Un sistema de fidelización electrónica basado en el uso de certificados de credencial *

Óscar Cánovas[1], Antonio F. Gómez[2], Antonio Ruiz[2]

[1] Departamento de Ingeniería y Tecnología de Computadores
[2] Departamento de Ingeniería de la Información y las Comunicaciones
Universidad de Murcia, España
ocanovas@ditec.um.es, {skarmeta, arm}@dif.um.es

Resumen La definición de mecanismos de fidelización electrónica es un campo abierto de investigación en el área del comercio electrónico. Desde el punto de vista de las empresas, la fidelización constituye un objetivo clave a la hora de mantener una posición sólida en el mercado. Para ello se han definido varias alternativas, entre las cuales merecen especial atención aquellas basadas en el pago de cuotas de suscripción a grupos de privilegio. En este artículo se presenta un mecanismo distribuido de gestión y aplicación de suscripciones electrónicas basado en el uso de certificados de credencial y sistemas de pago electrónico. Como se verá, la integración de los certificados digitales SPKI/SDSI y del protocolo SPEED permite definir un marco de trabajo capaz de proporcionar soluciones concretas tanto al problema del pago de las cuotas como al disfrute de los privilegios derivados de dichas suscripciones.

1. Introducción

La fidelización de clientes es uno de los principales objetivos de la mayoría de las empresas de cara a asegurar una determinada cuota de mercado. Las empresas buscan consolidar en el tiempo sus comunidades de clientes, lo cual suele repercutir positivamente en ambas partes. Para ello, se han diseñado multitud de fórmulas que tienen como objetivo poner al alcance de los clientes ventajas adicionales respecto al cliente eventual, casi siempre enfocadas al plano económico (descuentos especiales, ofertas, facilidades de pago, etc.). Uno de los mecanismos que más se ha empleado para este tipo de propósitos es la posibilidad de pagar una cuota de suscripción que asocie al cliente a un determinado grupo beneficiario. Dependiendo de la cuota, el cliente disfrutará de un conjunto de ventajas adicionales, las cuales serán mejores cuanto más alta sea la cuota de suscripción.

En este artículo, se expondrá una propuesta que proporciona los mecanismos necesarios tanto para realizar el pago de la cuota de suscripción como para hacer uso de la misma a la hora de comprar de forma electrónica a través de una red de comunicaciones. El sistema está basado en dos componentes principales.

* Financiado por el proyecto TIC2000-0198-P4-04 (ISAIAS) y la aportación de la CARM a través del proyecto 21885 (GIACA)

En primer lugar, se hace uso del protocolo SPEED [RMCG01], desarrollado en el seno de nuestro grupo de investigación, y el cual proporciona los medios necesarios para realizar de forma segura pagos basados en el uso del monedero electrónico, distribuir de forma electrónica el producto solicitado, generar toda la información necesaria para resolver posibles disputas que pudieran surgir en el futuro e intercambiar información relativa a atributos o credenciales de las entidades participantes.

Por otro lado, se ha utilizado la especificación SPKI/SDSI (Simple Public Key Infrastructure / Simple Distributed Security Infrastructure) [EFL+99b] para plasmar las distintas relaciones de pertenencia de los usuarios a los grupos definidos, así como para representar las ventajas derivadas de dicha pertenencia. Tal y como se verá en las siguientes secciones, el uso de SPKI/SDSI permite dotar al sistema de un carácter más descentralizado, el cual lo hace apropiado para entornos de comercio en los cuales no se presuma la existencia de controladores o entidades de confianza globales. Además, es capaz de representar de forma bastante fiel las características de los modelos RBAC [SCFY96] (Role Based Access Control), los cuales pueden ser aplicados con éxito para modelar los sistemas de suscripción.

El artículo está estructurado de la siguiente forma. En la sección 2 se realiza una breve descripción de las características del protocolo SPEED, especialmente de aquellas cuestiones relacionadas con su integración con los certificados de credencial. La sección 3 presenta los principales detalles de la especificación SPKI/SDSI, tales como los tipos de certificados, la reducción de autorizaciones y las posibilidades para la gestión del ciclo de vida. A continuación, la sección 4 expondrá tanto el modelo general de suscripción como los detalles relativos a la implementación del entorno de prueba basado en dicho modelo. Finalmente, el artículo presenta algunas de las conclusiones derivadas de este trabajo.

2. El protocolo 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 [MR02] han demostrado ser lo suficientemente seguras y flexibles, si bien no han alcanzado un alto grado de adopción en mercados reales.

En general, hay un conjunto de características de seguridad que debería reunir un protocolo de pago de cara a poder ser utilizado en un escenario real de comercio electrónico. Entre dichos requisitos se encuentra la siguiente lista:

- El 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 protocolo debe estar basado en estándares de seguridad reconocidos. Este requisito incrementa la sensación de seguridad percibida por los usuarios, y garantiza un diseño basado en propuestas debatidas y probadas por la comunidad científica.
- 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.

Aunque algunos de estos requisitos ya habían sido satisfechos por algunas de las propuestas ya existentes, con el fin de proporcionar una respuesta común a todos ellos se definió 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 para tarjeta inteligente con entrega cifrada de bienes. Aunque la información en detalle del protocolo puede encontrarse en [RMCG01], en esta sección haremos una breve descripción de sus características principales, participantes y modelo de compra.

2.1. Visión general

Una transacción SPEED transfiere bienes electrónicos desde un vendedor a un cliente, debitando el monedero electrónico del cliente e incrementando el saldo de la cuenta del vendedor por el valor del 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.

Su diseño se basa en el uso de estándares como ASN.1 [ITU95] para la especificación de la estructura de los mensajes, PKCS#7 [Lab97] como formato criptográfico para el intercambio de información protegida, certificados X.509v3 [HPFS02] para la identificación de los participantes en el escenario de compra y WG10 [CEN96] como sistema estándar de monedero electrónico.

2.2. Participantes

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 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.

Cada participante de SPEED (clientes, comerciantes y broker) poseerá una clave privada RSA y un certificado X.509. 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.

2.3. Modelo de compra

La figura 1 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 intercambian una serie de mensajes adicionales destinados a realizar el proceso de decremento del monedero electrónico (en la figura estos mensajes están representados por la línea punteada). Todas las comunicaciones están protegidas frente a ataques de entidades externas haciendo uso de criptografía simétrica principalmente.

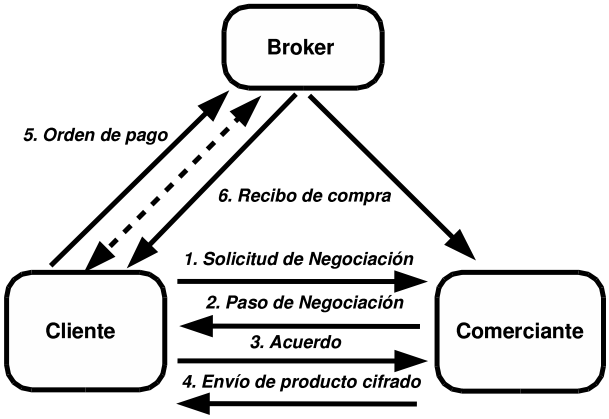

Figura 1. Modelo de compra de SPEED

A la hora de emplear este protocolo como componente de un sistema de suscripción electrónica, es importante analizar en detalle el formato del primer mensaje del protocolo (*NegotiationRequest*), el cual está encuadrado dentro de

la fase de negociación del precio del producto. Se trata de un mensaje firmado digitalmente que el cliente envía al vendedor para preguntar o proponer el precio de un determinado producto. Su estructura es la siguiente:

1 C $\Rightarrow$ V *NegotiationRequest* $\{\{NID, SeqN, ProductID, [Price], VendorID, EnKey, SignKey, Flag, Credential\}_{C^{-1}}\}_V$

Entre todos los campos que forman este mensaje, son de especial interés para esta sección los relacionados con la descripción del producto (*ProductID*), el precio (*Price*) y las credenciales (*Credential*):

- *ProductID (Product Identifier)*. Se trata de una cadena de octetos que representa al producto a comprar. Es totalmente dependiente del entorno de aplicación en el cual se encuentre ubicado el protocolo, y en este caso concreto servirá tanto para designar a los certificados de suscripción como a los productos finales a comprar.
- *Price*. Es el precio que el cliente está dispuesto a pagar por el producto. Se trata de un elemento opcional ya que es posible que el cliente no conozca de antemano el precio.
- *Credential*. Durante el proceso de diseño del protocolo SPEED ya se consideró la posibilidad de proporcionar un soporte especial que permitiera realizar la transmisión de información relativa a credenciales como parte del protocolo. El propósito genérico de este tipo de información era la modificación de la estrategia de negociación del proveedor, un cambio de estrategia que implicara ciertas ventajas para el cliente. Dicha información se incluye dentro del campo *Credential* y su formato concreto es totalmente transparente para el protocolo ya que éste sólo se encarga de transmitir la información sin interpretar su estructura.

Tal y como se verá más adelante, el uso de estos campos del protocolo permitirá diseñar tanto el escenario de solicitud de suscripción como el de disfrute de la misma. El resto de los campos así como de los mensajes del protocolo son totalmente independientes del mecanismo aquí presentado.

3. Certificados digitales SPKI/SDSI

La especificación SPKI/SDSI es el resultado de la unión de dos propuestas surgidas de forma independiente a mediados de la década de los noventa. Tanto el sistema SDSI (Simple Distributed Security Infrastructure) propuesto por Rivest et al. [RL] como la especificación SPKI (Simple Public Key Infrastructure) propuesta por Ellison et al. [EFL+99b], supusieron en su momento una ruptura drástica respecto a la filosofía del modelo X.509, principalmente en lo que se refería tanto al esquema de asignación de identidades como a la posibilidad de emplear los certificados también con fines de autorización. Si bien no han sido las únicas propuestas surgidas en materia de certificación de autorización, otros ejemplos son KeyNote o SAML, su unión si se ha consolidado como la alternativa más empleada a la hora de construir sistemas de control de acceso para diversos tipos de escenarios.

3.1. Tipos de certificados SPKI/SDSI

SPKI/SDSI define tres tipos de certificados diferentes, los cuales contienen al menos un emisor y una entidad receptora (subject), y pueden especificar periodos de validez, información de autorización e información de delegación.

El primer tipo de certificado SPKI/SDSI es el de identidad o nombramiento, el cual puede ser empleado para varios propósitos. Desde el punto de vista del trabajo presentado en este artículo, el uso más interesante es el de mecanismo de definición de grupos de usuarios. La creación de un grupo se consigue mediante la emisión de varios certificados que asocian el mismo nombre a distintos usuarios.

Los otros dos tipos de certificados, los de atributo y los de autorización, poseen estructura similar [EFL+99a], ya que la principal diferencia se encuentra en el campo *subject*, el cual puede referenciar a un usuario (certificado de autorización) o a un nombre (certificado de atributo). Los certificados de autorización se emplean para asignar privilegios directamente a claves, mientras que los certificados de atributo son útiles para asignar privilegios a grupos de entidades, lo cual encaja completamente en el escenario que se verá en la sección 4.

3.2. Cálculo de autorizaciones

Por cálculo de autorizaciones se hace referencia al método mediante el cual se determina si una solicitud satisface una política concreta. Hay que tener en cuenta que dicha determinación no es evidente, y no se limita a constatar simplemente que el usuario que presenta la solicitud de acceso al recurso está reflejado directamente en la política. El método debe ser capaz de resolver los casos en los que la clave del solicitante no aparezca listada explícitamente en la política, como cuando el acceso está basado en la pertenencia a un grupo determinado o en cadenas de delegación (o incluso en ambas cosas a la vez). Las políticas de autorización suelen representarse como listas de control de acceso (ACLs), las cuales son similares a los certificados, aunque no necesitan campos de emisor o firmas (puesto que se suponen que están controladas localmente por el poseedor del recurso al cual se le está controlando el acceso).

El proceso de cálculo de autorización es complejo. Los certificados de identidad pueden componerse para derivar nuevos nombres, y los certificados de autorización pueden combinarse a su vez para derivar nuevas autorizaciones, y ambos pueden emplearse para deducir nuevas autorizaciones a nombres. El procedimiento seguido, ampliamente expuesto en [Eli98], puede resumirse como la búsqueda en un grafo dirigido de un camino de certificación que tenga como nodo inicial la política de seguridad del sistema, y como nodo final la clave pública asociada al usuario que está realizando la solicitud. La construcción de dicho grafo está basada en el mecanismo de reducción de certificados expuesto en [EFL+99b].

3.3. Gestión del ciclo de vida de los certificados

Si bien la especificación SPKI/SDSI ha sido empleada con éxito en varios escenarios de aplicación distintos, la gestión de los certificados digitales, es decir,

la forma en la que los usuarios solicitan los certificados de autorización, el medio por el cual se distribuyen, o la política de autorización seguida para tal efecto suele ser dependiente del sistema y está implementada de forma demasiado sencilla y no distribuida. Aunque este enfoque puede funcionar correctamente en determinados escenarios, entornos más complejos pueden sacar a relucir ciertas carencias en materia de escalabilidad o interoperabilidad.

Conscientes de este hecho, nuestro grupo de investigación ha desarrollado un sistema para la gestión distribuida de certificados SPKI denominado DCMS (Distributed Credential Management System). DCMS [CG02] define cómo deben expresarse las solicitudes de certificación, proporciona mecanismos para satisfacer las distintas políticas de seguridad, identifica las entidades involucradas en un escenario de certificación y cómo dichas entidades pueden intercambiar información relativa a autorización. Aunque su explicación está fuera del ámbito de este artículo, es importante dejar constancia de que sus mecanismos han sido utilizados a la hora de poner en marcha el sistema de suscripción electrónica.

4. Diseño e implementación de la suscripción electrónica mediante certificados de credencial

El sistema de suscripción electrónica que se propone en este artículo tiene como base los componentes ya comentados en las secciones anteriores. Por un lado, el protocolo de pago SPEED que además de ofrecer características de seguridad, presenta la posibilidad de soportar la transmisión de credenciales. Por otro lado, la especificación SPKI/SDSI, así como el sistema de gestión DCMS, proporcionan los mecanismos necesarios para la creación y manejo de credenciales tanto de autorización como de nombramiento. En esta sección, se describe tanto un modelo general de suscripción electrónica, señalando los puntos donde estos componentes intervienen, como un escenario piloto aplicado al campo de la venta de billetes electrónicos de avión.

4.1. Modelo general de suscripción electrónica

El escenario de suscripción electrónica realizado está basado en la existencia de varias categorías de suscripción, gestionadas posiblemente por entidades distintas, y varios proveedores de servicios que ofrecen ventajas económicas a los suscriptores, las cuales variarán dependiendo del tipo de suscripción. Tal y como se muestra en la figura 2, los distintos proveedores de contenidos y servicios mantienen una relación de colaboración con los diferentes gestores de suscripciones. Los términos de dicha colaboración especificarán qué tipo de ventajas aplicará el proveedor a aquellos miembros de alguno de los grupos que controla el gestor (descuentos en algunos de sus productos, facilidades de pago, regalos, etc.).

Los usuarios finales tienen dos puntos de conexión con el sistema de suscripción. Por un lado deberán pagar la cuota correspondiente y obtener el justificante

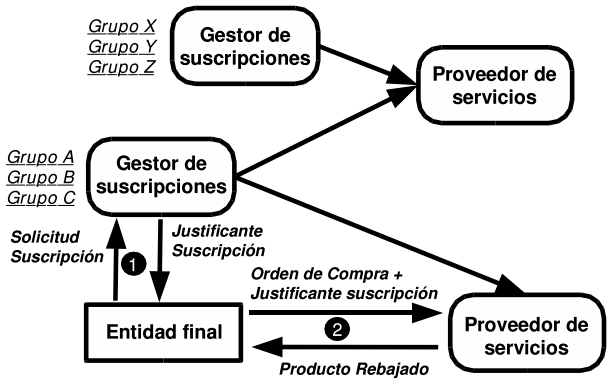

Figura 2. Modelo de suscripción electrónica

de suscripción. Por otro lado, deberán transmitir dicho justificante junto con cada solicitud de compra realizada a alguno de los proveedores relacionados con el grupo de suscripción.

Solicitud de suscripción La solicitud de suscripción se realiza a través del protocolo SPEED. Dado que dicho protocolo fue diseñado especialmente para el pago de productos digitales, es posible especificar cuál es el grupo concreto al cual se desea pertenecer, realizar el pago correspondiente y obtener el justificante de suscripción.

En relación con lo visto en la sección 2, la especificación del grupo está contenida en el campo *ProductID* del mensaje *NegotiationRequest*, el cual contendrá una s-expresión de tipo *issuer* [EFL$^+$99a] con la clave pública del gestor de suscriptores y el identificador del grupo. La suscripción, cuyo precio está especificado en el campo *Price*, podría estar sujeta al cumplimiento de ciertas condiciones de autorización (por ejemplo, ser mayor de edad, tener crédito disponible o cualquier otro criterio dependiente del entorno). En dicho caso, las evidencias necesarias para demostrar la posibilidad de ingreso en el grupo podrían transmitirse en el campo *Credential*.

Una vez que el broker transmite el recibo, el usuario final puede descifrar el justificante de suscripción, el cual recibió como parte del cuarto mensaje del protocolo. Dicho justificante estará representado mediante un certificado SPKI de identidad, el cual ligará la clave pública del usuario con el grupo de suscripción, todo ello durante el periodo de tiempo en el cual sea efectiva dicha asociación.

El uso de certificados digitales permite descentralizar el sistema puesto que no es necesario mantener almacenadas de forma central todas las relaciones existentes entre los usuarios del sistema y los grupos. En contraposición, la información de suscripción puede ser transmitida por los propios usuarios a la hora de realizar sus compras y será considerada válida por aquellas entidades que tienen una relación de confianza con la entidad emisora.

Presentación de justificantes Tras la adquisición del justificante, el usuario final puede proceder a la compra de los productos de alguno de los proveedores de servicios con los cuales tenga acuerdos el gestor de suscripciones. La descripción de dichos productos se incluirá en el campo *ProductID* del primer mensaje.

Por otro lado, haciendo uso del campo *Credential* del mensaje *Negotiation-Request*, el cliente puede transmitir al proveedor el justificante de suscripción, es decir, el certificado de identidad SPKI que le asocia a un determinado grupo. Una vez que el proveedor recibe el certificado, verifica su estado y determina la reducción en el precio del producto que ha sido solicitado. Dicha reducción depende del acuerdo establecido entre el proveedor y la entidad gestora de las suscripciones, el cual especificará el conjunto de productos afectados, los porcentajes de descuento u otras medidas favorecedoras, y el periodo de tiempo durante el cual permanecerá en vigor. En concreto, los proveedores de contenido actúan como autoridades de autorización, emitiendo certificados SPKI de atributo que especifican los acuerdos de los cuales se pueden beneficiar aquellos usuarios pertenecientes al grupo de suscriptores al que hace referencia el certificado. Dichos certificados pueden emplearse como prueba de los acuerdos alcanzados entre las entidades del sistema, lo cual es especialmente útil a la hora de decidir el grupo de suscriptores al cual se desea pertenecer.

4.2. Implementación del modelo para la compra de billetes de avión

En la vida cotidiana estamos acostumbrados a emplear sistemas de suscripción que ofrecen a los usuarios el pertenecer a un determinado colectivo a cambio de una serie de beneficios. Con esta vinculación al grupo, no sólo el usuario sale beneficiado, puesto que el proveedor obtiene beneficios derivados de la fidelización de los usuarios. Como ejemplo podríamos pensar en la tarjeta donde acumulamos los puntos de las compras realizadas en nuestro supermercado habitual.

El modelo ya presentado es el marco general sobre el cual se pueden definir sistemas de este tipo. Con el fin de mostrar su aplicabilidad a un posible entorno real implementamos un sistema de venta de billetes de avión que será descrito en los siguientes apartados.

Escenario de prueba En el entorno diseñado, las agencias de viajes ofrecen a sus clientes la suscripción a distintos grupos a cambio de una tasa que varía en función del grupo. Las diferentes categorías de suscripción son: *oro*, *plata* y *joven*. La pertenencia al grupo *oro* dará mejores privilegios que cualquier pertenencia a otro grupo, sin embargo, la cantidad a satisfacer por pertenecer al grupo será mayor. En este caso, los privilegios consisten en el descuento de un porcentaje preestablecido sobre el precio del billete de un vuelo en una determinada compañía aérea.

Por otro lado, cada compañía aérea ofrece la venta electrónica de billetes, pudiéndose presentar las credenciales de pertenencia al grupo de una agencia con el fin de obtener un descuento sobre el precio del billete.

Para facilitar a los usuarios la gestión y almacenamiento de las credenciales y los billetes electrónicos, se ha incorporado el uso de tarjetas Javacard [Mic03] y se han desarrollado distintos applets. Al permitir que tanto los certificados de autorización como los tickets electrónicos sean almacenados en la tarjeta, se proporciona al usuario movilidad para poder emplear distintos terminales.

Suscripción a una agencia de viajes Tanto la suscripción como la adquisición de billetes se realiza vía Web. Una vez que el usuario elige la agencia y la categoría, se muestra un página con un ActiveX firmado que se instala en la máquina del usuario. Este software permite al usuario visualizar la información contenida en los distintos certificados que indican los acuerdos a los que ha llegado la agencia con las distintas compañías aéreas. Los tags de dichos certificados de atributo expresan las características del vuelo así como el porcentaje de descuento a aplicar (un ejemplo aparece en la figura 3).

```
(tag
  (speedki
    (description
      (destination (europa/londres))
      (category (*))
      (season (*))
      (type (Regular)))
    (reduction
      (percentage (10))))
)
```

Figura 3. Tag de un certificado de atributo

Si el usuario decide hacer efectiva la suscripción al grupo, entonces tendrá lugar el inicio del protocolo SPEED que conduce al pago y la posterior obtención de un certificado de pertenencia al grupo. Aquí el gestor de suscripciones actúa, por un lado, como vendedor ya que recibe el pago por un producto que es un certificado y, por otro lado, actúa como autoridad de nombramiento al emitir un certificado que liga una determinada clave pública con un grupo de usuarios. Cuando el usuario recibe el certificado de identidad como consecuencia del pago, el ActiveX lo almacenará en la tarjeta inteligente y, opcionalmente, podrá también guardar los certificados de atributo correspondientes al grupo.

La estructura genérica de la s-expresión de un certificado de pertenencia a un grupo que se obtiene como resultado del pago es la mostrada en la figura 4.

Compra de billetes La compra de billetes de las distintas compañías se realiza también vía Web. Una vez el usuario elige la compañía con la que desea volar, se le muestran los vuelos disponibles. La elección del vuelo dará paso a la descarga de un ActiveX firmado de funcionalidad similar al ya comentado. En él se muestra la información referente al vuelo: compañía aérea, destino, tipo de vuelo, precio inicial, fechas y horas disponibles. Una vez el usuario ha elegido un vuelo concreto, se inicia la fase de pago que, en primer lugar, implica la obtención del certificado de identidad y los certificados de atributo de la tarjeta. A

```
(cert
  (issuer (name <agency-key> <group>)
  (subject <user-key>)
  (valid
    (not-before (<date>))
    (not-after (<date>)))
)
```

Figura 4. S-expresión del certificado de pertenencia a grupo

continuación, se elige, en función del tag con las características del vuelo, aquel certificado de identidad que proporcionará un mayor descuento en la compra. Estos certificados serán enviados en el campo *Credentials* del mensaje *NegotiationRequest* del protocolo. En el campo *ProductID* se envía la solicitud de compra de ticket para un vuelo en forma de s-expresión tal y como aparece en la figura 5.

```
(tag
  (speedki
    (description
      (destination (europa/londres))
      (category (business))
      (season (summer))
      (type (regular)))
    (reduction
      (percentage (*))))
  )
  (date (30/11/2003))
  (time (10:40))
)
```

Figura 5. Ejemplo S-expresión del certificado de pertenencia a grupo

El servidor, una vez que recibe el mensaje, realiza las verificaciones relacionadas con el billete solicitado y emplea el algoritmo de cálculo de autorización para determinar el descuento que se debe de aplicar. Si finalmente el usuario está de acuerdo con el precio final, se continúa con la ejecución del protocolo SPEED para obtener el billete solicitado, representado también mediante una s-expresión y firmado digitalmente por la compañía emisora.

Finalmente, el Activex almacena este ticket electrónico en el applet correspondiente con el fin de que el usuario pueda presentarlo posteriormente como ticket de embarque en el vuelo deseado.

5. Conclusiones obtenidas

Uno de los principales criterios de diseño del protocolo SPEED fue la posibilidad de ofrecer un mecanismo de negociación del precio de los productos que formara parte del propio protocolo, lo cual permitiría emplearlo en escenarios

basados en entidades mediadoras y gestionar comunidades con distintas prioridades. Respecto a este último aspecto, el uso de certificados de credencial ha permitido introducir de forma estructurada un servicio de fidelización que aprovecha parte de la funcionalidad ofrecida por el protocolo.

Como se ha podido comprobar, la integración de ambos elementos permite llegar a la definición de modelos generales de suscripción descentralizada, los cuales pueden adaptarse a entornos concretos mediante especificación del conjunto de grupos y privilegios que formarán parte del sistema. Además, la implementación desarrollada ilustra las posibilidades reales de implantación de este tipo de sistemas en entornos tan usuales como el de la compra de productos vía Web.

Referencias

[CEN96] CEN. *Inter-sector Electronic Purse, Part 2: Security Architecture*, 1546 edition, January 1996.

[CG02] O. Cánovas and A. F. Gómez. A Distributed Credential Management System for SPKI-Based Delegation Systems. In *Proceedings of 1st Annual PKI Research Workshop*, pages 65–76, 2002.

[EFL+99a] C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, and T. Ylonen. *Simple Public Key Certificate*. IETF Internet Draft, draft-ietf-spki-cert-structure-06.txt edition, July 1999.

[EFL+99b] C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, and T. Ylonen. *SPKI certificate theory*, September 1999. Request For Comments (RFC) 2693.

[Eli98] J. E. Elien. Certificate discovery using SPKI/SDSI 2.0 certificates. Master's thesis, M.I.T., May 1998.

[HPFS02] R. Housley, T. Polk, W. Ford, and D. Solo. *Internet Public Key Infrastructure, Part I: X.509 Certificate and CRL Profile*, April 2002. Request for Comments (RFC) 3280.

[ITU95] ITU-T. *ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*, 1995. Recommendation X.690.

[Lab97] RSA Laboratories. *PKCS#7: Cryptographic Message Syntax Standard Ver 1.5*, May 1997.

[Mic03] Sun Microsystems. *Java Card 2.2 Application Programming Interface*. World Wide Web, http://java.sun.com/products/javacard/specs.html, February 2003.

[MR02] S. Micali and R. L. Rivest. Micropayments revisited. In *Proceedings of the Cryptographer's Track at the RSA Conference 2002*, volume 2271 of *Lecture Notes in Computer Science*, pages 149–163. Springer, 2002.

[RL] R. Rivest and B. Lampson. *SDSI: A simple distributed security infrastructure*.

[RMCG01] A. Ruiz, G. Martinez, O. Canovas, and A. F. Gomez. SPEED Protocol: Smartcard-Based Payment with Encrypted Electronic Delivery. In *Proceedings of 4th Information Security Conference*, volume 2200 of *Lecture Notes in Computer Science*, pages 446–461. Springer, 2001.

[SCFY96] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman. Role-based access control models. *IEEE Computer*, 29(2), February 1996.