

TARJETAS INTELIGENTES – SMART CARDS

¿Qué son?

Las tarjetas inteligentes son dispositivos con las características físicas de las tarjetas de crédito, con un microprocesador incrustado que controla el acceso a la información que contiene.

Las tarjetas inteligentes son actualmente utilizadas para almacenar información de cualquier tipo, en cualquier mercado (banca, salud, gobiernos, etc.), para control de acceso y seguridad (por su capacidad de encriptación, manejo de claves públicas y privadas, etc.), para pago electrónico (monederos electrónicos), planes de fidelización, y más.



Tipos de tarjetas según su hardware - 1

Según las capacidades de su chip, las tarjetas más habituales son:

- ✓ **Memoria:** tarjetas que únicamente son un contenedor de ficheros pero que no albergan aplicaciones ejecutables. Éstas se usan generalmente en aplicaciones de identificación y control de acceso sin altos requisitos de seguridad.
- ✓ **Microprocesadas:** tarjetas con una estructura análoga a la de un ordenador (procesador, memoria volátil, memoria persistente Flash). Éstas albergan ficheros y aplicaciones y suelen usarse para el identificación y el pago con monederos electrónicos.

Tipos de tarjetas según su hardware - 2

✓ **Criptográficas:** tarjetas microprocesadas avanzadas en las que hay módulos hardware para la ejecución de algoritmos usados en cifrados y firmas digitales. En estas tarjetas se puede almacenar de forma segura un certificado digital (y su clave privada) y firmar documentos o autenticarse con la tarjeta sin que el certificado salga de la tarjeta (sin que se instale en el almacén de certificados de un navegador web, por ejemplo), ya que es el procesador de la propia tarjeta el que realiza la firma. Un ejemplo de estas tarjetas son las emitidas por la Fábrica Nacional de Moneda y Timbre (FNMT) española para la firma digital.

Tipos de tarjetas según su sistema operativo

✓ **Tarjetas de memoria.** Tarjetas que únicamente son un contenedor de ficheros pero que no albergan aplicaciones ejecutables. Disponen de un sistema operativo limitado con una serie de comandos básicos de lectura y escritura de las distintas secciones de memoria y pueden tener capacidades de seguridad para proteger el acceso a determinadas zonas de memoria.

✓ **Basadas en sistemas de ficheros,** aplicaciones y comandos. Estas tarjetas disponen del equivalente a un sistema de ficheros compatible con el estándar ISO/IEC 7816 parte 4 y un sistema operativo en el que se incrustan una o más aplicaciones (durante el proceso de fabricación) que exponen una serie de comandos que se pueden invocar a través de APIs de programación.

✓ **Tarjetas Java.** Una Java Card es una tarjeta capaz de ejecutar mini-aplicaciones Java. En este tipo de tarjetas el sistema operativo es una pequeña máquina virtual Java (JVM) y en ellas se pueden cargar dinámicamente aplicaciones desarrolladas específicamente para este entorno.

Aplicaciones comerciales destacables

La tarjetas inteligentes posibilitan fundamentalmente:

- ✓ La identificación del titular de la misma.
- ✓ El pago electrónico de bienes o servicios mediante dinero *virtual*.
- ✓ El almacenamiento seguro de información asociada al titular.

Escenarios para la programación / software

Al aproximarse a la programación de tarjetas inteligentes hay que distinguir dos ámbitos claramente diferenciados:

- Programación de aplicaciones para el chip de la tarjeta, es decir, de aplicaciones que se almacenan y ejecutan dentro del chip de la tarjeta cuando ésta recibe alimentación eléctrica de un lector.
- Programación de aplicaciones para los sistemas en los que se utiliza la tarjeta, esto es, aplicaciones que se ejecutan en ordenadores (en un sentido genérico, ya que pueden ser TPVs embebidos, cajeros automáticos, PCs de escritorio, etc.) a los que se conecta un lector de tarjetas en el que se inserta (o aproxima si es un lector sin contactos) una tarjeta inteligente. Estas aplicaciones se comunican con el lector, el cual se comunica con la tarjeta y sus aplicaciones.

Herramientas para la programación / software - 1

Existen varias APIs de programación estandarizadas para comunicarse con los lectores de tarjetas inteligentes desde un ordenador.

Las principales son:

- PC/SC (*Personal Computer/Smart Card*), especificado por el PC/SC Workgroup. Existe una implementación para Microsoft Windows y también el proyecto MUSCLE que proporciona una implementación casi completa de esta especificación para los sistemas operativos GNU Linux - UNIX.
- OCF (*OpenCard Framework*), especificado por un grupo de empresas. Este entorno intenta proporcionar un diseño orientado a objetos fácilmente extensible y modular. El consorcio OpenCard publica el API y proporciona una implementación de referencia en Java. Existe un adaptador para que OCF trabaje sobre PC/SC.

Herramientas para la programación / software - 2

En ambos casos, el modelo de programación que utilizan las tarjetas inteligentes está basado en protocolos de petición-respuesta.

La tarjeta (su software) expone una serie de comandos que pueden ser invocados. Estos comandos interactúan con los ficheros que subyacen a cada aplicación de la tarjeta y proporcionan un resultado.

Desde el terminal se invocan estos comandos a través de cualquiera de las APIs antes descritas componiendo APDUs (*Application Protocol Data Unit* - comandos con parámetros) que son enviados a la tarjeta para que ésta responda.

Zona única de pagos para el Euro (SEPA)

Europa tiene una moneda común desde hace casi una década, pero carece de un sistema unificado de pagos. Puede parecer una paradoja pero es la realidad que se ha vivido desde el 1 de enero de 2002. Aquella madrugada los bolsillos hicieron lugar para una nueva generación de billetes y monedas. Adiós al franco, la lira, el marco, la peseta... **pero los sistemas de pago electrónicos nacionales han pervivieron... hasta hoy.**

Las autoridades comunitarias han acometido la armonización de los desembolsos informatizados en un segundo momento. Así nació la zona única de pagos del euro (SEPA, en inglés). La Comisión Europea (CE) y el Banco Central Europeo (BCE), en contacto con el sector financiero, definieron unos **estándares técnicos comunes para transferencias, domiciliaciones y transacciones con tarjetas.** Gracias a esto, mandar dinero de Lisboa a Helsinki es igual de simple como hacerlo de Madrid a Burgos.

El dilema de que las transferencias caduquen

- ✓ La llegada de SEPA equipara las operaciones transfronterizas con las órdenes bancarias de ámbito nacional al crearse las transferencias y las domiciliaciones SEPA (SCT y SDD, en inglés).
- ✓ En España, la puesta en marcha de estas alternativas conlleva la sustitución del código de cuenta cliente (CCC) de toda la vida por el número internacional de cuenta bancaria (IBAN, en inglés), de aplicación paneuropea.
- ✓ El próximo noviembre todas las oficinas bancarias de Europa deben ser capaces de atender recibos provenientes de cualquier país.
- ✓ Aun así, queda abierto todavía el debate de si conviene o no fijar una fecha de caducidad para los sistemas nacionales de órdenes bancarias. La CE emitirá un informe al respecto este otoño que dará inicio al debate legislativo de rigor. La banca, agrupada en torno al Consejo de Pagos Europeos (EPC, en inglés), aboga porque el marco operativo que ha definido sea de aplicación universal.

Control del estándar

EMV se corresponde con las siglas del nuevo estándar para las operaciones financieras de cobro con tarjeta.

El estándar ha sido definido y es administrado por la entidad EMVco. La prueba de cumplimiento de EMV tiene dos niveles.

- ✓ El **nivel 1** cubre interfaces a nivel físico, eléctrico y de transporte.
- ✓ El **nivel 2** se refiere a la selección de aplicaciones de pago y el procesamiento de transacciones financieras mediante tarjetas.

El **31 de diciembre de 2010** todo el parque de tarjetas y de terminales deberá estar migrado a EMV.

EMVCo gestiona y mantiene EMV® Integrated Circuit Card Specifications para las tarjetas de pago basadas en un chip y los dispositivos que las admiten.

!!!! SORPRESA !!!

La banca española es la que va más retrasada en Europa en la adopción de la nueva tecnología para tarjetas. A cierre de marzo (últimas cifras comparables) estaba adaptado el 26,3% de los 73 millones de tarjetas del país. La media europea se sitúa en el 70%.

Fuentes financieras atribuyen el retraso al desinterés de la banca nacional en el estándar EMV (acrónimo formado por Europay, Mastercard y Visa).

EMV otorga mayor seguridad a las transacciones al exigir al titular teclear su clave (PIN) cada vez que efectúa una compra con su tarjeta chip. Pero en España las tasas de fraude eran menores que las del resto del continente, por lo que el incentivo económico para migrar perdía peso. La migración a EMV ha comenzado en serio este año 2010, a junio, según el Banco de España, el 42,5% de los plásticos había sido renovado

Cambio de responsabilidades

En caso de fraude, el perjuicio económico era tradicionalmente asumido por el emisor de la tarjeta. Ahora, el importe defraudado recae sobre la entidad dueña del cajero o del datáfono si la máquina no estaba adaptada a EMV.

Se prevé que España completará la migración de sus tarjetas al chip a lo largo del primer trimestre de 2011.

Incumplir el calendario establecido para SEPA no conlleva penalización alguna de las autoridades comunitarias.

Requerimientos del sistema EMV

- EMV es el estándar tecnológico y de seguridad de las tarjetas SEPA.
- El PIN debe ser soportado obligatoriamente por los terminales, quedando a criterio del emisor de la tarjeta su utilización.
- Los esquemas de pago deben introducir una regla de “cambio de responsabilidad” (al menos) y otras posibles medidas para incentivar la migración a EMV que está en marcha desde el 1 de enero de 2008.
- El 31 de diciembre del 2010, todo el parque de tarjetas en circulación, así como el parque de terminales debe haber migrado a EMV.
- Desde el 1 de enero de 2008, las entidades financieras ofrecen tarjetas EMV.
- Algunas partes del estándar están basadas en la interfaz IC Chip card, definida en el ISO 7816. El sistema es incompatible con las tarjetas Carte Bleue, desplegadas sistemáticamente en Francia desde 1992.

Diferencias y ventajas

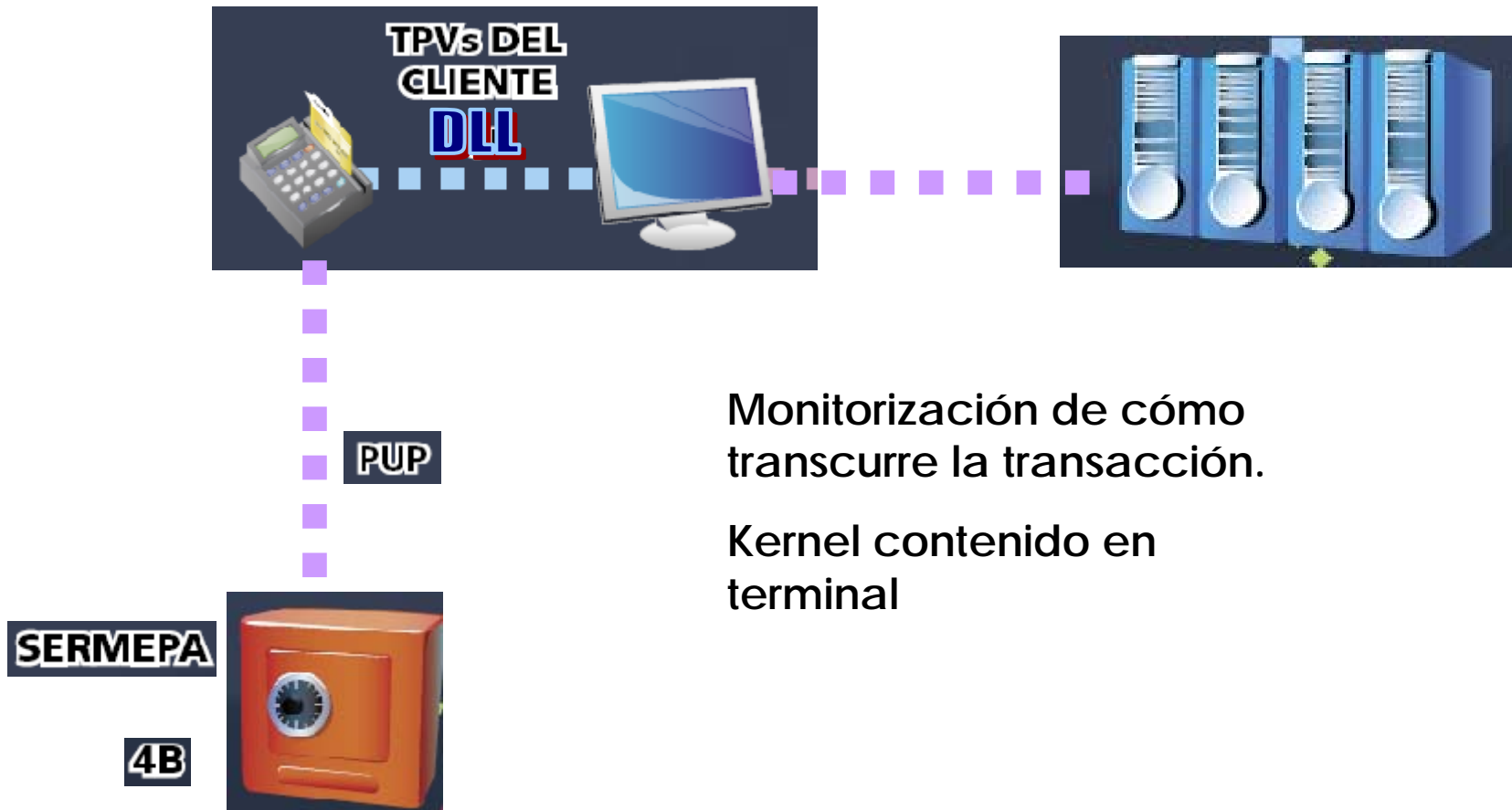
- ✓EMV es permitir una interoperabilidad segura, a nivel mundial, entre tarjetas IC y terminales de pago de tarjetas de crédito que cumplan el mismo.
- ✓Mayor seguridad, lo que implica una reducción del fraude, así como la posibilidad de controlar de forma detallada la aprobación de transacciones off-line **(CUIDADO CON LOS TERMINALES DESASISTIDOS)**
- ✓Las transacciones financieras mediante EMV ofrecen una mayor protección contra el fraude que los pagos tradicionales mediante tarjeta de crédito con banda magnética. Esto se debe al uso de algoritmos de cifrado como DES, Triple-DES, RSA y SHA para la provisión de autenticación por parte de la tarjeta al terminal que lo procesa, y al centro que se encarga de la transacción.

Un nuevo horizonte

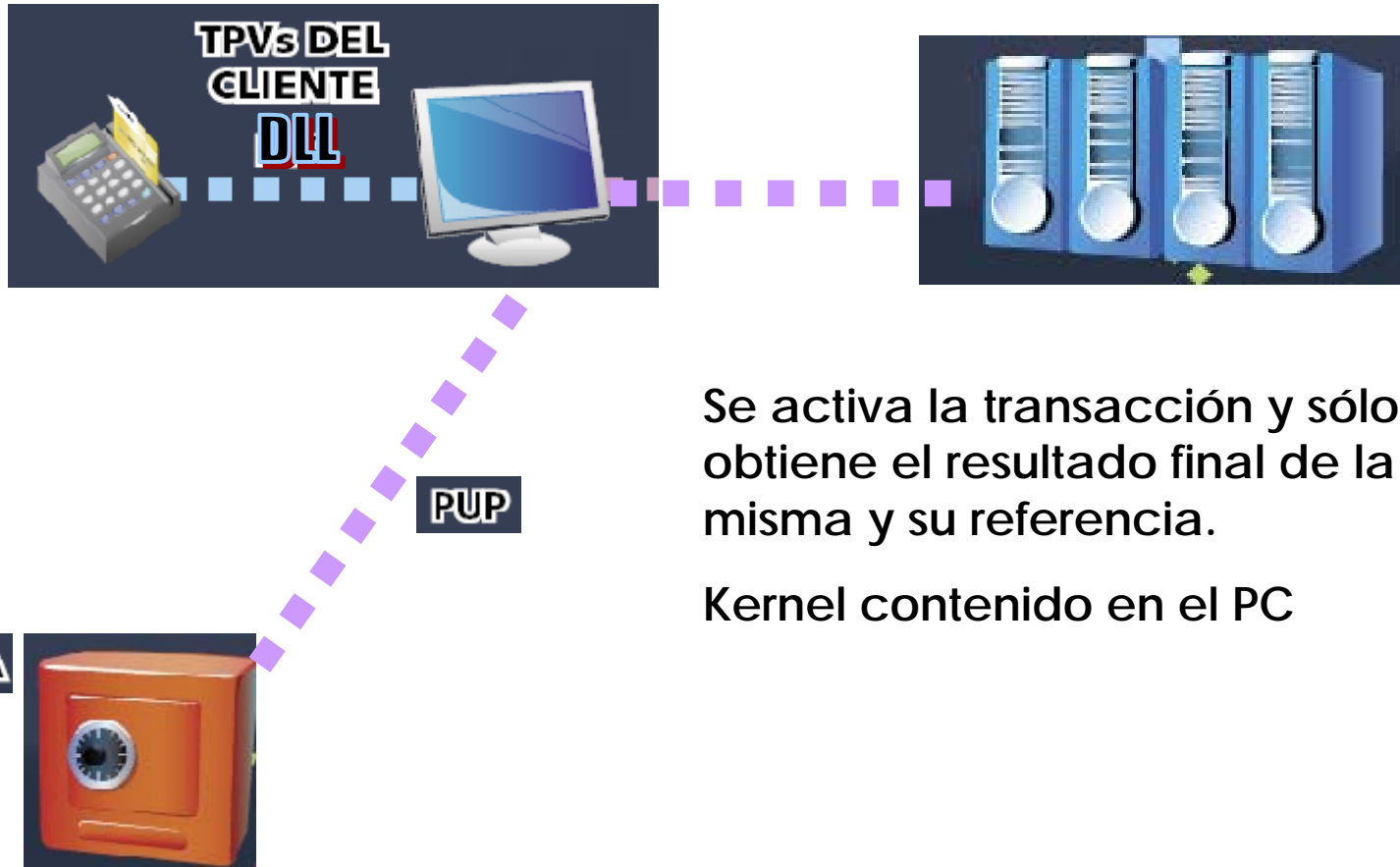
Sin duda, se trata de un nuevo horizonte al que deben asomarse tanto comercios y grandes superficies como entidades financieras de la Unión Europea. De hecho, éstas últimas realizarán la migración progresiva de sus tarjetas a EMV según su propio calendario y objetivos, dentro del marco establecido por el EPC (en castellano, Consejo Europeo de Pagos) para SEPA (2008-2010).

La mayoría de las tarjetas en circulación en España utilizan la marca compartida con VISA y Mastercard, lo que permite utilizar dichas tarjetas en toda la zona única de pagos. El marco normativo de las tarjetas de la SEPA acordado por el EPC, dispone que las tarjetas multiuso que se emitan a partir del 1 de enero de 2008 deben cumplir el estándar EMV”.

Conexión directa terminal-centro autorizador en máquina desatendida

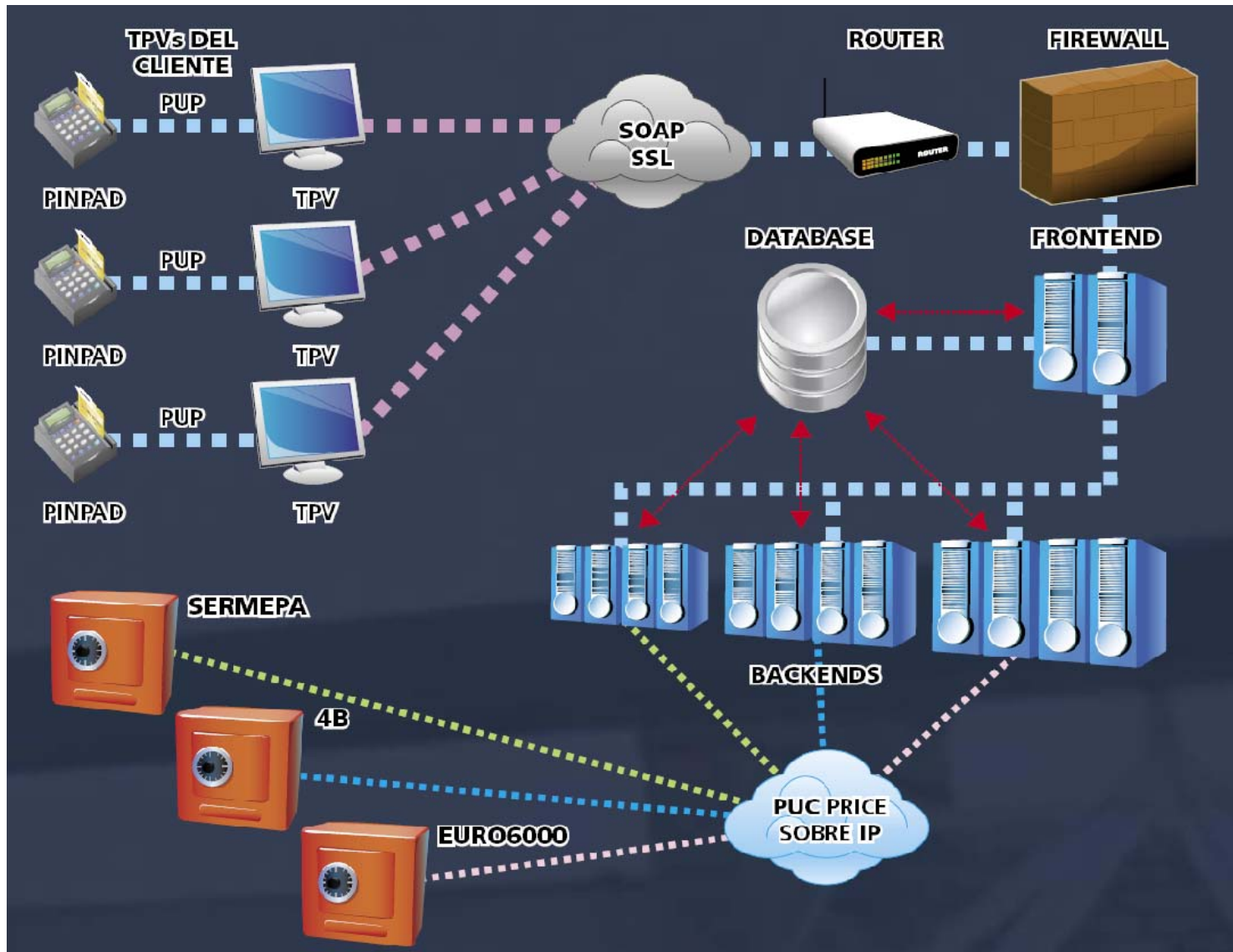


Conexión directa PC-centro autorizador en maquina desatendida



Se activa la transacción y sólo se obtiene el resultado final de la misma y su referencia.

Kernel contenido en el PC



Aplicaciones comerciales en ciernes

La tarjetas inteligentes posibilitan fundamentalmente que se proporcionen servicios como los que VISA apunta en su WEB, www.visaeurope.es :

- ✓ V Pay, tarjeta de débito.
- ✓ PayWave, tarjeta MV sin contacto (SC) para pequeños importes.
- ✓ Claves de autenticación dinámicas, pago por teléfono, internet, mail.
- ✓ Visa Money Transfer, transferencia de dinero de una VISA a otra VISA u oficina bancaria.