R. Roman, and J. Lopez, "Especificación de Sistemas Electrónicos de Microdonaciones", *III Simposio Español de Comercio Electrónico*, pp. 95-104, 2005.
NICS Lab. Publications: https://www.nics.uma.es/publications

Especificación de Sistemas Electrónicos de Microdonaciones

Rodrigo Román Castro, Javier López Muñoz

E.T.S. Ingeniería Informática, Universidad de Málaga, 29071, Málaga, España.
roman@lcc.uma.es, jlm@lcc.uma.es

Resumen. Los sistemas electrónicos de pago permiten que un comprador adquiera a un vendedor una serie de productos y servicios de forma virtual. Sin embargo, estos sistemas no tienen en cuenta el escenario en el que un comprador se convierte en donante, accediendo al servicio de forma gratuita. En este artículo se presenta el concepto y características de las microdonaciones, o la donación de cantidades tan pequeñas como un céntimo de euro en el contexto del comercio electrónico. También se muestra como la microdonación es algo necesario en el contexto actual de Internet, y como es posible su implementación basándose en sistemas de micropago.

1. Introducción

El descenso de los precios y el incremento en la capacidad de procesamiento de los ordenadores, así como los avances en las tecnologías de comunicación y la progresión en los sistemas de transferencia de valores, ha culminado en la realización de pagos a través de las redes de ordenadores, dando lugar a los denominados sistemas electrónicos de pago [1].

Estos sistemas electrónicos de pago permiten la adquisición de un producto o servicio de forma digital, por lo que un vendedor puede ser capaz de ofrecer sus productos a un comprador situado en cualquier parte del globo que tenga acceso a una red. Los productos ofrecidos pueden ser tanto algo físico y tangible (un coche o un libro) como una pieza de información virtual (una canción codificada o el artículo de un periódico).

Sin embargo, existen ciertos escenarios en los que un vendedor ofrece su producto, el cual suele encontrarse en formato digital (webcomics, software de código abierto, etc), sin obligar a posibles compradores a pagar por él, por lo que la única posibilidad de obtener algún tipo de beneficio es a través de donaciones. De esta forma, los compradores se convierten en donantes, eligiendo si desean pagar o no por un servicio al que pueden acceder libremente.

Actualmente, es posible realizar donaciones utilizando sistemas de pago electrónico como PayPal [2]. No obstante, este tipo de sistemas no permite la donación de canti-

dades monetarias pequeñas, del orden de un céntimo de euro. A este tipo de donaciones se les denomina microdonaciones. El objetivo de este artículo es el de introducir las características de este tipo de donación electrónica, y como sería posible su implementación aprovechando la existencia de sistemas de micropago [3].

Este artículo se organiza de la siguiente forma: En la sección 2 se introducen los esquemas de pago electrónico, junto con la definición de macropagos y micropagos y sus diferencias. En la sección 3 se introduce el concepto de microdonación, explicando sus características respecto a los demás sistemas de pago. En la sección 4 se muestra como implementar un sistema de microdonación adaptando y optimizando los principales sistemas de micropago existentes, y se concluye el artículo en la sección 5.

2. Esquemas de pago electrónico

2.1 Introducción

Todos los sistemas electrónicos de pago actualmente disponibles difieren en algunos detalles. Sin embargo, tienen básicamente el mismo propósito: facilitar la transferencia de valores monetarios entre dos o más entidades.

En general, los pagos electrónicos involucran a un comprador y a un vendedor y, evidentemente, la acción de transferir de forma segura los valores monetarios de uno hasta otro. Tal transferencia se lleva a cabo mediante un conjunto completo y no ambiguo de pasos, los cuales establecen un protocolo de pago electrónico. Este protocolo de pago debe garantizar la seguridad de los datos involucrados en su ejecución, incluso aunque el medio no sea seguro. Es decir, en el caso de que el medio sea atacado el atacante no deberá obtener más que un flujo de datos de nula utilidad.

Para proporcionar este tipo de seguridad la mayoría de los sistemas electrónicos de pago hacen uso de técnicas criptográficas más o menos sofisticadas [4]. Además, requieren de la participación de, al menos, una institución financiera para poder enlazar los datos intercambiados en el propio protocolo con el valor de la correspondiente transferencia monetaria. La institución financiera participa o bien interactuando con el cliente o bien interactuando con el vendedor, pero rara vez con ambos.

De forma adicional, puede existir algún tipo de entidad que ejerza de mediador para la resolución de disputas. En muchos de los sistemas la presencia de tal entidad no es explícita, incluso aunque sean muchas las pruebas generadas durante la ejecución del protocolo. Por lo general, las disputas se resuelven fuera del sistema de pago, y en muchos casos el protocolo ni siquiera especifica cómo gestionarlas.

Finalmente, existen sistemas que involucran a otros tipos de entidades, como Autoridades de Registro, Autoridades de Certificación y, en general, Terceras Partes Confiables.

Los sistemas electrónicos de pago pueden clasificarse en función de la relación existente entre la ocurrencia de dos eventos:

(i) el momento en el que el cliente considera que finaliza el pedido, y
(ii) el momento en el que se realiza el cargo en cuenta por la correspondiente cantidad monetaria.

De esta forma, se puede realizar la siguiente clasificación en categorías:

- *Sistemas de prepago:* Se procede a retirar una cierta cantidad de dinero de la cuenta del cliente con antelación a la realización de pedidos. De forma directa o indirecta, tal cantidad de dinero será utilizada con posterioridad para llevar a cabo los pagos. Los monederos electrónicos basados en tarjetas, y ciertos tipos de cheques electrónicos entran dentro de esta categoría.

- *Sistemas de pago instantáneo:* El cargo en la cuenta del cliente se produce en el mismo instante en el que es realizada la compra. En esta categoría son comunes los pagos mediante tarjetas de débito.

- *Sistemas de post-pago:* En éstos, el ingreso en la cuenta del vendedor se realiza antes de que se produzca el correspondiente cargo en la cuenta del comprador. Los pagos efectuados con tarjetas de crédito habituales se sitúan dentro de esta clase.

2.2 Sistemas de Macropago y Micropago

Los sistemas de pago electrónico también pueden clasificarse en función de la cantidad de dinero intercambiada en el transcurso de una única transacción. De esta forma, se puede realizar la siguiente clasificación en categorías:

- *Sistemas de macropago:* En este tipo de sistemas, un usuario transfiere una cantidad de dinero considerable, superior a un euro, en una única transacción. El servicio obtenido puede ser tanto físico (p. ej. un libro) como digital (p. ej. una película).

- *Sistemas de micropago:* En estos sistemas los clientes pueden realizar transferencias de una cantidad tan pequeña como un céntimo de euro, a cargo de servicios digitales (como el artículo de un periódico).

Todos los sistemas de macropago y micropago comparten un diseño base, ya que su objetivo principal es común (transferir una cantidad monetaria determinada de un

comprador a un proveedor). No obstante, existen ciertas diferencias a la hora de definir los requisitos de seguridad y la presencia de terceras partes confiables durante las transacciones, debido a las características intrínsecas a cada sistema.

El coste de perder una transacción en un sistema de macropagos es normalmente alto, debido a dos razones: el precio que el servicio puede alcanzar, y los costes asociados al suministro del servicio (como la entrega de una mercancía real y tangible). No obstante, perder una transacción en un sistema de micropago no tiene un coste tan alto (no hay mercancías a enviar, el coste del servicio es muy bajo), por lo que estos sistemas pueden aguantar un grado determinado de fraude. Consecuentemente, a la hora de diseñar un sistema de macropago, éste debe contar con unos requisitos de seguridad más fuertes que los de un sistema de micropago.

Respecto a la presencia de terceras partes confiables (TTP), en los sistemas de macropago una TTP debe permanecer accesible de forma continuada para que ésta compruebe tanto las credenciales del cliente como las credenciales del proveedor del servicio, y para verificar que la transacción digital se realiza de forma correcta. Esto no es necesario en un esquema de micropago, ya que el recibo o los "tokens" intercambiados durante la transacción son los que contienen las credenciales necesarias, y la interacción con la TTP se realizará únicamente para hacer que el usuario pague al proveedor. Así se evitan los costes infraestructurales asociados a mantener la TTP accesible el 99.99% del tiempo, incluyendo horas punta en las que el número de transacciones puede incrementarse hasta un factor de 100 respecto a la media.

3. Microdonaciones

3.1 Definición

En todo el mundo existe una gran cantidad de usuarios que ofrecen un determinado servicio (software de código abierto [5], páginas web de libre acceso, webcomics u otras formas de arte [6],…) de forma gratuita, y que viven de las donaciones realizadas por los visitantes. En este modelo, el usuario visita y utiliza el servicio de forma totalmente gratuita, y luego elegirá si desea donar alguna cantidad de dinero al proveedor del servicio. Las donaciones que pueden llegar a ser tan pequeñas como un céntimo de euro se denominan microdonaciones. La primera referencia a las microdonaciones provino de un weblog [7], en referencia al "Amazon Honor System", un sistema orientado a proporcionar donaciones a páginas web manejadas por Amazon.

Actualmente, la posibilidad de realizar una microdonación a un proveedor de servicio depende de los esquemas de pago digital disponibles. La mayoría de las transacciones realizadas a través de Internet se realiza mediante sistemas de macropago, como tarjetas de crédito o Paypal [2], que no son capaces de transferir cantidades

pequeñas de dinero. Por lo tanto habría que utilizar sistemas de micropago, que sí permiten al usuario donar una pequeña cantidad de dinero.

Es por tanto posible realizar microdonaciones de forma más eficiente utilizando sistemas de micropago. Sin embargo, las donaciones pueden considerarse como un subconjunto de los pagos, con un proceder distinto a éstos. En principio, el proveedor de servicio en una donación ofrece su servicio "a priori" de forma gratuita, ya que no espera retribución por parte del usuario. Además, no es necesario que el proveedor compruebe o incluso conozca la identidad del donante, y es posible que el donante no reciba ningún tipo de recibo producto de la transacción. Finalmente, el proveedor del servicio no necesita percibir de forma inmediata el dinero producto de la transacción.

Como ejemplo, puede considerarse a los esquemas de micropago como a vendedores de caramelos, y a los esquemas de microdonaciones como un mendigo. El vendedor de caramelos recibe una cantidad pequeña de dinero, y proporciona un caramelo. El mendigo sencillamente recibe el dinero, sin dar nada a cambio – solo las gracias si él lo desea así. Si un comprador consigue robar un caramelo, el vendedor está sufriendo una pérdida. El mendigo, por su parte, no puede perder nada, salvo las monedas que ya tiene.

3.2 Barreras Económicas y Sociales ante las Microdonaciones

Actualmente, es difícil aplicar un sistema de micropago en un entorno real. Las razones económicas y sociales que han impedido esto han sido exploradas por expertos informáticos [8] y economistas [9, 10], y se pueden extraer tres conclusiones principales: Problemas en los costes infraestructurales y el modelo de mercado, proveedores de servicio como creadores, y los "costes de la transacción mental" (simplicidad).

El coste de crear una infraestructura de micropago suele ser elevado, tanto para los vendedores como para las entidades financieras [9], ya que es necesario disponer de un sistema capaz de procesar un gran número de pequeñas transacciones y ofrecer el servicio digital a una velocidad aceptable. Además, desde el punto de vista del modelo de mercado, los beneficios de un vendedor se maximizan cuando éste ofrece sus productos dentro de un lote [10], mientras que los micropagos se basan en la compra de servicios según su uso.

Otro problema es la mentalidad de los proveedores. La mayoría de los posibles consumidores de esquemas de micropago son creadores (poseedores de weblogs, proyectos de código abierto) cuya principal prioridad no son los beneficios, sino la posibilidad de ser vistos y leidos. Además, si alguno de estos proveedores obligara a pagar a sus usuarios una tarifa, es seguro que (en la mayoría de los casos) los usuarios buscarían a otro proveedor que proporcionara los mismos servicios.

Finalmente, el último problema ante el que se encuentran los sistemas de micropago es los "costes de la transacción mental" (la energía requerida para decidir que me-

rece la pena comprar un producto, independientemente de su precio). La mayoría de los esquemas de micropago requieren que el usuario tenga que tomar una decisión para comprar un producto que, en la mayoría de los casos, ni siquiera han visto. Y debido a la complejidad para disponer de una cuenta de micropago (suele ser un proceso tedioso, y en la mayoría de los casos se necesita una tarjeta de crédito), los usuarios no van a realizar el esfuerzo de crear esa cuenta solo para pagar unos pocos céntimos en primera instancia.

Los esquemas de microdonación no se encontrarían ante la mayoría de los problemas técnicos que sufren los esquemas de micropago, por lo que su implantación sería económicamente menos costosa. Además, en las microdonaciones los usuarios no son forzados a pagar por un servicio, sino que desean pagar por algo que ya han visto o utilizado. Asimismo las microdonaciones son ideales para los proveedores de servicios gratuitos, ya que actualmente éstos suelen proporcionar un mecanismo para recibir donaciones en forma de esquemas de macropago, por lo que se llenaría un nicho de mercado.

El problema ante el que se encontrarían los esquemas de microdonación es los "costes de la transacción mental". Si un esquema de microdonación obliga al usuario a comenzar una acción física (p. ej. dirigirse a un banco), es seguro que en la mayoría de los casos el usuario no realizará esa donación. La clave está entonces en la simplicidad de uso: Cuanto menos esfuerzo se requiera para realizar la donación, mayor será en número de usuarios que querrán donar.

3.3 Barreras Técnicas y de Seguridad ante las Microdonaciones

Todos los sistemas de micropago deben ser técnicamente eficientes para ser viables desde un punto de vista económico. Por lo tanto, es necesario reducir la complejidad computacional en los cálculos realizados durante las transacciones, e involucrar lo menos posible a instituciones financieras y mediadores puesto que encarecerían el coste de cada transacción.

Al mismo tiempo, es necesario mantener unos requisitos de seguridad mínimos que permitan la aplicación de micropagos a entornos reales. Es necesario que los compradores y vendedores que actúen de buena fe no sufran pérdida alguna debido a sus transacciones, y que aquellas partes que traten de abusar del sistema sean debidamente penalizadas.

Ambos requisitos, técnicos y de seguridad, están en continuo conflicto. Un sistema perfectamente seguro, en el que cada transacción emplease técnicas de clave pública para ofrecer servicios de no-repudio y fuese supervisada por las instituciones financieras, no sería viable desde el punto de vista económico debido a que los gastos de cada transacción serían mayores que el propio valor de la transacción. Al mismo tiempo, un sistema completamente eficiente que no dependiera de tecnologías criptográficas sería incapaz de ofrecer protección ante un participante que engañara al sistema.

Como resultado, es necesario balancear la eficiencia del sistema con la seguridad que éste puede ofrecer. Esto conlleva ciertos sacrificios, como la utilización de métodos criptográficos alternativos pero más eficientes (funciones resumen o "hash"), la admisión de cierto grado de fraude por parte de un comprador determinado, o el agrupamiento de los micropagos en una factura global retrasando así la recepción de los beneficios del vendedor.

Las microdonaciones deben tener la misma eficiencia que los mecanismos de micropago, por lo que sigue siendo necesario el uso de técnicas tales como el agrupamiento de transacciones. No obstante, sus requerimientos de seguridad son aún menores. No es posible que un donante cometa un fraude al donar dinero por el servicio (p.ej. pagando en moneda falsa), ya que de todas formas el servicio puede accederse gratuitamente. Además, ciertas operaciones, como la notificación al vendedor de la finalización del proceso de pago, no son necesarias. Todo esto conlleva una mayor eficiencia a la hora de realizar una transacción simple, un menor coste de la infraestructura, y por ende un menor coste del servicio.

4. Esquemas de Microdonación

A la hora de proporcionar servicios de microdonación, es posible utilizar los sistemas de micropago previamente existentes. No obstante, debido a las características de las microdonaciones, es posible simplificar tanto el funcionamiento de los sistemas de micropago como sus requisitos de seguridad.

A continuación, se muestran los principales tipos de sistemas de micropago, junto a las modificaciones que pueden sufrir para poder ofrecer servicios de microdonación sin menoscabo de la seguridad o de la eficiencia del sistema.

4.1 Sistemas de Moneda Electrónica

Los sistemas de moneda electrónica se basan en la creación de monedas electrónicas (e-coins) específicas para los usuarios y los proveedores de servicio. Existen varios escenarios en la creación de las monedas electrónicas. Es posible que una TTP (que representa a la entidad financiera en el mundo virtual) genere las "e-coins" y las venda a los usuarios, de tal forma que cada "e-coin" tiene asociada la identidad de su usuario [11]. Por otro lado, los usuarios pueden obtener un certificado de la TTP, y utilizarlo para establecer una relación con un proveedor y para crear monedas electrónicas usadas durante las transacciones con ese proveedor [11].

Los principales problemas en el uso de monedas electrónicas son el "Doble Gasto", donde un usuario gasta dos o más veces una misma unidad monetaria electrónica, o la "Moneda Falsa", donde un usuario genera su propia moneda sin tener ninguna cuenta con una entidad financiera. Así pues, es necesario guardar una base de datos con las

monedas que han sido gastadas, lo cual requiere acceder a una entidad mediadora en cada transacción (costoso) o cada cierto número de transacciones (inseguro).

Este tipo de problemas se minimiza cuando las monedas electrónicas se aplican a las microdonaciones, ya que no puede existir fraude por parte del comprador/donante. De todas formas la eficiencia del sistema debe mantenerse, por lo que habría que balancear el acceso a entidades mediadoras (utilizando por ejemplo sistemas probabilísticos de comprobación) para evitar que "fraudes masivos" cometidos por los donantes hicieran que estas entidades mediadoras sufrieran un coste computacional elevado al realizar operaciones de agrupación.

4.2 Sistemas de Monedero Electrónico

En los sistemas de monedero electrónico, el cliente paga por adelantado, y seguidamente puede acceder a un conjunto de productos o servicios – sea por un periodo de tiempo determinado (suscripción) o por el uso del servicio (monedero). Los sistemas de suscripción son muy comunes para controlar el acceso a una información centralizada (foros de discusión, páginas web, etc), mientras que los sistemas de monedero se utilizan para proporcionar acceso a servicios de distintos vendedores.

Un sistema de monedero electrónico puede utilizarse como sistema de microdonación si se incluye dentro de su arquitectura la transferencia directa de dinero entre sus usuarios. Esto es posible y rentable en entornos de micropago con una gran cantidad de vendedores y de servicios ofrecidos, como BitPass [12]. El acceso al servicio sería directo, y el donante tendría la posibilidad de donar una cantidad fija. Esta operación sería menos costosa para el sistema que una microdonación, ya que no es necesario proteger el acceso al servicio, y por lo tanto notificarle que la transferencia ha sido correcta.

4.3 Sistemas Probabilísticos

Los sistemas probabilísticos se dividen principalmente en dos categorías: probabilísticos de comprobación y probabilísticos de cobro. Ambos esquemas se basan en el siguiente axioma: Solo n de cada m transacciones, siendo $n << m$, deben ser procesadas por una entidad externa a la transacción directa entre comprador y vendedor.

En los sistemas probabilísticos de comprobación, las entidades financieras o mediadoras comprueban si una transacción realizadas por un comprador determinado es correcta con una probabilidad n/m [13]. Por otro lado, los sistemas probabilísticos de cobro se encargan de transferir una cantidad monetaria mayor a la transferencia actual con una probabilidad n/m [14, 15].

En los sistemas probabilisticos de cobro, la probabilidad de que n transacciones sean elegidas es determinista, para evitar así problemas tales como pérdidas económicas.

Además, existen diversos mecanismos para que un comprador no tenga que pagar una cantidad mayor que la que debe al vendedor una vez se realiza el pago, como la inclusión de números de serie en cada transferencia. De esta forma, este tipo de sistemas puede aplicarse a escenarios reales [16].

Al procesar las transacciones dentro de un sistema probabilístico de cobro, es necesario que la validez de cada una de ellas sea comprobada por el vendedor, para así poder proporcionar el servicio. No obstante, en entornos de microdonación, solo sería necesario comprobar la validez de la transferencia que provocara el pago, simplificando así la tarea del vendedor.

La presencia de los números de serie dentro de cada transacción, que cuenta cuanto dinero lleva el donante gastado hasta entonces, permite que el cliente done lo que realmente debe. En caso de que el cliente quiera hacer trampas, lo más que puede hacer es cambiar el número de serie de la transferencia elegida probabilísticamente para así donar menos, lo cual no importa demasiado al ser una donación (el cliente dona únicamente lo que quiere).

5. Conclusiones

En este artículo se ha presentado el concepto de microdonación, aplicado a entornos de comercio electrónico. Las microdonaciones se encuentran al mismo nivel que los sistemas de micropago, permitiendo la transferencia de cantidades monetarias tan pequeñas como un céntimo de euro. No obstante, en una microdonación no existe la obligación de proporcionar un servicio, por lo que tanto sus requerimientos de seguridad como los cálculos a realizar por transacción son menores.

Es por tanto posible, como se ha expuesto en este artículo, optimizar esquemas de micropago para proporcionar servicios de microdonación. La utilidad de las microdonaciones queda patente por el nicho de mercado que existe, donde un gran conjunto de creadores y artistas podrían salir beneficiados de la existencia de un sistema seguro y fiable de donación electrónica.

Referencias

1. C. Dragon et al. “Les moyens de paiement: Des espèces à la monnanie èlectronique”. Banque Editeur, 1997.
2. Paypal. http://www.paypal.com/
3. Jorge Dávila, Javier López. “Sistemas Electrónicos de Micropago”. Revista de Contratación Electrónica, Vol. 22, pp 3-22, Diciembre 2001.
4. B. Schneier "Applied Cryptography". John Wiley & Sons, 1996.
5. Apache Software Foundation. http://www.apache.org/
6. Scott McCloud. http://www.scottmccloud.com/
7. Captain Cursor’s Weblog. http://www.captaincursor.com/archive/2001_02_04_blog.xml

8. Clay Shirky. “Fame vs Fortune: Micropayments and free contents”. http://www.shirky.com
9. I. Papaefstathiou, C. Manifavas. “Evaluation of Micropayment Transaction Costs”. Journal of Electronic Commerce Research, Vol. 5, No. 2, pp. 99-113, 2004.
10. P. C. Fishburn, A. M. Odlyzko, R. C. Siders. “Fixed fee versus unit pricing for information goods: competition, equilibria, and price wars”. Internet Publishing and Beyond: The Economics of Digital Information and Intellectual Property, MIT Press, 2000.
11. R. Rivest, A. Shamir. “Payword and Micromint: two simple micropayment schemes”. Proceedings of the 1996 RSA Data Security Conference, Enero 1996.
12. BitPass. http://www.bitpass.com
13. S. Jarecki, A. Adlyzko. “An efficient micropayment system based on probabilistic polling”. Proceedings of 1st Financial Cryptography Conference, Febrero 1997.
14. R. J. Lipton, R. Ostrovsky. “Micro-Payments via Efficient Coin-Flipping”. Proceedings of 2nd Financial Cryptography Conference, Febrero 1998.
15. S. Micali, R. Rivest. “Micropayments Revisited”. Proceedings of Cryptography Track at RSA Security Conference 2002, Febrero 2002.
16. Peppercoin. http://www.peppercoin.com