes inteligentes y sensores.

WiFi supone la evolución de las redes locales (LAN) basadas en cable y en los clásicos estándares de Ethernet 802.3 hacia

"La quinta generación WiFi, denominada 802.11ac, alcanza velocidades superiores a 1 Gbit y permite la transmisión de video de muy alta definición."

redes inalámbricas definidas en el estándar 802.11. La versión actualmente utilizada es la 802.11n que permite alcanzar velocidades de hasta 600 Mbits. Este estándar "n" funciona en la misma banda de 2,4 GHz que utilizan los sistemas anteriores y que está próxima a su saturación, por lo que ya se ha desarrollado la quinta generación WiFi, denominada 802.11ac que también permite la banda de 5 GHz y aunque con menos cobertura, alcanza velocidades superiores a 1 Gbit y permite la transmisión de video de muy alta definición.

Las capacidad de comunicaciones de los estándares WiFi y Bluetooth complementan las funciones de la comunicación de cercanía y sin contacto de NFC; de esta forma los servicios de marketing que requieren un mayor ancho de banda por los contenidos multimedia requeridos, pueden utilizar WiFi y/o Bluetooth, mientras que la operación de compra final puede utilizar NFC para interactuar con el Terminal de Punto de Venta de una manera más segura.

>4
Servicios de pago por móvil y otros nuevos servicios

"Los pagos por móvil son aquellos en los que la orden y confirmación de pago se realizan a través de las funciones disponibles en los móviles."

Los móviles inteligentes se han convertido en un instrumento de uso cotidiano en la vida de los consumidores y usuarios profesionales, por ello resulta natural su utilización en las operaciones de pago para la adquisición de bienes o uso de servicios. Los pagos por móvil son aquellos en los que la orden y confirmación de pago se realizan a través de las funciones disponibles en los móviles. En este sentido podemos distinguir dos categorías principales: pagos móviles a distancia y pagos móviles de proximidad.

Pagos móviles a distancia

En estas operaciones el comercio o punto de venta se encuentra habitualmente lejos del consumidor y la comunicación con el sistema de pago se realiza a través de internet. Estas operaciones normalmente se realizan a través de la web, en tiendas o sistemas de servicios online.

Los medios habituales de pago en este caso son:

- Pagos con tarjetas de crédito/débito: su uso es casi universal en el entorno de las tiendas online. En algunos portales, los usuarios sólo pueden darse de alta tras registrar una tarjeta válida.
- Transferencias o adeudos domiciliados: habitualmente son sistemas nacionales, y particularmente en el entorno de la Administración y Servicios Públicos, en los que se utiliza el sistema online del banco elegido por el consumidor para la confirmación del pago.
- Pagos a través de proveedores de pagos electrónicos: algunas tiendas online permiten el pago a través de cuentas personales abiertas en medios de pago electrónico tipo PayPal o AmazonPayments.

Pagos móviles de proximidad

Son los que se realizan directamente en el comercio o puntos de venta. Estos pueden ser atendidos por personal o ser dispensadores automáticos. Los consumidores utilizan su teléfono para interactuar directamente con el Terminal de Punto de Venta (TPV). Esta comunicación se realiza directamente a través de protocolos de comunicación de proximidad:

- NFC (*Near Field Communication*): el teléfono y el TPV interactúan gracias a esta tecnología que permite una comunicación bidireccional.
- Códigos de barra bidimensionales: el teléfono presenta un código de transacción que escanea el TPV o viceversa.

Los medios de pago utilizados en estos casos son habitualmente tarjetas de crédito/débito almacenadas en el propio teléfono, que se comporta en estos casos como si fuera una tarjeta física de plástico.

La Caixa instaló los primeros cajeros *Contactless* del mundo en 2011 con tecnología de Fujitsu. Durante 2012 comenzó el despliegue masivo en otras entidades financieras (Santander, BBVA, Banco Sabadell, etc.). En paralelo también se están sustituyendo las tarjetas de sus clientes con tarjetas inteligentes con NFC. A finales de 2013 se estimaba que el número de terminales de venta adaptados al servicio *Contactless* sumaba más de 300.000. Este importante desarrollo ha situado a España como unos de los países pioneros en su implantación y es el motivo por el que Vodafone ha lanzado su servicio Vodafone Wallet en España.

Documentos de identificación personal

El DNI electrónico (DNI-e) comenzó a expedirse en el año 2006 y se basa en tarjetas inteligentes con microchip según la normativa ISO 7816[2]. Actualmente no soporta tecnología *Contactless*, a diferencia del pasaporte, que sí está preparado.

El objetivo del nuevo DNI es fomentar el desarrollo de la sociedad de la información y para ello almacena digitalmente los siguientes elementos:

- Certificado electrónico para autenticar la personalidad del ciudadano.
- Certificado de firma electrónica, con la misma validez jurídica que la firma manuscrita.
- Certificado de la autoridad de certificación emisora.
- Claves para su utilización.
- Plantilla biométrica de la impresión dactilar.
- Fotografía digitalizada del ciudadano.
- La imagen digitalizada de la firma manuscrita.
- Datos de la filiación del ciudadano.

Si bien el despliegue del nuevo DNI ha sido masivo, dado que en la renovación se han ido sustituyendo paulatinamente, la aplicación práctica hasta la fecha no ha sido satisfactoria. Esta se reduce, de forma minoritaria, a la utilización

— 2
ISO 7816
http://goo.gl/VLcYhj

"Resulta sorprendente comparar la lentitud en la incorporación de las nuevas tecnologías para el acceso a los servicios de salud, y el dinamismo e innovación presentes en el desarrollo de los servicios bancarios."

del certificado de autenticación y firma para el acceso a servicios online de la administración pública, y en particular a los relativos a la agencia tributaria.

La razón de este uso minoritario radica, por una parte, en la dificultad para instalar el equipamiento y software necesarios en los ordenadores personales de los usuarios, y por otra, en que no se han desarrollado aplicaciones prácticas para su utilización en otros ámbitos privados y públicos.

El plan estratégico de la Policía contempla la introducción de una nueva versión, el DNI 3.0, en 2016. Esta nueva versión podría incluir tecnología de proximidad tipo NFC *Contactless*, de tal forma que se podría aprovechar el despliegue masivo de lectores con esta tecnología en los comercios, gracias al desarrollo del modelo de pago con tarjetas de crédito/débito y pago por móvil.

Tarjetas sanitarias

El pasado 20 de septiembre de 2013 el Gobierno de España aprobó en el Consejo de Ministros la creación de la Tarjeta Sanitaria Individual común para todo el territorio nacional. El decreto ley 702/2013[3] especifica los datos básicos comunes y las especificaciones técnicas básicas que permitirán su interoperabilidad en las 17 comunidades autónomas. Estas especificaciones incluyen la posibilidad de utilización de tarjetas inteligentes con chips sujetos a la normativa UNE-EN1387:1997.

El Sistema Nacional de Salud (SNS) deberá implantar la infraestructura necesaria que permita el acceso seguro desde los diferentes organismos de salud de las comunidades a los historiales médicos, utilizando para ello el Código de Identificación del Paciente (CIP) a nivel nacional, denominado CIPSNS.

Resulta sorprendente comparar la lentitud en la incorporación de las nuevas tecnologías para el acceso a los servicios de salud, y el dinamismo e innovación presentes en el desarrollo de los servicios bancarios. La integración en el ámbito del sector bancario y las telecomunicaciones de los servicios

— 3
Real Decreto 702/2013, de 20 de septiembre, http://goo.gl/LJ42Rw

móviles, con las tecnologías de tarjetas inteligentes y de comunicación de proximidad NFC, podría ser la oportunidad para que los servicios de salud recuperasen el retraso tecnológico.

Títulos de transporte público

La tarjeta inteligente, como sustituto de los billetes de banda magnética en el sector del transporte publico, es una de las aplicaciones que más se ha implantado en los últimos años. La necesidad de facilitar el pago, evitando el uso de efectivo, ha hecho que en las principales ciudades españolas se estén implantado sistemas basados en la tecnología *NFC-Contactless*.

La utilización de la tarjeta inteligente permite adicionalmente establecer modelos más flexibles de tarifas que se adecuen a las necesidades de los usuarios:

- En Madrid el abono transporte mensual ya no se expende únicamente por meses naturales, sino que es el propio usuario el que decide el momento de activarlo.
- En Barcelona este billete electrónico permitirá suprimir los 84 títulos de transporte distintos que existen.

La identificación de los trayectos que efectúan los viajeros individualmente permitirá, además, conocer en detalle la demanda y planificar de una forma más adecuada las rutas, frecuencias y horarios.

Tarjetas de fidelización y cupones descuento

Estas tarjetas, ofrecidas por entidades comerciales y otros sectores como la hostelería y el transporte, ofrecen bonificaciones a sus clientes en forma de descuentos o premios por su nivel de fidelización con la marca o marcas emisoras de la tarjeta. En general son gratuitas para los clientes y actualmente se basan en tecnología de banda magnética.

Estos sistemas de fidelización se complementan con servicios web que permiten a los clientes:

- Realizar el seguimiento de las compras realizadas y de los puntos obtenidos.
- Canjear los puntos por los premios del catálogo online.

"Otra de las aplicaciones de marketing relacional que permite la tecnología inalámbrica es que los usuarios puedan recibir voluntariamente información de productos y servicios de una manera sencilla."

- Acceder a promociones personalizadas.
- Obtener el mapa de establecimientos.

La migración de este tipo de tarjetas a tecnología *Contactless*, y su integración con los sistemas de pago por móvil, permitirá una mayor penetración de uso. Además las compañías emisoras podrán ofrecer servicios más personalizados de marketing, por ejemplo utilizando las funciones de localización geográfica de los móviles.

Carteles inteligentes

Otra de las aplicaciones de marketing relacional que permite la tecnología inalámbrica es que los usuarios puedan recibir voluntariamente información y/o promociones de productos y servicios de una manera sencilla. Este servicio es similar a la utilización de los códigos de barra 2D, con la diferencia de que se puede elevar el nivel de conectividad y personalización con la identificación del usuario.

Sistemas de acceso físico/lógico

Las credenciales de identificación del usuario, tipo eDNI, permitirían utilizar el dispositivo seguro del teléfono como llave electrónica, tanto para el acceso lógico a sistemas informáticos, como físico para acceder a edificios, viviendas o incluso vehículos. El desarrollo de la tecnología NFC y los sistemas M2M[4] permitirá generalizar el uso de dispositivos conectados tanto en proximidad (NFC) como en remoto (GSM).

— 4
Machine to Machine (intercambio de datos entre dos máquinas remotas).

>5
Monedero electrónico

"El monedero electrónico móvil también permite servicios de valor añadido para mejorar la experiencia de los usuarios ofreciendo, por ejemplo, promociones de los comercios cercanos."

El monedero electrónico (*eWallet*) es un organizador digital al que se accede a través de un dispositivo móvil, ya sea teléfono o tablet, o un ordenador personal, y que permite gestionar las diferentes tarjetas y servicios que incorpora, de forma similar a una cartera o monedero físico.

Las funciones que proporcionan incluyen tanto las orientadas al control y seguridad de los contenidos, tales como activación o desactivación de servicios y gestión de claves de seguridad, como las orientadas al seguimiento de las operaciones realizadas.

Los monederos electrónicos pueden contener entre otros los siguientes elementos:

- Sistemas de pago tipo tarjeta de crédito/débito.
- Documentos de identificación y firma electrónica (eDNI).
- Credenciales y licencias: tipo tarjeta sanitaria, carnet de conducir, seguros, etc.
- Tarjetas de fidelización, cupones y descuentos comerciales.
- Abonos y títulos de transporte.
- Entradas de espectáculos.
- Claves electrónicas para el acceso a sistemas online o edificios.

El monedero electrónico móvil también permite servicios de valor añadido para mejorar la experiencia de los usuarios y consumidores ofreciendo, por ejemplo, promociones de los comercios situados en la proximidad, o mostrando las entradas adquiridas para un determinado espectáculo al acercarse a la entrada del mismo.

"Los monederos electrónicos están en una situación incipiente, dado que aún no existen sistemas capaces de ofrecer un entorno completamente abierto e interoperable."

Los monederos electrónicos pueden clasificarse según los siguientes parámetros:

Proveedor de servicios:

- Vertical: proporcionado por un único proveedor. Incluye, por defecto, determinados servicios que posteriormente pueden incrementarse a través del mismo proveedor.
- Horizontal: diseñado para acomodar múltiples proveedores de servicios.

Entidad Comercial:

- Cerrado: creado específicamente para los servicios de un determinado comercio.
- Abierto: integra servicios de diferentes entidades.

Localización:

- Local: el software del monedero se localiza totalmente en el terminal móvil. Esto permite realizar operaciones sin necesidad de tener acceso a la red móvil.
- Remoto: el software del monedero se aloja parcialmente en servicios en la nube, lo cual facilita el uso desde diversos terminales y asegura su disponibilidad más inmediata en casos de pérdida o robo del terminal, aunque como contrapartida requiere disponibilidad de red en todo momento.

Los monederos electrónicos están en una situación incipiente, dado que aún no existen sistemas capaces de ofrecer un entorno completamente abierto e interoperable, siguiendo las recomendaciones de los diversos organismos implicados en su estandarización (ver capítulo *Regulación y normativa*).

Por otra parte el monedero electrónico es el interfaz principal del usuario con los servicios, por lo que su control puede reportar, al proveedor que lo proporcione, ventajas competitivas que pueden ser muy relevantes, tal y como ha ocurrido en el ámbito de los navegadores web y sistemas operativos móviles. Algunas de las compañías que ya han anunciado y lanzado monederos electrónicos son:

- Operadores móviles: Vodafone Wallet http://goo.gl/1AKGEh
- Compañías de internet: Google Wallet http://www.google.com/wallet/
- Entidades financieras: BBVA Wallet http://goo.gl/pAqzcB
- Fabricantes de móviles: Apple Passport http://goo.gl/Y9OxR0
- Cadenas comerciales: MCX Wallet http://www.mcx.com/

>6 Modelo operativo

Transacción de pago mediante tarjeta

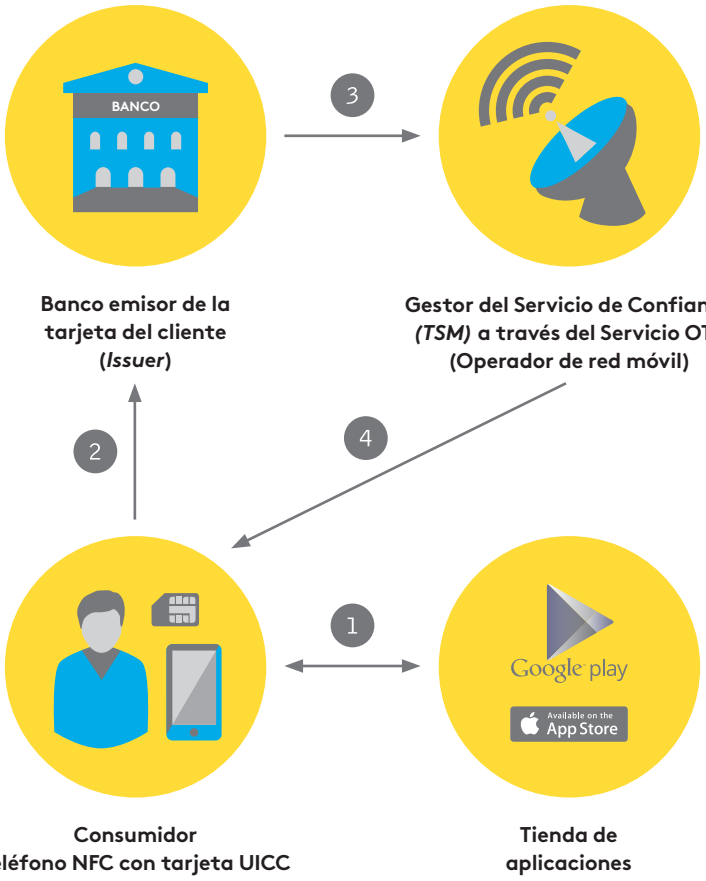
Los pagos NFC (incluyendo los móviles) en España se realizan del siguiente modo, de acuerdo al modelo SEPA (*Single Euro Payment Area*):

1. El cliente que posee una tarjeta bancaria (proporcionada por el banco emisor) y un teléfono compatible NFC realiza la solicitud de pago en un comercio que, a su vez, dispone del servicio de pago con tarjeta (proporcionado por el banco adquiriente) y de un Terminal de Punto de Venta compatible con NFC.
2. Se establece la comunicación de la petición de pago entre el banco adquiriente y el emisor a través del sistema o red común de pago. En caso de confirmarse la autorización, esta se recibe en el Terminal de Punto de Venta y en el teléfono del cliente. La operación queda completada y se almacena en los registros de ambos dispositivos. La transacción queda registrada igualmente en las cuentas correspondientes del consumidor y el comercio, en el banco emisor y adquiriente respectivamente.
3. Posteriormente se realiza un proceso offline de consolidación de pagos entre los bancos.

"El consumidor descarga una app de monedero, solicita al banco la emisión de la tarjeta de pago por móvil, y éste traslada la petición de activación al Gestor de Servicio de Confianza para que confirme el alta y la clave de acceso."

Provisión de servicios de pago con tarjeta

Partiendo de que el consumidor dispone de un móvil con capacidad NFC y está suscrito al servicio de un operador móvil que le ha proporcionado una tarjeta SIM-UICC, compatible con los servicios de pago NFC por móvil, la provisión del servicio de tarjeta de acuerdo al modelo *customer-centric*[5] se realizaría siguiendo este esquema:



1. El consumidor descarga desde la tienda online correspondiente una aplicación de monedero compatible con los servicios de su banco y operador móvil.
2. Posteriormente solicita al banco la emisión de la tarjeta de pago por móvil requerida, indicando la cuenta corriente de pago y el número de teléfono y operador móvil para su activación.
3. El banco emisor, tras aceptar la solicitud de su cliente, da de alta la tarjeta correspondiente y traslada la petición de activación móvil al Gestor de Servicios de Confianza, acompañando dicha petición con la información de identificación de usuario y tarjeta correspondiente.
4. El Gestor de Servicio de Confianza, a través del servicio OTA (*Over The Air*) del operador móvil (GSM o WIFI), descarga en la tarjeta SIM-UICC del teléfono las aplicaciones, acreditaciones y claves necesarias para activar el servicio. Se produce la notificación de confirmación de alta de servicio y disponibilidad de la clave de acceso al cliente.

— 5
What Does It Mean to Be Customer Centric?, http://goo.gl/E6DSwR

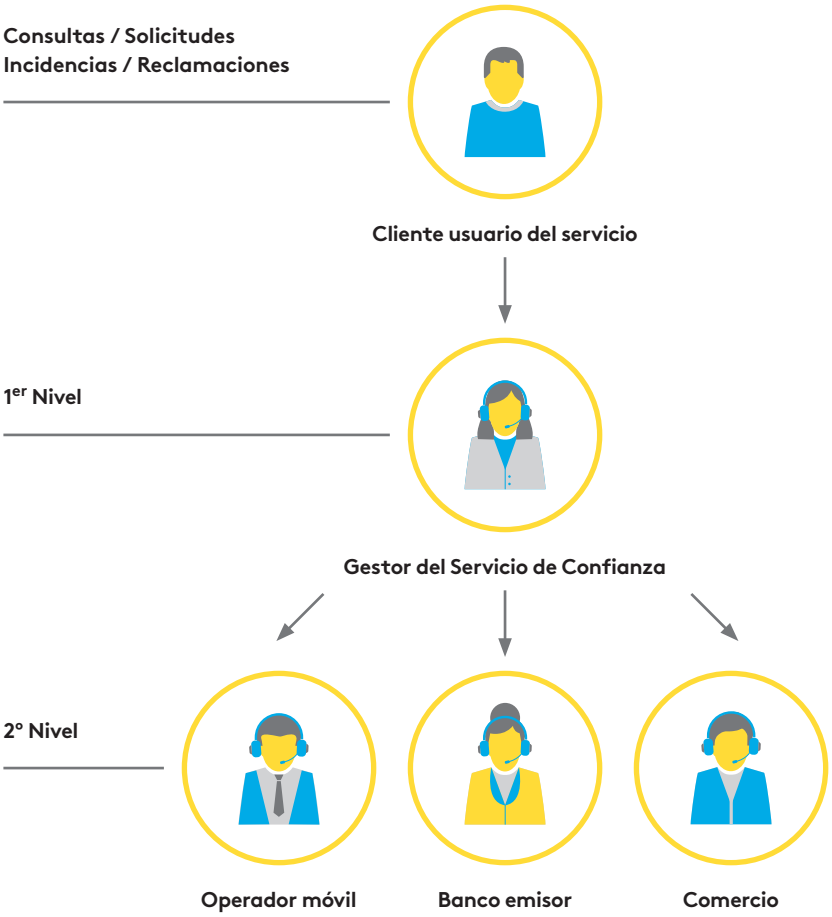
"Con el modelo transversal de atención al cliente, el usuario accede a un único centro que resuelve consultas e incidencias comunes."

Servicio de atención al cliente

El servicio de atención al cliente se puede desplegar siguiendo básicamente dos modelos:

1. Vertical: cada uno de los proveedores de servicio proporciona su propia atención al cliente, atendiendo las consultas, incidencias y reclamaciones relativas a la responsabilidad de los servicios que proporciona. Cuando el centro de atención detecta que la incidencia no es del ámbito de su responsabilidad redirige al cliente o le invita a ponerse en contacto con el centro de atención pertinente. Muchos de los servicios actuales funcionan con este modelo, dado que no implica costes adicionales para la transformación de los sistemas y procesos actuales.
2. Trasversal: el usuario accede a un centro integrado de atención al cliente, que proporciona un primer nivel de atención con una capacidad de resolución que permita resolver las consultas e incidencias más comunes. De esta forma se evita que el cliente tenga que ponerse en contacto directo con otros centros, salvo en casos muy específicos por su complejidad. En este modelo encaja perfectamente el papel del Gestor de Servicios de Confianza.

Modelo de Atención Integrada Transversal



>7
Seguridad de la información y las transacciones

"Uno de los factores más críticos para el desarrollo de los servicios de pago por móvil es la seguridad de los mismos. Si no se garantiza, los usuarios se mostrarán reticentes a utilizarlos."

Uno de los factores más críticos para el desarrollo de los servicios de pago por móvil es indudablemente la seguridad de los mismos. Si no se garantiza, los usuarios se mostrarán reticentes a utilizarlos. Por otra parte, el alto coste del fraude y el robo puede impedir a las empresas rentabilizar las inversiones requeridas para el desarrollo y gestión de estos servicios.

La seguridad en este ámbito es un reto realmente complicado debido a las características que conforman el ecosistema:

- El elemento final gestionado es el dinero, por lo que no hay nada más atractivo para los posibles delincuentes.
- La tecnología utilizada es relativamente reciente y sujeta a cambios y adaptaciones al entorno.
- La cadena de valor es compleja e intervienen una gran número de actores.
- Algunos de los actores involucrados son nuevos en este ámbito de los pagos móviles y el fraude y robo asociados.
- Los comercios históricamente han sido uno de los puntos más vulnerables en los medios de pago con tarjeta.
- El terminal móvil, por su pequeño tamaño y uso continuo casi en cualquier situación, es propenso a la perdida o robo.
- La movilidad se realiza con la comunicación inalámbrica, tanto de información del usuario como de la transacción correspondiente, y esto implica siempre un cierto riesgo de vulnerabilidad.
- Los usuarios de los servicios no siempre son conscientes de los riesgos y en general no toman las precauciones adecuadas.

Para disminuir los riesgos en cada uno de los ámbitos citados se hace necesario implantar y gestionar tanto tecnologías seguras como los procesos adecuados para la gestión operativa de la misma. También es imprescindible establecer medidas de control y auditoria por parte de organismos independientes que garanticen continuamente el nivel de seguridad requerido.

Aunque en los protocolos de comunicación empleados por estos sistemas se utilizan algoritmos avanzados de encriptación (que hacen casi imposible descifrar la información), existen algunos puntos vulnerables en el proceso. Estos se producen cuando se requiere tratar la información no codificada, tanto en el origen (el terminal del usuario), como en los sistemas de pago intermedios o de destino.

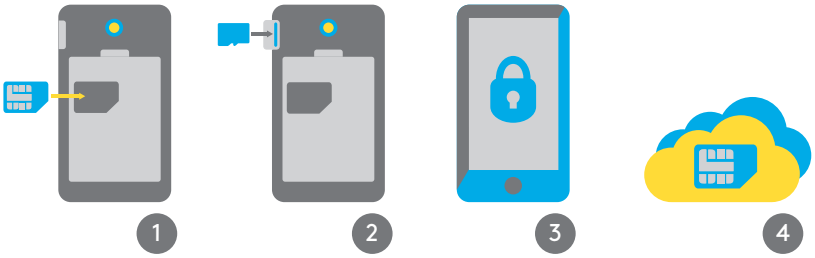
A continuación se describen los diferentes elementos que intervienen en el proceso de sistemas de pago que requieren un control adecuado para evitar la fuga de información sensible y su uso fraudulento.

"Es imprescindible establecer medidas de control y auditoria por parte de organismos independientes que garanticen continuamente el nivel de seguridad requerido."

Dispositivos Seguros (*SE: Secure Element*)

Los servicios de medios de pagos e identificación requieren la existencia de un elemento seguro en el terminal móvil que contenga las credenciales de los usuarios y las claves de uso, así como las aplicaciones que las utilizan para el acceso a los servicios correspondientes. Estos componentes de software del dispositivo seguro se incluyen en un chip integrado que adicionalmente proporciona los sistemas criptográficos de acceso a los mismos.

El Dispositivo Seguro puede implementarse de tres formas diferentes:



1 Tarjeta SIM-UICC:
El sistema más generalizado actualmente es el de integración en la tarjeta UICC, que además de la SIM (Subscriber Identity Module), puede contener simultáneamente múltiples aplicaciones seguras independientes. Este modelo promovido por los operadores móviles, permite de una manera sencilla la provisión y gestión de servicios de forma remota vía GSM mediante el método denominado OTA (*Over The Air*).

2 Tarjeta MicroSD o USB:
El uso de dispositivos tipo microSD, con capacidad NFC, permite más flexibilidad al usuario para utilizar el Dispositivo Seguro en otros terminales, en general requiere un teléfono que soporte directamente NFC.

3 En el propio teléfono:
Fabricado directamente en el teléfono móvil, permite a los fabricantes diseñar y certificar en sus dispositivos (hardware y sistema operativo) el cumplimiento de la normativa de seguridad NFC.

4 Como servicio en la nube:
La utilización de un Dispositivo Seguro virtual, creado como un servicio en la nube, permitiría flexibilizar e independizar los servicios del dispositivo físico utilizado. Sin embargo se añade la necesidad de un esquema de seguridad muy riguroso. Para la utilización de TPVs NFC, aún sería necesario un terminal NFC compatible y conectividad a la red.

Los despliegues comerciales actuales están utilizando principalmente el modelo de tarjeta UICC-SIM y, recientemente,

"Los modelos de seguridad considerados se basan en métodos biométricos (reconomiento de huella dactilar, voz, iris...), o en la utilización de factores múltiples."

el modelo de servicio en la nube. Ambos responden a diferentes modelos de negocio por lo que entrarán en competencia.

Usuarios del servicio

Uno de los puntos más críticos para la seguridad de los pagos mediante móviles es probablemente la utilización que hace el usuario del teléfono. Los problemas en este ámbito los podemos clasificar en tres áreas:

1 Pérdida o robo del teléfono:
Este riesgo es inherente a las características del dispositivo (pequeño y omnipresente). La activación de claves de seguridad permite disminuir el riesgo, y entorpecer la extracción de información, durante el tiempo que se tarda en notar la perdida y solicitar al operador que bloquee el terminal o las tarjetas de pago e identidad.

El sistema iOS ofrece la posibilidad de localización remota del teléfono perdido y, en caso de necesidad, el borrado automático de todos los datos del terminal.

La tendencia a dejar el móvil encima de la mesa o en cualquier sitio puede disminuir en la medida que utilicemos el móvil como medio de pago. Nadie deja su cartera encima de la mesa mientras se sienta a tomar un café o charlar.

2 Utilización de claves no seguras:
La necesidad de establecer y recordar claves para las diferentes cuentas de los usuarios (PIN SIM, bloqueo de teléfono, banca online, cuenta de correo...) hace que muchos usuarios utilicen la misma clave o un esquema de definición simple de claves. Los fabricantes de teléfonos exploran la posibilidad de utilización de credenciales de usuario comunes para el acceso transversal a todas las aplicaciones, pero aún estamos lejos de contar con mecanismo seguros estandarizados.

Los modelos de seguridad considerados se basan principalmente en métodos biométricos, o en la utilización de factores múltiples de seguridad. La próxima generación de teléfonos inteligentes es probable que empiece a incluir el acceso seguro a través de diferentes métodos biométricos tales como el sistema *TouchID* del iPhone 5S, basado en el acceso mediante

"Un 77% de las amenazas de *malware* podría haberse evitado con la actualización a la última versión del sistema operativo."

huella dactilar. Otros métodos basados en reconocimiento facial, de iris, o voz, también están siendo considerados.

3 Aplicaciones malintencionadas (*malware*):
El crecimiento del *malware* en los móviles es preocupante, particularmente en los terminales Android, que alcanzaban el 70% del mercado a finales del 2013.
La estrategia abierta de esta plataforma y la diversidad de versiones y tiendas de aplicaciones, ha hecho que sea blanco fácil para los hackers. Se estima que un 77% de estas amenazas podría haberse evitado con la actualización a la última versión del sistema operativo. Cuando sólo un 4% de los usuarios totales de Android tienen el sistema actualizado. La mayor parte del *malware* trata de explotar agujeros en los sistemas de pago por móvil o el acceso a servicios *Premium SMS*.

En los teléfonos con iOS el riesgo hasta la fecha ha sido menor debido el carácter propietario de este sistema operativo y gracias al control que realiza Apple al incluir nuevas aplicaciones en su tienda online. Sin embargo algunas aplicaciones malintencionadas pueden saltarse este mecanismo de control y activar funciones no seguras posteriormente[6]. Por otra parte algunos usuarios de iOS, para flexibilizar la carga de aplicaciones y el acceso a contenidos, liberan sus terminales del bloqueo de Apple (*Jailbreak*), este desbloqueo naturalmente aumenta el riesgo de infecciones por *malware*.

Dado que los fabricantes de móviles y desarrolladores de sistemas operativos no son lo suficientemente rápidos para detectar y eliminar los agujeros de seguridad, al igual que ha ocurrido con los ordenadores personales, será necesario contar con el valor añadido de las aplicaciones especializadas en antivirus de confianza.

Comercios y Terminales de Punto de Venta

Los Terminales de Punto de Venta (TPV) en general son dispositivos que procesan los pagos mediante su comunicación, por una parte, con el dispositivo (móvil o tarjeta) del usuario, y por otra, con el sistema de medios de pago. Estos dispositivos pueden ser terminales específicos TPV, ordenadores fijos tipo PC adaptados a esta función o incluso móviles estándar con un software y/o hardware específico.

En cualquiera de los tres casos, estos terminales deben estar conectados a la red de medios de pago, bien a través de la red Móvil GSM directamente, o mediante la red fija por medio de ADSL o fibra. En muchas de las aplicaciones, los TPVs se comunican vía WIFI con el enrutador (router)

— 6
The Inquirer: Apple App Store bypassed to spread malware on iOS, Aug. 2013.

"En los comercios que requieran una configuración con conexión a internet, se recomienda la utilización de un sistema de protección tipo *firewall* que garantice la zona segura de la red local de TPVs."

que a su vez comunica con la red publica, y ésta enlaza con el sistema de medios de pago.

En estas configuraciones más complejas existen tres puntos de vulnerabilidad:

- Comunicación teléfono - TPV mediante NFC (*Contactless*).
- Comunicación TPV - enrutador mediante WiFi.
- Enlace enrutador - internet.

El punto más crítico de esta cadena es el enlace exterior del enrutador hacia internet, debido a posibles intrusiones malintencionadas a través de internet:

- En las entidades del sector financiero los enlaces exteriores conectan con una red privada virtual (RPV), por lo que se garantiza un nivel de seguridad superior al uso directo de las redes públicas.
- En los pequeños comercios con uno o dos TPVs, estos se pueden conectar directamente a la red GSM, por lo que se evita su conexión directa a internet.
- En los comercios que requieran una configuración con conexión a internet, se recomienda la utilización de un sistema de protección tipo *firewall* que garantice la zona segura de la red local de TPVs.

En los sistemas tradicionales de medios de pago, la tarjeta bancaria ha ido evolucionando para mejorar la seguridad en los comercios y evitar su manipulación o copia:

1. Inicialmente la tarjeta tenía los datos de identificación impresos en el plástico y la operación se realizaba offline, mediante la copia de dichos datos a través de un mecanismo de presión con papel autocopiativo. El elemento de seguridad era la firma del cliente en el impreso correspondiente. El fraude en estos casos consistía en pasar varias veces la tarjeta en impresos en los que posteriormente se falsificaba la firma.
2. Posteriormente se añadió la banda magnética que evitaba el tratamiento manual, dificultando el fraude. Pronto la duplicación de bandas magnéticas se hizo más accesible, permitiendo a los delincuentes obtener duplicados de tarjetas en comercios e incluso cajeros de entidades financieras. Los TPV evolucionaron también permitiendo la utilización de pines de seguridad establecidos por los usuarios.
3. Las última generación de tarjetas añadió la utilización de un CHIP con aplicaciones criptográficas que añaden un nivel de seguridad adicional para dificultar la duplicación de las mismas.

"El sistema de comunicación NFC no proporciona inherentemente un mecanismo de seguridad, sino que son las aplicaciones que lo utilizan las que deben garantizar la protección de la información."

Comunicación sin contacto entre el teléfono y el TPV

La comunicación entre los teléfonos y los TPVs se realiza a través de NFC. Este sistema de comunicación no proporciona inherentemente un mecanismo de seguridad, sino que son las aplicaciones que lo utilizan las que deben garantizar la protección de la información.

Por ejemplo en las aplicaciones tipo TAG o cartel inteligente, no se incluyen mecanismos de seguridad avanzados pues lo que se persigue es comunicar de forma pública la información que se considera pertinente. Para ello existen multitud de aplicaciones que pueden leer e incluso clonar TAGs de tipo NFC[7].

Sin embargo las aplicaciones de pagos móviles incluyen en las tarjetas con CHIP-NFC mecanismos de protección basados en criptografía con claves asimétricas del tipo RSA, con el mismo estándar EMV que se utilizan en las tarjetas con microchip. Estos algoritmos criptográficos impiden que se pueda descifrar la información incluso si se tiene acceso cercano al dispositivo emisor.

Redes de comunicaciones móviles

La red GSM incluye su propio sistema de seguridad adicional sobre la comunicación de datos que se produce entre los dispositivos móviles, que a su vez pueden utilizar otros mecanismos de seguridad entre las aplicaciones de origen en el dispositivo seguro y la aplicación de destino en el sistema de transacciones de pago.

Los operadores móviles pueden intervenir en el proceso de provisión del dispositivo seguro (ver apartado *Gestores de Servicio de Confianza*).

Redes/Sistemas de Medios de Pago y Bancos

El sistema tradicional de pago a través de tarjetas se ha consolidado mundialmente como un sistema con un alto nivel de seguridad, particularmente con la introducción del modelo EMV promovido por Europay, Mastercard y VISA (ver capítulo *Regulación y normativa*).

Gestores de Servicio de Confianza

La complejidad del sistema de medios de pago e identificación personal, en el cual intervienen múltiples actores (bancos, operadores móviles, entidades gubernamentales, compañías de comercio y servicios, fabricantes, compañías de servicios de

— 7
NFC TagInfo by NXP y NFC Tag Cloner by Thomas Rorvik Skjolberg, ambas en Google Play.

internet, etc.), ha creado la necesidad de definir un Gestor de Servicio de Confianza independiente y neutral (*Trusted Service Manager, TSM*). La responsabilidad del TSM se sitúa entre el responsable del dispositivo seguro (en general operadores móviles) y los proveedores de servicio (bancos, comercios, etc.), evitando de esta manera la dificultad operativa de establecer un modelo de relación directo entre todos los operadores móviles y todos los proveedores de servicios.

La principal función del TSM en este contexto es facilitar la carga inicial y el posterior mantenimiento de las aplicaciones y credenciales que cada usuario requiere. Esto puede incluir tarjetas de crédito o débito de diversas entidades bancarias, tarjetas de comercios, credenciales de usuario, abonos de transporte, tarjetas de fidelización, etc.

El proceso de carga y mantenimiento en los dispositivos seguros debe realizarse en remoto a través de las redes móviles o WiFi (*OTA: Over The Air*). Este proceso además de ser complejo, al utilizarse infraestructura y sistemas de los operadores móviles, requiere mecanismos de seguridad avanzada, tanto en los sistemas como en los procesos utilizados.

Los Gestores de Servicios de Confianza pueden ofrecer también servicios de atención al cliente, facilitando la operativa de entrega y mantenimiento de los servicios globales, al presentar a los clientes un interfaz integrado hacía los servicios específicos de los operadores móviles, bancos y comercios.

Por otra parte, los Gestores de Confianza podrían facilitar el proceso de negociación de los términos de servicios entre los múltiples actores, actuando como puntos de intermediación común, evitando así la negociación y cierre de contratos multilateral que podría retrasar o limitar el lanzamiento de los servicios correspondientes.

El papel del Gestor de Servicios de Confianza tiene mucho sentido en el modelo de dispositivo seguro implementado en la tarjeta UICC-SIM del teléfono. Sin embargo en un modelo de dispositivo virtual seguro en red, este papel puede ser asumido por las empresas de servicios de internet.

>8
Regulación y normativa

"Para facilitar la interoperabilidad, calidad y seguridad de los servicios, existen diversas entidades que están desarrollando recomendaciones y normativas de estandarización."

El desarrollo de los servicios móviles tanto para pago como para identificación, y en general de comercio electrónico móvil, está en una fase muy inicial y pendiente de definición en algunos de los aspectos más relevantes.

Para facilitar la interoperabilidad y garantizar la calidad y seguridad de los servicios, existen diversas entidades que, en un entorno colaborativo y desde cada una de las perspectivas que intervienen en el ecosistema, están desarrollando recomendaciones y normativas de estandarización:

El **Consejo Europeo de Pago** (*EPC: European Payment Council*) es un organismo privado formado por bancos europeos cuya misión es coordinar y facilitar la toma de decisiones en el ámbito de pagos. El objetivo inmediato actual del EPC es promover y dar soporte para la implantación de la Zona Única de Pagos en Euros (SEPA: Single Euro Payments Area).
www.europeanpaymentscouncil.eu

La Asociación **GSM** (*GSMA*) es un organismo que representa los intereses a nivel mundial (con presencia en 220 países) de las compañías del sector de las comunicaciones móviles, y que agrupa unos 800 operadores de redes móviles y más de 200 empresas proveedoras de equipos, sistemas, servicios y consultoría.
www.gsma.com

La **Smart Card Alliance** es una organización multisectorial sin fines de lucro, que trabaja para estimular la comprensión, adopción, uso y aplicación generalizada de la tecnología de tarjetas inteligentes, principalmente en EEUU y otros paises americanos. La alianza invierte en la educación sobre los usos apropiados de la tecnología para la identificación, pago y otras aplicaciones, y aboga por el uso de la tecnología de tarjetas inteligentes de una manera que proteja la privacidad y mejore la seguridad e integridad de los datos.
www.smartcardalliance.org

El **NFC Forum** fue formado para promover el uso de la tecnología *Near Field Communication* mediante el desarrollo de especificaciones, garantizando la interoperabilidad entre los dispositivos y los servicios, y educando al mercado sobre la tecnología NFC. Creado en 2004, el foro cuenta con 190 miembros. Los fabricantes, desarrolladores de aplicaciones, e instituciones de servicios financieros trabajan juntos para promover el uso de la tecnología NFC en electrónica de consumo, dispositivos móviles, y PC, entre otros.
www.nfc-forum.org

EN 1999, las compañías Europay, MasterCard y Visa fundaron **EMVCo** con el propósito de desarrollar especificaciones para transacciones de pago seguras. Posteriormente se unieron

a este grupo American Express, JCV y UnionPay. Los miembros de EMVCo han trabajado conjuntamente en los últimos años para desarrollar especificaciones que definen un conjunto de requisitos para garantizar la interoperabilidad entre tarjetas chips y terminales a nivel mundial, sin importar el fabricante, la institución financiera, o cuándo se utiliza la tarjeta. También se han publicado especificaciones para tarjetas Chip NFC y para integración en móviles con tarjetas UICC.
www.emvco.com

GlobalPlatform es una asociación multisectorial sin ánimo de lucro y cuyo objetivo es identificar, desarrollar y publicar especificaciones que facilitan el despliegue y la gestión segura e interoperable de múltiples aplicaciones integradas en la tecnología de chips.

Las especificaciones de GlobalPlatform se han focalizado en los Dispositivos Seguros (SE) así como en los Entornos de Ejecución Segura de Aplicaciones (TEE). Estas especificaciones permiten soluciones de confianza de extremo a extremo que sirven a múltiples actores y apoyan varios modelos de negocio.
www.globalplatform.org

El **Consejo de Normativas para la Seguridad del Sector de Pagos con Tarjeta** es un foro mundial abierto, creado en 2006 y responsable del desarrollo, la gestión, la educación y el conocimiento de las normativas de seguridad en el ámbito de los medios de pago con tarjeta. Estas normas incluyen el Estándar de Seguridad de Datos (PCI DSS), el Estándar de Aplicaciones de Pago (PA-DSS) y los requisitos para el PIN de transacciones seguras (PTS). Los cinco fundadores del consejo (American Express, Discover Financial Services, JCB International, MasterCard, y Visa Inc.) han acordado incorporar la normativa PCI[8] para los requisitos técnicos de cada uno de sus programas de cumplimiento de seguridad de datos.
es.pcisecuritystandards.org

— 8
Payment Card Industry Data Security Standard,
http://goo.gl/Z51QG4

>9
Cadena de valor y modelo económico

Agente	Servicios	Flujo económico
Desarrolladores de apps para móviles.	Proporcionan la aplicación de usuario.	Las aplicaciones en general son gratis para el usuario y el coste lo soporta la entidad comercial, el banco, la empresa de internet o el operador móvil.
Fabricantes de terminales móviles.	Ofrecen el terminal (hardware y software básico).	El terminal móvil corre a cargo del usuario directamente, o de forma compartida con el operador móvil mediante un contrato de permanencia.
Operadores móviles.	Aportan los servicios de red y generalmente los teléfonos móviles.	Las comunicaciones de datos necesarias para las transacciones de compra las soporta el usuario del servicio a su operador móvil.
Redes/Sistemas de pago.	Permiten el intercambio de los datos de pago entre los comercios y bancos emisores y adquirientes.	Los bancos pagan a los sistemas de pago correspondientes por cada transacción realizada.
Bancos.	Emiten las tarjetas de pago y proporcionan la gestión de las cuentas bancarias de crédito (emisión) y abono de las operaciones (adquiriencia).	Los bancos pueden cobrar una comisión a los usuarios por la emisión de las tarjetas, un interés mensual en las de crédito y una comisión de recarga en las tarjetas con esta modalidad. También reciben una comisión de los comercios sobre el valor de la compra.
Operadores de redes fijas.	Proveen las redes de comunicaciones a los bancos y redes de pago y también a los comercios que dispongan de red fija.	Los bancos y redes pagan a los operadores por el acceso y gestión de la red de datos en función de las capacidades y servicios demandados.
Fabricantes de TPVs.	Suministran los dispositivos y el software básico para los comerciantes.	El coste de estos terminales los puede soportar el banco adquiriente del comercio incluido en su servicio o el propio comercio.
Desarrolladores de software de Punto de Venta.	Proporcionan el software para la gestión de ventas de los comercios.	Los grandes comercios pagan a las empresas de software las aplicaciones necesarias. En pequeños comercios pueden ser servicios completos en la nube.
Comercios.	Ofrecen a los clientes los productos o servicios demandados.	Los usuarios pagan por los productos o servicios a través del móvil.
Proveedores de Servicios de Confianza (TSM).	Gestionan el alta de los usuarios finales, las credenciales y las claves de acceso. También puedan gestionar la atención al cliente para la carga de las aplicaciones en el terminal móvil.	Cobran por alta y actualización de aplicaciones y claves.
Compañías de internet puntocom.	Proporcionan a los usuarios las aplicaciones de los terminales móviles y pueden proveer servicios de pago, tanto a usuarios como a comercios, con medios tradicionales o propios.	Las aplicaciones proporcionadas a los usuarios en general son gratis, los servicios de pago propios que se puedan proporcionar estarán sujetos a comisiones tanto de alta del medio como por transacción o recarga de crédito realizada.

"El acceso de los bancos a los medios de pago supone obtener más información de perfiles y comportamientos de compra para rentabilizar su publicidad."

Las tensiones en el flujo económico del ecosistema de medios de pago se producen en los dos objetivos principales de negocio que definen las estrategias correspondientes para los principales actores: proteger el negocio actual y captar nuevas fuentes de ingresos.

Operadores móviles	El negocio actual de los operadores no está amenazado directamente, dado que la infraestructura de la red que posibilita los servicios básicos no es fácilmente replicable. Sin embargo la oportunidad para los operadores móviles es proporcionar más servicios de valor añadido desde la red. En este ámbito, los operadores no han obtenido resultados destacables hasta el momento.	Los operadores pueden optar a obtener ingresos adicionales en su base de clientes: 1. A través de cuotas a los proveedores de servicios por la gestión de las aplicaciones de pago en el móvil. 2. Comisiones en función del importe económico de las transacciones.
Bancos	Las entidades financieras son el principal agente que intermedia en los medios de pago y se posicionan para seguir haciéndolo en los pagos por móvil, dado que es una fuente de ingresos muy significativa.	El modelo de pago por móvil permite extender los pagos con tarjetas a las transacciones de bajo importe que hasta la fecha se realizaban principalmente en efectivo.
Empresas de servicios en internet (puntocom)	En este nuevo entorno de medios de pago por móvil no sufren amenazas sobre su negocio actual, pero necesitan rentabilizar su conocimiento sobre los usuarios de sus servicios.	El acceso a los medios de pago supondría tres beneficios básicos: 1. Mantener el control de los clientes a través de las aplicaciones finales (monedero electrónico). Este punto ha sido crítico con los navegadores y sistemas operativos y lo seguirá siendo con los monederos electrónicos. 2. Obtener más información de perfiles y comportamientos de compra para rentabilizar su negocio de publicidad. 3. En un futuro las empresas puntocom podrían ofrecer servicios bancarios básicos, dado que cuentan con los sistemas de software necesarios y una amplia cartera de clientes.
Empresas de distribución	El negocio de las empresas tradicionales de comercio sufre el impacto de las compras online. En este ámbito las puntocom como Amazon o eBay pueden captar una parte de mercado mayor gracias a las compras online a través del móvil. Las empresas tradicionales deberían posicionarse igualmente como proveedores de comercio online para disminuir o frenar esta amenaza.	Los comercios que se posicionen mejor en el nuevo modelo de pagos por móvil podrán incrementar su cartera de clientes y también establecer nuevos esquemas de fidelización.

>10
Beneficios y oportunidades

"Para lograr el despliegue masivo de los medios de pago por móvil es necesario que los servicios proporcionados respondan a la demanda de los usuarios."

Beneficios para los usuarios

La asociación GlobalPlatform plantea la necesidad de desarrollar un modelo de negocio de servicios móviles basado en el cliente (*customer-centric*) y no en los emisores de las tarjetas (*issuer-centric*). En este modelo es el cliente quien controla y decide las aplicaciones que se cargan en el Dispositivo Seguro de su móvil, al igual que hace accediendo a las tiendas de aplicaciones móviles (*app-Stores*) para adquirir y cargar aplicaciones.

Los posibles beneficios para los clientes serían:

- Mayor seguridad que en el pago con tarjetas tradicionales.
- Identificación segura con la inclusión del eDNI y pasaporte.
- Integración de diversas tarjetas en un único Dispositivo Seguro.
- Mejor control y seguimiento de gastos.
- Menor necesidad de disponer de dinero en efectivo.
- Facilidad para el pago en parkings, dispensadores automáticos, etc.
- Acceso a promociones, descuentos y premios de fidelización.

Para lograr el despliegue masivo de los medios de pago por móvil es necesario que los servicios proporcionados respondan a la demanda de los usuarios, cumpliendo las expectativas y necesidades planteadas:

- Sin coste adicional sobre los servicios actuales.
- Servicios seguros con riesgo de fraude nulo para el usuario.
- Un amplio catálogo de terminales con capacidad NFC.
- Una manera clara y sencilla de gestionar los servicios a través del teléfono móvil.
- Disponibilidad de múltiples servicios tanto de medios de pago, como de identificación, tarjetas de fidelización, transporte, etc.
- Un servicio de atención al cliente integrado que no requiera contactar con múltiples compañías.
- Facilidad y flexibilidad para la portabilidad de servicios entre operadores móviles.
- Un interfaz consistente entre múltiples proveedores de servicio y operadores móviles.
- Servicios de valor añadido para la gestión y el seguimiento de operaciones.

Comercios y empresas de servicios

Estas compañías deben proporcionar a sus clientes servicios avanzados de comercio electrónico móvil que permitan facilitar el consumo e incrementar su fidelidad. Los medios de pago por móvil y otras aplicaciones adicionales permiten establecer canales de comunicación más personalizados, y desarrollar un marketing relacional de valor añadido tanto para el cliente como para el comercio.

"El sector financiero se está posicionando como impulsor del modelo y sentando las bases para competir con los nuevos entrantes, tanto operadores móviles como compañías de internet."

Beneficios:

- Facilitar el consumo con medios de pago por móvil.
- Tarjetas de fidelización, cupones y descuentos.
- Aplicaciones de comercio electrónico móvil.
- Puntos de venta con menor coste de mantenimiento.
- Introducción de nuevos modelos de negocio.

Los requerimientos básicos prácticamente son los mismos que tienen los usuarios finales de los servicios, y se podrían añadir:

- Acceso flexible a clientes de múltiples operadores móviles.
- Acceso flexible a múltiples redes de pago con tarjeta bancaria.
- Fácil desarrollo e integración de aplicaciones móviles propias.
- Disponibilidad de un amplio catálogo de TPV-NFC e interoperabilidad con teléfonos de clientes.
- Integración e interoperabilidad con los sistemas actuales de puntos de venta.
- Carteles inteligentes internos/externos con capacidad NFC.
- Posibilidad de transformar el modelo de cajas centrales en las tiendas por un modelo de caja distribuida en cada dependiente.

Entidades financieras

Las entidades financieras son líderes naturales del modelo de intermediación en los pagos por móvil. En un contexto de transformación tecnológica, el sector se está posicionando como impulsor del modelo y sentando las bases para competir con los nuevos entrantes, tanto operadores móviles como compañías de internet.

Los beneficios para los bancos se centran en el posicionamiento diferencial sobre la competencia y en la posibilidad de captar un mercado mayor al acceder a pagos de menor cantidad. Además, el sistema de pagos seguros por móvil puede reducir considerablemente el fraude de las tarjetas, aunque requiere una inversión superior para adaptar los sistemas y mejorar los procesos de gestión de los datos de los usuarios y las transacciones correspondientes.

Los requerimientos para los bancos deben ser principalmente los requerimientos de sus clientes, tanto comercios como consumidores finales.

Operadores de servicios móviles

Los operadores móviles juegan un papel central en el despliegue de los servicios de medios de pago por móvil. Para este mercado próximo al nivel de saturación en los países desarrollados supone, por una parte, el acceso a nuevas fuentes de ingresos, y por otra,

"Los operadores han entendido la necesidad de establecer un marco colaborativo centrado en el cliente, que permita un desarrollo rápido y eficiente de los nuevos servicios, y facilite el acceso masivo de los usuarios."

la extensión de servicios de valor añadido que podría incrementar la demanda de teléfonos inteligentes de última generación.

Los operadores han entendido la necesidad de establecer un marco colaborativo centrado en el cliente, que permita un desarrollo rápido y eficiente de los nuevos servicios, y facilite el acceso masivo de los usuarios. En este sentido tanto en EEUU (ISIS: at&t, Verizon, T-Mobile) como en en el Reino Unido (WEVE: Orange, T-Mobile, Telefónica, O2, Vodafone) se han establecido acuerdos entre operadores para el desarrollo de los nuevos servicios de comercio electrónico móvil y particularmente el monedero electrónico móvil.

El lanzamiento del modelo de emulación de tarjeta mediante servicios en la nube (*HCE: Host Card Emulation*) puede desintermediar a las operadores móviles en este mercado, dado que ya no es necesaria su participación en la definición de los servicios finales. En este caso puede ocurrir lo mismo que ha pasado con el mercado de contenidos digitales y los proveedores de servicios sobre internet (*OTT: Over-the-top*[9]).

Fabricantes de terminales

El despliegue de NFC permitirá a los fabricantes posicionarse frente a la competencia y captar nuevos mercados que anteriormente no eran accesibles.

Fabricantes de teléfonos móviles

Los grandes fabricantes de teléfonos inteligentes, excepto Apple, ya tienen un amplio catálogo de teléfonos compatibles que abarca más de 100 modelos, entre ellos están versiones de los modelos más representativos de las principales marcas: Samsung Galaxy S4 y S3; Sony Xperia Z; LG Optimus L5, L7 y L9; Nokia Lumia; HTC ONE; Blackberry Z10.

Fabricantes de terminales de puntos de venta y cajeros bancarios

Los principales fabricantes ya producen versiones NFC de sus productos, entre ellos Ingénico, Verifone, Fujitsu y NCR. También se están sacando al mercado dispositivos y software que permite a los teléfonos móviles y tabletas actuar como Terminales de Punto de Venta.

Proveedores de software

Para estas compañías el mercado de los servicios de comercio electrónico móvil es una gran oportunidad por el despliegue masivo que se está produciendo en estos momentos.

— 9
Over-the-top content,
http://goo.gl/5X1sey

En este ámbito se están posicionando nuevas compañías especializadas en servicios y software para las diversas necesidades del mercado:

Gemalto es un líder global en seguridad digital y su experiencia abarca todo el proceso de creación de soluciones digitales de seguridad, tanto en el área de desarrollo de software y sistemas operativos seguros que se integran en dispositivos de confianza (tarjetas UICC, tarjetas bancarias, fichas, pasaportes electrónicos o tarjetas de identificación), como en la personalización de estos dispositivos y el despliegue y mantenimiento del software y los servicios de gestión.
www.gemalto.com

Oberthur Technologies (OT) desarrolla productos y soluciones de software necesarios para implementar y poner en práctica servicios móviles seguros. Su experiencia en los últimos años abarca los mercados de pagos, telecomunicaciones, transporte, y control de acceso e identidad.
www.oberthur.com

Monitise es un líder mundial en la tecnología de pagos por móvil. Su plataforma de software ha sido elegida por los principales bancos, compañías de pagos, compañías de comercio minorista y operadores de redes móviles para desarrollar sus servicios móviles.
www.monitise.com

Giesecke & Devrient (G&D) desarrolla, produce y distribuye productos y soluciones para el pago, la comunicación segura y la administración de identidades. G&D mantiene una posición como líder tecnológico y empresarial en estos mercados. El grupo tiene como clientes a bancos centrales y comerciales, proveedores de telefonía móvil, empresas, gobiernos y administraciones públicas.
www.gi-de.com

FirstData es un proveedor líder de servicios de comercio y procesamiento de pagos electrónicos para las instituciones financieras, los gobiernos y los comerciantes en más de 50 mercados de todo el mundo, y ofrece:
www.firstdata.com

- Sistemas de proceso de datos de crédito y pago.
- Gestión de cajeros automáticos y Terminales de Punto de Venta.
- Servicios de valor añadido, tales como la gestión de riesgos y fraude.
- Servicios de provisión, centros de atención a clientes y *back office*.

Los nuevos entrantes puntocom

La oportunidad de entrar en el nuevo negocio de servicios móviles de pago es un entorno natural para compañías como Google, Apple y Amazon. Estas

"Las compañías puntocom superan en número de clientes y conocimiento de su comportamiento a los mayores bancos y operadores globales."

"La entrada de los nuevos actores depende de su estrategia de posicionamiento, a la espera que desaparezcan las barreras de entrada y se clarifique la regulación."

compañías tienen las claves para posicionarse frente a los líderes de los negocios tradicionales que están en proceso de transformación (principalmente el sector financiero y los operadores de servicios móviles):

- Cartera de clientes y/o usuarios directos: cualquiera de estas compañías supera en número de clientes a los mayores bancos y operadores globales y no sólo es el número, sino el conocimiento del comportamiento de sus clientes.
- Capacidad de desarrollo de aplicaciones móviles: estas compañías han nacido gracias a sus capacidades para el desarrollo de aplicaciones de software en internet y llevan casi 20 años perfeccionando su propuesta de valor a base de desarrollos propios y adquisiciones.
- Control de los sistemas operativos y navegadores de los smartphones. Google, Apple y Microsoft controlan los sistemas operativos y navegadores que proporcionan la ventana de los usuarios al mundo de las aplicaciones y las tiendas online.

La entrada de estos nuevos actores está marcada por una estrategia de posicionamiento previo en su desarrollo de capacidades, a la espera que desaparezcan las barreras de entrada y se clarifique el entorno regulatorio.

Hasta la fecha los hechos más significativos en este posicionamiento son:

- **Google** (*Wallet*) fue el primero en lanzar un servicio tipo monedero con capacidad para almacenar tarjetas y realizar pagos asociados a tarjetas de crédito tradicionales. Para usuarios de Gmail en EEUU permite transferencias directas de saldo a la cuenta del monedero. Actualmente está promoviendo el modelo de servicio de pagos por móvil con emulación de tarjeta en la nube (*HCE: Host Carda Emulation*). www.google.com/wallet

- **Amazon** (*Payments*) ha desarrollado un servicio que permite al usuario pagar sus compras online en otras tiendas a través de su cuenta en Amazon. También permite la transferencia de fondos entre usuarios. payments.amazon.com

- **Apple** hasta la fecha solo ha lanzado un servicio pre-monedero denominado *Passbook*, que permite almacenar de forma conjunta tarjetas de fidelización, billetes de transporte, entradas y cupones regalo. También está promoviendo la utilización de los iBeacons. www.apple.com

- El Servicio **Paypal**, adquirido por eBay, permite a sus usuarios comprar online sin necesidad de utilizar directamente sus tarjetas con las tiendas web en las que opera. www.paypal.com

"Apple debe afianzar su estrategia de innovación para continuar con su posicionamiento de exclusividad. Aunque en una primera fase no se había posicionado en el mercado NFC, sí lo está haciendo con las tecnologías iBeacon."

iBeacon: el posicionamiento de Apple

En el año 2013 Apple se situó como el segundo fabricante global de smartphones por ventas tras Samsung, con una cuota del 18%. Esto supone un disminución del 3,5 % respecto de su posicionamiento en 2012. Aunque las ventas del iPhone crecieron un 16%, Apple no pudo captar el potencial de crecimiento global del mercado en el último trimestre de 2013, que fue del 36%.

Esta situación de pérdida de posicionamiento global con respecto a las plataformas Android y principalmente en relación a su principal competidor Samsung, no sólo es debido a la extensión del mercado de smartphones a segmentos más orientados al precio, sino también a que sus competidores han alcanzado e incluso superado las prestaciones y funcionalidades del iPhone.

En este entorno competitivo Apple debe afianzar su estrategia de innovación para continuar con su posicionamiento de exclusividad. Una de las áreas de desarrollo tecnológico que puede tener mayor impacto de negocio es el de los servicios de pago por móvil, y aunque Apple en una primera fase no se había posicionado en el mercado NFC, sí lo está haciendo de una forma más rupturista con las tecnologías iBeacon http://es.wikipedia.org/wiki/IBeacon.

iBeacon es una tecnología que se incluyó en el 2013 como una característica de iOS 7 y consiste en la utilización de Bluetooth de bajo consumo como sistema de notificaciones emergentes en los móviles iPhone. A través de pequeños dispositivos con capacidad Bluetooth, denominados balizas, y que se fijan en paredes de edificios, comercios o en otros lugares públicos, la tecnología iBeacon permite, a las empresas u otras entidades, enviar a los propietarios de teléfonos compatibles notificaciones emergentes personalizadas en función de su ubicación y la proximidad a las tiendas y productos.

Este sistema está siendo considerado por las grandes marcas como la próxima gran oportunidad en la publicidad:

- Apple ya está comenzando el despliegue del sistema de iBeacon en sus tiendas: al entrar, los usuarios de iPhone podrán recibir las ofertas del día y al acercarse a una nueva tableta iPad recibirán el video de presentación del producto.

- Coca-Cola, por ejemplo, ha instalado balizas iBeacon durante el mundial de futbol de Brasil, permitiendo a los usuarios de iPhone localizar dispensadores de Coca-Cola en función de su posicionamiento.

- Philips está ya en fase de pruebas de un sistema de iluminación LED con balizas iBeacon integradas que permite a las tiendas

enviar información de sus productos a los usuarios de iPhone. Estos, a través de una app específica, pueden visualizar el mapa de la tienda e incluso su posicionamiento en ella.

Aunque el iPhone actual no es compatible con NFC, Apple está desarrollando diversas patentes para lo que podrían ser nuevas funcionalidades en el iPhone: NFC integrado en el sensor dactilar e integración de protocolos NFC y Bluetooth.

Por otra parte los fabricantes de carcasas protectoras para móviles como INCUBO, han desarrollado modelos que añaden capacidad NFC a los iPhone 5 y que ya han sido homologados en servicios de monedero móvil como el de ISIS compatible con las redes de AT&T, Verizon y T-Mobile en USA.

>11 Barreras y amenazas

Aceptación de los usuarios

Probablemente la mayor barrera para la penetración de los servicios de pago por móvil es que los posibles usuarios finales no los utilicen en la medida que se espera para que el mercado crezca hasta el umbral que permita su desarrollo. A continuación se detallan los principales motivos que respondieron los consumidores en EEUU a una encuesta de la Reserva Federal Americana[10] realizada en marzo de 2013:

38% - Me preocupa la seguridad de los pagos por móvil

36% - Es más fácil pagar por otros medios

35% - No veo ningún beneficio en los pagos por móvil

30% - No tengo la funcionalidad necesaria en mi teléfono

16% - No me fío de la tecnología

14% - No entiendo la diferencia entre todas las opciones

10% - No necesito hacer ningún pago

10% - El coste de acceso de datos en el móvil es muy alto

9% - No conozco tiendas que acepten el pago con móvil

7% - Otros motivos

5% - Instalar el servicio y activarlo es difícil y lleva mucho tiempo

4% - Las tiendas en las que compro no aceptan el pago por móvil

2% - No contesta

"La mayor barrera para la penetración de los servicios de pago por móvil es que los posibles usuarios finales no los utilicen en la medida que se espera."

Las compañías lideres del desarrollo del mercado de medios de pago móvil, particularmente los bancos, operadores móviles y entidades comerciales, deben orientar sus estrategias para responder a las necesidades planteadas por los usuarios. En general estas estrategias deben plantearse de forma colaborativa a través de acuerdos multisectoriales. La administración pública debe facilitar esta aproximación estableciendo una regulación que garantice el desarrollo de la libre competencia en cada uno de los sectores.

Seguridad de la información

La seguridad de la información de los usuarios y sus transacciones es sin lugar a dudas un requerimiento esencial, no solo para los usuarios sino también para los bancos y comercios. Existe una alarma generalizada ante los continuos casos de fraude y uso abusivo de datos en diferentes empresas del sector.

Según un estudio de Verizon de 2014[11], en Europa solo el 31% de las empresas (cadenas minoristas y proveedores de servicio) que gestionan información de tarjetas de pago cumplen los 12 requisitos de las recomendaciones PCI (ver apartado *Seguridad de la información y transacciones*).

— 10
Consumers and Mobile Finances Services 2013, Federal Reserve, PDF: http://goo.gl/0P2OL2

— 11
Verizon 2014 PCI Compliance Report: http://goo.gl/Jtth6f

"Se debe reconsiderar la situación de que estos estándares de seguridad sean recomendaciones y pasen a ser normativas de uso obligatorio."

"La administración pública es responsable de regular servicios públicos como seguridad e identificación, salud, transporte... Y debe tener un papel de liderazgo junto al resto de los actores."

Esto sitúa a Europa muy por detrás de EEUU, con un 56%, y la región de Asia-Pacífico, con un 75%.

Se debe reconsiderar la situación de que estos estándares de seguridad sean recomendaciones y pasen a ser normativas de uso obligatorio, al igual que ha ocurrido con la Ley de Protección de Datos.

También se debe considerar la necesidad y viabilidad del uso de autenticación de doble factor, según configuración del usuario o para cantidades superiores a cierto umbral. Este sistema de doble factor consistente en la utilización, además del código secreto (PIN), de un código de operación de un solo uso recibido a través de SMS o dispositivo tipo *token*.

Disponibilidad e interoperabilidad de los servicios

La flexibilidad que exigen los clientes para que los servicios sean interoperables está siendo amenazada por algunos planteamientos proteccionistas sectoriales, tanto de los operadores móviles como de los bancos y otros proveedores de servicios.

- El sector de los operadores móviles, que posee el control del Dispositivo Seguro (el móvil), se ha propuesto tener un papel significativo en el nuevo negocio de pagos móviles, no limitándose a la mera transmisión de datos, al igual que ha ocurrido en el mercado de contenidos y aplicaciones en internet.

- El sector bancario, que posee el control de los servicios de pago con tarjeta, tiene el objetivo de hacer crecer su negocio en el ámbito de las aplicaciones de comercio electrónico móvil.

- Los proveedores de terminales, aplicaciones y servicios internet se han propuesto aprovechar la infraestructura de operadores móviles y bancos para captar nuevo negocio, en este caso apalancándose en el control final de la aplicaciones o los terminales.

Esta situación de control distribuido de la cadena de valor puede originar una situación de mercado con soluciones fragmentadas no interoperables, que retrasaría el desarrollo del mismo. Por otro lado, la administración pública es responsable directa de regular servicios públicos críticos, tales como seguridad e identificación (DNI y pasaporte), salud (tarjeta sanitaria) y transporte (tarjetas de abono y billetes) y por ello debe tener también un papel de liderazgo junto al resto de los actores principales.

>12 Atributos de los servicios de pago por móvil

El mercado de los servicios de pago por móvil se encuentra en una fase de definición del modelo inicial y desarrollo posterior hacia el modelo final. Por lo tanto, es necesario reflexionar sobre las bases en las que se asienta el modelo para asegurar que dicha evolución permitirá cumplir la expectativas de los clientes, asegurando la viabilidad de los modelos de negocio de las empresas que contribuyen en la cadena de valor.

Para dinamizar esta reflexión se plantean los siguientes atributos que, desde una perspectiva centrada en el cliente, son imprescindibles para la adopción de los nuevos servicios y el desarrollo pleno del mercado:

Atributos	Descripción
1. Seguridad	Los datos de identificación y claves de los clientes, así como las transacciones, deben ser seguras, utilizándose mecanismos de encriptación de extremo a extremo que garanticen la confidencialidad. Los procesos de tratamiento de información deberán estar certificados y sujetos a auditorías periódicas.
2. Transparencia y confidencialidad	Los usuarios de los servicios deberán tener capacidad de control y acceso a la información personal y transacciones que manejan los proveedores de los servicios, de tal forma que se asegure el grado de confidencialidad que los usuarios requieran.
3. Universalidad del servicio	Los medios de pago por móvil deberán ser aceptados de forma generalizada en cualquier tipo de entidad comercial que acepte tarjetas. No debe existir umbral mínimo de gasto. La emisión de tarjetas de pago a débito no podrá denegarse a ningún usuario.
4. Portabilidad	Los usuarios podrán portar sus servicios de pago o identificación de un operador móvil a otro de forma inmediata y sin coste adicional, al igual que se realiza actualmente para el servicio telefónico móvil. Para el usuario no será necesario volver a reactivar o contratar los servicios de pago que ya estuviera disfrutando.
5. Simplicidad y consistencia	El interfaz de acceso para la configuración de los medios de pago e identificación deberá ser simple para que cualquier usuario, independientemente de sus conocimientos técnicos, sea autosuficiente en la puesta en marcha de los servicios. Los procesos y funciones básicas deberán ser homogéneas e independientes del proveedor de servicios, dado que en caso contrario pueden inducir a los usuarios a errores en su utilización.
6. Accesibilidad y fiabilidad	La cobertura geográfica del servicio deberá ser máxima, por lo que será necesario que existan acuerdos entre los operadores móviles para maximizar la disponibilidad del servicio tanto en exteriores como interiores. Los proveedores de servicios de pago deberán proporcionar acuerdos de nivel de servicio que incluyan indicadores de disponibilidad del sistema y del tiempo de respuesta de la operaciones.
7. Servicios de valor añadido	Los servicios finales de monedero electrónico tendrán una funcionalidad básica común homogénea sobre la que se podrán definir servicios de valor añadido diferenciales (registro de operaciones, alarmas de uso, análisis de gasto, etc.).
8. Gratuidad del servicio universal	La utilización de los servicios de pago por móvil no estará sujeta a comisiones para los usuarios. Los servicios premium de pago sólo podrán asociarse a servicios de valor añadido diferenciales.

>13 Conclusión y recomen-daciones

"El crecimiento del negocio puede verse estancado o experimentar un crecimiento mayor si se orienta hacia un modelo sostenible centrado en las necesidades de los clientes y que asegure la viabilidad de las empresas."

Los servicios de pago por móvil y otros nuevos servicios móviles asociados contribuyen de una forma muy importante al desarrollo de la sociedad de la información y tienen un alto impacto en la vida cotidiana de los usuarios. El crecimiento actual de este negocio, que es superior al 30% anual, puede verse estancado o experimentar un crecimiento mayor si se orienta hacia un modelo sostenible centrado en las necesidades de los clientes, y que asegure la viabilidad de las empresas que contribuyen en la cadena de valor.

Las empresas en los principales sectores implicados (entidades financieras, operadores móviles, compañías proveedoras de equipamientos, software y servicios) corren el riesgo de centrarse en estrategias basadas en modelos protectores del status de su respectivo sector como consecuencia, pueden bloquear las iniciativas de desarrollo de modelos abiertos transversales centrados en las necesidades de los clientes. Este enfoque podría tener éxito a corto plazo, pero está abocado al fracaso en un mercado en continua transformación como el de las TIC.

Para reforzar las estrategias transversales abiertas, en un ecosistema tan fragmentado y complejo, es imprescindible que los organismos de regulación y estandarización establezcan planteamientos ambiciosos que favorezcan un entorno colaborativo, a la vez que competitivo, entre los diferentes actores principales. Se debe garantizar la universalidad, seguridad, simplicidad, flexibilidad y calidad del servicio al cliente.

Por último, los organismos de la administración pública tienen la oportunidad y el deber de participar en el ecosistema, no solo como espectadores, sino también liderando la definición de un modelo que facilite el desarrollo eficiente de servicios públicos como el de la sanidad, la identificación y el transporte.

>14 Referencias

Green Paper: Towards an integrated European market for card, internet and mobile payments. European Commission, Final Document, 2012 - http://goo.gl/gfhL9v

Mobile Contactless Payments Service Management Roles. European Payments Council / GSMA, Version 2.0, October 2010 - http://goo.gl/utQH7G

Mobile Wallet Payments. European Payments Council, Version 2.0, January 2014 - http://goo.gl/gFzakI

Consumers and Mobile Financial Services 2013. Board of Governors of The Federal Reserve System, March 2013 - http://goo.gl/QxMHlb

White Paper: The Mobile Payments and NFC Landscape: A U.S. Perspective. Smart Card Alliance, September 2011 - http://goo.gl/nqxWta

A New Model: The Consumer-Centric Model and How It Applies to the Mobile Ecosystem. GlobalPlatform Whitepaper, March 2012 - http://goo.gl/LzcaVW

A Guide To EMV, EMVCo, Version 1.0, May 2011 - http://goo.gl/RrG6UR

Mobile Threats Report. Juniper Networks, Third Annual 2013 - http://goo.gl/eEFGh2

nae_
doing ahead

Nae trabaja con operadores de telecomunicaciones, grandes empresas y administraciones públicas para anticipar los retos de crecimiento y transformación del mercado, mejorando su estrategia de negocio y eficiencia operativa. Nuestro modelo de trabajo garantiza la experiencia y el conocimiento de nuestros profesionales, así como la metodología y las herramientas para gestionar retos estratégicos en entornos de alta competitividad y complejidad.

www.nae.es

@nae_es

www.linkedin.com/company/nae_es

info@nae.es