# PISCIS: Comercio Electrónico basado en Infraestructuras de Certificación Avanzadas y Sistemas de Tarjeta Inteligente *

Óscar Cánovas Reverte[1], Antonio F. Gómez Skarmeta[2], Gregorio Martínez Pérez[2]

[1] Departamento de Ingeniería y Tecnología de los Computadores
[2] Departamento de Ingeniería de la Información y las Comunicaciones
Facultad de Informática - Campus de Espinardo, s/n
30071 Murcia, España
ocanovas@ditec.um.es, {skarmeta, gregorio}@dif.um.es

**Abstract.** El proyecto PISCIS tiene como principal objetivo rellenar el importante vacío de entornos piloto de comercio electrónico serios que hay en la actualidad. Para ello, y haciendo uso de novedosas propuestas de investigación relacionadas con la seguridad en las comunicaciones, se ha definido una infraestructura completa de certificación sobre la cual se ha desarrollado un sistema de comercio electrónico avanzado, donde conceptos como el de proveedor de servicios criptográficos, basado en Web y tarjetas inteligentes, y el de modelo de pago adaptado al tipo de producto y servicios a comercializar, han jugado un papel muy importante. Mención especial merece el esfuerzo que se está realizando por definir un entorno real de aplicación sobre el cual los clientes finales tienen la oportunidad de aportar su impresión, la cual será utilizada para refinar el sistema y adaptarlo a las necesidades e intereses reales de los usuarios.

## 1 Introducción

Frente a las expectativas de desarrollo de los sistemas de comercio electrónico, la falta de entornos piloto ha retrasado su implantación. Teniendo en cuenta esta realidad, los responsables de los grupos de investigación ANTS-CIRCuS [2] de la Universidad de Murcia y CriptoLab [7] de la Universidad Politécnica de Madrid, en estrecha colaboración con la empresa proveedora de servicios a través de redes de cable ONO, se pusieron en marcha para definir una nueva propuesta al amparo de la convocatoria de proyectos Feder. Dicha propuesta tomó el nombre de Proyecto PISCIS, o Proyecto Piloto de definición de una Infraestructura de Seguridad para el Comercio Inteligente de Servicios.

Como indica el propio nombre, el objetivo principal del proyecto es diseñar e implementar una infraestructura de seguridad sobre la cual tener la posibilidad de crear y poner en marcha un sistema de comercio electrónico caracterizado por hacer uso de

* Financiado por el proyecto TEL-IFD97-1426 EU FEDER (PISCIS)

los últimos avances de investigación en lo que a seguridad en las comunicaciones se refiere; este objetivo ha dado lugar al desarrollo de infraestructuras de certificación avanzadas, la adaptación de sistemas de tarjeta inteligente a los modelos de seguridad definidos por los principales clientes Web y el desarrollo de un modelo de pagos adaptado a los requisitos impuestos por el propio entorno real de aplicación.

Todos estos elementos, una vez diseñados e implementados, están siendo validados en un entorno real de aplicación, lo que nos está aportando una interesante retroalimentación desde el punto de vista del usuario final.

En otro orden de cosas, comentar que en éste, como en todo sistema de comercio electrónico, el objetivo final es poder comercializar productos haciendo uso de los avances que nos aportan las tecnologías de la información. En nuestro caso concreto, ya desde la definición del propio proyecto, se decidió que el tipo de producto a comercializar estaría basado en aquellos bienes y servicios que pudieran contar con una representación digital, como por ejemplo, música, periódicos, libros, las claves para acceder a una retransmisión en modo pago-por-visión, etc.

En este artículo presentamos las características más importantes y diferenciadoras del modelo de comercio electrónico que se ha creado como resultado del proyecto de investigación PISCIS. En este sentido, se pretende resaltar las características más interesantes de la infraestructura de certificación desarrollada, la integración realizada de un sistema de tarjetas inteligentes dentro de la arquitectura de seguridad planteada en los entornos Microsoft Windows, y el modelo de pago que se ha creado al amparo de los dos componentes que se acaban de comentar. Por último se presenta de manera breve el escenario de pruebas en el cual se está trabajando en la actualidad para conseguir la validación por parte de los usuarios finales del sistema propuesto. El artículo finaliza con una breve reflexión sobre el trabajo realizado, a modo de conclusiones, así como una lista de algunas de las actividades de investigación futuras relacionadas con el proyecto.

## 2 Una Infraestructura de Certificación Avanzada

Entre las primeras etapas del proyecto, encontramos la necesidad de definir y construir una infraestructura de certificación capaz de dotar de identidad digital a las entidades participantes en el proyecto. Como se verá más adelante, los servicios desarrollados dentro del marco del entorno piloto requieren de la existencia de una PKI (Public Key Infrastructure) que gestione el ciclo de vida de los certificados de identidad X.509v3 [10] de los usuarios así como de los procesos o máquinas. Nuestro grupo de investigación, que viene trabajando desde hace ya unos años en el ámbito de la especificación e implementación de PKIs, participó en la implantación de la infraestructura de certificación que actualmente da soporte a los miembros de la Universidad de Murcia [13]. La PKI del proyecto PISCIS constituye la evolución de esa infraestructura original, e incorpora nuevas características y servicios en materia de certificación propuestos recientemente, así como algunas ideas innovadoras de investigación surgidas en el seno de nuestro grupo. Uno de los elementos claves de la infraestructura original, la tarjeta inteligente como contenedor de información

criptográfica (claves privadas y certificados digitales), sigue siendo uno de los pilares centrales de la nueva PKI, pero además con un mayor soporte para otro tipo de tarjetas inteligentes, como las tarjetas criptográficas RSA, o tarjetas Java Card.

Actualmente, podemos dividir la infraestructura en 3 bloques constructivos independientes. En primer lugar, se encuentran definidos los servicios básicos de gestión del ciclo de vida de certificados (creación, publicación, renovación y revocación). Un segundo bloque lo constituyen servicios de valor añadido como el servidor de OCSP [16] (Online Certificate Status Protocol) o el servicio de sellado digital de tiempo (Time Stamp). Por último, la infraestructura incorpora también un bloque de servicios avanzados que reflejan algunas ideas de investigación del grupo, como pueden ser el servicio de autorrevocación o el refirmado de certificados. Esta sección se encargará de proporcionar una descripción de cada uno de estos bloques constructivos y de su implicación en el entorno del proyecto.

### 2.1 Servicios básicos

Por servicios básicos de certificación entendemos todos aquellos que forman parte de la gran mayoría de infraestructuras existentes y que constituyen el núcleo de la gestión del ciclo de vida de los certificados digitales, es decir, solicitud de certificación, validación, publicación, solicitudes de renovación, y mecanismos de revocación de certificados digitales. Para llevar a cabo tales servicios, el sistema dispone de un conjunto de entidades administrativas que asumen diversas funciones:

- *Autoridad de Registro (RA)*. Normalmente, es la primera entidad de contacto con la infraestructura de certificación. En líneas generales, su función principal es la de validar e identificar a los usuarios que solicitan alguno de los servicios que ofrece la infraestructura. Para realizar sus funciones toma en consideración las opciones determinadas por la política de certificación del sistema, documento digital que se actualiza periódicamente.
- *Servidor de solicitudes*. Se encarga de almacenar todas las solicitudes de servicio realizadas tanto por la autoridad de registro como por los propios usuarios del sistema. Dichas solicitudes serán posteriormente recuperadas por la Autoridad de Certificación para tramitarlas como corresponda.
- Autoridad de Certificación (CA). Entidad encargada de tramitar las solicitudes de servicio realizadas por ciertas entidades del sistema. En general, está encargada de emitir los certificados digitales del sistema, las listas de revocación, firmar las políticas de certificación, y publicar la información en los repositorios de datos tanto internos como públicos.
- *Repositorio público*. Dicha entidad almacena los certificados digitales (tanto de usuarios y procesos como de las propias entidades que componen el núcleo de la PKI) y las listas de revocación de certificados emitidas por la CA.
- Base de datos interna. Almacena cada una de las solicitudes y documentos emitidos por la infraestructura.
- *Administrador*. Es la entidad encargada de la configuración de los parámetros de funcionamiento de la infraestructura. Entre dichos parámetros se encuentra la

política de la PKI, que no es más que el reflejo digital de las prácticas de certificación del sistema, y que constituirá el elemento clave que guiará a gran parte de procesos a la hora de gestionar el ciclo de vida de los certificados.

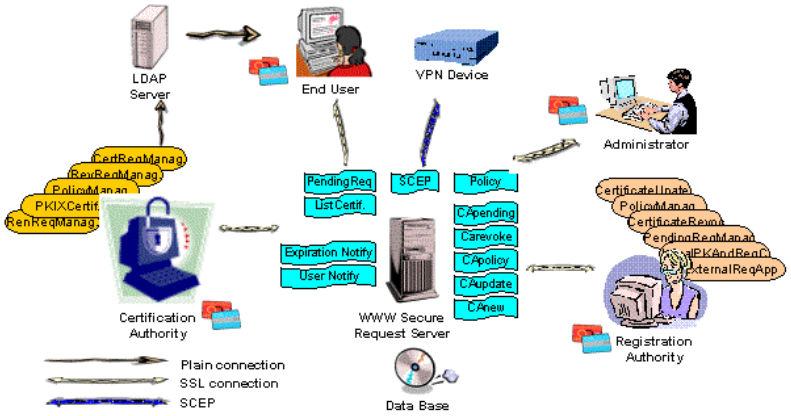


**Figura 1**. Servicios básicos de la PKI

En la Figura 1 se pueden apreciar las entidades previamente comentadas, así como la relación existente entre las mismas. Dicha figura hace también referencia a las operaciones llevadas a cabo dentro del bloque de servicios denominados como básicos:

– *Solicitud de certificación*. La solicitud de un nuevo certificado puede llevarse a cabo mediante diversos métodos. Por un lado, los usuarios pueden realizar su solicitud acudiendo a la RA con documentos acreditativos de su identidad y con la tarjeta inteligente que contendrá la clave privada generada. Dicha solicitud es comprobada respecto a la política del sistema, y si no la viola, el par de claves generado en la RA se utiliza de la siguiente forma: la clave pública junto con la información de identificación forma parte de una solicitud PKCS#10 [22] que se envía posteriormente al servidor de solicitudes mediante una conexión SSL con autenticación de todas las entidades participantes; la clave privada se almacena en la tarjeta inteligente del usuario (en el caso de tarjetas criptográficas RSA, el par de claves se genera en la tarjeta y la RA sólo tiene acceso a la clave pública). Por otro lado, los administradores de servicios pueden acudir a la RA con una solicitud PKCS#10 previamente generada con el software del servicio, y con la intención de que ésta sea validada y dé lugar al correspondiente certificado. También se encuentra disponible un servicio de tramitación de solicitudes realizadas utilizando el protocolo SCEP [12], orientado a ofrecer servicios de certificación a routers involucrados en el establecimiento de redes privadas virtuales. En último lugar, existe la posibilidad de que los usuarios generen su propia solicitud de certificación vía Web utilizando su propio navegador y lector de tarjetas inteligentes. En este caso, la tramitación de la solicitud se realiza previa validación en la RA de los datos contenidos en dicha solicitud.

- *Obtención del certificado digital*. Una vez que el certificado ha sido emitido por la CA, el usuario debe recuperarlo para poder empezar a utilizarlo. En el caso concreto de nuestra infraestructura, la recuperación se realiza a través del navegador, en un proceso por el cual tanto el certificado del usuario como el de la autoridad de certificación se insertan en la tarjeta inteligente haciendo uso del proveedor de servicios criptográficos (CSP) que se ha desarrollado para el proyecto (y que será analizado más adelante). Los certificados de procesos (como por ejemplo el de un servidor web seguro) pueden obtenerse directamente de la base de datos interna de la PKI o de un repositorio público haciendo también uso del navegador.
- *Solicitud de renovación*. Dependiendo de lo especificado en la política de la infraestructura, las entidades tienen la posibilidad de renovar la validez del par de claves asociado a su certificado actual. En el caso de que esté permitido, las entidades pueden solicitar esta renovación acudiendo a la RA y acreditando su identidad, o bien realizarlo directamente mediante su navegador haciendo uso de una conexión SSL autenticada de cliente y servidor, y usando para ello el mismo certificado que desean renovar. El sistema dispone también de un sistema que notifica a los usuarios la proximidad de la caducidad de los certificados mediante un correo electrónico firmado digitalmente usando S/MIME [7].
- *Solicitud de revocación*. En ciertas condiciones excepcionales, como la pérdida o el compromiso de la tarjeta inteligente, los certificados digitales deben dejar de ser válidos antes de que se agote su periodo inicial de validez. Los usuarios del sistema tienen dos opciones a la hora de solicitar que se realice la revocación de su certificado (además de una tercera opción que será comentada posteriormente). Por un lado, la RA puede enviar una solicitud de revocación al servidor de solicitudes tras autenticar al usuario implicado. La otra opción es que el propio usuario revoque su certificado haciendo uso de su navegador y del certificado en cuestión mediante una conexión SSL autenticada de cliente. Esta última opción sólo es posible en el caso de que el cliente siga teniendo acceso a su clave privada.
- *Establecimiento de la política del sistema*. Ciertos usuarios del sistema tienen el derecho para establecer la política de seguridad que rige el funcionamiento de la infraestructura. Una política es un documento digital que contiene un número de serie, una fecha de emisión, una fecha de próxima emisión y un conjunto de elementos de política. Dicho conjunto indica qué restricciones de la política deben ser aplicadas a qué conjunto de certificados. Por ejemplo, un elemento de política podría ser el tamaño de clave RSA o el periodo de validez a asignar a los certificados. El administrador accede a través de su navegador a la página de definición de políticas, donde puede crear una nueva política o cambiar elementos de la actual. Una vez establecida, la CA firma la política y la deja accesible a todas las entidades del sistema para que puedan utilizarla.

## 2.2 Servicios adicionales.

Además de las funciones explicadas anteriormente, la PKI ofrece una serie de servicios de valor añadido destinados a enriquecer más la gama de posibilidades que ofrece la infraestructura. Entre ellos encontramos el soporte para el protocolo de sellado de tiempo TSP [1] y el servicio de chequeo en-línea del estado de los certificados OCSP [16]. En la Figura 2 puede verse un esquema de la integración de ambos en el sistema.

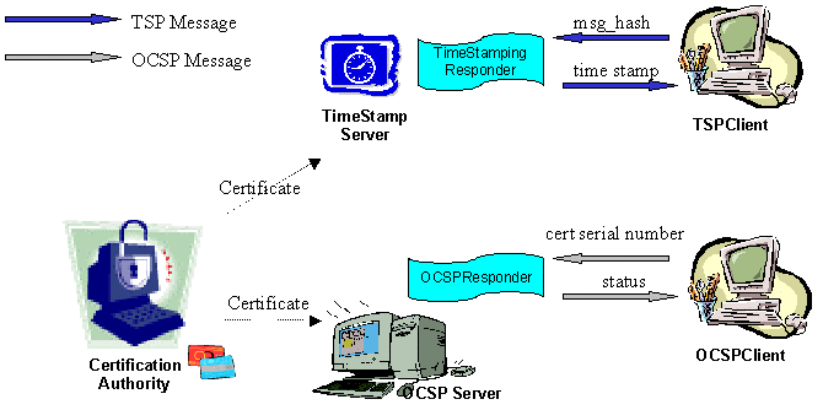


**Figura 2.** Integración de los servicios OCSP y TSP

El servicio de sellado digital de documentos asocia una marca temporal confiable a cualquier tipo de documento. Según el protocolo seguido, el resumen digital de los documentos a sellar se le envía al servidor de tiempo con el fin de obtener una sentencia firmada digitalmente por dicho servidor que establezca una vinculación temporal entre dicha información y el instante en el que fue enviado al servidor. Se ha seguido la notación especificada en [1] tanto para los mensajes de solicitud como para los de respuesta. La respuesta incluye un número de serie de referencia, una marca temporal, extraída de un servidor NTP de nivel 3, y el resumen del documento, todo ello firmado digitalmente por el servidor TSP.

El servicio OCSP fue incluido para dotar al sistema de una mayor precisión a la hora de determinar la validez de un certificado de la que proporciona el uso de las tradicionales CRLs [19]. Con OCSP el usuario obtiene una validación instantánea del estado en el cual se encuentra el certificado al que se está haciendo referencia. El sistema se articula mediante un servidor que acepta solicitudes OCSP, verifica el estado del certificado referenciado por el número de serie y el identificador de emisor, y devuelve el estado en el cual se encuentra (válido, revocado o desconocido). La comprobación de la validez del certificado se realiza frente a la base de datos interna de la PKI, la cual contiene la información más actualizada.

### 2.3 Otros servicios

La infraestructura de certificación incorpora algunos servicios propuestos por nuestro grupo de investigación. Uno de ellos está pensado para ofrecer un servicio de autorrevocación de certificados aún en circunstancias en las que el acceso a la clave privada del usuario no es posible. El otro servicio está relacionado con aquellos entornos en los cuales se requiere tener la certeza de que el certificado es válido en el instante en el que se está haciendo uso de él, como escenarios de cierta seguridad relacionados con pagos electrónicos. Este último se trata de una alternativa a OCSP que intenta descargar a los servidores (proveedores de servicios en general) de la tarea de tener que verificar cada certificado presentado mediante consultas OCSP.

A grandes rasgos, el servicio de autorrevocación es un sistema de dos etapas que permite a los usuarios revocar su propio certificado mediante la introducción de un login y un password. En primer lugar, los usuarios establecen una conexión SSL totalmente autenticada con el servicio de autorrevocaciones con el fin de realizar una solicitud de revocación por anticipado. Dicha solicitud queda almacenada, de forma cifrada mediante una clave derivada del password suministrado por el propio usuario, y a la espera de ser activada por él. Posteriormente, cuando el certificado del usuario deba ser revocado, éste tendrá sólo que suministrar el login y el password que protege su solicitud de revocación con el fin de que ésta se haga efectiva en ese instante.

La otra característica adicional está pensada como un servicio de valor añadido en el campo de la validación del estado de certificados. Además de la publicación de CRLs y el servicio OCSP, la infraestructura dispone de un sistema de refirmado de certificados mediante el cual puede alterarse de forma cómoda y automática la fecha de inicio de validez de un certificado (*Not-Before*) y situarla en el momento de la solicitud de actualización. Los distintos servidores del proyecto pueden establecer como política que consideran válidos todos aquellos certificados que hayan sido emitidos durante las últimas *h* horas (donde *h* es un parámetro configurable por cada emisor). De esa forma, el usuario haciendo uso del sistema tendría que refirmar una única vez su certificado y podría utilizarlo frente a todos los servidores sin necesidad de comprobaciones adicionales en un intervalo de *h* horas, en contraste con las continuas validaciones que requiere OCSP (una por acceso y servidor). Una descripción más detallada del sistema en el cual está basado este servicio puede encontrarse en [2].

## 3 Seguridad en las Transacciones Web sobre Tarjeta Inteligente

Uno de los criterios principales que subyacen al modelo de comercio que se ha creado es el uso del Web, que sin duda aporta facilidad de uso a todo el sistema. Junto a ello, otro componente que juega un rol significativo en el desarrollo de todo el proyecto es la tarjeta inteligente, la cual sirve como medio de identificación y autenticación de usuarios (tal y como se ha comentado en el apartado anterior) y base tecnológica sobre la cual implementar un monedero electrónico (cuyo uso será comentado en el apartado siguiente).

Estos dos componentes dieron lugar a la necesidad de analizar la arquitectura de seguridad y las posibilidades de integración de las tarjetas inteligentes que planteaban los dos navegadores más utilizados en la actualidad: Netscape Communicator y Microsoft Internet Explorer.

Con respecto al primero de ellos, Netscape Communicator, ha sido suficiente con adaptar los trabajos de análisis y diseño que en su día se llevaron a cabo en el marco del Proyecto SSL de la Universidad de Murcia. En dicho proyecto, fruto de la colaboración existente con el Servicio de Informática de la misma universidad, se realizó una implementación completa de un módulo criptográfico PKCS#11 [23].

### 3.1 La Arquitectura de Seguridad de Microsoft Windows

Tomando como punto de partida la necesidad de incorporar la tecnología de tarjetas inteligentes dentro del navegador Microsoft Internet Explorer en particular, y del sistema operativo Microsoft Windows en general, el primer estándar que nos sirve de referencia es PC/SC [18], el cual aporta la interoperabilidad necesaria entre este tipo de dispositivos y los sistemas operativos donde mayor nivel de implantación ha alcanzado.

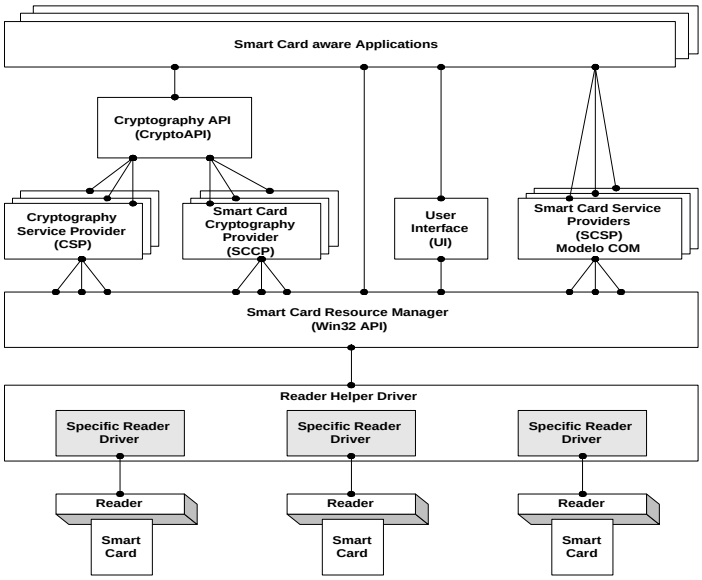


**Figura 3**. Arquitectura PC/SC

La arquitectura PC/SC, ver Figura 3, está basada en una serie de niveles y diferentes APIs. De entre todas esas APIs de interacción (hasta cuatro hay definidas) existe una, conocida como CryptoAPI [14], de especial interés cuando, como es nuestro caso, el integrador de servicios desea tener una comunicación directa entre una aplicación definida sobre páginas Web y los servicios criptográficos ofrecidos por una tarjeta inteligente.

CryptoAPI, que realmente forma parte de la arquitectura de seguridad del propio sistema Microsoft Windows (no es exclusivo de PC/SC, aunque es uno de sus componentes más importantes) ofrece una completa interfaz para funcionalidades criptográficas (firma digital, cifrado, envoltura digital, etc.) definida con independencia del proveedor final que las proporcione, de la implementación y de la existencia o no de un dispositivo hardware que soporte dicha gestión criptográfica. En este sentido, permite al desarrollador final hacer uso de criptografía sin necesidad de conocer los detalles de un cierto algoritmo o una cierta implementación hardware o software; sólo es necesario seleccionar el proveedor criptográfico o CSP [15] (acrónimo en inglés de Cryptographic Service Provider) que se crea más conveniente en cada caso.

### 3.2 El desarrollo de un módulo CSP para PISCIS

En el entorno definido por el proyecto PISCIS, dos son los entornos de aplicación que hacen uso real de las tarjetas inteligentes y, por extensión, del CSP que se ha desarrollado para habilitar dicho acceso a través de la interfaz CryptoAPI: la infraestructura de certificación y el protocolo SPEED (ver Figura 4).

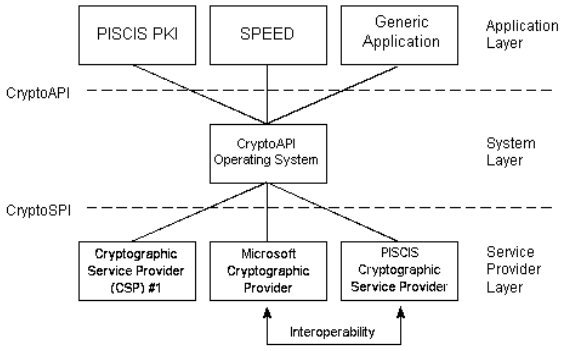


**Figura 4**. Arquitectura de seguridad de PISCIS en sistemas Microsoft Windows

En el primero de los casos, se utiliza el CSP, a través de unas librerías conocidas como Certificate Enrollment Control [16], para generar el par de claves que identificarán de manera unívoca a un usuario dentro del sistema, y para almacenar la clave privada y el certificado asociado a la clave pública, junto con el certificado de la CA raíz, dentro de la tarjeta inteligente.

En el segundo de los casos, el protocolo SPEED requiere sobre todo la utilización de dicha clave privada, y del certificado, para la autenticación y validación de los mensajes enviados por los interlocutores que participan en una transacción de comercio electrónico.

Teniendo en cuenta estos requisitos, se ha implementado un CSP completo (FULL RSA) acorde con la especificación aportada por Microsoft y haciendo uso de las tarjetas inteligentes del proyecto PISCIS. De manera adicional, y para comprobar el correcto funcionamiento de este CSP se han realizado tests de interoperabilidad con

distintas aplicaciones Windows que hacen uso de él (sistema de logon, PKI de Windows 2000, etc.) y con otros CSP (como el CSP base proporcionado por Microsoft). Recientemente, el CSP desarrollado en PISCIS ha obtenido la firma oficial de Microsoft para poder ser distribuido como un componente válido dentro de los sistemas Windows.

Por último destacar, que una vez se ha implementado el módulo CSP en forma de DLL, y al no tratarse de un objeto COM, es necesario habilitar algún mecanismo que permita su utilización desde un navegador Web. En este sentido, la opción que se ha tomado es la de crear un control ActiveX que hace las veces de enlace entre ambos elementos, a la vez que permite filtrar de manera adecuada qué servicios criptográficos se ofrecen a qué aplicaciones.

## 4 Un Modelo de Pago: SPEED

En los últimos años, la comunidad científica ha ido tomando conciencia de la necesidad de diseñar e implementar nuevas formas de pago adaptadas al comercio electrónico que hagan un buen uso de la tecnología existente y proporcionen al usuario un cierto grado de percepción de seguridad. En general, cada uno de estos sistemas propuestos intenta satisfacer las necesidades del entorno en el cual está definido, y por tanto no podemos considerar que haya un sistema válido para cualquier entorno. Algunas de estas propuestas, como PayWord [20], MicroMint [20], Millicent [9], o NetBill [6], han demostrado ser lo suficientemente seguras y flexibles, aunque ninguna de ellas haya alcanzado un alto grado de penetración en mercados reales.

El marco en el cual se encuadra el proyecto determina varios requisitos que deben ser exigibles al sistema de pagos a utilizar. La siguiente lista enumera algunos de ellos:

- el sistema debe ser lo suficientemente ligero como para ser capaz de gestionar gran número de transacciones por unidad de tiempo, sobre todo considerando el gran número de usuarios potenciales del sistema,
- el propio sistema de pagos debe ser capaz de ofrecer medios para negociar el precio de los productos o servicios ofrecidos por los comerciantes,
- la entrega electrónica de los bienes adquiridos debe formar parte del sistema,
- el sistema no debe dificultar la movilidad de los usuarios. Debe ser posible permitir a los usuarios la máxima movilidad a la hora de realizar sus compras o negocios,
- el sistema a utilizar debe estar basado en estándares de seguridad reconocidos. Este requisito incrementa la sensación de seguridad percibido por los usuarios, y garantiza un diseño basado en propuestas debatidas y probadas por la comunidad,
- se debe disponer de elementos de arbitraje capaces de ejercer como mediadores y como entidades de confianza a la hora de mediar en conflictos y situaciones excepcionales,

– el sistema debe ser capaz de ofrecer varias formas de pago posibles. En el caso que aquí nos ocupa estas opciones se concretan en el pago basado en monedero electrónico y el pago tradicional basado en tarjeta de crédito.

### 4.1 Características Generales de SPEED

Aunque algunos de estos requisitos han sido satisfechos por propuestas ya existentes, con el fin de proporcionar una respuesta común a todos ellos en nuestro entorno de trabajo, hemos definido un nuevo sistema de pago llamado SPEED (Smartcard-based Payment with Encrypted Electronic Delivery), el cual proporciona, como su propio nombre indica, un sistema de pago basado en monedero electrónico y tarjeta inteligente con entrega cifrada de bienes. Aunque la información en detalle del protocolo puede encontrarse en [24], en esta sección haremos una breve descripción de sus características principales, participantes y modelo de compra.

Su diseño se basa en el uso de estándares como ASN.1 [11] para la especificación de la estructura de los mensajes, PKCS#7 [21] como formato criptográfico para el intercambio de información protegida, certificados X.509v3 [10] para la identificación de los participantes en el escenario de compra, y WG10 [4] como sistema estándar de monedero electrónico.

Una transacción SPEED transfiere bienes electrónicos desde un vendedor a un cliente, debitando el monedero electrónico del cliente (o su cuenta) e incrementando el saldo de la cuenta del vendedor por el valor de producto. El diseño de SPEED consiste en una serie de fases que incluyen la negociación del precio, la entrega del producto y su pago. Además, hay dos modos posibles de operación: el modo normal incluye la capacidad de negociación del precio del producto, y ha sido diseñado para proporcionar el mayor número de características de seguridad (como por ejemplo la prevención de ataques de denegación de servicio y la autenticación completa de las partes participantes antes del suministro del producto); el modo rápido de operación está compuesto por un número menor de mensajes que el modo normal, y está pensado para la venta de bienes de menor tamaño o escenarios con menores requisitos de seguridad.

### 4.2 Participantes de SPEED

El modelo de negocio de SPEED está compuesto por tres entidades principales: el cliente, el comerciante y el intermediario (broker). El broker gestiona las cuentas de los comerciantes (y opcionalmente las de los clientes) y mantiene el conjunto de módulos de seguridad (SAM) que realizan las operaciones de decremento sobre el monedero electrónico del cliente. Esta entidad no interviene hasta la fase de pago, una vez que el cliente envía la solicitud de transacción.

En una primera instancia, el cliente y el vendedor acuerdan el producto a comprar y su precio, lo cual puede ser llevado a cabo después de una fase de negociación de ofertas que es opcional. El producto se transmite al cliente cifrado con una clave simétrica, que sólo le es proporcionada al cliente una vez que el pago correspondiente

se ha materializado. Cuando dicho pago se ha realizado, tanto el cliente como el vendedor obtienen una prueba del resultado de la transacción (denominada recibo). Todas las comunicaciones están protegidas frente a ataques de entidades externas haciendo uso de criptografía simétrica y, en casos especiales, de criptografía asimétrica.

Cada participante de SPEED (clientes, comerciantes y broker) posee una clave privada RSA almacenada en su tarjeta inteligente y un certificado X.509 emitido por la infraestructura de clave pública comentada anteriormente. De hecho, SPEED asume la existencia de relaciones de confianza entre las entidades participantes. Los brokers son considerados las entidades de mayor confianza, seguidos de los comerciantes y por último de los clientes (en los cuales podría no tenerse ningún tipo de confianza). Los brokers juegan el rol de participar como entidades intermediarias y los comerciantes poseen relaciones a largo plazo con los brokers de la misma forma que lo harían con un banco. La reputación del broker dentro del sistema es un punto importante, ya que resulta vital que asuman su papel según lo establecido con el fin de no perder la confianza del resto de las entidades participantes del sistema.

### 4.3 Modelo de Compra

La Figura 5 muestra un esquema global de las comunicaciones que componen una secuencia de compra de SPEED en el modo normal de operación. Los mensajes 1, 2 y 3, intercambiados entre el cliente y el comerciante, constituyen la fase de negociación del producto. El mensaje 4 contiene el producto cifrado con una clave simétrica generada aleatoriamente por el comerciante, y que será proporcionada al cliente una vez que el pago se haya realizado (mensajes 5 y 6). El broker y el cliente intercambiarán una serie de mensajes adicionales en aquellos casos en los que se haya elegido como medio de pago el monedero electrónico (en la figura estos mensajes están representados por la línea punteada).

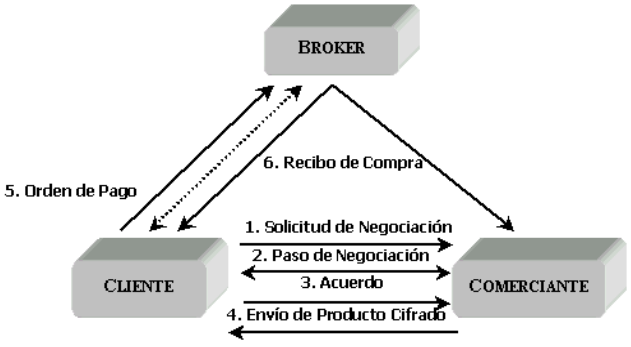


**Figura 5.** Mensajes SPEED del modo normal

## 5 PISCIS como Entorno Real de Comercio Electrónico

El objetivo final del proyecto PISCIS es conseguir un entorno piloto de comercio electrónico que haga uso de los últimos avances en lo que a investigación en la seguridad en las comunicaciones se refiere, y que permita que los usuarios finales puedan tener un ejemplo claro de que un sistema bien desarrollado no tiene por qué crear las reticencias, que sobre todo en el ámbito de seguridad, existen en la actualidad sobre estas arquitecturas de negocio digital.

Para conseguir esto último, los responsables de este proyecto en estrecha colaboración con la empresa proveedora de servicios a través de redes de cable ONO, han definido un entorno completo de pruebas que incluye una conexión entre las redes de ambas instituciones (ver Figura 6), la creación de un portal de comercio y el diseño de un demostrador, conocido como *Gramola Virtual*.

Respecto a la red de pruebas, como se puede apreciar en la figura, se ha establecido una conexión punto a punto entre la Universidad de Murcia y la red privada de ONO. Los servicios principales del piloto se han situado en una red de área local que se encuentra en la universidad, mientras que ciertas aplicaciones como la Autoridad de Certificación permanecen en la red interna de la universidad sin posibilidad de acceso desde el exterior. Los clientes de ONO hacen uso de la red de dicho proveedor para acceder a los servicios de certificación y de adquisición de productos.

En lo referente al portal de comercio, que ya se encuentra disponible dentro de la red de ONO, éste permite que los usuario finales puedan, haciendo uso de su tarjeta inteligente, registrarse como usuarios válidos del sistema, obtener una clave privada y un certificado (a través de las páginas Web de la infraestructura de certificación) y realizar transacciones seguras de comercio para adquirir canciones en formato MP3 mediante el protocolo SPEED, utilizando para ello, o bien el monedero electrónico WG10 o bien la información de la cuenta bancaria (que también está almacenada en el microprocesador de la tarjeta).

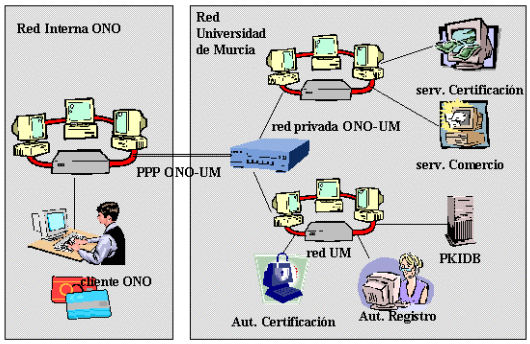


**Figura 6**. Red de comunicaciones del piloto

Por su parte la Gramola Virtual, que se encuentra en fase de implementación, tiene por objetivo actuar como un dispositivo cerrado, disponible en establecimientos de

ocio, como bares y restaurantes, en los cuales los usuarios podrán adquirir las canciones que deseen a través de la red de cable de ONO. Para ello utilizarán su tarjeta inteligente como monedero electrónico y podrán seleccionar de una pantalla plana táctil lo que deseen escuchar. En realidad se trata de una evolución de la clásica gramola.

Con todo ello, lo que se pretende es obtener sistemas finales que se adecuen a las necesidades de cada entorno (venta de música, adquisición de libros, etc.) y, sobre todo, poder recoger la impresión de los usuarios finales en lo que se refiere a facilidad de uso, impresión sobre la seguridad del sistema, etc.

## 6 Conclusiones y vías futuras

En este artículo se han presentado los resultados que hasta ahora se han conseguido en el año y medio que lleva activo el proyecto PISCIS.

Su infraestructura de certificación se caracteriza por ofrecer, además de los servicios básicos de certificación, una serie de características que la hacen ser muy versátil y adaptable a cualquier entorno u organización donde se requiera seguridad en las comunicaciones. De entre estas características destacan sobremanera la utilización de políticas de certificación como base para la gestión de toda la infraestructura, la realización de todas las operaciones de manejo y gestión de certificados desde un navegador y la inclusión de tarjetas inteligentes. En el apartado de nuevos servicios, destacan las implementaciones de OCSP, como protocolo para determinar de forma instantánea el estado de los certificados, SCEP como protocolo para realizar solicitudes de certificados IPsec, y el sistema completo de sellado de tiempo.

Haciendo uso de esta infraestructura de certificación y de tarjetas inteligentes, se ha desarrollado un módulo criptográfico dentro del navegador Microsoft Internet Explorer, y por extensión dentro del sistema operativo Microsoft Windows, que viene a complementar la implementación del estándar PKCS#11 que ya realizó nuestro grupo de investigación en anteriores proyectos. Este módulo criptográfico, conocido como módulo CSP, permite acceder a las distintas funcionalidades criptográficas ofrecidas por la tarjeta inteligente desde aplicaciones Web tales como la interfaz cliente de la infraestructura de certificación o el protocolo de pagos SPEED.

Estos servicios criptográficos ofrecidos por el CSP, se utilizan como base para el protocolo de pagos que se ha diseñado de acuerdo con los requisitos del proyecto. Dicho protocolo, conocido como SPEED, ofrece seguridad, eficiencia, plena integración con monedero electrónico, entrega cifrada del producto y posibilidad de negociación de precios. Su implementación, que está basada en estándares ampliamente aceptados, cuenta también con la posibilidad de trabajar sobre tarjeta de crédito, lo cual da más versatilidad, si cabe, al modelo de comercio desarrollado.

Por último, y con el objetivo en mente de validar toda la arquitectura de negocio que se ha diseñado, se está trabajando en la creación de un entorno de demostración que permita mostrar al usuario final el sistema desarrollado y cuya realimentación conceda a nuestro proyecto un carácter diferenciador frente a otras propuestas que existen en la actualidad.

En lo que respecta a las vías futuras de trabajo, cada una de las líneas individuales en las cuales se ha dividido el proyecto, tiene asociado una serie de temas que, o bien se están tratando en la actualidad, o bien están en fase de pre-análisis con el objetivo de ser abordados en los próximos meses.

En la línea de las infraestructuras de certificación, cabe destacar el trabajo que se está realizando respecto a la posibilidad de incorporar los nuevos sistemas propuestos de certificados de atributo, así como la extensión del sistema para el soporte de doble clave (cada usuario poseería un certificado de firma y otro de cifrado).

En relación con las tarjetas inteligentes, cabe mencionar que se está realizando el estudio (para la posterior integración en el CSP) de nuevas arquitecturas como por ejemplo, sistemas contactless, tarjetas de tercera generación, o tarjetas Java Card [25].

Respecto a los aspectos relacionados con los medios de pago, se está barajando la posibilidad de extender el sistema con el fin de soportar arquitecturas de pago basadas en el nuevo estándar de monedero electrónico CEPS [5].

A todo esto cabe añadir la reciente incorporación al proyecto de dispositivos móviles, como PDAs (Personal Digital Assistant), que con una conexión WLAN y un lector de tarjetas inteligentes PCMCIA permiten reproducir los resultados actuales que se han alcanzado en PISCIS pero en entornos móviles, consiguiendo una primera y acertada aproximación a un entorno de m-commerce.

## Bibliografía


1. C. Adams, P. Cain, D. Pinkas, R. Zuccherato. *Time Stamp Protocol*. IETF draft. draft-ietf-pkix-time-stamp-15.txt, Mayo 2001.
2. ANTS-CIRCuS Web Pages, Grupo de Investigación ANTS-CIRCUS, http://ants.dif.um.es/circus/
3. O. Cánovas, A. F. Gómez y G. Martínez. A PKI Scenario for High-Security Communications: Re-issued Certificates, in *Proc. of the eBusiness and eWork 2000 Conference (EMMSEC 2000)*, Octubre 2000
4. CEN/TC224/WG10, *Inter-sector Electronic Purse, Part 2: Security Architecture*, prEN 1546-2, Enero 1996
5. CEPSCO LLC, *Common Electronic Purse Specifications*, Marzo 1999
6. B. Cox, et al. NetBill security and transaction protocol in *Proceedings of First USENIX Workshop on Electronic Commerce*, 1995
7. CriptoLab Web site, Grupo de Investigación CriptoLab, http://tirnanog.ls.fi.upm.es/
8. S. Dusse, P. Hoffman, B. Ramsdell, J. Weinstein, *S/MIME Version 2 Message Certificate Handling*, Request for Comments (RFC) 2312, Marzo 1998
9. S. Glassman, et al. The Millicent protocol for inexpensive electronic commerce. In *World Wide Web Journal, Fourth International World Wide Web Conference Proceedings*, p. 603-618. O'Reilly, Diciembre 1995
10. R. Housley, W. Ford y D. Solo, *Internet Public Key Infrastructure, Part I: X.509 Certificate and CRL Profile*, Request for Comments (RFC) 2459, Enero 1999
11. ITU-T Recommendation X.690. *ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*, 1995
12. X. Liu et al. *Simple Certificate Enrollment Protocol*. IETF draft. draft-nourse-scep-04.txt, Febrero 2001

13. G. Martínez et al. Providing security to university environment communications, *In Proc. of the TERENA NORDUnet Networking Conference '99*, Lund (Suecia), Junio 1999.
14. Microsoft Corporation, MSDN Library, CryptoAPI Definition
15. Microsoft Corporation, MSDN Library, Cryptographic Service Providers
16. Microsoft Corporation, MSDN Library, Certificate Enrollment Control
17. M. Myers et al. *Online Certificate Status Protocol*, Request For Comments (RFC) 2560, Junio 1999.
18. PC/SC Workgroup, http://www.pcscworkgroup.com
19. R. L. Rivest. Can we eliminate Certificate Revocation Lists? *In Proc. Financial Cryptography '98*. Lecture Notes in Computer Science 1465, 1998
20. R. L. Rivest y A. Shamir. PayWord and MicroMint--Two Simple Micropayment Schemes. *Proceedings of 1996 International Workshop on Security Protocols*, Lecture Notes in Computer Science 1189, p. 69-87, 1996
21. RSA Laboratories, *PKCS #7: Cryptographic Message Syntax Standard* Ver. 1.5, Mayo 1997
22. RSA Laboratories, *PKCS #10: Certification Request Syntax Standard* Ver. 1.7, Mayo 2000
23. RSA Laboratories, PKCS #11: *Cryptographic Token Interface Standard* Ver. 2.10, Diciembre 2000
24. A. Ruiz, G. Martínez, O. Cánovas y A. F. Gómez. SPEED Protocol: Smartcard-based Payment with Encrypted Electronic Delivery, in *Proc. Information Security Conference '01*, Lecture Notes in Computer Science, Octubre 2001, *Aceptado*
25. Sun Microsystems, *Java Card 2.1.1 Specifications*, Mayo 2000