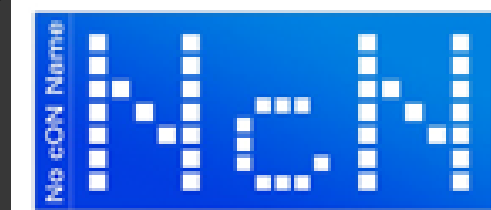


Give me your credit card

The NFC way

Jose Miguel Esparza
@EternalTodo



Agenda

- Introducción
- Inseguridad en NFC
- Tarjetas bancarias NFC
- Tengo tus datos, ¿ahora qué?
- Conclusiones

Introducción

- ◎ **Near Field Communication (NFC)**
- ◎ **ISO/IEC 18092** (Diciembre 2003)
- ◎ **Extensión de diferentes estándares**
 - ISO 14443 A/B (RFID)
 - ISO 15693 (FeliCa - Sony)



Introducción

⦿ **Tecnología de comunicación inalámbrica**

- Corta distancia: $< 10\text{cm}$
- Alta frecuencia: 13'56 MHz
- Baja velocidad: $< 424\text{ kbps}$
- Comunicación bidireccional

Funcionamiento

- **Modelo *Iniciador-Objetivo* (*Initiator-Target*)**
 - El *Iniciador* crea un pequeño campo electromagnético
 - El *Objetivo* se activa y responde con su contenido
 - No necesita energía adicional



Funcionamiento

⦿ Modos de comunicación

- Pasivo

- Un *Iniciador* y un *Objetivo*, sin cambiar los roles

- Activo

- Ambos dispositivos se alternan el rol de *Iniciador*
 - Ambos son capaces de generar el campo
 - Permite velocidades superiores (hasta 6'78Mbits/s)

Funcionamiento

⦿ Modos de operación

- Reader / Writer
 - Escritura y lectura de los tags definidos por NFC
 - NDEF
- Peer to Peer (P2P)
 - Intercambio de datos entre dos dispositivos
- Card emulation
 - El dispositivo emula un tag o tarjeta (modo pasivo)

Usos

- **Sistemas de acceso**
- **Transporte**
- **Etiquetado**
- **Marketing**
 - SmartPosters
 - Cupones descuento
 - Tarjetas fidelidad
- **Intercambio de datos**
- **Medicina/Farmacia**
 - Recetas
 - Histórico



Usos

- ⦿ **Conectividad más sencilla y rápida**
 - Autenticación Bluetooth
- ⦿ **Acciones basados en lectura de tags**
 - Modo silencio, vuelo, etc
 - Activación / Desactivación Wifi / GPS / Bluetooth
 - Sincronización de correo
 - ...



Usos

◉ Micropagos

- Limite sin introducir PIN
- Pagos cotidianos: hostelería, transporte, servicios...



Inseguridad en NFC

- ⦿ **Sniffing o eavesdropping**
- ⦿ **Modificación / Corrupción de datos**
- ⦿ **Relay**
- ⦿ **Acciones automáticas en móviles**
- ⦿ **Spoofing de tags**
- ⦿ **Aplicaciones maliciosas**
- ⦿ **NFC Zapper**
- ⦿ **Privacidad**

Inseguridad en NFC

⦿ Sniffing o eavesdropping

- Monitorización de las comunicaciones
- Muy corta distancia
 - Antenas con mayor alcance
 - En 2004, Bluetooth, de 10m a 1'7km



Inseguridad en NFC

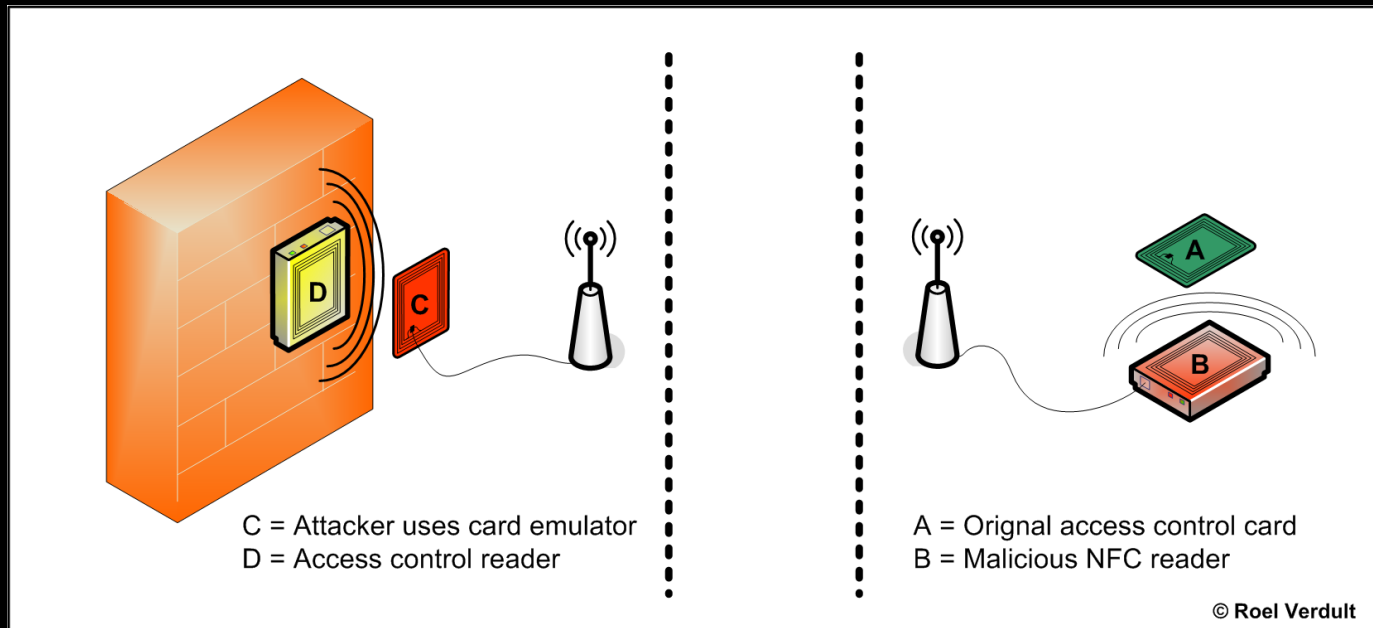
⦿ **Modificación / Corrupción de datos**

- Modificar la comunicación entre dos dispositivos
 - Corrupción de datos → Errores al tratarlos
 - Modificación de ciertos datos
- El emisor recibe los mismos datos
 - Fácil detección

Inseguridad en NFC

Relay

- Monitorización + Envío en tiempo real de los datos
 - Sistemas de acceso



Inseguridad en NFC

⦿ Acciones automáticas en móviles

- SmartPosters incluyen un campo Action

Value	Action
0	Do the action (send the SMS, launch the browser, make the telephone call)
1	Save for later (store the SMS in INBOX, put the URI in a bookmark, save the telephone number in contacts)
2	Open for editing (open an SMS in the SMS editor, open the URI in an URI editor, open the telephone number for editing).
3..FF	RFU

Inseguridad en NFC

⦿ **Acciones automáticas en móviles**

- Modificar un contacto
- Llamadas / SMS / Códigos USSD
- Conexión Bluetooth + Envío de datos (Charlie Miller)
- Visitar una URL maliciosa
 - Existen exploits para Android!!

Inseguridad en NFC

⦿ Acciones automáticas en móviles

- Modificar un contacto
- Llamadas / SMS / Códigos USSD
- Conexión Bluetooth + Envío de datos (Charlie Miller)
- Visitar una URL maliciosa
 - Existen exploits para Android!!

Android WebKit Use-After-Free Exploit

by **SecurityXploded** » Thu Mar 17, 2011 4:16 pm

New POC code for **Android Webkit** Use-After-Free Exploit has been posted on [exploit-db.com](#) versions 2.0, 2.1 & 2.1.1.

Author of this Exploit - **MJ Keith** - has presented the same in the bsides presentation.

Here is the complete Exploit POC code

Inseguridad en NFC

- ⦿ **Acciones automáticas en móviles**
 - Demo con **Galaxy Nexus S**
 - **Android Ice Cream Sandwich (4.0)**

Inseguridad en NFC

- ⦿ **Acciones automáticas en móviles**
 - Demo con **Galaxy Nexus S**
 - **Android Ice Cream Sandwich (4.0)**
 - URL
 - Códigos USSD

Inseguridad en NFC

- **Spoofing de tags**
 - Superposición de tags
 - Destrucción del tag legítimo o no



Inseguridad en NFC

⦿ **Aplicaciones maliciosas**

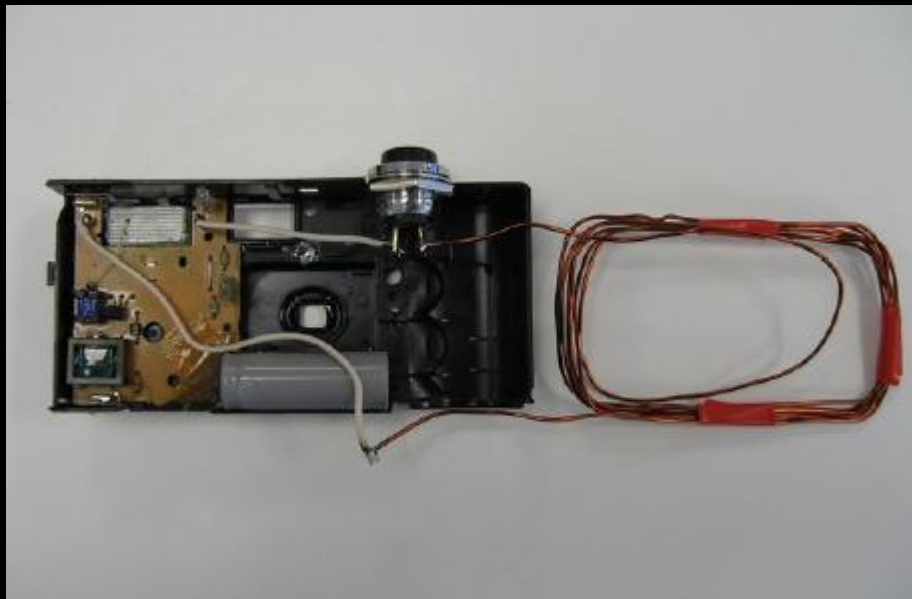
- Auge de aplicaciones NFC
 - No todas serán buenas...



Inseguridad en NFC

⦿ NFC Zapper

- Denegación de servicio
- Envío de microondas a los tags NFC
 - Destrucción definitiva del tag



Inseguridad en NFC

⦿ Privacidad

- Datos de usuario sin cifrar
- Monitorización
 - Robo de identidad
 - Vigilancia
 - Compras ilegales

Inseguridad en NFC

- ◎ Privacidad en tarjetas bancarias
 - 2010-2012: Identity Stronghold
 - 30-01-2012: Kristin Paget (Shmoocon)
 - 13-04-2012: Renaud Lifchitz (HES)
 - 13-06-2012: Thomas Skora
 - ...

Inseguridad en NFC

- ◎ Privacidad en tarjetas bancarias
 - 2010-2012: Identity Stronghold
 - 30-01-2012: Kristin Paget (Shmoocon)
 - 13-04-2012: Renaud Lifchitz (HES)
 - 13-06-2012: Thomas Skora
 - 02-11-2012: YO ;p

Tarjetas bancarias NFC

- ◉ Desde hace años en Japón / Corea
- ◉ En auge en España
 - Sin PIN $\leq$ 20€



Tarjetas bancarias NFC



Particulares

> Negocios > Empresas

ente / área privada

[¿Olvidado tu contraseña?](#)

[Entrar](#)

[Acceso con DNI electrónico](#)

no eres usuario de

Solicita tu acceso:

[Alta usuario](#)

¿cómo pagas tus operaciones?

Particulares > Gestionar el día a día > Tarjetas > Contactless

Tarjetas

Preparados, listos, ¡Contactless! : ¿Qué es?

Las tarjetas BBVA ya incorporan* la tecnología Contactless

Contactless es una **nueva funcionalidad** que incorporaremos a las Tarjetas BBVA y que te permite pagar tus **compras inferiores a 20€** de forma rápida, cómoda y segura. Con solo acercar tu tarjeta al terminal TPV y **sin necesidad de introducir el PIN ni esperar recibo**.

Ventajas:

- **Comodidad:** no necesitas llevar monedas.
- **Rapidez:** puedes pagar sin tener que esperar más tiempo del deseado.
- **Flexibilidad:** también puedes usarla para importes pequeños.
- **Seguridad:** realizas tus operaciones de forma segura.
- **Control:** controlas mejor tus gastos y tienes claro en qué utilizas tu dinero.
- **Sin costes:** con esta nueva funcionalidad, no pagas de más.

*Disponible ya para tarjetas Antes, Ahora, Después y A Tu Ritmo en algunas regiones. El ámbito geográfico se irá ampliando de forma paulatina a toda España.



- ¿Qué es?
- ¿Cómo funciona?
- ¿Dónde puede utilizarse?
- Preguntas frecuentes

[Ver más](#)



Si deseas más información acércate a tu **Oficina BBVA**, llama a la **Línea BBVA 902 22 44 66** o solicita **tu Asesor BBVA Contigo**.

Tarjetas bancarias NFC

Català | Castellano

contactless))) La nueva forma de pagar sin contacto

Me gusta 27 |  Twittear 0

Particulares > Tarjetas > Contactless

**Infórmate sobre contactless**

**Ventajas y promociones**

**Solicitar tu tarjeta**

**¿Dónde usar contactless?**

Así de fácil

1

El comercio tecleará el importe, como en cualquier otra compra



2

Acerca tu tarjeta o móvil **contactless** al TPV...



Para importes superiores a



Contactless

Compra hoy como el mundo lo hará mañana



Tarjetas bancarias NFC

Caja Rural Castilla-La Mancha lanza su tarjeta "SINcontacto"



31 de Agosto de 2012

Publicado por Ismael en tarjetas de crédito, tarjetas de débito

Caja Rural Castilla-La Mancha (no confundir con la nacionalizada y posteriormente vendida CCM) acaba de lanzar su primera **tarjeta de crédito "sin contacto"** también conocidas como **"tarjetas contactless"**; un servicio que permite realizar compras con sólo acercar la tarjeta o el teléfono móvil a Terminales Punto de Venta (TPV) preparados para tal fin, tal y como hacemos cuando pagamos con el bonobús.

Con las **tarjetas "contactless"** se quiere conseguir inmediatez en el pago así como eliminar la manipulación de efectivo para los comerciantes. La mayoría de **tarjetas contactless** (y la de Caja Rural Castilla-La Mancha no iba a ser menos) **incluyen también el Chip EMV y la banda magnética** con lo que todavía podremos seguir pagando mediante los dispositivos de pago más tradicionales así como sacar dinero en cajeros, que todavía no disponen de esta tecnología.

Tarjetas bancarias NFC

 902 323 000

Particulares Empresas BSMarkets BS Online

Banca a Distancia

Hipotecas

Préstamos y créditos

Depósitos

Fondos de inversión

Bolsa y mercados

Ahorro-inversión

Planes de pensiones

Cuentas

Tarjetas

- ▶ **Tarjetas Contactless**
- ▶ Tarjetas con Chip Electrónico
- ▶ Personalización tarjetas
- ▶ Tarjeta Prepago
- ▶ BS Card MasterCard
- ▶ Tarjeta Visa Classic
- ▶ Tarjeta Visa Oro
- ▶ Tarjeta Visa SIN

Está en: [Particulares](#) > [Tarjetas](#) > [Tarjetas Contactless](#)

Pagar las compras en menos de un segundo

Tarjetas Contactless

En Banco Sabadell simplificamos los pequeños pagos diarios de nuestros clientes en los comercios de proximidad, con la adopción de la tecnología Contactless en nuestras tarjetas.

Así, con las tarjetas sin contacto estas transacciones son más cómodas, ágiles y rápidas para usted.



Ventajas de las tarjetas Contactless

[ocultar](#)

Tarjetas bancarias NFC



Tarjetas bancarias NFC

jrodriguez | Jueves, 9 de agosto de 2012

Banco Santander impulsa el pago sin contacto

Banco Santander, presidido por **Emilio Botín**, colabora con el **Gobierno de Cantabria** y el **Ayuntamiento de Santander**, en la firma de un convenio con el que pondrán en marcha la implantación en toda la región de un modelo innovador de pago sin contacto en los ámbitos del comercio, el turismo y el transporte.

Según han avanzado fuentes del Ejecutivo cántabro, el acuerdo será suscrito por el presidente regional, Ignacio Diego; el alcalde de Santander, Íñigo de la Serna; y el director territorial del **Banco Santander** en Cantabria, Carlos Hazas, en un acto que se celebrará en la sede del Gobierno de Cantabria, en Santander.

Previamente a la firma del convenio, el presidente mantendrá un breve encuentro con De la Serna y Hazas en su despacho, en el que también estará presente el consejero de Innovación, Industria, Turismo y Comercio, Eduardo Arasti.

Tarjetas bancarias NFC

10-01-2012

BBVA y Bankia revolucionan los medios de pago con el lanzamiento de 'Madrid Contactless'



Notas relacionadas

- BBVA y Radioteléfono Taxi firman un acuerdo que lleva los pagos 'contactless' a los taxis de Madrid
- Huawei y BBVA anuncian un acuerdo de colaboración para mejorar la financiación y tecnología de sus clientes
- BBVA inaugura uno de los centros de proceso de datos más avanzados del mundo

- Visa Europe ha colaborado con ambas entidades en el desarrollo de este proyecto y considera este despliegue como un paso fundamental para la adopción masiva de los pagos con móvil en España
- El cliente podrá realizar pagos de hasta 20 euros sólo con acercar la tarjeta a un lector, sin firmar recibo ni teclear PIN
- En una primera fase se beneficiarán un millón de clientes dentro del anillo de la M-30, fundamentalmente de zonas comerciales. El objetivo es llegar a los dos millones de clientes en 2012
- BBVA y Bankia instalarán 7.000 nuevos terminales en comercios donde se realicen pagos de bajo importe

Tarjetas bancarias NFC

BANCOS

La Caixa y Caprabo incorporarán la tecnología NFC de pago

🕒 28 MAYO, 2012 13:23 👤 ADMIN 💬 DEJA TU COMENTARIO



Los supermercados **Caprabo**, en colaboración con **La Caixa**, permitirán el pago sin contacto mediante tarjetas y dispositivos móviles con soporte del estándar NFC. Esta apuesta supondrá el cambio de los 1.800 terminales de la compañía de sus 343 tiendas en los próximos meses.

Tarjetas bancarias NFC

Taxis de la ciudad de Pamplona integran terminales de punto de venta que admiten pago con tarjeta sin contacto

POR MIGUEL TOMÁS ROMERO – 10 ABRIL, 2012

PUBLICADO EN: AVANCES TÉCNICOS, DESTACADO

 Imprimir

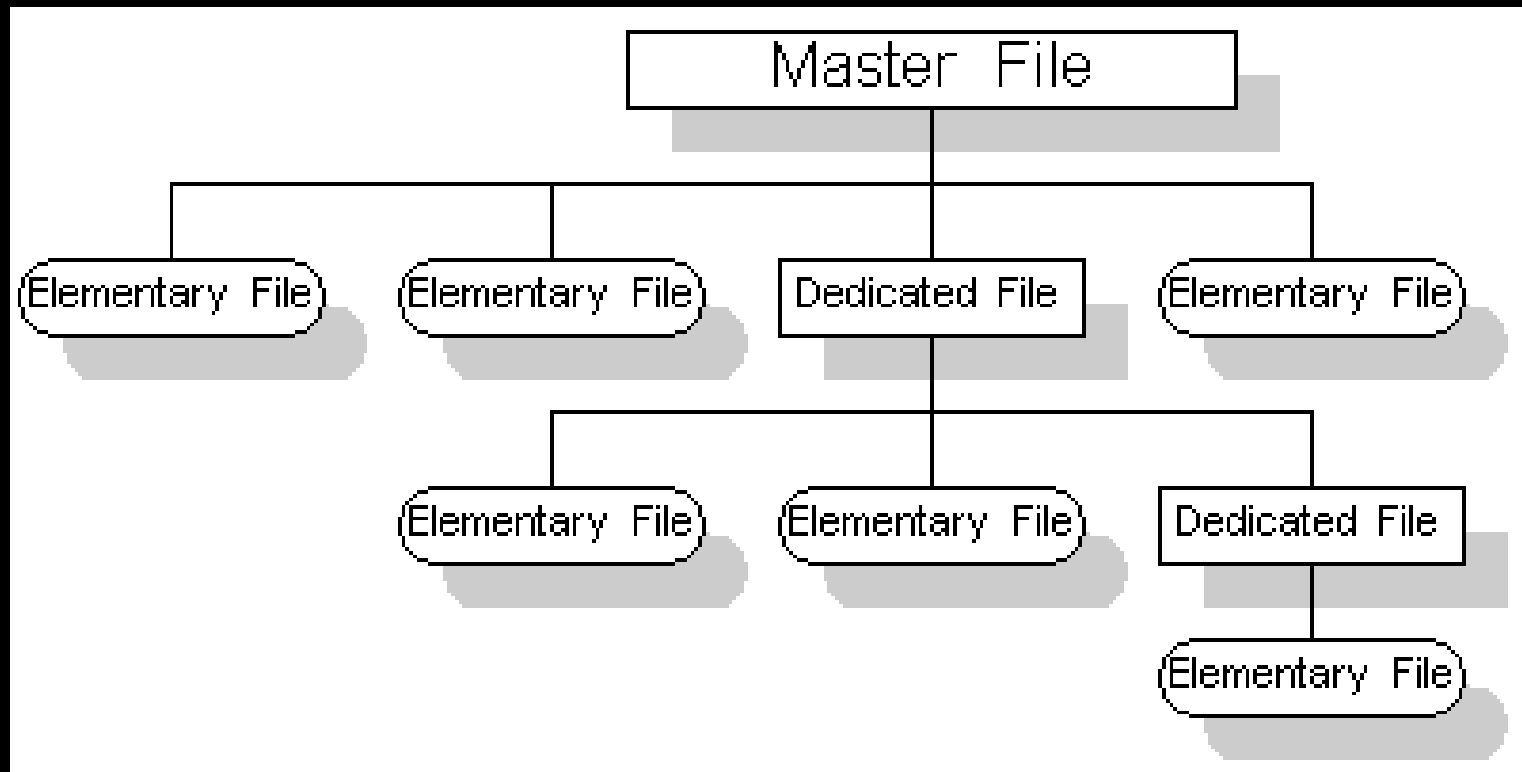


Pamplona, 26 mar (EFE).- Los taxis de la Comarca de Pamplona integrados en la empresa Teletaxi San Fermín integrarán paulatinamente y desde ahora los nuevos terminales de punto de venta (TPV) que admitirán el pago con tarjeta sin contacto, una forma más cómoda, segura y rápida de abonar los servicios.

Según ha informado la empresa en una nota, Teletaxi San Fermín será la primera organización del taxi que adopte este método de pago en España, dentro del programa de pago en comercios con tarjeta SINcontacto en Navarra.

Tarjetas bancarias NFC

- Estructura EMV



Tarjetas bancarias NFC

- ⦿ ¿Qué datos hay?
 - Información de la banda magnética
 - Track1
 - Track2

Tarjetas bancarias NFC

- ⦿ ¿Qué datos hay?
 - Nombre del titular
 - Número de la tarjeta
 - Fecha de caducidad
 - País
 - Log de transacciones

Tarjetas bancarias NFC

⦿ ¿Qué datos hay?

- Modos de operación
- Método de verificación del titular
- *Terminal Verification Results* (TRV)
- Clave pública de la tarjeta
- Clave pública de la entidad

Tarjetas bancarias NFC

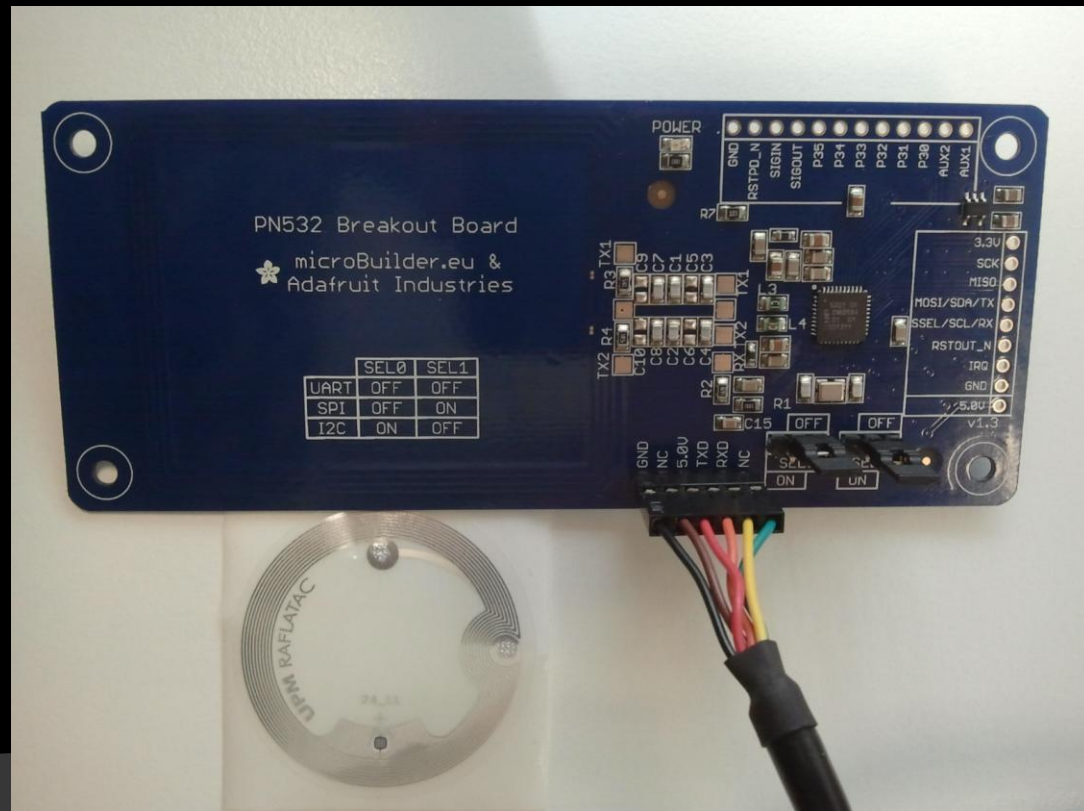
- ⦿ ¿Cómo nos comunicamos con la tarjeta?
 - Interfaz NFC + Comandos EMV (chip)
 - BER-TLV (Tag-Length-Value)
 - 5F 20 – Titular
 - 5F 28 – País de la entidad
 - 5F24 – Fecha de caducidad
 - 5A - Número de tarjeta (PAN)
 - ...

Tarjetas bancarias NFC

- ⦿ ¿Cómo nos comunicamos con la tarjeta?
 - Interfaz NFC + Comandos EMV (chip)
 - BER-TLV (Tag-Length-Value)
 - **5f 20** // Cardholder Name Tag
 - **1a** // Length
 - **45 53 50 41 52 5a 41 ...** // Value: “ESPARZA...”

Tarjetas bancarias NFC

- ¿Cómo nos comunicamos con la tarjeta?
- Ejemplo: Lector PN532 + libnfc



Tarjetas bancarias NFC

- ⦿ ¿Cómo nos comunicamos con la tarjeta?
 - Ejemplo: Lector PN532 + libnfc
 - *InListPassiveTarget*
 - **0x4A** MaxTg BrTg [InitiatorData]

Tarjetas bancarias NFC

- ⦿ ¿Cómo nos comunicamos con la tarjeta?
 - Ejemplo: Lector PN532 + libnfc
 - *InListPassiveTarget*
 - 0x4A **MaxTg** BrTg [InitiatorData]
 - **MaxTg** is the maximum number of targets to be initialized by the PN532.
 - The PN532 is capable of handling 2 targets maximum at once, so this field should not exceed 0x02. For Jewel card, only one target can be initialized.

Tarjetas bancarias NFC

- ⦿ ¿Cómo nos comunicamos con la tarjeta?
 - Ejemplo: Lector PN532 + libnfc
 - *InListPassiveTarget*
 - 0x4A MaxTg **BrTg** [InitiatorData]
 - **BrTg** is the baud rate and the modulation type to be used during the initialization
 - 0x00 : 106 kbps type A (ISO/IEC14443 Type A)
 - 0x01 : 212 kbps (FeliCa polling)
 - 0x02 : 424 kbps (FeliCa polling)
 - 0x03 : 106 kbps type B (ISO/IEC14443-3B)
 - 0x04 : 106 kbps Innovision Jewel tag

Tarjetas bancarias NFC

- ⦿ ¿Cómo nos comunicamos con la tarjeta?
 - Ejemplo: Lector PN532 + libnfc
 - *InListPassiveTarget*
 - 0x4A MaxTg **BrTg** [InitiatorData]
 - **BrTg** is the baud rate and the modulation type to be used during the initialization
 - **0x00 : 106 kbps type A (ISO/IEC14443 Type A)**
 - 0x01 : 212 kbps (FeliCa polling)
 - 0x02 : 424 kbps (FeliCa polling)
 - **0x03 : 106 kbps type B (ISO/IEC14443-3B)**
 - 0x04 : 106 kbps Innovision Jewel tag

Tarjetas bancarias NFC

- ⦿ ¿Cómo nos comunicamos con la tarjeta?
 - Ejemplo: Lector PN532 + libnfc
 - *InListPassiveTarget*
 - 0x4A MaxTg BrTg [**InitiatorData**]
 - **InitiatorData []** is an array of data to be used during the initialization of the target(s). Depending on the Baud Rate specified, the content of this field is different

Tarjetas bancarias NFC

- ⦿ ¿Cómo nos comunicamos con la tarjeta?
 - Ejemplo: Lector PN532 + libnfc
 - *InListPassiveTarget*
 - **0x4A** MaxTg BrTg [InitiatorData]
 - **0x4A 0x01 0x00** (ISO/IEC14443 Type A)
 - **0x4A 0x01 0x03 0x00** (ISO/IEC14443-B)

Tarjetas bancarias NFC

- ⦿ ¿Cómo nos comunicamos con la tarjeta?
 - Ejemplo: Lector PN532 + libnfc
 - *InDataExchange*
 - **0x40** Tg [DataOut]

Tarjetas bancarias NFC

- ⦿ ¿Cómo nos comunicamos con la tarjeta?
 - Ejemplo: Lector PN532 + libnfc
 - *InDataExchange*
 - 0x40 **Tg** [DataOut]
 - *Tg* is a byte containing the logical number of the relevant target.
 - This byte contains also a More Information (MI) bit (bit 6) indicating, when set to 1, that the host controller wants to send more data that all the data contained in the DataOut [] array.

Tarjetas bancarias NFC

- ⦿ ¿Cómo nos comunicamos con la tarjeta?
 - Ejemplo: Lector PN532 + libnfc
 - *InDataExchange*
 - 0x40 Tg [**DataOut**]
 - **DataOut** is an array of raw data (from 0 up to 262 bytes) to be sent to the target by the PN532

Tarjetas bancarias NFC

- ⦿ ¿Cómo nos comunicamos con la tarjeta?
 - Ejemplo: Lector PN532 + libnfc
 - *InDataExchange*
 - **0x40** Tg [DataOut]
 - **0x40 0x01** [Comandos EMV]

Tarjetas bancarias NFC

- ⦿ ¿Cómo nos comunicamos con la tarjeta?
 - Comandos EMV (ISO 7816-4)
 - Formato del comando

CLA	INS	P1	P2	Lc	Data	Le
← Mandatory Header ² →				← Conditional Body →		

- Formato de la respuesta

Data	SW1	SW2
← Body →	← Trailer →	

Tarjetas bancarias NFC

- ⦿ ¿Cómo nos comunicamos con la tarjeta?
 - Comandos EMV (ISO 7816-4)
 - **Select**
 - Abre un canal lógico con la tarjeta en el MF/DF seleccionado
 - 0x00 0xA4 P1 P2 Lc Data Le

Tarjetas bancarias NFC

- ⦿ ¿Cómo nos comunicamos con la tarjeta?
 - Comandos EMV (ISO 7816-4)
 - **Select**
 - Abre un canal lógico con la tarjeta en el MF/DF seleccionado
 - 0x00 0xA4 **P1** P2 Lc Data Le
 - **P1**: Selección por path, nombre de DF o identificador

Tarjetas bancarias NFC

- ⦿ ¿Cómo nos comunicamos con la tarjeta?
 - Comandos EMV (ISO 7816-4)
 - **Select**
 - Abre un canal lógico con la tarjeta en el MF/DF seleccionado
 - 0x00 0xA4 P1 **P2** Lc Data Le
 - **P2**: Elige el canal y el tipo de datos de respuesta

Tarjetas bancarias NFC

⦿ ¿Cómo nos comunicamos con la tarjeta?

- Comandos EMV (ISO 7816-4)

- **Select**

- Abre un canal lógico con la tarjeta en el MF/DF seleccionado
 - 0x00 0xA4 P1 P2 Lc Data Le
 - **0x00 0xA4 0x04 0x00 0x07 xx xx xx xx xx xx xx**
 - Selección por nombre de DF (AID)
 - Coge el primer resultado de plantilla FCI

Tarjetas bancarias NFC

⦿ ¿Cómo nos comunicamos con la tarjeta?

- Comandos EMV (ISO 7816-4)

- **Select**

- Abre un canal lógico con la tarjeta en el MF/DF seleccionado
 - 0x00 0xA4 P1 P2 Lc Data Le
 - **0x00 0xA4 0x04 0x00 0x07 xx xx xx xx xx xx xx**
 - Selección por nombre de DF (AID)
 - AID depende del tipo de tarjeta
 - VISA, Mastercard, Visa Electron, Carte Bleu...
 - Coge el primer resultado de plantilla FCI

Tarjetas bancarias NFC

⦿ ¿Cómo nos comunicamos con la tarjeta?

- Comandos EMV (ISO 7816-4)

- **Select**

- Abre un canal lógico con la tarjeta en el MF/DF seleccionado
 - 0x00 0xA4 P1 P2 Lc Data Le
 - 0x00 0xA4 0x04 0x00 0x07 **xx xx xx xx xx xx xx**
 - **0xA0 0x00 0x00 0x00 0x03 0x10 0x10 (VISA)**
 - **0xA0 0x00 0x00 0x00 0x03 0x20 0x10 (VISA Electron)**
 - **0xA0 0x00 0x00 0x00 0x04 0x10 0x10 (Mastercard)**
 - ...

Tarjetas bancarias NFC

- ⦿ ¿Cómo nos comunicamos con la tarjeta?
 - Comandos EMV (ISO 7816-4)
 - **Read record**
 - Lee el registro especificado
 - 0x00 0xB2 P1 P2 Lc Data Le

Tarjetas bancarias NFC

- ⦿ ¿Cómo nos comunicamos con la tarjeta?
 - Comandos EMV (ISO 7816-4)
 - **Read record**
 - Lee el registro especificado
 - 0x00 0xB2 **P1** P2 Lc Data Le
 - **P1**: Número de registro o identificador

Tarjetas bancarias NFC

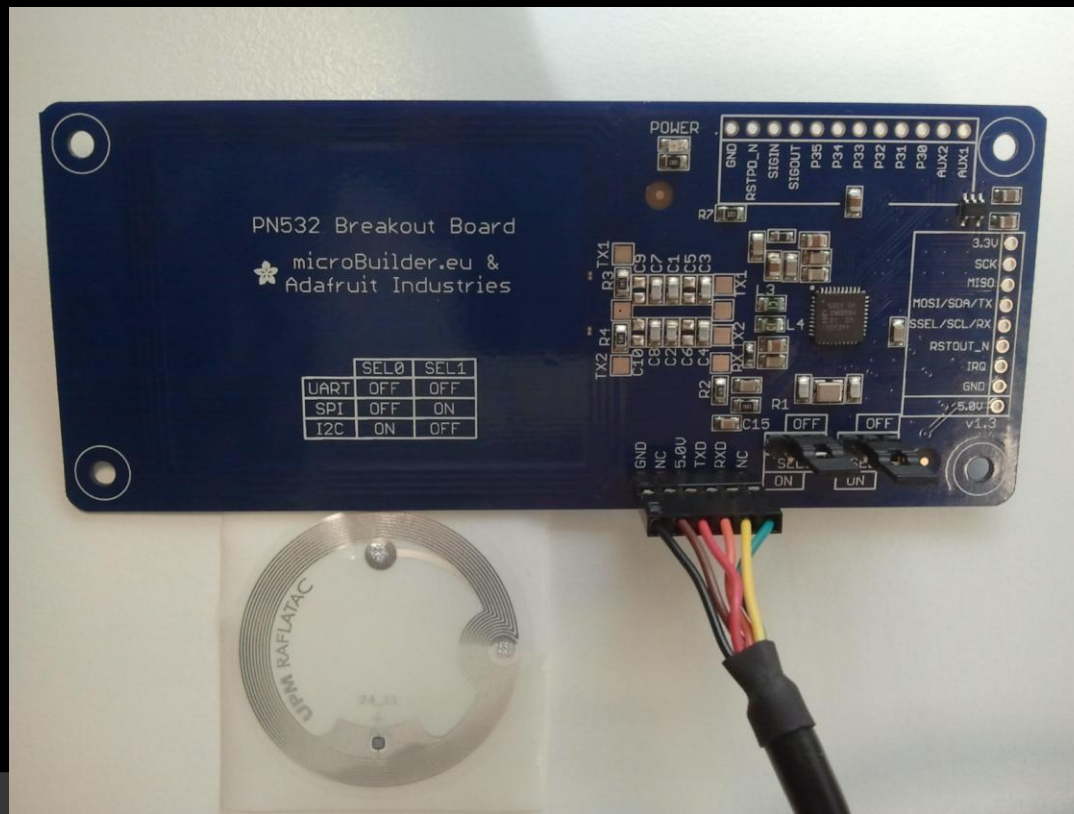
- ⦿ ¿Cómo nos comunicamos con la tarjeta?
 - Comandos EMV (ISO 7816-4)
 - **Read record**
 - Lee el registro especificado
 - 0x00 0xB2 P1 **P2** Lc Data Le
 - **P2**: Elige cuántos registros y qué registros o identificadores tiene que leer

Tarjetas bancarias NFC

- ⦿ ¿Cómo nos comunicamos con la tarjeta?
 - Comandos EMV (ISO 7816-4)
 - **Read record**
 - Lee el registro especificado
 - 0x00 0xB2 P1 P2 Lc Data Le
 - **0x00 0xB2 0x01 0x0C**
 - Lee el registro número 1 del EF = 1

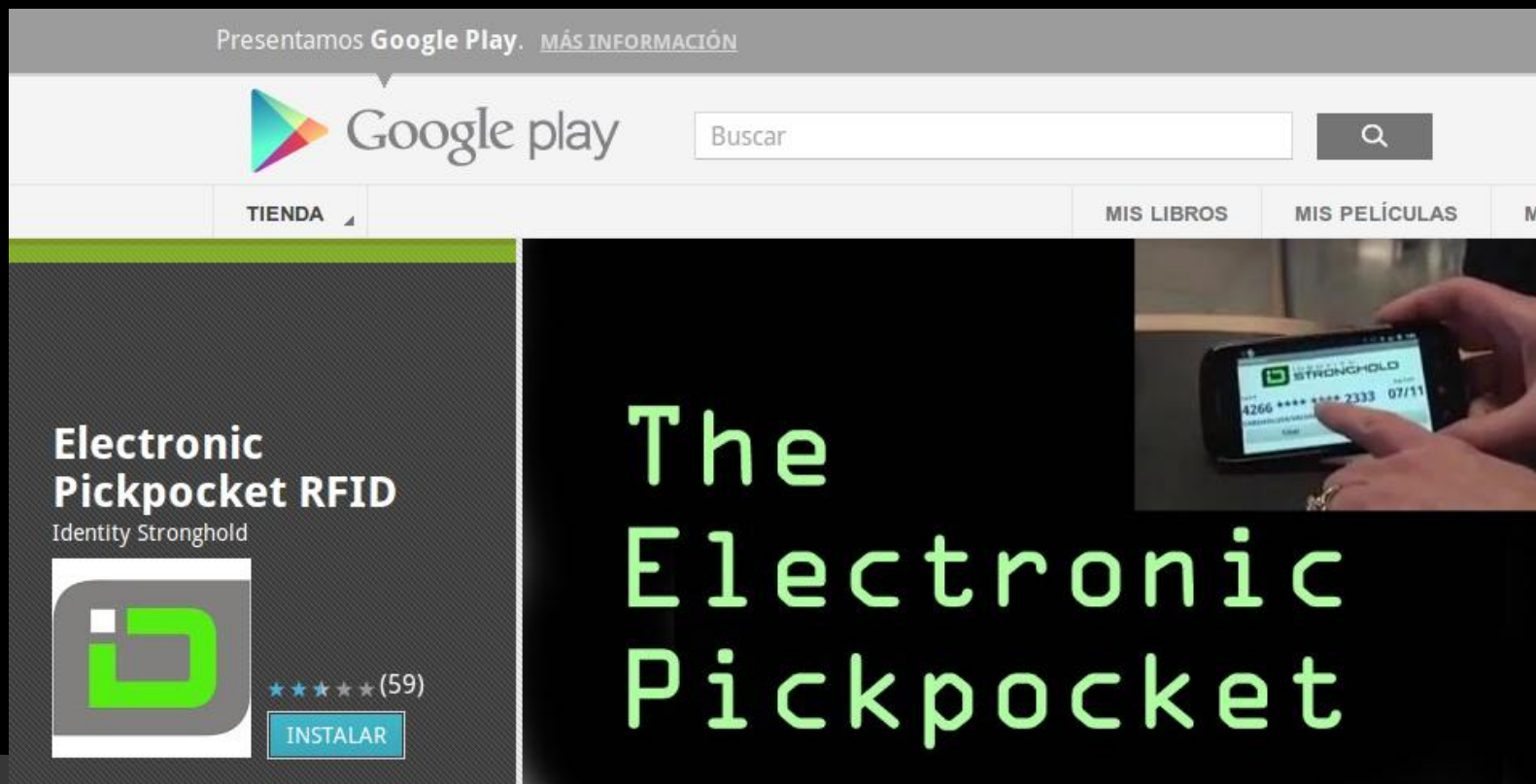
Tarjetas bancarias NFC

- ¿Cómo nos comunicamos con la tarjeta?
- Demo



Tarjetas bancarias NFC

- Publicaciones sobre el tema
 - Mayo 2011



Tarjetas bancarias NFC

- Publicaciones sobre el tema
 - Enero 2012



Tarjetas bancarias NFC

- Publicaciones sobre el tema
 - Abril 2012



*Hacking the NFC credit cards
for fun and debit ;)*

Renaud Lifchitz – BT
renaud.lifchitz@bt.com
Hackito Ergo Sum 2012 – April 12,13,14 – Paris, France

Tarjetas bancarias NFC

- Publicaciones sobre el tema
 - Junio 2012

Thomas Skora 13/06/2012 - Público (bloqueada) 

Ich hab eben den Source-Code für den EC/GeldKarten-Leser bei Github veröffentlicht: <https://github.com/thomasskora/android-nfc-paycardreader>

Bitte bedenkt: der Code ist auf die schnelle zusammengehackt worden und hat noch sehr viel Verbesserungspotential. Vieles ist auch aufgrund fehlender Karten noch ungetestet.

 **android-nfc-paycardreader »**
android-nfc-paycardreader - NFC card reader Android app. Currently reads the german GeldKarte and some credit cards.

 +1  +2

Tarjetas bancarias NFC

- Incumplimiento de PCI DSS

“Requisito 4: Cifrar los datos de los propietarios de tarjetas e información confidencial transmitida a través de redes públicas abiertas.”

Tengo tus datos, ¿ahora qué?

- ⦿ ¿Qué se puede hacer con estos datos?
 - Nombre del titular
 - Número de la tarjeta (PAN)
 - Fecha de caducidad

Tengo tus datos, ¿ahora qué?

- ⦿ ¿Qué se puede hacer con estos datos?
 - Compras telefónicas

Tengo tus datos, ¿ahora qué?

- ⦿ ¿Qué se puede hacer con estos datos?
 - Compras online

Tengo tus datos, ¿ahora qué?

- ⦿ ¿Qué se puede hacer con estos datos?
 - Compras online
 - ¿¿Sin CVV??

Tengo tus datos, ¿ahora qué?



COMPRUEBA TU COMPRA

TUS DATOS

DATOS DE PAGO

CONFIRMACIÓN

[Comprobar pedido](#)

☒ Tarjeta de crédito.

☐ Transferencia.

☐ Contrareembolso.

Tipo de tarjeta

Visa

Fecha de caducidad

Mes

Año

Número de tarjeta:

Nombre del titular:

☒ He leído y acepto las [condiciones de compra](#).

Una vez pulsado el botón "Finalizar Compra" esperar a que aparezca en pantalla la confirmación de compra.

[Finalizar compra »](#)

AYUDA ONLINE

Contacto
Registro

¿Dónde enviamos?
Transporte

Formas de pago
Cambios y devoluciones

Confidencialidad
Condiciones de compra

Tengo tus datos, ¿ahora qué?



COMPRUEBA TU COMPRA

TUS DATOS

DATOS DE PAGO

CONFIRMACIÓN

[Comprobar pedido](#)

☒ Tarjeta de crédito.

☐ Transferencia.

☐ Contrareembolso.

Tipo de tarjeta

Visa

Fecha de caducidad

Mes

Año

Número de tarjeta:

Nombre del titular:

☒ He leído y acepto las [condiciones de compra](#).

Una vez pulsado el botón "Finalizar Compra" esperar a que aparezca en pantalla la confirmación de compra.

[Finalizar compra »](#)

AYUDA ONLINE

Contacto
Registro

¿Dónde enviamos?
Transporte

Formas de pago
Cambios y devoluciones

Confidencialidad
Condiciones de compra

Tengo tus datos, ¿ahora qué?



COMPRUEBA TU COMPRA

TUS DATOS

DATOS DE PAGO

CONFIRMACIÓN

[Comprobar pedido](#)

☒ Tarjeta de crédito.

☐ Transferencia.

☐ Contrareembolso.

Tipo de tarjeta

Visa

Fecha de caducidad

Mes

Año

Número de tarjeta:

Nombre del titular:

☒ He leído y acepto las [condiciones de compra](#).

Una vez pulsado el botón "Finalizar Compra" esperar a que aparezca en pantalla la confirmación de compra.

[Finalizar compra »](#)

AYUDA ONLINE

Contacto
Registro

¿Dónde enviamos?
Transporte

Formas de pago
Cambios y devoluciones

Confidencialidad
Condiciones de compra

Tengo tus datos, ¿ahora qué?



COMPRUEBA TU COMPRA

TUS DATOS

DATOS DE PAGO

CONFIRMACIÓN

[Comprobar pedido](#)

☒ Tarjeta de crédito.

☐ Transferencia.

☐ Contrareembolso.

Tipo de tarjeta

Visa

Fecha de caducidad

Mes ▼

Año ▼

Número de tarjeta:

Nombre del titular:

☒ He leído y acepto las [condiciones de compra](#).

Una vez pulsado el botón "Finalizar Compra" esperar a que aparezca en pantalla la confirmación de compra.

[Finalizar compra »](#)

AYUDA ONLINE

Contacto
Registro

¿Dónde enviamos?
Transporte

Formas de pago
Cambios y devoluciones

Confidencialidad
Condiciones de compra

Tengo tus datos, ¿ahora qué?



The screenshot shows a web browser window with the address bar displaying www.forumsport.com/ayuda/servidor-seguro.html. The page has a red header with a search bar and a 'Buscar' button. Below the header is a navigation bar with links: 'Nuestras marcas', 'Nuestros deportes', 'Nuestras promociones', and 'Nuestras tiendas'. The main content area has a breadcrumb trail: 'Te encuentras en: Inicio >> Ayuda a la compra >> Servidor Seguro'. The title of the page is 'Servidor Seguro'. The text explains the security measures taken by Forum Sport, mentioning the use of a secure server and a certificate from Thawte. It also provides contact information for customer support.

www.forumsport.com/ayuda/servidor-seguro.html

Buscar [Búsqueda Avanzada](#)

Nuestras marcas Nuestros deportes Nuestras promociones Nuestras tiendas

Te encuentras en: Inicio >> Ayuda a la compra >> Servidor Seguro

Servidor Seguro

Comprendemos que la seguridad es una preocupación cuando se compra a través de internet. Por eso, hemos tomado todas las medidas posibles para asegurar el manejo de su información, tanto financiera como personal.

En el momento en que accedas a cualquiera de las páginas en las que envías información personal o financiera, accederás a nuestro servidor seguro. En la casilla superior donde aparece la dirección de la página, aparecerá una letra "s" después de http, es decir, aparecerá <https://www.forumsport.com>, en vez de <http://www.forumsport.com>.

El software del servidor seguro de **Forum Sport tienda on-line** junto al certificado obtenido de la entidad certificadora Thawte (www.thawte.com) encripta toda la información personal, incluyendo el número de tu tarjeta de crédito, de tal forma que no pueda ser leída por terceras personas mientras viaja desde tu ordenador al nuestro.

Tu navegador te indicará que la zona es segura, mostrando un icono en la barra de estado (candado, llave, etc.), y una ventana de aviso, en caso de que tengas esta opción configurada en el navegador. Pinchando sobre el candado, llave, etc. se abrirá una ventana que le facilitará información sobre el certificado y vigencia de transacciones seguras de **Forum Sport tienda on-line**.

Si aún así no estas totalmente seguro, puedes realiar tu pedido en el 902 11 87 05 de lunes a viernes de 9:00 a 19:00 horas.

Toda la información sobre nuestros clientes es confidencial y no es facilitada a ninguna empresa u organización, excepto los datos de entrega que son facilitados al operador logístico, el cual tiene prohibido usarlos para otro fin diferente a la entrega del pedido.

Tengo tus datos, ¿ahora qué?



The screenshot shows a web browser window with the address bar displaying www.forumsport.com/ayuda/servidor-seguro.html. The page has a red header with a search bar and a 'Buscar' button. Below the header is a navigation bar with four tabs: 'Nuestras marcas', 'Nuestros deportes', 'Nuestras promociones', and 'Nuestras tiendas'. The main content area has a breadcrumb trail: 'Te encuentras en: Inicio >> Ayuda a la compra >> Servidor Seguro'. The title 'Servidor Seguro' is highlighted with a red box. The text explains the website's security measures, mentioning the use of a secure server and a Thawte certificate to encrypt personal and financial information. It also provides contact information for customer support.

www.forumsport.com/ayuda/servidor-seguro.html

Buscar [Búsqueda Avanzada](#)

Nuestras marcas Nuestros deportes Nuestras promociones Nuestras tiendas

Te encuentras en: Inicio >> Ayuda a la compra >> Servidor Seguro

Servidor Seguro

Comprendemos que la seguridad es una preocupación cuando se compra a través de internet. Por eso, hemos tomado todas las medidas posibles para asegurar el manejo de su información, tanto financiera como personal.

En el momento en que accedas a cualquiera de las páginas en las que envías información personal o financiera, accederás a nuestro servidor seguro. En la casilla superior donde aparece la dirección de la página, aparecerá una letra "s" después de http, es decir, aparecerá <https://www.forumsport.com>, en vez de <http://www.forumsport.com>.

El software del servidor seguro de **Forum Sport tienda on-line** junto al certificado obtenido de la entidad certificadora Thawte (www.thawte.com) encripta toda la información personal, incluyendo el número de tu tarjeta de crédito, de tal forma que no pueda ser leída por terceras personas mientras viaja desde tu ordenador al nuestro.

Tu navegador te indicará que la zona es segura, mostrando un icono en la barra de estado (candado, llave, etc.), y una ventana de aviso, en caso de que tengas esta opción configurada en el navegador. Pinchando sobre el candado, llave, etc. se abrirá una ventana que le facilitará información sobre el certificado y vigencia de transacciones seguras de **Forum Sport tienda on-line**.

Si aún así no estas totalmente seguro, puedes realiar tu pedido en el 902 11 87 05 de lunes a viernes de 9:00 a 19:00 horas.

Toda la información sobre nuestros clientes es confidencial y no es facilitada a ninguna empresa u organización, excepto los datos de entrega que son facilitados al operador logístico, el cual tiene prohibido usarlos para otro fin diferente a la entrega del pedido.

Tengo tus datos, ¿ahora qué?



www.forumsport.com/ayuda/servidor-seguro.html

Buscar [Búsqueda Avanzada](#)

Nuestras marcas Nuestros deportes Nuestras promociones Nuestras tiendas

Te encuentras en: Inicio >> Ayuda a la compra >> Servidor Seguro

Servidor Seguro

Comprendemos que la seguridad es una preocupación cuando se compra a través de internet. Por eso, hemos tomado todas las medidas posibles para asegurar el manejo de su información, tanto financiera como personal.

<https://www.forumsport.com/>, en vez de <http://www.forumsport.com/>.

El software del servidor seguro de **Forum Sport tienda on-line** junto al certificado obtenido de la entidad certificadora Thawte (www.thawte.com) encripta toda la información personal, incluyendo el número de tu tarjeta de crédito, de tal forma que no pueda ser leída por terceras personas mientras viaja desde tu ordenador al nuestro.

Tu navegador te indicará que la zona es segura, mostrando un icono en la barra de estado (candado, llave, etc.), y una ventana de aviso, en caso de que tengas esta opción configurada en el navegador. Pinchando sobre el candado, llave, etc. se abrirá una ventana que le facilitará información sobre el certificado y vigencia de transacciones seguras de **Forum Sport tienda on-line**.

Si aún así no estas totalmente seguro, puedes realiar tu pedido en el 902 11 87 05 de lunes a viernes de 9:00 a 19:00 horas.

Toda la información sobre nuestros clientes es confidencial y no es facilitada a ninguna empresa u organización, excepto los datos de entrega que son facilitados al operador logístico, el cual tiene prohibido usarlos para otro fin diferente a la entrega del pedido.

Tengo tus datos, ¿ahora qué?



www.forumsport.com/ayuda/servidor-seguro.html

Buscar [Búsqueda Avanzada](#)

Nuestras marcas Nuestros deportes Nuestras promociones Nuestras tiendas

Te encuentras en: Inicio >> Ayuda a la compra >> Servidor Seguro

Servidor Seguro

Comprendemos que la seguridad es una preocupación cuando se compra a través de internet. Por eso, hemos tomado **todas las medidas posibles** para asegurar el manejo de su información, tanto financiera como personal.

<https://www.forumsport.com/>, en vez de <http://www.forumsport.com/>.

El software del servidor seguro de **Forum Sport tienda on-line** junto al certificado obtenido de la entidad certificadora Thawte (www.thawte.com) encripta toda la información personal, incluyendo el número de tu tarjeta de crédito, de tal forma que no pueda ser leída por terceras personas mientras viaja desde tu ordenador al nuestro.

Tu navegador te indicará que la zona es segura, mostrando un icono en la barra de estado (candado, llave, etc.), y una ventana de aviso, en caso de que tengas esta opción configurada en el navegador. Pinchando sobre el candado, llave, etc. se abrirá una ventana que le facilitará información sobre el certificado y vigencia de transacciones seguras de **Forum Sport tienda on-line**.

Si aún así no estas totalmente seguro, puedes realiar tu pedido en el 902 11 87 05 de lunes a viernes de 9:00 a 19:00 horas.

Toda la información sobre nuestros clientes es confidencial y no es facilitada a ninguna empresa u organización, excepto los datos de entrega que son facilitados al operador logístico, el cual tiene prohibido usarlos para otro fin diferente a la entrega del pedido.

Tengo tus datos, ¿ahora qué?



www.forumsport.com/ayuda/servidor-seguro.html

Buscar [Búsqueda Avanzada](#)

Nuestras marcas Nuestros deportes Nuestras promociones Nuestras tiendas

Te encuentras en: Inicio >> Ayuda a la compra >> Servidor Seguro

Servidor Seguro

Comprendemos que la seguridad es una preocupación cuando se compra a través de internet. Por eso, hemos tomado **¿? todas las medidas posibles para asegurar el manejo de su información, tanto financiera como personal.**

<https://www.forumsport.com/>, en vez de <http://www.forumsport.com/>.

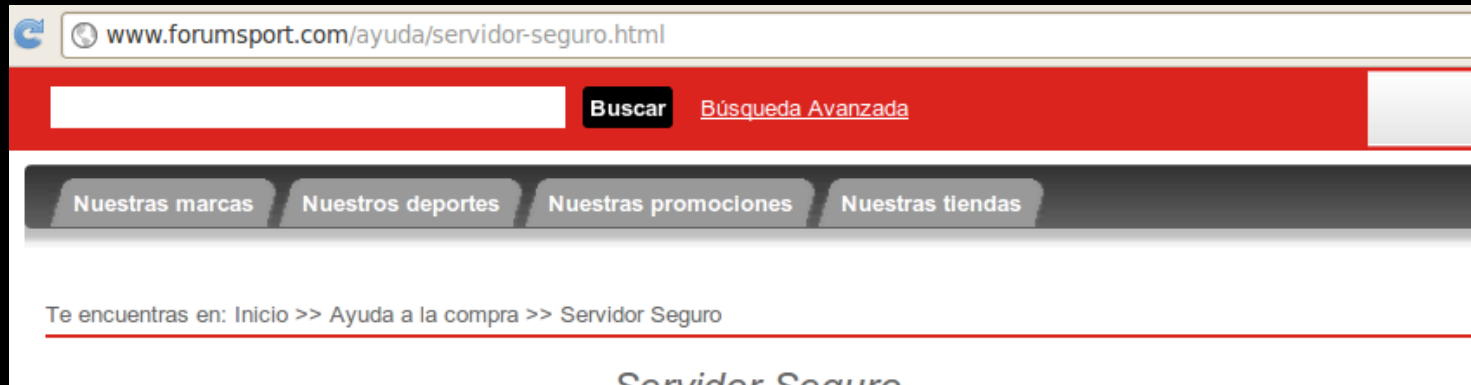
El software del servidor seguro de **Forum Sport tienda on-line** junto al certificado obtenido de la entidad certificadora Thawte (www.thawte.com) encripta toda la información personal, incluyendo el número de tu tarjeta de crédito, de tal forma que no pueda ser leída por terceras personas mientras viaja desde tu ordenador al nuestro.

Tu navegador te indicará que la zona es segura, mostrando un icono en la barra de estado (candado, llave, etc.), y una ventana de aviso, en caso de que tengas esta opción configurada en el navegador. Pinchando sobre el candado, llave, etc. se abrirá una ventana que le facilitará información sobre el certificado y vigencia de transacciones seguras de **Forum Sport tienda on-line**.

Si aún así no estas totalmente seguro, puedes realiar tu pedido en el 902 11 87 05 de lunes a viernes de 9:00 a 19:00 horas.

Toda la información sobre nuestros clientes es confidencial y no es facilitada a ninguna empresa u organización, excepto los datos de entrega que son facilitados al operador logístico, el cual tiene prohibido usarlos para otro fin diferente a la entrega del pedido.

Tengo tus datos, ¿ahora qué?



El software del servidor seguro de **Forum Sport tienda on-line** junto al certificado obtenido de la entidad certificadora Thawte (www.thawte.com) encripta toda la información personal, incluyendo el número de tu tarjeta de crédito,

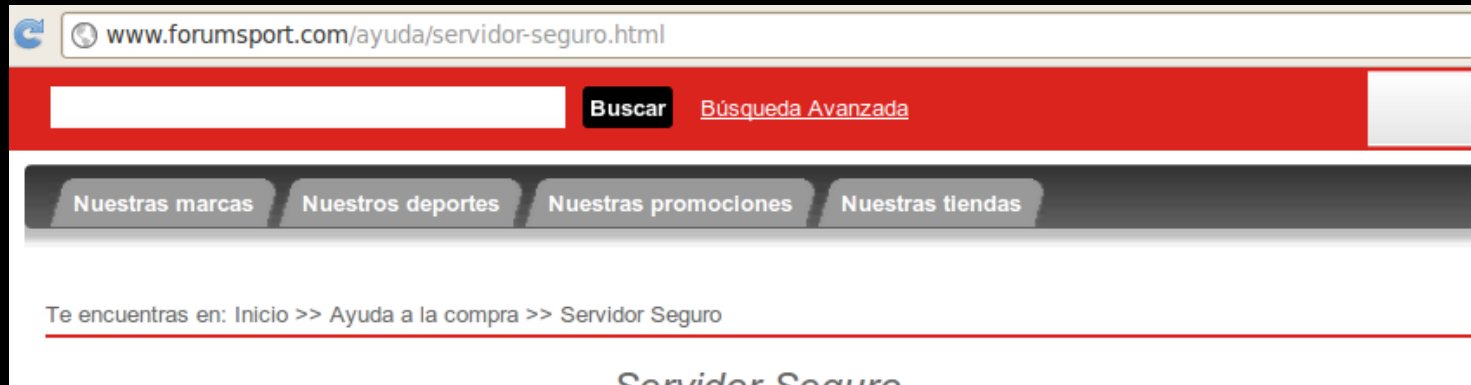
El software del servidor seguro de **Forum Sport tienda on-line** junto al certificado obtenido de la entidad certificadora Thawte (www.thawte.com) encripta toda la información personal, incluyendo el número de tu tarjeta de crédito, de tal forma que no pueda ser leída por terceras personas mientras viaja desde tu ordenador al nuestro.

Tu navegador te indicará que la zona es segura, mostrando un icono en la barra de estado (candado, llave, etc.), y una ventana de aviso, en caso de que tengas esta opción configurada en el navegador. Pinchando sobre el candado, llave, etc. se abrirá una ventana que le facilitará información sobre el certificado y vigencia de transacciones seguras de **Forum Sport tienda on-line**.

Si aún así no estas totalmente seguro, puedes realizar tu pedido en el 902 11 87 05 de lunes a viernes de 9:00 a 19:00 horas.

Toda la información sobre nuestros clientes es confidencial y no es facilitada a ninguna empresa u organización, excepto los datos de entrega que son facilitados al operador logístico, el cual tiene prohibido usarlos para otro fin diferente a la entrega del pedido.

Tengo tus datos, ¿ahora qué?



El software del servidor seguro de **Forum Sport tienda on-line** junto al certificado obtenido de la entidad certificadora Thawte (www.thawte.com) **encripta** toda la información personal, incluyendo el número de tu tarjeta de crédito,

El software del servidor seguro de **Forum Sport tienda on-line** junto al certificado obtenido de la entidad certificadora Thawte (www.thawte.com) encripta toda la información personal, incluyendo el número de tu tarjeta de crédito, de tal forma que no pueda ser leída por terceras personas mientras viaja desde tu ordenador al nuestro.

Tu navegador te indicará que la zona es segura, mostrando un icono en la barra de estado (candado, llave, etc.), y una ventana de aviso, en caso de que tengas esta opción configurada en el navegador. Pinchando sobre el candado, llave, etc. se abrirá una ventana que le facilitará información sobre el certificado y vigencia de transacciones seguras de **Forum Sport tienda on-line**.

Si aún así no estas totalmente seguro, puedes realizar tu pedido en el 902 11 87 05 de lunes a viernes de 9:00 a 19:00 horas.

Toda la información sobre nuestros clientes es confidencial y no es facilitada a ninguna empresa u organización, excepto los datos de entrega que son facilitados al operador logístico, el cual tiene prohibido usarlos para otro fin diferente a la entrega del pedido.

Tengo tus datos, ¿ahora qué?

**CADA VEZ QUE ALGUIEN DICE
ENCRIPtar**



**DIOS MATA UN
GATITO**

memegenerator.net

El softv
obtenid
informa

tificado
la

Tengo tus datos, ¿ahora qué?

https://www.amazon.es/gp/buy/shipaddressselect/handlers/continue.html/ref=ox_shipaddress_ship_to_this_1#d=1

amazon.es BIENVENIDO DIRECCIÓN PRODUCTOS ENVOLTORIO ENVÍO PAGO CONFIRMACIÓN

¿Cómo quieres pagar?

Tus tarjetas de crédito

 **Visa / 4B / Euro6000** que termina en 

Nombre en la tarjeta  Caduca el 

Continuar

(Puedes revisar el pedido antes de finalizarlo)

Más opciones de pago

Tarjetas de crédito o débito

Introduce la información de la tarjeta:

Número de tarjeta Nombre en la tarjeta Fecha de vencimiento 01 ▼ 2012 ▼

Añadir mi tarjeta

 **Cheques regalo y Códigos promocionales**

Aplicar

Introduce un cheque regalo o un código promocional.

Continuar

(Puedes revisar el pedido antes de finalizarlo)

Tengo tus datos, ¿ahora qué?

https://www.amazon.es/gp/buy/shipaddressselect/handlers/continue.html/ref=ox_shipaddress_ship_to_this_1#d=1

amazon.es BIENVENIDO DIRECCIÓN PRODUCTOS ENVOLTORIO ENVÍO PAGO CONFIRMACIÓN

¿Cómo quieres pagar?

Tus tarjetas de crédito

	Nombre en la tarjeta	Caduca el
 Visa / 4B / Euro6000 que termina en 		

Continuar (Puedes revisar el pedido antes de finalizarlo)

Más opciones de pago

Tarjetas de crédito o débito

Introduce la información de la tarjeta:

Numero de tarjeta	Nombre en la tarjeta	Fecha de vencimiento
		01 ▼ 2012 ▼

Añadir mi tarjeta

Cheques regalo y Códigos promocionales

Aplicar

Introduce un cheque regalo o un código promocional.

Continuar (Puedes revisar el pedido antes de finalizarlo)

Tengo tus datos, ¿ahora qué?

https://www.amazon.es/gp/buy/shipaddressselect/handlers/continue.html/ref=ox_shipaddress_ship_to_this_1#d=1



BIENVENIDO

DIRECCIÓN

PRODUCTOS

ENVOLTORIO

ENVÍO

PAGO

CONFIRMACIÓN

¿Cómo quieres pagar?

Tus tarjetas de crédito

Nombre en la tarjeta

Caduca el



VISA

Visa / 4B / Euro6000 que termina en

Continuar

(Puedes revisar el pedido antes de finalizarlo)

Más opciones de pago



Tarjetas de crédito o débito



Introduce la información de la tarjeta:

Numero de tarjeta

Nombre en la tarjeta

Fecha de vencimiento

01

2012

Añadir mi tarjeta



Cheques regalo y Códigos promocionales

Aplicar

Introduce un cheque regalo o un código promocional.

Continuar

(Puedes revisar el pedido antes de finalizarlo)

Tengo tus datos, ¿ahora qué?

https://www.amazon.es/gp/buy/shipaddressselect/handlers/continue.html/ref=ox_shipaddress_ship_to_this_1#d=1

amazon.es BIENVENIDO DIRECCIÓN PRODUCTOS ENVOLTORIO ENVÍO PAGO CONFIRMACIÓN

¿Cómo quieres pagar?

Tus tarjetas de crédito

	Nombre en la tarjeta	Caduca el
 Visa / 4B / Euro6000 que termina en 		

Continuar 
(Puedes revisar el pedido antes de finalizarlo)

Más opciones de pago

Tarjetas de crédito o débito

Introduce la información de la tarjeta:

Numero de tarjeta	Nombre en la tarjeta	Fecha de vencimiento
		01 ▼ 2012 ▼

Añadir mi tarjeta

Cheques regalo y Códigos promocionales

 **Aplicar**

Introduce un cheque regalo o un código promocional.

Continuar 
(Puedes revisar el pedido antes de finalizarlo)

Tengo tus datos, ¿ahora qué?

The screenshot shows the Amazon.es website interface. At the top, the Amazon logo is followed by navigation links: 'Mi Amazon.es', 'Esta semana...', 'Cheques regalo', and 'Ayuda'. Below this is a search bar with the text 'Todos los departamentos' and a 'Buscar' button. To the right of the search bar, there's a 'Ir' button and a greeting 'Hola. Identificar Mi cuenta'. The main content area is titled 'Ayuda' and includes a breadcrumb trail: 'Seguridad, Accesibilidad y Condiciones de Uso > Información en castellano > Seguridad del servidor'. A search bar for the help pages is also present. The left sidebar, titled 'Temas', lists various topics under 'Seguridad del servidor', including 'Identificar correos electrónicos falsos', 'Dispositivo anticopia', 'Retirada de productos del mercado y Seguridad de los productos', 'Compra de Aparatos Eléctricos y Electrónicos en Amazon.es', 'Recomendaciones para ti - Guía', 'Compra Online Segura', 'Facilidades de acceso a Amazon', 'Opiniones de los clientes', 'Condiciones de Uso y Venta', 'Derechos legales del cliente', 'Acuerdo para el Envío de Materiales Relativos a la Valoración del Embalaje', 'Garantía legal', and 'Suscripciones de e-mail y'. The main content area features the heading 'Seguridad del servidor' in orange, followed by a paragraph: 'Compras seguras en Amazon.es gracias a nuestro servidor seguro. Amazon le asegura que su información está totalmente protegida y que sus compras son seguras.' Below this, another paragraph states: 'En Amazon usamos una tecnología muy avanzada para mantener los altos niveles de seguridad de nuestra plataforma online. Nuestro servidor seguro (SSL) encripta toda la información personal que nos facilita (nombre, dirección, datos de su tarjeta, etc.) para poder tramitar su pedido.' At the bottom of the main content area, there's a link: 'Para más información consulte la Política de privacidad de Amazon' and a link: 'Ir a la página de ayuda'.

amazon.es

Mi Amazon.es | Esta semana... | Cheques regalo | Ayuda

Todos los departamentos ▼

Buscar

Todos los departamentos ▼

Ir

Hola. Identificar Mi cuenta

Ayuda > Seguridad, Accesibilidad y Condiciones de Uso > Información en castellano > Seguridad del servidor

Temas

- < Seguridad, Accesibilidad y Condiciones de Uso
- < Información en castellano
 - Aviso de Privacidad de Amazon.es
 - Seguridad del servidor**
 - Identificar correos electrónicos falsos
 - Dispositivo anticopia
 - Retirada de productos del mercado y Seguridad de los productos
 - Compra de Aparatos Eléctricos y Electrónicos en Amazon.es
 - Recomendaciones para ti - Guía
 - Compra Online Segura
 - Facilidades de acceso a Amazon
 - Opiniones de los clientes
 - Condiciones de Uso y Venta
 - Derechos legales del cliente
 - Acuerdo para el Envío de Materiales Relativos a la Valoración del Embalaje
 - Garantía legal
 - Suscripciones de e-mail y

Buscar en las páginas de ayuda:

Buscar

Seguridad del servidor

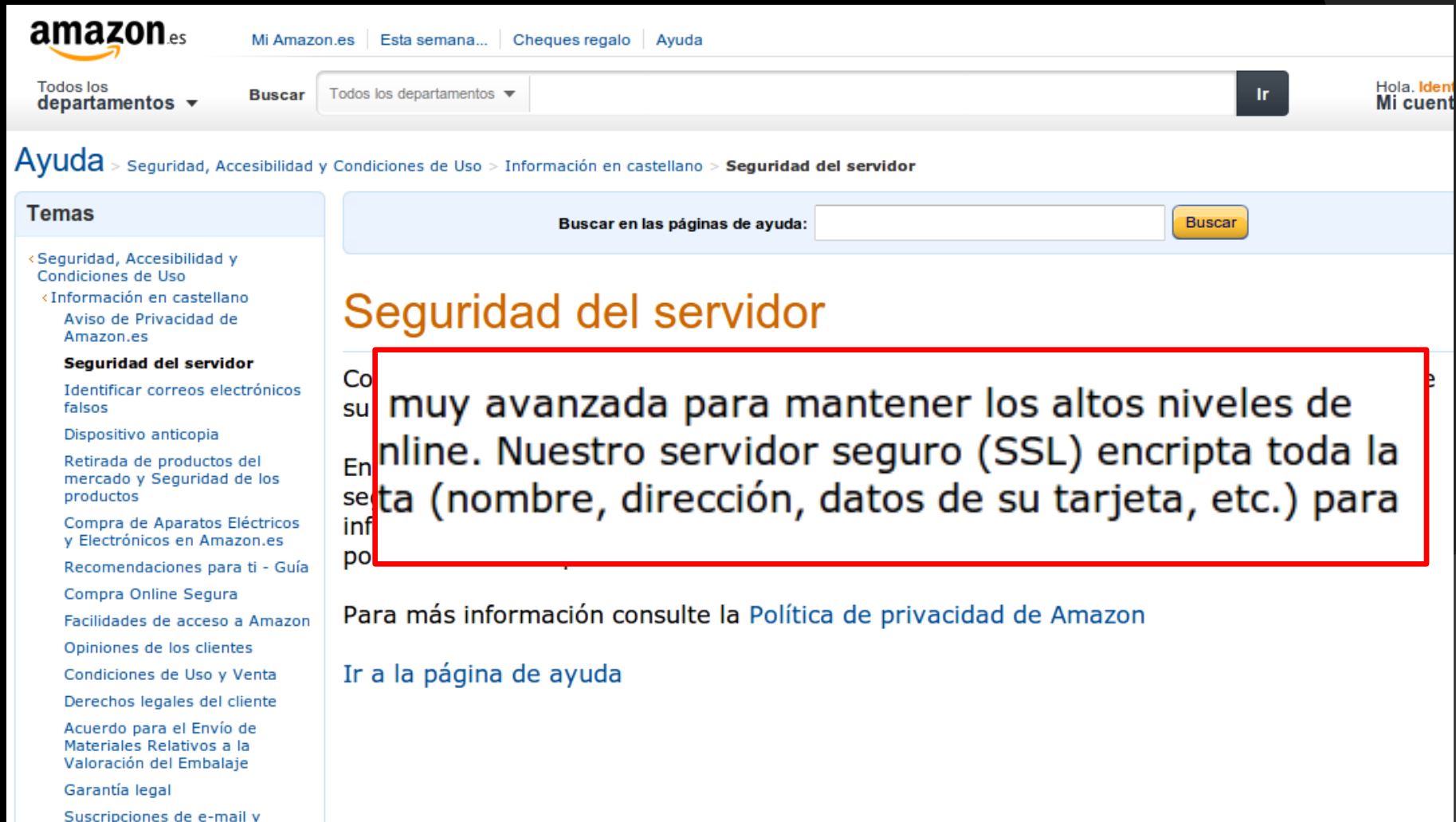
Compras seguras en Amazon.es gracias a nuestro servidor seguro. Amazon le asegura que su información está totalmente protegida y que sus compras son seguras.

En Amazon usamos una tecnología muy avanzada para mantener los altos niveles de seguridad de nuestra plataforma online. Nuestro servidor seguro (SSL) encripta toda la información personal que nos facilita (nombre, dirección, datos de su tarjeta, etc.) para poder tramitar su pedido.

Para más información consulte la [Política de privacidad de Amazon](#)

[Ir a la página de ayuda](#)

Tengo tus datos, ¿ahora qué?



The image is a screenshot of the Amazon.es website's help section. At the top, the Amazon logo is on the left, and navigation links like 'Mi Amazon.es', 'Esta semana...', 'Cheques regalo', and 'Ayuda' are on the right. Below the logo, there's a search bar with 'Todos los departamentos' and a 'Buscar' button. The main navigation bar shows the breadcrumb path: 'Ayuda > Seguridad, Accesibilidad y Condiciones de Uso > Información en castellano > Seguridad del servidor'. On the left side, there's a 'Temas' (Topics) sidebar with a list of links. The main content area has a search bar for the help pages and a large heading 'Seguridad del servidor'. Below the heading, there's a paragraph of text about SSL encryption, which is highlighted with a red box. At the bottom, there's a link to the Amazon privacy policy and another link to the help page.

amazon.es Mi Amazon.es Esta semana... Cheques regalo Ayuda

Todos los departamentos **Buscar** Todos los departamentos Ir Hola. Identificar Mi cuenta

Ayuda > Seguridad, Accesibilidad y Condiciones de Uso > Información en castellano > Seguridad del servidor

Temas

- < Seguridad, Accesibilidad y Condiciones de Uso
- < Información en castellano
 - Aviso de Privacidad de Amazon.es
 - Seguridad del servidor**
 - Identificar correos electrónicos falsos
 - Dispositivo anticopia
 - Retirada de productos del mercado y Seguridad de los productos
 - Compra de Aparatos Eléctricos y Electrónicos en Amazon.es
 - Recomendaciones para ti - Guía
 - Compra Online Segura
 - Facilidades de acceso a Amazon
 - Opiniones de los clientes
 - Condiciones de Uso y Venta
 - Derechos legales del cliente
 - Acuerdo para el Envío de Materiales Relativos a la Valoración del Embalaje
 - Garantía legal
 - Suscripciones de e-mail y

Buscar en las páginas de ayuda: **Buscar**

Seguridad del servidor

Co su muy avanzada para mantener los altos niveles de online. Nuestro servidor seguro (SSL) encripta toda la ta (nombre, dirección, datos de su tarjeta, etc.) para

En se inf po

Para más información consulte la [Política de privacidad de Amazon](#)

[Ir a la página de ayuda](#)

Tengo tus datos, ¿ahora qué?

The screenshot shows the Amazon.es website's help section. At the top, the Amazon logo and navigation links like 'Mi Amazon.es', 'Esta semana...', 'Cheques regalo', and 'Ayuda' are visible. Below the navigation bar, there's a search bar with the text 'Buscar' and a dropdown menu for 'Todos los departamentos'. The main content area is titled 'Ayuda' and includes a breadcrumb trail: 'Seguridad, Accesibilidad y Condiciones de Uso > Información en castellano > Seguridad del servidor'. A sidebar on the left lists various topics under 'Temas', with 'Seguridad del servidor' highlighted. The main content area features a search bar and a section titled 'Seguridad del servidor'. A red box highlights a paragraph of text that discusses data security, mentioning 'muy avanzada para mantener', 'Nuestro servidor seguro', and 'encrypta'. The text is partially obscured by the red box and the sidebar.

amazon.es Mi Amazon.es Esta semana... Cheques regalo Ayuda

Todos los departamentos Buscar Todos los departamentos Ir Hola. Identificar Mi cuenta

Ayuda > Seguridad, Accesibilidad y Condiciones de Uso > Información en castellano > Seguridad del servidor

Temas

- < Seguridad, Accesibilidad y Condiciones de Uso
- < Información en castellano
 - Aviso de Privacidad de Amazon.es
 - Seguridad del servidor**
 - Identificar correos electrónicos falsos
 - Dispositivo anticopia
 - Retirada de productos del mercado y Seguridad de los productos
 - Compra de Aparatos Eléctricos y Electrónicos en Amazon.es
 - Recomendaciones para ti - Guía
 - Compra Online Segura
 - Facilidades de acceso a Amazon
 - Opiniones de los clientes
 - Condiciones de Uso y Venta
 - Derechos legales del cliente
 - Acuerdo para el Envío de Materiales Relativos a la Valoración del Embalaje
 - Garantía legal
 - Suscripciones de e-mail y

Buscar en las páginas de ayuda: Buscar

Seguridad del servidor

Co muy avanzada para mantener tos niveles
su online. Nuestro servidor seguro **!!! encrypta !!!** la
En ta (nombre, dirección, datos de irjeta, etc a
se inf po

Para más información consulte la [Política de privacidad de Amazon](#)

[Ir a la página de ayuda](#)

Tengo tus datos, ¿ahora qué?



Tengo tus datos, ¿ahora qué?

Tengo tus datos, ¿ahora qué?

- Ahora te robo

Tengo tus datos, ¿ahora qué?

- ⦿ Ahora te robo
 - Escenario malpensado

Tengo tus datos, ¿ahora qué?

- ⦿ Ahora te robo
 - Escenario malpensado (Mikel dixit :p)

Tengo tus datos, ¿ahora qué?

- ⦿ Ahora te robo
 - Escenario malpensado (Mikel dixit :p)
 - Zeus → Cuenta de Amazon

Tengo tus datos, ¿ahora qué?

- ⦿ Ahora te robo

- Escenario malpensado (Mikel dixit :p)
 - Zeus → Cuenta de Amazon
 - Ataque cebolleta → Datos tarjeta

Tengo tus datos, ¿ahora qué?

- Ataque cebolleta → Datos tarjeta



Tengo tus datos, ¿ahora qué?

- Ataque cebolleta → Datos tarjeta



Tengo tus datos, ¿ahora qué?

- Ataque cebolleta → Datos tarjeta



Tengo tus datos, ¿ahora qué?

- ⦿ Ataque cebolleta → Datos tartaleta



Arrimando

cebolleta

Tengo tus datos, ¿ahora qué?

- ⦿ Ahora te robo

- Escenario malpensado (Mikel dixit :p)
 - Zeus → Cuenta de Amazon
 - Ataque cebolleta → Datos tarjeta
 - Elijo una dirección ajena o espero en el portal

Tengo tus datos, ¿ahora qué?

- ⦿ Ahora te robo

- Escenario malpensado (Mikel dixit :p)
 - Zeus → Cuenta de Amazon
 - Ataque cebolleta → Datos tarjeta
 - Elijo una dirección ajena o espero en el portal
 - **Profit!**

Tengo tus datos, ¿ahora qué?

- ⦿ ¿Qué se puede hacer con estos datos?
 - Banda magnética
 - Track1
 - Track2

Tengo tus datos, ¿ahora qué?

- ⦿ ¿Qué se puede hacer con estos datos?
 - Banda magnética
 - Track1
 - Track2



Tengo tus datos, ¿ahora qué?

- ⦿ ¿Qué se puede hacer con estos datos?
 - Pagos en establecimientos (extranjero)



Tengo tus datos, ¿ahora qué?

- ⦿ ¿Qué se puede hacer con estos datos?
 - Pagos en establecimientos (identidad falsa)



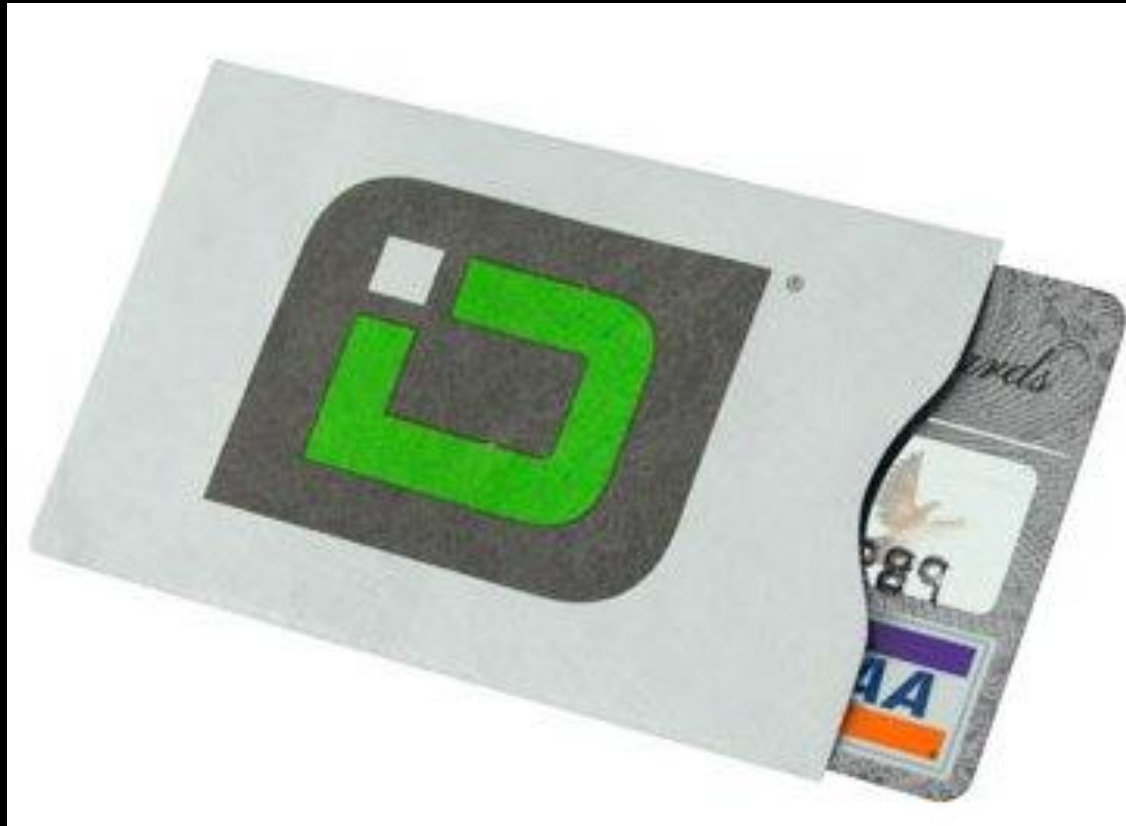
Tengo tus datos, ¿ahora qué?

- ⦿ ¿Qué se puede hacer con estos datos?
 - Pagos no atendidos
 - Peajes
 - Gasolineras
 - Vending
 - Parkings



Recomendaciones

- **Jaula de Faraday para tarjetas NFC**



Recomendaciones

- **Jaula de Faraday para tarjetas NFC**

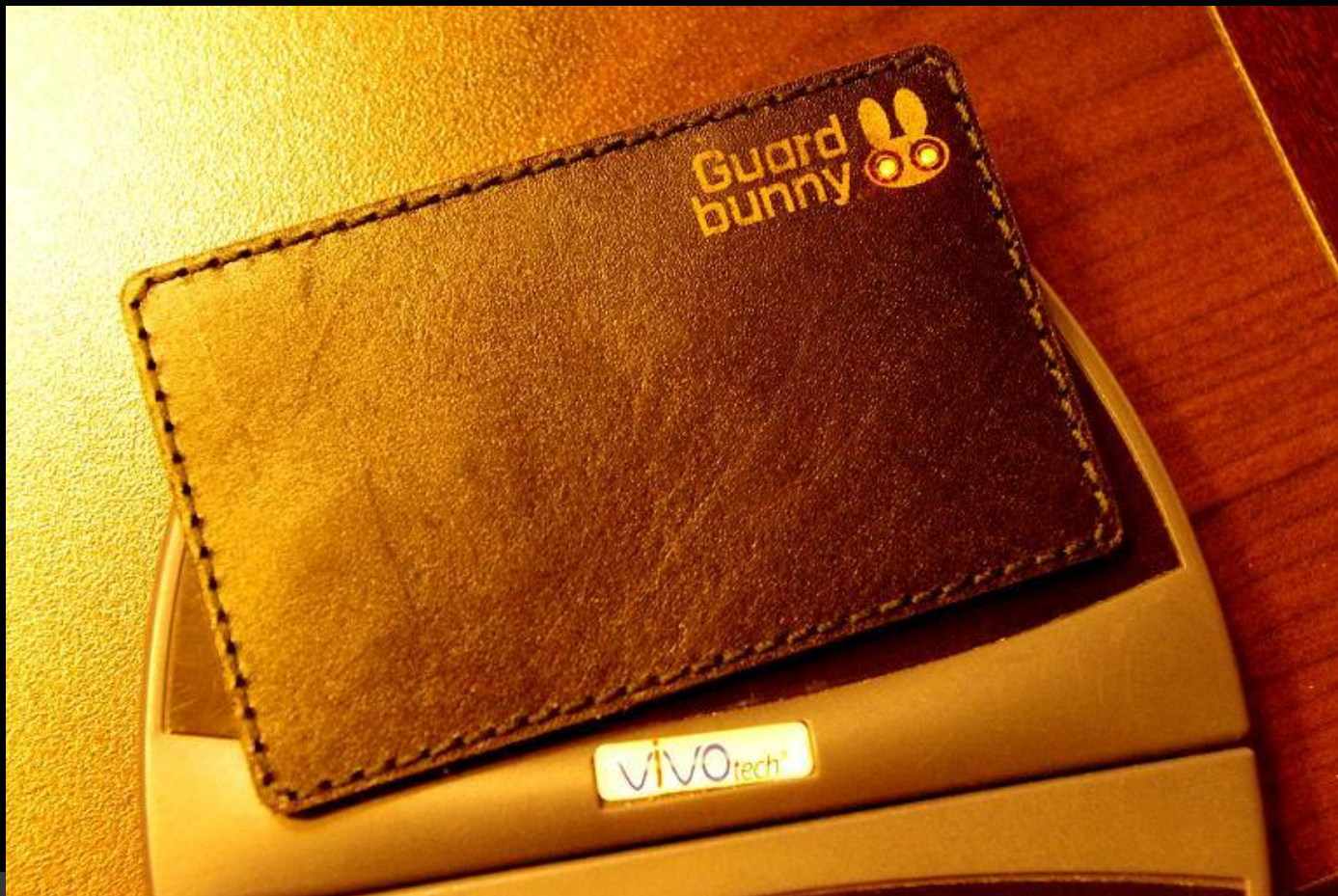


TIN FOIL

FREE YOUR MIND

Recomendaciones

- **Jaula de Faraday para tarjetas NFC**



Recomendaciones

- ⦿ Usar sólo tags firmados por entidades legítimas
- ⦿ Anular acciones automáticas asociadas a tags
- ⦿ Comprobación de aplicaciones para móviles
- ⦿ Actualizaciones de aplicaciones / firmware
- ⦿ Autenticación de doble factor en sistemas de acceso
- ⦿ Conciencia de que el terminal es un medio de pago
- ⦿ Asegurarse del cifrado de datos personales
- ⦿ Cifrado de comunicaciones a alto nivel

Conclusiones

- ⦿ NFC es una tecnología prometedora
 - Sencillez y rapidez de uso
 - Usos cotidianos
- ⦿ En proceso de maduración
 - Desde 2003...
 - La crisis no ayuda
 - Seguridad en entredicho
 - *Passbook* de Apple
- ⦿ **¿La sociedad quiere usarlo?**

Conclusiones

- ⊙ NFC es una tecnología prometedora
 - Sencillez y rapidez de uso
 - Usos cotidianos
- ⊙ En proceso de maduración
 - Desde 2003...
 - La crisis no ayuda
 - Seguridad en entredicho (tampoco ayuda)
 - *Passbook* de Apple
- ⊙ **¿La sociedad quiere usarlo?**

Conclusiones

- ⊙ NFC es una tecnología prometedora
 - Sencillez y rapidez de uso
 - Usos cotidianos
- ⊙ En proceso de maduración
 - Desde 2003...
 - La crisis no ayuda
 - Seguridad en entredicho (tampoco ayuda)
 - *Passbook* de Apple (y esto menos aún)
- ⊙ **¿La sociedad quiere usarlo?**

Agradecimientos

- Mikel Gastesi - @mgastesi
- Marc Rivero - @seifreed
- Carlos Escalada
- Dani Creus
- Javi Barrios
- Thomas Skora - @blubbfiction
- Renaud Lifchitz
- ...

¿Preguntas?



¡¡Gracias!!

Jose Miguel Esparza
@EternalTodo



<http://eternal-todo.com>