Un sistema versátil de pagos electrónicos para un servicio remoto de apuestas

Ana Isabel González-Tablas, Javier Carbó

Resumen

En este artículo se proponen una serie de mecanismos para asegurar el proceso de cobro electrónico de una apuesta premiada al tiempo que pretende reflejar fielmente las peculiaridades que este tipo de pago requiere. Las apuestas involucran un tipo de transacción comercial que difiere de los protocolos clásicos de pago electrónico en algunos aspectos sustanciales. Fundamentalmente, el mecanismo de cobro de apuestas premiadas puede ser muy diferente en función de la cuantía del premio. Además, la proliferación de peñas que comparten la propiedad de la apuesta puede complicar aún más el mecanismo de cobro. Por último, la naturaleza periódica de estas apuestas también afecta a la solución propuesta. La complejidad de las situaciones que pueden darse requiere de la combinación de distintas formas de pago. Nuestra contribución consiste en un sistema versátil que describe el protocolo a seguir por cada una de las partes en función de las circunstancias que afrontan, sin descuidar los problemas de eficiencia que pueden surgir.

Palabras Clave: Comercio Electrónico, Protocolos Criptográficos.

1 Introducción

Las comunicaciones electrónicas a través de la red Internet permiten una rápida disponibilidad de una ingente cantidad de información en poco tiempo y con independencia de su situación geográfica. La popularización de este medio de comunicación, inicialmente pensado para otros fines, llevó a un uso comercial del mismo. Numerosos servicios y productos están ya a la venta a través de esta red. Un servicio de apuestas electrónicas puede, así mismo, beneficiarse de las ventajas que Internet proporciona.

Las transacciones y el proceso que debe incluir un servicio de apuestas (tanto electrónico como físico), tienen unas características específicas de esta actividad que deben tenerse en cuenta a la hora de dar este servicio con medios electrónicos. El objeto de las apuestas puede ser de lo más variado, y no tiene porqué ser relevante en el proceso más que por el carácter periódico que suelen tener. El tiempo es pues, un factor importante a la hora de aceptar un pronóstico sin que ningún apostante adquiera una posición de ventaja. El plazo del que se dispone para reclamar los premios también suele estar restringido.

Al hacer efectiva una apuesta, los apostantes en su gran mayoría realizan un pago de escasa cuantía y con dinero en metálico. En el establecimiento autorizado se le entrega un resguardo donde figura el pronóstico en el que el apostante confía. Este resguardo se presentará como prueba en el caso de que la apuesta resulte premiada. En el establecimiento autorizado se guarda también constancia del pago y del pronóstico efectuado.

En el caso de que el premio que corresponda a la apuesta sea de considerable valor, el propietario del resguardo ha de identificarse para cobrar el premio. En otro caso (cuando el premio es de una cuantía limitada) se entrega el premio de forma anónima, siendo suficiente la presentación del correspondiente resguardo.

Cuando múltiples apostantes acuerdan presentar un pronóstico en común, el precio de la apuesta suele ser más elevado, y el premio, en caso de un pronóstico acertado, debería dividirse entre los apostantes que actuaron conjuntamente. Aunque esta división suele ser un proceso independiente de la ejecución de la apuesta, se generan de esta forma conflictos al actuar ilegítimamente el depositario del resguardo.

Estas peculiares características de las apuestas son las que pretendemos emular de forma electrónica en el presente documento. A continuación describiremos brevemente algunas de las más representativas formas de pago electrónico y sus rasgos más relevantes. Finalizaremos presentando nuestra propuesta.

2 Formas de pago electrónico

El área de la Seguridad de la Información ha dedicado un considerable esfuerzo a la protección de las comunicaciones. Estas comunicaciones siguen un protocolo que describe la secuencia y contenido de los mensajes a intercambiar. Un protocolo, sea cual sea su intención en la comunicación, puede proporcionar ciertos servicios de seguridad: autenticación, integridad, confidencialidad y no repudio [1]. Habitualmente los protocolos se clasifican por su finalidad: de distribución de claves, de autenticación, de transacción, etc. Y las transacciones constan típicamente de tres comunicaciones: reintegro, pago y depósito. La traslación electrónica de estas comunicaciones forma un sistema de pago electrónico.
La clasificación más común atiende al mecanismo de pago del mundo real que pretende emular (cheques, tarjetas de crédito, dinero en metálico, de uso restringido, etc.). Los sistemas de pago electrónico también se pueden clasificar por otras características, fundamentalmente: su modo (prepago, al instante, a crédito), su ámbito (universal, propietario) o por los medios físicos que utiliza (con/sin dispositivos a prueba de manipulaciones).
Usualmente estos dispositivos físicos se denominan tarjetas inteligentes porque además de almacenar y proteger el acceso a determinada información (p.e. claves), tienen una cierta capacidad de proceso. Estas tarjetas almacenan un contador que representa al dinero que posee el usuario. Este tipo de pagos necesita de un dispositivo lector adicional, lo que encarece notablemente su uso extensivo.
Los pagos cuya seguridad no reside en la posesión física de un determinado dispositivo basan la protección y autenticación del dinero mediante criptografía de clave pública. Esto ocurre tanto en los pagos basados en el envío del nº de tarjeta de crédito (SSL [2] y SET [3]), como en los basados en cheques electrónicos (NetBill [5] y NetCheque [6]). Los principales inconvenientes del uso de cifrado asimétrico

residen en la ausencia de anonimato y en el tiempo de proceso que requieren. La primera de estas desventajas trató de paliarla David Chaum con ecash [7]. Sin embargo, el mecanismo para firmar a ciegas que utiliza esta forma de pago presenta algunas limitaciones [8] [9].
Únicamente los micropagos (pe. Payword y Micromint [4]) no se basan en dispositivos físicos ni en cifrado asimétrico, pero la seguridad asociada está comprometida hasta el punto de que su uso es inviable cuando la cantidad a transferir es mínimamente significativa.

3 Nuestro sistema de pagos electrónicos dedicado a las apuestas

3.1 Desiderata

Por desgracia ninguna de estos mecanismos de pagos electrónicos puede por sí solo reflejar el proceso de pago implícito en un sistema de apuestas. Un sistema de pago electrónico dedicado a las apuestas debe conseguir:

1. Realizar apuestas y cobrar premios de forma remota.
2. Retirar y/o modificar la apuesta durante el tiempo permitido por la organización de apuestas previo a la ocurrencia de la circunstancia que es objeto de apuesta.
3. Proteger el anonimato del apostante excepto con grandes premios.
4. En el caso del cobro de un premio de gran valor, se requerirá revelar la identidad del apostante.
5. En caso de pérdida del resguardo, el apostante podrá comprobar si su apuesta ha resultado premiada tras haberse identificado.

Además el sistema debe cumplir con los siguientes requisitos:

a) **Integridad de los resguardos electrónicos**. El sistema debe evitar la alteración de los datos de la apuesta realizada.

b) **Autenticación del apostante y el cobrador como la misma persona**. El sistema debe evitar el uso fraudulento de copias de resguardos por personas distintas del apostante. Un estafador no debe poder cobrar el premio de una apuesta que no pronosticó ni pagó.

c) **Protección de la intimidad**. El sistema debe proteger el anonimato del apostante tanto en los pagos como en los cobros de escasa cuantía.

d) **Compartición de secretos**. El sistema debe permitir la realización de apuestas por parte de coaliciones de apostantes o peñas.

3.2 Condiciones iniciales y finales

La organización de apuestas obtendrá un certificado digital que la acredite de una Autoridad de Certificación confiable, y establecerá una relación con dicha AC (posiblemente una entidad financiera) para que emita tarjetas inteligentes a prueba de manipulaciones a petición de los futuros apostantes de esa temporada.
Previamente al comienzo de la temporada de apuestas establecida, el apostante deberá solicitar una tarjeta a la AC. Para obtener la tarjeta, el solicitante se deberá presentar personalmente ante la AC, quien comprobará la identidad del solicitante así como el número de su cuenta bancaria a la cual irá asociada la tarjeta de apuestas.
Por supuesto, las claves públicas de la organización de apuestas y de la AC serán de conocimiento público, y disponibilidad libre y gratuita. Así mismo, las claves de los apostantes caducarán una vez termine la temporada de apuestas para las que fueron emitidas.
La tarjeta de apuestas se podrá cargar en cualquier momento en un estanco con dinero pagado en metálico. Esta operación quedará registrada mediante la actualización de un contador.

3.3 La apuesta y el resguardo

La apuesta se compondrá de los siguientes campos:

a) **Datos de la apuesta**. Éstos serán la jornada, los pronósticos y el precio.

b) **Identidad del apostante**. Ésta será el número de cuenta bancaria del apostante cifrada con la clave pública de la AC.

c) **Resumen del desafío**. El apostante genera el resumen de un número aleatorio (desafío) con el que demostrará ser el legítimo dueño de la apuesta para comprobar si resultó premiada y para cobrar el premio en el caso de ser de escasa cuantía.

d) **Seudo-firma de la apuesta**. El apostante generará un resumen de los campos anteriores y los cifrará simétricamenta con su única clave almacenada en la tarjeta.

El resguardo de la apuesta comprenderá el desafío, la apuesta y un sello de tiempos que emitirá la organización de apuestas sobre la apuesta recibida. El desafío lo utilizará la organización de apuestas para comprobar si ese boleto resultó premiado. La apuesta junto con el sello de tiempos servirán para asegurar no repudio del receptor, es decir, se podrán utilizar como prueba ante terceros si se produjese el impago de un premio.

3.4 Los protocolos

A continuación veremos en detalle cada una de estas comunicaciones.

3.4.1 Solicitud de apuesta

El apostante realiza el pronóstico de la jornada mediante un formulario disponible en una página Web que calcula el precio y codifica esta información para introducirla en la tarjeta del apostante. A continuación se descuenta el precio de la apuesta del dinero almacenado en la tarjeta de apuestas y la tarjeta genera el número aleatorio que servirá de desafío y realiza un resumen de él. Después la tarjeta añade a la apuesta su identidad cifrada con la clave pública de la Autoridad de Certificación. Ésta estaba previamente calculada y almacenada en la tarjeta. Y por último la tarjeta realiza un resumen de toda la información anterior y lo cifra simétricamente con su clave única almacenada en la tarjeta de apuestas. Formalmente, quedaría:

$$H\{Desafio\}, Apuesta, \{H\{H\{Desafio\}, \{Identidad\}PK_{AC}\}\}K_{tarjeta}$$

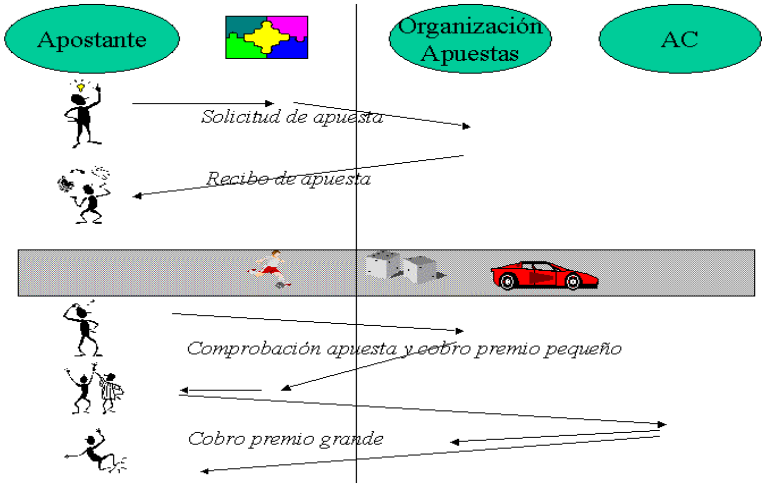

Figura 1: Un esquema de los protocolos

3.5 Recibo de apuesta

La organización de apuestas emite un sello de tiempo sobre la información recibida que se envía al apostante como respuesta.

3.5.1 Solicitud de comprobación de apuesta

El apostante envía el resumen de su desafío junto con su desafío a la organización de apuestas.

3.6 Respuesta a comprobación de apuesta

La organización de apuestas buscará la apuesta cuya comprobación se solicita en la base de datos de apuestas indexada mediante el resumen del desafío. Después, la organización verifica el resumen del desafío. Luego, la organización comprobará

si esa apuesta ha resultado premiada y comunicará el resultado al apostante. Entonces, en el caso de haber sido premiada la apuesta con una cantidad reducida, la organización enviará un mensaje cifrado con su propia clave privada a la tarjeta del apostante. Esta interpretará este mensaje como un incremento del saldo asociado correspondiente a la cantidad premiada.

3.6.1 Solicitud de cobro de un premio de gran cuantía

El apostante envía a la Autoridad de Certificación la comunicación de apuesta premiada de la organización de apuestas que incluye el resguardo de la apuesta premiada.

3.6.2 Respuesta a cobro de un premio de gran cuantía

Primero, la Autoridad de Certificación verifica la firma de la organización sobre el resguardo. Luego la Autoridad de Certificación descifra la identidad del apostante. Después la AC comprueba la firma digital de la apuesta utilizando la clave pública corrspondiente a la clave privada almacenada en la tarjeta de apuestas. Entonces, la AC ingresa la cuantía del premio en la cuenta bancaria del apostante. La AC, por último, comunica la identidad del apostante a la organización de apuestas.

3.7 El caso de la coalición de apostantes (las peñas)

Cada peña habrá nombrado un delegado o gestor de la peña que se encargará de realizar la apuesta común de la peña. Es a este gestor a quien cada participante envía su identidad cifrada con la clave pública de la Autoridad de Certificación. Posteriormente, cada apostante debe comprobar que tanto su pronóstico como su identidad cifrada están contenidas en el resguardo sellado por la organización de apuestas, que el gestor debe enviar a cada miembro.
En este caso los miembros de la peña confían en el gestor para cobrar premios de pequeña cuantía. Un desafío común, generado por el gestor de la peña, permite que el gestor cobre el premio. Al igual que con el pronostico y su identidad cifrada, cada miembro de la peña debe comprobar que el resumen del desafío que incluye el resguardo sellado se corresponde con el que envió el gestor.

En el caso de premios pequeños se justifica que los miembros de la peña confien en el gestor. En caso de obtener un premio cuantioso, no se debería permitir que el gestor cobre todo el premio, y en su lugar se requiere que cada miembro de la peña cobre su parte del premio.

4 Conclusiones

La protección de las transacciones económicas juega un papel fundamental en el desarrollo de cualquier actividad comercial y las apuestas no son una excepción. En este artículo hemos observado que las características específicas de los pagos involucrados en las apuestas no se ajustan a ninguno de los distintos sistemas de pago electrónico conocidos.
Por esta razón la combinación de mecanismos criptológicos propuestos en este trabajo forman un sistema de pago electrónico que se adapta al funcionamiento real de las apuestas de una forma segura y eficiente.

Referencias

[1] National Institute of Standards and Technology, Agency Use of Public Key Technology for Digital Signatures and Authentication, *National Institute of Standards and Technology Special Publication*, **25** (2000).

[2] A. Freier, P. Karlton y P. Kocher, *The SSL Protocol version 3.0 Internet Draft*, Netscape Communications Corporation, http://home.netscape.com/eng/ssl3/ (1996).

[3] VISA & MASTERCARD Corporation, *Secure Electronic Transaction Specifications*, http://www.setco.org/set_specifications.html (1997).

[4] R. Rivest y A. Shamir, Payword and Micromint: Two Simple Micropayment Schemes, *CryptoBytes*, **2** (1996).

[5] M. Sirbu y J. Chuang, NetBill: an Electronic Commerce System Optimized for Network Delivered Information and Services, Proceedings IEEE Compcon (1995).

[6] B. Clifford Neuman y G. Medvinsky, Requirements for Network Payment: The NetCheque Perspective, Proceedings of IEEE Compcon (1995).

[7] D. Chaum, Blind Signatures for Untraceable *Payments, Advances in Cryptology*: Proceedings of CRYPTO (1983).

[8] M. Stadler, J.M. Piveteau y J. Camenisch, Fair blind signatures, *Lecture Notes on Computer Science*, **921** (1995).

[9] S. von Solms y D. Naccache, On blind signatures and perfect crime, *Computer and Security*, **11** (1992).

Ana Isabel González-Tablas, Javier Carbó
Departamento de Informática
Universidad Carlos III de Madrid
Av. Universidad 30,
28911, Leganés, Madrid.
E-mail: aigonzal@inf.uc3m.es , jcarbo@inf.uc3m.es