Cuaderno de notas del
OBSERVATORIO
INTECO
Instituto Nacional de Tecnologías de la Comunicación

LA TECNOLOGÍA NFC: APLICACIONES Y GESTIÓN DE SEGURIDAD

En los últimos años estamos siendo testigos del escalado de tecnologías y funcionalidades en los terminales móviles, convirtiéndose en dispositivos multifunción y provocando que se deje de pensar en ellos como meros teléfonos. Estas incorporaciones han sido varias, desde la tecnología Bluetooth implantada hace tiempo, pasando por la localización GPS y la conexión a Internet través de Wi-Fi y 3G, hasta tecnologías más incipientes que nos permitan nuevos usos.

Una de estas últimas incorporaciones es la tecnología inalámbrica de comunicación de corto alcance NFC (siglas de *Near Field Communication)*. Así es como se denomina a la tecnología que se plantea como una de las principales alternativas para el futuro del pago electrónico y la interacción con el consumidor.

Se trata de una tecnología que puede considerarse heredera de la ya conocida RFID, que viene usándose de forma habitual desde finales de los 70, y por tanto pariente de las ya clásicas tarjetas de identificación. Sobre su implementación en teléfonos móviles, un método similar para el pago electrónico (FeliCa) lleva años siendo usado en Japón. Sin embargo, en el resto del mundo la tecnología NFC se está acogiendo con mayor lentitud.

Es este Cuaderno se analizará cómo funciona NFC, su incorporación a los dispositivos móviles y cuáles son sus aplicaciones posibles, además de analizar su seguridad.

I Antecedentes

NFC es una extensión del estándar ISO 14443 (RFID) en el que basa gran parte de su tecnología. Este estándar define las tarjetas de identificación electrónica y de proximidad.

Los orígenes de la tecnología RFID se sitúan en diversos puntos. En la década de los 40, coincidiendo con la Segunda Guerra Mundial, se comenzaron a desarrollar tecnologías de identificación por radiofrecuencia e incluso dispositivos de escucha pasivos. Por otro lado, algunos autores remontan su origen al MIT de los años 20. Sin embargo, el origen comúnmente aceptado es el trabajo de Harry Stockman *"Communication by Means of Reflected Power"* publicado en 1948. En él se definía el método de comunicación punto a punto en la que el emisor no genera energía, sino que refleja y modula la energía transmitida por el elemento receptor para transmitir información. Este es el fundamento en el que se asienta la tecnología RFID y por extensión, NFC.

Sin embargo, no es hasta los años 70 cuando, gracias a la reducción del coste de los elementos electrónicos y al desarrollo la tecnología necesaria, se comienza a explotar la tecnología RFID. Finalmente en los años 80 se implementa masivamente.

Hoy día, se pueden encontrar usos de la tecnología RFID en todos los ámbitos de la vida cotidiana. Por ejemplo, muchas mascotas tienen un chip RFID implantado para su seguimiento, productos como los zapatos pueden tener uno por ejemplo en su suela, y muchas empresas utilizan tarjetas de identificación con ellos para que sus trabajadores fichen al inicio y al final de su jornada laboral[1].

Con la tecnología ya RFID implantada, y tras la popularización del teléfono móvil, se comenzó a investigar la forma de incluir en ellos estos métodos de comunicación. Con este objetivo se depuraron algunas de sus características, como por ejemplo reducir el alcance de la señal o diseñar el almacenamiento de ciertos tipos de datos.

A partir de estas nuevas especificaciones, en 2002 nace el primer estándar bajo el nombre de *mobile RFID* o NFC, realizado por el organismo ECMA (ECMA-340). Posteriormente, este modelo fue remitido a ISO/IEC como propuesta de estándar internacional que finalmente fue aprobado el 8 de diciembre de 2003 como el ISO/IEC 18092, incluyendo los estándares ISO 14443 (Tipos A y B) y *FeLica*.

Pero el verdadero hito en el camino de la tecnología NFC hacia la estandarización llegó el 18 de marzo de 2004[2], cuando Nokia, Philips y Sony se asociaron para crear el NFC Forum, una agrupación de empresas para colaborar en especificación de la tecnología NFC, basándose para ello en ISO/IEC 18092. Hoy, el NFC Forum ha elaborado varias especificaciones relacionadas, entre ellas quizá las más importantes sean NFCIP-1 y 2, que definen el protocolo de comunicación entre dos dispositivos NFC. Además, promueven el logotipo N Mark como distintivo de la tecnología[3].

Ilustración 1: Logotipo N Mark

Fuente: NFC Forum

[1] Shrouds of Time. The history of RFID. http://www.transcore.com/pdf/AIM%20shrouds_of_time.pdf

[2] Nokia, Philips And Sony Establish The Near Field Communication (NFC) Forum. http://www.nfc-forum.org/news/pr/view?item_key=d8968a33b4812e2509e5b74247d1366dc8ef91d8

[3] About the NFC Forum N-Mark. http://www.nfc-forum.org/resources/N-Mark/

II Funcionamiento de la tecnología NFC

Características

Las características básicas del sistema NFC y que a la postre lo definen son las siguientes:

- Comunicación inalámbrica por proximidad: Este tipo de comunicación, similar al de otras tecnologías como tarjetas de inteligentes, se realiza usando inducción electromagnética. Los dispositivos compatibles con NFC deben contar con una pequeña antena en espiral que genera un campo electromagnético de radiofrecuencia. Cuando un dispositivo entra en el campo electromagnético de otro, puede establecerse la comunicación. El alcance del campo electromagnético para la tecnología NFC es muy pequeño, pudiendo ser en teoría de entre 10 y 20 centímetros pero aplicándose en la práctica una distancia de 4 centímetros o inferior. Esto provoca que los dispositivos necesiten casi entrar en contacto físico para poder comunicarse.

- Pequeñas transacciones de datos: Los dispositivos NFC se pueden comunicar con cuatro velocidades de comunicación de datos: 106, 212, 424 o 848 Kbit/s, aunque esta última no está reflejada en ISO/IEC 18092. Esta limitación se debe a que la tecnología NFC no está orientada a la transmisión masiva de datos, sino a pequeñas comunicaciones entre dispositivos. Sólo se permiten velocidades mayores, del orden de 6,78 Mbit/s, en la comunicación entre dos dispositivos orientada al intercambio masivo de datos.

- Operaciones en la frecuencia ISM: En las transmisiones de dispositivos NFC se utiliza la banda de frecuencia alojada en los 13,56 Mhz, tradicionalmente asignada a las etiquetas RFID en modo pasivo (como etiquetas de identificación de productos farmacéuticos, documentos de identidad, etc.). Esta frecuencia pertenece al conjunto de bandas de radio ISM, que son utilizadas generalmente con fines industriales, científicos y médicos (de ahí su nombre ISM, *Industrial, Scientific and Medical*). Para el uso de estas bandas no es necesaria una licencia, pero se debe garantizar que no se produzcan interferencias entre los dispositivos. Esto representa una ventaja para la implantación y uso de NFC, ya que el canal de trasmisión es libre y no tiene un coste de uso asociado. Otros sistemas que también utilizan estas bandas de frecuencia son, por ejemplo, Bluetooth y Wi-Fi.

Modos y roles de comunicación

Los dispositivos NFC pueden actuar en dos modos básicos:

- Activo: Si es capaz de crear su propio campo de radiofrecuencia, normalmente utilizando para ello alimentación eléctrica, usualmente baterías o pilas.

- Pasivo: Si el dispositivo no genera su propio campo, sino que recibe alimentación del campo de radiofrecuencia de otro dispositivo.

Íntimamente vinculados a estos modos de actuación, se encuentran los roles que un dispositivo NFC puede tomar en una comunicación. Al basarse la transmisión en el concepto de pregunta y respuesta, un dispositivo sólo puede responder a otro si y sólo si ha iniciado una comunicación con él. Estos roles son dos, y en toda comunicación son necesarios ambos, asumiendo cada dispositivo uno de ellos:

- Iniciador: El dispositivo que da comienzo a la interacción. Aunque se trate de una comunicación en la que ambos dispositivos lleguen a ejercer un papel activo, el dispositivo que comience la comunicación será el considerado como iniciador hasta que se finalice la comunicación.

- Objetivo: El dispositivo que responde a la comunicación establecida por el iniciador.

Según estas definiciones, se puede deducir que hay determinadas combinaciones de modos y roles no compatibles. Un dispositivo activo puede actuar como iniciador o como objetivo en una comunicación, sin embargo un dispositivo pasivo no puede ser nunca iniciador, ya que no puede generar su propio campo de radiofrecuencia ni, por tanto, emitir una señal a otro dispositivo por sí solo.

Tradicionalmente, una de las configuraciones más usadas es la que comunica un dispositivo activo que actúa como iniciador y uno pasivo que es el objetivo. En este escenario, el elemento activo emite un campo de radiofrecuencia, que alimentará electromagnéticamente al dispositivo pasivo haciendo que este responda modulando la señal con cierta codificación. Esta configuración es heredada de RFID y la base para construir las etiquetas NFC.

Con la especificación NFCIP-1 se introduce el concepto de la comunicación peer-to-peer entre dos dispositivos activos. En este caso, un dispositivo activo “A” actúa como iniciador de la comunicación mandando un mensaje a un dispositivo “B”. Mientras espera respuesta, el dispositivo “A” desactiva su campo de radiofrecuencia, mientras que “B” lo activa para emitir. Así, durante la comunicación los dispositivos van alternándose en la activación sus campos de radiofrecuencia para enviar y recibir datos entre ellos.

En este último caso es importante no confundir los modos y roles. Aunque desactiven sus campos de radiofrecuencia, ambos dispositivos siguen siendo por definición activos. Además, aunque “B” transmita datos, el iniciador de la comunicación en el origen seguirá siendo siempre el dispositivo “A” hasta que finalice la comunicación.

A pesar de sus posibilidades, el sistema NFC tiene diferentes limitaciones. La limitación principal es que un dispositivo activo no puede comunicarse con varios dispositivos pasivos a la vez aunque estos sí serían capaces de responder al estar bajo la influencia del campo de radiofrecuencia. Por ello, esta comunicación se limita a la elección de uno de los elementos pasivos antes de iniciar la transferencia de datos. El iniciador debe seleccionar qué dispositivo pasivo es el receptor del mensaje, siendo ignorado por el resto. Así, los mensajes de difusión o *broadcast*, en los que varios dispositivos reciben información de un mismo emisor, no están permitidos en esta tecnología.

III Obtención de información: Etiquetas NFC

Las etiquetas NFC son pequeños dispositivos NFC pasivos que pueden contener fragmentos de información. Básicamente se trata de pequeñas espirales de metal a las que se les añaden componentes de memoria y comunicación. Su diseño completamente plano las hace ideales para presentarse en formatos como pegatinas, tarjetas de visita, llaveros e incluso pulseras.

Su funcionamiento es parecido al de los códigos de barras y de los códigos QR, sin la necesidad del reconocimiento óptico del código. Así, un dispositivo NFC activo (incorporado en un teléfono inteligente, por ejemplo) actúa como lector. Al acercarlo a una etiqueta NFC, el campo de radiofrecuencia que el lector aplica sobre la etiqueta la activa y hace que le transmita los datos que almacena en su interior.

Estos datos dependerán, entre otros factores, del tipo de etiqueta NFC, ya que existen varias clases en función de su memoria, su tasa de transferencia de datos y los modos de interacción. Estos tipos fueron estandarizados por el NFC Forum y se pueden observar en la siguiente tabla:

Tabla 1: Tipos de etiquetas NFC

Tipo	Estándar	Modos	Memoria	Velocidad
Tipo 1	ISO14443 Tipo A	Sólo lectura Lectura/Escritura	96 bytes Ampliable a 2 kbytes	106 kbit/s
Tipo 2	ISO14443 Tipo A	Sólo lectura Lectura/Escritura	48 bytes Ampliable a 2 kbytes	106 kbit/s
Tipo 3	Sony FeliCa	Sólo lectura	2 kbytes	212 kbit/s
Tipo 4	ISO14443 Tipo A y B	Sólo lectura Lectura/Escritura	32 kbytes	106 kbit/s 424 kbit/s

Fuente: NFC Forum

En el interior de la etiquetas, la información se almacena en un formato especial llamado Formato de Intercambio de Datos o NDEF (NFC *Data Exchange Format*). Este formato

indica cómo deben ser guardados y encapsulados los datos dentro de las etiquetas u otros dispositivos para asegurar la interoperabilidad, es decir, que cualquier dato NFC pueda ser leído por cualquier lector, independientemente del fabricante de los dispositivos implicados.

Un mensaje NDEF se compone de una serie de registros, los cuales contienen una cabecera y el cuerpo. Esta cabecera contiene información sobre el tipo y la longitud de los datos almacenados en el cuerpo. Posteriormente, se encuentran los datos propiamente dichos o *payload*.

Estos datos pueden ser de diferentes clases, por ejemplo URIs o cualquiera de los tipos de datos específicos para NFC identificados por las Definiciones de Tipos de Registros o RTD (*Record Type Definition*). Los RTD son formatos optimizados para la transmisión entre dispositivos NFC.

- RTD Texto: Es el tipo más simple y contiene una cadena de texto en codificación Unicode. Puede utilizarse como si de texto en plano se tratara, aunque realmente se ideó para añadir metadatos de otros registros dentro de la etiqueta.

- RTD URI: Se trata de una serie de datos que identifican un recurso en concreto (estas siglas se refieren a *Uniform Resource Identifie*, identificador uniforme de recursos). Los recursos a identificar pueden ser de diferentes tipos, ya que las informaciones almacenadas pueden ser teléfonos, direcciones de correo electrónico y web, etc. Así, la etiqueta que incorpore esta información permitiría remitir al usuario a un determinado recurso. Un registro URI puede utilizarse de forma aislada o formando parte de otros registros, como el *Smart Poster*.

  Además de la URI en cuestión, en el RTD se define un campo URI *Identifier*, que contiene el protocolo a utilizar. Están soportados hasta 35 protocolos diferentes, incluyendo HTTP, FTP, telnet, incluso Samba o Bluetooth. Esto hace que los dispositivos no necesiten implementar un protocolo para las URIs, ya que este se encuentra especificado en el propio dato.

- RTD *Smart Poster*: Es el RTD por excelencia y el que engloba la mayor parte de los usos finales. Se define como una estructura que contiene a los RTDs anteriores además de un icono y acciones de control recomendado (hacer una acción, editar un contenido o guardarlo). Por ejemplo, puede contener información de un contacto, con nombre en un RTD texto, correo y página web en URI, foto en un tipo MIME image/jpeg o cualquier otro dato representable con estos tipos.

- RTD de control genérico: Da acceso a funciones o aplicaciones que no puedan ser expresadas mediante otros RTD. Además permite enviar órdenes a otros

dispositivos, pudiendo incluso seleccionar qué aplicación desea que ejecute la orden.

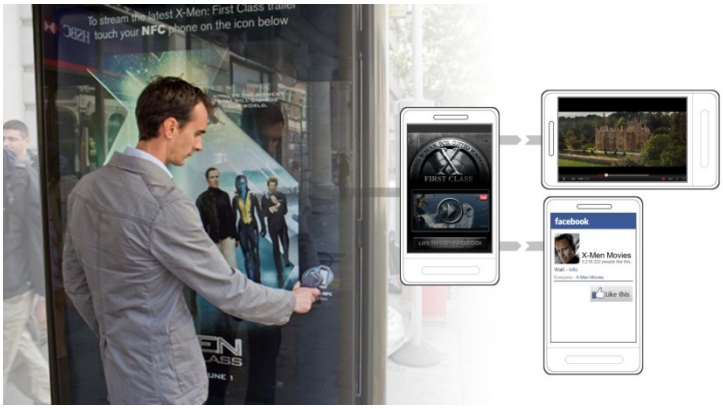
- RTD firma: Contiene en la etiqueta una firma digital para los contenidos como método de seguridad. Soporta firmados DSA, ECDSA y PKCS#1, que además aporta cifrado, y certificados X.509 y X9.68. Se puede usar una sola firma para todo el contenido, o firmar sólo otros registros o grupos de registros, además de poder usarse diferentes firmas para diferentes registros.

IV Aplicaciones basadas en NCF

a) Anuncios inteligentes o *SmartPosters*

Se trata del caso de uso por excelencia. Son incontables las aplicaciones que se le han dado a las etiquetas *SmartPoster* embebidas en carteles, anuncios, logotipos, etc. En muchos casos, en las etiquetas se guardan URIs que llevarán a sitios web con campañas publicitarias.

Ilustración 2: Usuario utilizando un *SmartPoster*



Fuente: Proxama

Un famoso uso de los *SmartPosters* se dio en el año 2011 en Londres. Con motivo del estreno de una película, se distribuyeron carteles de la película en distintas localizaciones de la ciudad[4]. Estos incluían una zona donde los usuarios podían acercar su teléfono móvil con dispositivo NFC, y directamente eran conducidos a un tráiler exclusivo en Internet y a la página de Facebook de la película.

Otro uso sobre el que se están realizando pruebas es el acceso a sistemas de compra de entradas embebidas en carteles de conciertos, teatro, etc. En este caso, la URI dirigiría al sitio web de venta oficial, desde el que se podría realizar la compra.

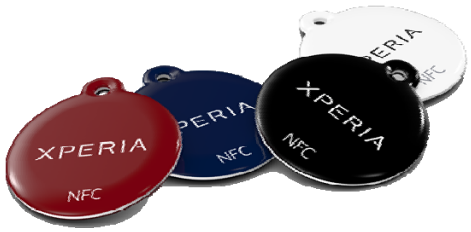
[4] UK's first NFC marketing campaign is delivered by Proxama for X-Men movie. http://www.proxama.com/news/uks-first-nfc-marketing-campaign-is-delivered-by-proxama/

b) Configuración de dispositivos y aplicaciones

En el día a día los usuarios realizan ciertas acciones de configuración en sus dispositivos que van más allá de las modificaciones más simples como pueden ser las relacionadas con los perfiles de sonido: activar el manos libres y el GPS al entrar al coche, configurar el despertador y bajar el volumen de las llamadas al acostarse, activar la conectividad a través de Wi-Fi al llegar a algún lugar concreto, e incontables ejemplos más. Si estas acciones son diarias, pueden representar una molestia y una pérdida de tiempo o incluso no llegar a realizarse por olvidos o descuidos.

Estas configuraciones pueden resumirse en comandos de control genérico y URIs que, almacenadas en etiquetas NFC distribuidas en nuestro entorno, pueden evitar pérdidas de tiempo y complejidades. De este modo, las configuraciones que el usuario considere ideales para cada momento o lugar podrían activarse con solo acercar el dispositivo a la etiqueta NFC señalada. Por ejemplo, en el caso del sistema manos libres y el GPS para la conducción, una etiqueta NFC en el coche facilitaría esta configuración de modo que el usuario solamente debería acercar el teléfono a la etiqueta, y automáticamente se configuraría en modo conducción.

Ilustración 3: Etiquetas NFC para terminales móviles



Fuente: Proxama

El principal problema en la adopción de las etiquetas NFC es que, a pesar de que los dispositivos compatibles son cada vez más comunes, no hay etiquetas NFC que leer. La venta de etiquetas reescribibles para el público es reducida, quizá porque no se conocen muy bien las capacidades de la tecnología o cómo pueden escribirse las etiquetas. Además, el uso que las empresas y organismos le dan a la tecnología actualmente no va mucho más allá del enlace a una web de campaña incrustado en un *SmartPoster*.

c) Pago móvil NFC

La tecnología NFC también se está intentando implantar como un nuevo canal de pago. Al estar este uso muy vinculado a su incorporación a los dispositivos móviles será tratado en el siguiente epígrafe, ya que es necesario un análisis en mayor profundidad.

V La tecnología NFC incorporada a dispositivos móviles

Tal y como se ha expuesto hasta ahora, los principales usos y desarrollos se han enfocado a la utilización de esta tecnología a través de teléfonos móviles, existiendo diversas implementaciones de NFC para estos dispositivos:

- Modo lectura/escritura: Se utiliza para la lectura y escritura de etiquetas NFC. En este caso, el teléfono puede actuar como iniciador y único elemento activo de la comunicación. El funcionamiento de este modo está descrito en la sección sobre etiquetas NFC. Además, al estar basado en el estándar ISO 14443, es posible la compatibilidad con tecnologías anteriores como RFID o *SmartCards*.

- Peer-to-peer: Es la forma en la que dos dispositivos NFC activos se intercambian datos alternando la generación de campos radiofrecuencia. Estos datos pueden ser varios, desde la configuración de Wi-Fi o Bluetooth, hasta fotografías, documentos, etc. Actualmente, se está investigando un modo fiable y seguro para realizar trasferencias bancarias entre dos personas a través de este método.

- Emulación de etiqueta: En este caso, el dispositivo emula ser una etiqueta NFC o una *SmartCard* tradicional ante otro dispositivo lector. De esta forma se pueden utilizar las posibilidades de las etiquetas sin necesidad de escribirlas o de portar un objeto diferente al teléfono móvil. Es utilizada en ciertos métodos de pago y entradas.

Ilustración 4: Uso peer to peer de dispositivos NFC

Fuente: NFC Forum

Funcionamiento de los pagos con dispositivos móviles basados en NFC

Esta aplicación es quizá la más publicitada para los dispositivos que cuentan con la tecnología NFC y, sin embargo, la que más lentamente se está implantando. Posiblemente esto se deba a la cantidad de agentes implicados en las transacciones y a la infraestructura necesaria para poner en marcha el sistema a gran escala.

Dependiendo del modo utilizado y del rol de los dispositivos, se han desarrollado varias implementaciones del pago móvil. Este análisis se centrará en la que parece tener mayor aceptación de la industria y mejores perspectivas de futuro: la cartera virtual.

Ilustración 5: Uso de la cartera virtual para el pago a través de NFC

Fuente: NFC Forum

En este caso se hace uso de la función de emulación de etiqueta del chip NFC para transformar el teléfono móvil en una cartera virtual que contendrá no sólo tarjetas bancarias, sino también cupones de descuento, tarjetas de fidelización y cualquier otro documento que pueda usarse en una compra.

Para poder implementar esta función de forma segura (lo cual es indispensable para su uso en transacciones bancarias) el dispositivo compatible estará equipado con un hardware seguro llamado *Secure Element* o Elemento Seguro que será accesible por el chip NFC aun estando en modo pasivo.

Este Elemento Seguro puede ser un hardware adicional en el interior del teléfono, estar integrado en la tarjeta SIM o en otros dispositivos externos, por ejemplo una tarjeta SD insertada en el teléfono. Aun no hay un acuerdo sobre el estándar de implementación del SE, aunque parece que las soluciones más populares son las dos primeras.

El SE integrará un entorno seguro y una solución de cifrado para las aplicaciones de pago y los datos bancarios del usuario. Del envío y almacenamiento de estos datos en el teléfono se hace cargo una entidad conocida genéricamente como *Trusted Service*

Manager, que es quien posee las claves públicas para los Elementos Seguros y actúa como tercero de confianza.

Actualmente hay gran cantidad de proyectos piloto basados en la tecnología NFC. Cada uno de ellos es desarrollado por un número pequeño de actores diferentes: un banco, conjuntamente con algún operador móvil y alguna cadena comercial, y utiliza diferentes formatos y protocolos de mensajes. Esta situación no se puede considerar como la ideal para desarrollar la tecnología, ya que en un futuro podría ralentizar y obstaculizar su progreso debido a incompatibilidad de formatos o desacuerdos entre actores.

Para solucionar esta situación surge la figura de los *Trusted Service Manager* (TSM), que actúan como enlace entre los diferentes actores, facilitando el intercambio de datos entre ellos. Además, es la figura que se encarga de proporcionar seguridad en las conexiones entre los diversos actores y sobre los datos del consumidor.

Tanto los TSM como otros actores forman parte de lo que la *SmartCard Alliance* llama "modelo colaborativo", que viene a explicar el flujo de información entre las entidades que forman parte del ecosistema del modelo de pago mediante NFC. Un ejemplo de primera provisión de un teléfono seguiría el siguiente flujo:

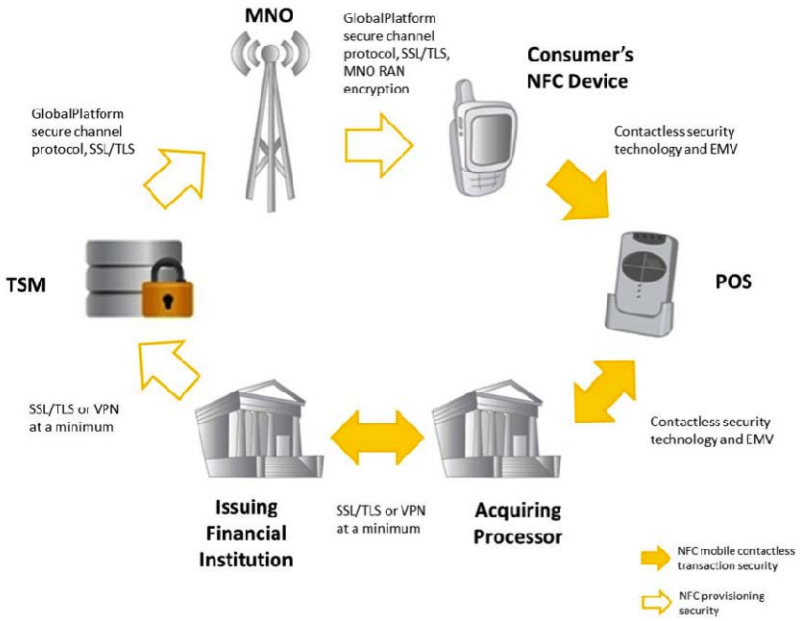
- Las entidades financieras generan los datos bancarios que van a almacenarse en el Elemento Seguro del teléfono.
- Estos datos son enviados a las TSM a través de interfaces diseñadas para la comunicación entre ambos, y se almacenan en una base de datos segura.
- Cuando el usuario pide la provisión del teléfono, se hace una petición al TSM a través de las redes móviles, que responderá con los datos de pago del usuario.
- Una vez en el teléfono, estos datos se almacenarán cifrados en el Elemento Seguro.

Evidentemente, es necesario que estos datos se envíen cifrados y no en texto en claro. Cada uno de los actores es responsable del cifrado de su parte del proceso. Así, las entidades financieras son responsables del cifrado de los datos, el TSM de las interfaces con las entidades financieras y los operadores de red móvil, además de la securización de sus bases de datos. Estos últimos, por su parte, deben garantizar que los datos no puedan ser capturados. Todos estas comunicaciones se aseguran usando tecnologías ya probadas y fiables, como conexiones TLS/SSL y cifrado PKI, además del cifrado aplicado por GSM o CDMA. En total, en la transmisión de estos datos se aplicarán hasta tres capas de cifrado, lo que hace que la comunicación se considere confiable.

En cuanto a la red de pago, las entidades financieras (tanto bancarias como entidades de pago) deben habilitar el pago a través de NFC en sus redes. Esto en realidad no debería

suponer un obstáculo, ya que el pago móvil utiliza las mismas condiciones que las tarjetas de crédito y tarjetas inteligentes.

Ilustración 6: Modelo colaborativo con seguridad en las conexiones



Fuente: Smart Card Alliance

El otro gran grupo de agentes implicados está formado por los operadores de telefonía móvil. Estos están encargados de las comunicaciones entre los demás actores y debe garantizar la seguridad en las comunicaciones de datos, además de ser en última instancia los propietarios de la tarjeta UICC o SIM (en caso de que el Elemento Seguro esté implementado en ella).

Otros actores importantes son los fabricantes de dispositivos móviles y electrónica en general, que son los últimos responsables de la introducción de la tecnología NFC en los dispositivos y en la sociedad, incluyendo la tecnología en sus productos.

Aplicaciones NFC de pago móvil basadas en NFC

***FeliCa* (Japón)**

El mayor campo de pruebas para el pago a través de móvil, al igual que otras tecnologías, es Japón. Actualmente este país es líder en su uso, con unos 78 millones[5] de dispositivos preparados para el pago móvil en circulación ya a finales de 2009.

[5] Stephen Ezell, Contactless Mobile Payments (2009). http://www.itif.org/files/2009-slides-mobile-sezell.pdf

Para comprender el éxito de este sistema debemos remontarnos a 1997, año en que Sony presentó su sistema *Felicity Card* o *FeliCa*. Se trata de un chip RFID embebido en una tarjeta similar a las de crédito que se comenzó a usar en un primer momento para la recarga del bono de trasporte interurbano, para posteriormente habilitarse como tarjeta pre-pago, a partir de 1999, a través de diversas empresas.

Este sistema fue el germen para que en 2004 Sony, junto al operador móvil NTT DoCoMo y la *Japan Rail Pass* constituyeran la sociedad *FeliCa Network* con la misión de trasladar el éxito de la *Felicity Card al* pago móvil. Así nació el sistema *Mobile FeliCa*, que consiste en un chip *FeliCa* integrado en los dispositivos.

Varios son los servicios que hacen uso de la tecnología *Mobile FeliCa*, pero el estándar de facto en Japón es el servicio *Osaifu-Keitai* (cartera móvil en japonés) de *NTT DoCoMo*. Funciona en modo de emulación de etiqueta NFC, y en su interior puede almacenar desde bonos de transporte a tarjetas de crédito, a través de diversos servicios de prepago y postpago.

En febrero de 2012, se contaba con unas 516 millones[6] de tarjetas *IC FeliCa* en todo el mundo, ya sea de forma autónoma o integradas en dispositivos.

Hay que remarcar que a pesar de la gran base de pago móvil, en Japón sólo entre el 20% y 25% de los usuarios con teléfonos móviles compatibles usan los servicios de *Osaifu-Keitai*[7], y el porcentaje de aquellos que lo usan activamente es aún menor. Estas cifras, aunque están muy por debajo del objetivo inicial teniendo en cuenta que esta tecnología surgió hace ocho años, siguen siendo los datos de uso más altas mundialmente.

A pesar de ello es necesario realizar una matización en la exposición de este modelo, ya que las etiquetas *FeliCa* forman parte del estándar NFC siendo el modelo de tarjeta NFC-F o tipo 3, por lo que cualquier lector NFC puede leer una tarjeta *FeliCa*. Sin embargo, FeliCa es un estándar local de Japón que no contempla los tipos NFC-A y B de tarjeta. En resumen, los dispositivos NFC pueden leer los elementos *FeliCa*, pero no ocurre lo mismo al contrario, NFC no es compatible con *FeliCa*.

Esto se debe en parte a que Sony incluye en sus tarjetas una capa de cifrado y autenticación propietaria no existente en el resto de tarjetas NFC. Por tanto, la introducción de NFC en Japón, teniendo ya una infraestructura similar pero incompatible, requiere un esfuerzo de las empresas japonesas para adoptar el estándar internacional.

[6] Gemalto and Sony establish Global Agreement for FeliCa / Near Field Communication Technology . http://www.gemalto.com/press/archives/2012/2012-02-28_sony_FeliCa.pdf

[7] Mediba survey shows Edy to be the most used mobile wallet system. http://japan.internet.com/wmnews/20100114/8.html

***Google Wallet* (EEUU)**

Por su parte, en Estados Unidos el servicio basado en el pago a través de NFC que se está consiguiendo imponerse es *Google Wallet*. Presentado en mayo de 2011, ofrece los mismos servicios que *Osaifu-Keitai* (tarjetas de crédito, tarjetas de fidelidad, etc.) pero usando para ello estrictamente tecnología NFC. El propio logotipo de *Google Wallet* se inspira en la representación típica que ondas de radiofrecuencia.

Para su lanzamiento, Google llegó a acuerdos con Mastercard y la entidad Citibank para que el sistema *Wallet* pudiera utilizar los puntos de pago *Mastercard PayPass* en los comercios. *PayPass* funciona con tecnología RFID a través de un pequeño chip en las tarjetas de crédito y débito. Así, los teléfonos sólo tendrían que usar el modo de emulación de etiqueta para poder ser leídos por los puntos de venta. El primer teléfono con un Elemento Seguro compatible fue Sprint Nexus S 4G.

Esta colaboración permitió a Google asegurar la existencia de una red donde los usuarios pudieran utilizar *Wallet*, que es uno de los principales escollos a salvar para la implantación de este tipo de tecnologías.

A pesar de los esfuerzos de todos los implicados, parece que los usuarios que se han descargado la aplicación *Google Wallet* no llegan a los 100.000[8], y sólo un pequeño porcentaje de ellos son activos.

En buena medida, se puede considerar que la causa de esta escasa adopción es que para usar *Google Wallet* son necesarios demasiados requisitos. Por un lado el teléfono debe ser compatible con NFC, a su vez su Elemento Seguro debe ser compatible con *Wallet* (actualmente sólo hay cuatro posibilidades en el mercado), además el usuario debe tener una tarjeta *Martercard Paypass* de Citi aceptada en el comercio en cuestión, y por último, el usuario debe querer utilizar este servicio.

Primeras experiencias en España

En España también se han realizado varios proyectos piloto de pago con teléfonos móviles. Bajo el título “Sitges Mobile Shopping”, Telefónica, junto a La Caixa, Visa Europe y Samsung, iniciaron en 2010 un proyecto piloto que duró seis meses[9]. Se asignaron 1500 teléfonos Samsung S5230 compatibles con NFC a clientes de Telefónica y La Caixa, y se habilitaron 500 puntos de venta en los comercios de la zona.

[8] Google Said to Rethink Wallet Strategy Amid Slow Adoption. http://www.bloomberg.com/news/2012-03-21/google-said-to-rethink-wallet-strategy-amid-slow-adoption.html

[9] "La Caixa", Telefónica y Visa finalizan con éxito la primera experiencia de pago por móvil en España. http://saladeprensa.telefonica.com/jsp/base.jsp?contenido=/jsp/notasdeprensa/notadetalle.jsp&id=0&origen=portada&idm=es&pais=1&elem=15900&titulo=%22la%20Caixa%22,%20Telef%F3n

Los pagos inferiores a 20 € se realizaban tan sólo acercando el teléfono, mientras que los superiores a esta cifra debían autorizarse mediante la introducción de un PIN, ya fuera en el terminal de punto de venta o en el propio teléfono.

Tras finalizar el piloto, se puede considerar que el sistema ha funcionado correctamente y el proyecto fue un éxito. El 90% de los usuarios realizaron pagos por móvil en el 80% de los comercios participantes. Fue utilizado sobre todo para pequeñas transacciones, ya que el 60% fueron de un valor inferior o igual a 20€. Los usuarios incrementaron la utilización del pago a través de tarjeta en un 30% y el valor de sus compras en un 23%. El sistema, además, demostró que esta tecnología no está limitada a los más jóvenes, ya que la edad media de los usuarios activos fue de 46 años.

Sobre la opinión de los usuarios, el 85% califico el sistema como suficientemente seguro y el 90% afirmo que seguiría utilizando el sistema. En resumen, los participantes otorgaron al sistema una puntuación de 8 sobre 10.

Visto el éxito, el pago móvil quedo implantado en Sitges, donde se continúa utilizando después del piloto.

VI Riesgos de seguridad en NFC

Al ser una tecnología inalámbrica, NFC tiene su punto débil en materia de seguridad en su medio de comunicación, el aire. Además, existen varios vectores de ataque al dispositivo móvil que actualmente no está suficientemente claro cómo asegurarán. Hay que recordar que esta tecnología, en cualquiera de sus aplicaciones, está en periodo de pruebas y no será hasta que su uso se torne masivo cuándo comenzarán a aparecer problemas, como fraudes organizados o a gran escala, que aprovechen vulnerabilidades tanto de la tecnología como de los dispositivos donde está integrada.

Por tanto, en este momento sólo se puede basar el análisis de la seguridad NFC en estudios realizados por investigadores. Estos arrojan las siguientes posibles vulnerabilidades:

a) Interceptación o Sniffing/Eavesdropping

Se trata de una amenaza a la que se enfrentan todas las comunicaciones que se transmiten a través del aire, incluso la comunicación hablada. En este sentido, el esquema es similar a un fisgón que intenta escuchar la conversación entre dos personas.

Para interceptar la comunicación, este intruso necesita que se cumplan dos requisitos: primero, que los interlocutores hablen lo “suficientemente alto”, y segundo, que pueda “entender” la comunicación.

En este sentido, teóricamente, un atacante remoto podría interceptar la comunicación entre dos dispositivos NFC a través de una antena especialmente manipulada. A pesar

de ello, hay que señalar que aún no se ha probado a qué distancia debería estar este atacante, ya que las señales de radiofrecuencia que generan los dispositivos son de corto alcance (*no hablan lo suficientemente alto*) y además depende del modo de comunicación. Teóricamente, una comunicación activa podría captarse a 10 metros, mientras que una pasiva necesitaría que el atacante esté a tan sólo un metro del emisor.

De cara a evitar el segundo requisito (que el atacante entienda la comunicación), se puede considerar que la tecnología NFC tiene incorporados suficientes mecanismos como para poder evitarlo en buena medida. Recordemos que las comunicaciones NFC, sobre todo las asociadas al pago móvil, pueden tener varias capas de cifrado. Un atacante, además, de poder captar la información, necesitará poder descifrarla para entender esta comunicación.

Por otro lado, si estos requisitos se dieran, la intercepción de la señal aun dependería de varios factores ambientales, como el nivel de ruido, obstáculos para la señal (como por ejemplo paredes), geometría de la antena del emisor y atacante, etc.

b) Corrupción de datos

Este posible problema de seguridad consiste en que un atacante, una vez con la capacidad de interceptar los datos que se están enviando, trate de impedir la comunicación. En el supuesto más simple únicamente intentaría hacer la comunicación suficientemente confusa como para que el dispositivo lector no la pudiera entender, provocando una denegación de servicio.

Para esto el atacante necesitaría poder transmitir datos en una frecuencia válida y en un momento determinado, el cual es calculable si se conoce bien la forma de modulación y codificación.

c) Modificación de datos

Este ataque supondría un paso más allá respecto a la corrupción de datos, ya que en lugar de limitarse a impedir la comunicación, el atacante intentaría cambiar el contenido de la misma con contenido válido aunque manipulado por el atacante.

En este caso, es necesario que el atacante conozca la codificación que utiliza el emisor para poder cambiar los bits que le llegarán al receptor. Según esta codificación, sería posible que el atacante cambiase sólo algunos bits o todos. En cualquier caso, el éxito del ataque dependería en gran medida de la exactitud en la modulación de la señal que el atacante emita.

d) Inserción de datos

En este caso, en lugar de insertar piezas de datos en una comunicación legítima, el atacante trataría de insertar una respuesta completa, haciéndose pasar por el dispositivo objetivo de la comunicación.

Este ataque sólo sería posible en casos donde el dispositivo objetivo tardara mucho en dar respuesta al iniciador, tiempo que aprovecharía el atacante para insertar su mensaje. En caso de no ser así, atacante y objetivo emitirían señales que se solaparían, dando lugar a la antes comentada corrupción de datos.

e) Ataques "*Man in the Middle*" o de intermediario

En un ataque MitM la comunicación no sólo es interceptada por el atacante, como ocurre en el caso del *eavesdropping*, sino que además pasa a través de él. Básicamente, dispositivos emisor y receptor creen estar comunicándose directamente cuando en realidad lo están haciendo a través del atacante, que aprovecha esta situación para manipular la información que se intercambian. En el contexto de una comunicación NFC, hay que diferenciar según el modo de comunicación.

- Comunicación activo-pasivo: El atacante inicialmente debería interceptar los datos enviados por el dispositivo activo iniciador (estando lo suficientemente cerca) y, a su vez, asegurarse de que el pasivo no recibe los datos corrompiendo la comunicación entre ellos. Esta situación sería posible, pero dado que los dispositivos NFC cuentan con detección de colisiones, el ataque sería detectado por el dispositivo activo y la comunicación terminada.

  Aun en el caso de que la colisión no llegara a detectarse, el atacante debería comunicarse con el objetivo. Para esto, debe generar un campo de radiofrecuencia. El impedimento al que se enfrentaría es que el iniciador también lo estaría generando, y dos campos de radiofrecuencia no pueden convivir al mismo tiempo. La única solución para el atacante es alinear perfectamente su campo de radiofrecuencia con el del iniciador. Esto en la práctica es imposible, y no hay posibilidad de ataque Hombre en el medio con esta configuración.

- Comunicación activo-activo: Al igual que en el caso anterior, el atacante primero debería interceptar la comunicación del iniciador y asegurarse de que el dispositivo objetivo no recibe datos, todo esto sin ser detectado.

  Si no es detectado, la comunicación con el objetivo sería más probable. Al haber apagado el iniciador su campo de radiofrecuencia en espera de respuesta, el atacante puede enviar su mensaje manipulado al objetivo. Pero el atacante se encontraría con otro inconveniente, ya que al activar el campo de radiofrecuencia para enviar, la comunicación manipulada también llegará al iniciador, que

permanecería a la escucha. El iniciador, al comprobar que los datos recibidos no son una respuesta, detectaría un problema en el protocolo y cerraría la comunicación.

Por tanto, y en resumen, un ataque hombre en el medio en NFC no es posible.

f) Redirección a sitios maliciosos a través de las etiquetas NFC

Debido a que en un primer momento no se sabe a dónde puede dirigir una URI en una etiqueta NFC, quizá no sea buena idea leerla ya que el destino podría ser una web maliciosa. En el pasado se han detectado ataques de *spoofing* de sitios web mediante códigos QR, los cuales llevaban a sitios web que contenían *exploits* del navegador del móvil. Por tanto, no sería extraño ver en la tecnología NFC una URI que dirigiera a sitios con ataques *cross-site scripting, exploits* o cualquier uso fraudulento basado en web que se conozca (*phishing* y troyanos, entre ellos). Es por ello que hay que tener precaución a la hora de abrir estos enlaces.

De hecho, este es el motivo por el que se incluyo el RTD firma en los tipos de datos de etiquetas. Así, un fabricante podría firmar el contenido de un campo URI. Este certificado permitiría conocer si el sitio web donde lleva la etiqueta NFC es de confianza. Una buena práctica a seguir sería no acceder a URIs sin firmas contenidas en etiquetas NFC.

g) Robo del terminal

Una pregunta recurrente entre las personas a las que se les presenta el sistema de pago móvil es qué ocurriría en caso de robo o extravío del terminal.

En los diversos pilotos de pago mediante NFC se ha estudiado el mejor método para introducir una capa de autenticación adicional, esencialmente un PIN para autorizar las transacciones. Sin embargo, esta medida es precisamente uno de los problemas que se quería eliminar con el uso de NFC para aportar mayor fluidez y rapidez en el pago. Dado que de momento no se ha encontrado una solución mejor, la más implementada es autorizar automáticamente las transacciones de pequeñas cantidades y requerir un PIN para las de mayor cuantía. Por tanto, ante el robo de un terminal, habría un rango de valores que sí podrían usarse de forma fraudulenta.

Sobre los datos almacenados en el interior del teléfono, se debe señalar que están protegidos por el Elemento Seguro. Por tanto, el vector de ataque se centra principalmente en las aplicaciones que tienen acceso a él. En febrero de 2012 apareció la primera vulnerabilidad en *Google Wallet*, que permitía a un usuario acceder al código de operación con el Elemento Seguro. Dado que *Google Wallet* almacenaba esta clave cifrada en el teléfono, a través de la aplicación maliciosa se podía descifrar y tener acceso a los datos bancarios. Sin embargo, era necesario actuar a través de un superusuario en el sistema (algo que no todos los terminales tienen configurado) y tener

acceso físico, además de pasar sobre el resto de barreras de seguridad que los dispositivos móviles incluyen hoy día (y que una tarjeta bancaria no posee).

En general, ante la pérdida de un dispositivo con NFC habilitado para pagos, se deberían tomar las mismas medidas que se toman en el caso de una tarjeta bancaria. De hecho, se prevé que las mismas operadoras móviles habiliten números especiales para ello al igual que ocurre en el caso de las actuales tarjetas bancarias.

VII Recomendaciones

Debido a que la tecnología NFC se encuentra en proceso de desarrollo, no se pueden establecer unas recomendaciones precisas y concretas respecto al diseño de sistemas y su uso. Si bien esto es cierto, sí se pueden establecer una serie de líneas generales que guíen la actuación, tanto de desarrolladores como de usuarios, en relación a la tecnología NFC.

A su vez, se pueden tomar otras tecnologías, y las recomendaciones establecidas para su uso, como modelos a seguir para así poder anticiparse a los posibles inconvenientes que se presenten con la generalización de la tecnología NFC.

a) Mantener actualizado el sistema operativo del dispositivo y sus aplicaciones

Actualmente se trata de una de las recomendaciones básicas para la utilización de cualquier dispositivo. La actualización del software supone la puesta al día en lo que se refiere al descubrimiento de vulnerabilidades y su solución. Por ello se recomienda mantener actualizados estos sistemas, incluyendo especialmente aquellos que impliquen la utilización de tecnología NFC pero también los que no lo requieran.

b) Instalar solamente aplicaciones de confianza

Al igual que ocurre con las aplicaciones actuales, es necesario descargar e instalar únicamente las aplicaciones que provengan de desarrolladores de confianza. Esto evitará que aplicaciones maliciosas sean instaladas en el dispositivo y sus acciones sean desconocidas por el usuario. Esta recomendación es de especial importancia en el caso de aplicaciones utilizadas para realizar transacciones económicas, pero debe ser tenida en cuenta en todos los casos ya que una aplicación maliciosa podría llegar a acceder a todas las informaciones.

En este aspecto también es de especial importancia comprobar los datos a los que se permite acceder a las aplicaciones instaladas y las acciones que se les permite realizar.

c) Leer solamente etiquetas NFC correctamente firmadas

Del mismo modo que se debe comprobar que las aplicaciones a instalar provienen de un desarrollador de confianza, al leer etiquetas NFC se debe comprobar que quien las crea y

pone a disposición de los demás no tiene intenciones maliciosas. Por ello es recomendable no leer las etiquetas NFC que no provengan de fuentes confiables. Para esto sería posible configurar el sistema NFC de modo que las etiquetas que no estén debidamente firmadas no puedan ser leídas.

d) Evitar cualquier acción automática por parte del sistema

El sistema NFC facilita diferentes acciones, pero para poder realizarlas de forma segura, es recomendable que el usuario deba dar su visto bueno a todas las acciones. Por ello es recomendable que se configure el sistema NFC de modo que no se permita la realización de acciones automáticas.

e) Mantener el sistema desactivado cuando no se esté utilizando

Al igual que ocurre con otros sistemas de comunicación, como por ejemplo Bluetooth, es recomendable mantener estos sistemas desactivados siempre que no se estén utilizando. De este modo se pueden evitar diferentes problemas como intrusiones o acciones involuntarias.

f) Primar el cifrado en el almacenamiento de información y en las comunicaciones

En cuanto a la elección de dispositivos y servicios que utilicen la tecnología NFC, al igual que en el caso de otras tecnologías y especialmente las inalámbricas, se debe primar el uso de cifrado en el almacenamiento de la información y en su comunicación. De este modo, aunque un atacante pudiera acceder a las comunicaciones o a la propia información, para poder utilizarla debería poder también descifrarla, suponiendo así otra barrera de seguridad. Así pues, se recomienda utilizar únicamente dispositivos y aplicaciones que utilicen algún método de cifrado.

g) Establecer limitaciones en la cuantía de pago a partir de las cuales se necesitaría autenticación

A pesar de que uno de los objetivos del pago mediante el sistema NFC es agilizar este proceso, parece ser necesario establecer ciertas limitaciones para que en caso de extravío o robo nadie pueda utilizarlo. Actualmente, el método que parece ser más utilizado, y que establece un equilibrio entre la comodidad en el uso y la seguridad, es limitar las cuantías que pueden ser pagadas mediante el sistema NFC sin necesidad de autenticación. De este modo, los pagos de menor cuantía podrían realizarse de forma más ágil, mientras que aquellos que superen dicho límite requerirían de una autorización por parte del usuario mediante algún sistema, por ejemplo el uso de un PIN.

h) Si se usa para pagar hay que actuar como si de un medio de pago más se tratase

Es necesario que desde el momento en que se configure el sistema para poder realizar pagos a través de él se comience a considerar el dispositivo como un medio de pago más, actuando en consecuencia. De este modo, es necesario establecer las mismas precauciones que se mantienen con los demás medios de pago. Por ejemplo, al igual que nadie pone dinero en efectivo, la cartera o una tarjeta de crédito encima de una mesa, y mucho menos abandona dicha mesa momentáneamente dejando estos medios de pago en ella, tampoco se debería actuar de este modo con los dispositivos que integren el pago mediante NFC.

Por otro lado, en caso de pérdida o robo se debe actuar como si de un medio de pago más se tratase, poniéndose en contacto inmediatamente con el servicio de atención al cliente que el proveedor tenga habilitado con el fin de anular dicho dispositivo.