Protocolo de intercambio justo para comercio electrónico basado en políticas de firma

Jorge L. Hernández-Ardieta, Ana Isabel González-Tablas, Benjamín Ramos Álvarez
Grupo de Seguridad de la Información y las Comunicaciones
Departamento de Ingeniería Informática
Universidad Carlos III de Madrid
jlopez@inf.uc3m.es, aigonzal@inf.uc3m.es, benja1@inf.uc3m.es

Resumen

La aparición del comercio electrónico ha permitido a empresas y particulares la compraventa de todo tipo de productos y servicios a través de Internet. No obstante, durante la transacción de compra se produce una situación en la cual el vendedor posee la información necesaria del comprador – típicamente la información de la tarjeta de crédito – para realizar el cargo del importe correspondiente, mientras que el comprador no ha recibido todavía nada del vendedor. Esta situación deja al comprador claramente en desventaja frente al vendedor, y es, junto con el temor al fraude, una de las causas de la falta de confianza en el comercio electrónico. Este artículo presenta un protocolo de intercambio de información justo basado en políticas de firma con el fin de resolver la problemática anterior. Se realiza una evaluación de las características de justicia y completitud del protocolo.

1. Introducción

La aparición del comercio electrónico ha permitido a empresas y particulares la compraventa de todo tipo de productos y servicios a través de Internet de una manera rápida, cómoda y eficaz. Las formas más comunes de interacción son B2C (Business to Client) y B2B (Business to Business). En el primer caso el comprador es un particular, mientras que en B2B es otra empresa.

Aunque el contexto es distinto, el objetivo en ambos casos es el mismo: la compraventa de un producto o servicio (recurso).

Jorge L. Hernández-Ardieta es Consultor Senior del *Dpto. de Seguridad de NET2S* (jorge.lopez@net2s.com)

Dicha compraventa conlleva una transacción electrónica en la cual se pueden diferenciar las siguientes fases principales:

1. El comprador realiza una selección del recurso que desea comprar.
2. Posteriormente el vendedor solicita al comprador determinada información, con el fin de poder realizar el cargo del importe correspondiente al recurso. En B2C, esta información es típicamente los datos de la tarjeta de crédito del comprador.
3. A continuación se lleva a cabo un proceso de validación de la información anterior, con el fin de detectar si los datos son correctos y, en algunos casos, si el comprador posee fondos para la compra del recurso. Este paso se suele realizar por medio de una pasarela de pago.
4. Si la validación anterior ha sido satisfactoria, el vendedor procede a cargar en la cuenta del comprador el importe correspondiente.
5. Por último, el vendedor notifica el resultado de la operación al comprador. Si éste es satisfactorio, el vendedor suele proporcionar al comprador un justificante de compra o acuse de recibo o incluso el propio producto en sí.

En caso que en el paso 5 el comprador no recibiera el producto, bien debido a su naturaleza bien por el modo de funcionamiento del vendedor, el único elemento de que dispondría el comprador para realizar cualquier reclamación futura sería un justificante de compra o similar. Este tipo de justificante actúa como evidencia de que realmente se llevó a cabo una transacción de compraventa dada. Dentro del contexto del comercio electrónico, el justificante de compra puede ser incluso una factura electrónica.

No obstante, la posesión de determinada información no siempre se traduce en un compromiso contractual o legal. Es posible que el comprador auto genere justificantes de compra o incluso que el vendedor realice tantos cargos a la cuenta del comprador como desee una vez conocidos sus datos bancarios. Es por ello que un comprador podría rechazar haber tomado parte en una transacción electrónica, o que el vendedor rechazase realizar determinados envíos de un recurso a un comprador si creyera que ha existido fraude en la operación.

Para resolver esta problemática se hace uso de lo que se conoce como evidencias [26]. Éstas se generan durante la transacción, y obligan al comprador y al vendedor a adquirir determinado compromiso en la compraventa. Normalmente las evidencias consisten en firmas digitales [7] realizadas sobre información intercambiada en la transacción. Por ejemplo, el comprador generaría su evidencia sobre el pedido realizado y sus datos bancarios y el vendedor sobre el justificante de compra o acuse de recibo. Además, debido a la naturaleza de la evidencia, el compromiso no es repudiable. De esta manera, el comprador se comprometería al pago de la cantidad acordada por el recurso mientras que el vendedor haría lo propio respecto a la entrega de dicho recurso. Y ninguno podría rechazar en una disputa posterior haber adquirido dicho compromiso.

Sin embargo, la mera generación de evidencias no resuelve el problema anterior. Debido a la división de una transacción electrónica en distintas fases o etapas, es posible que el vendedor obtenga la evidencia del comprador junto con sus datos bancarios pero que no responda con su evidencia correspondiente.

Para poder otorgar al proceso de intercambio de información de completas garantías de cara a los implicados, es necesario que tanto el protocolo como las evidencias generadas aten a comprador y vendedor por igual. De esta forma, ninguno obtendría una ventaja sobre el otro durante la ejecución del protocolo. A este tipo de protocolos se les conoce como protocolos de intercambio justos [23]. El diseño de estos protocolos se sustenta en los protocolos de no repudio justos [6, 21, 24, 25], donde la información intercambiada son las evidencias de no repudio en sí.

En la mayoría de los casos el objetivo es permitir al origen obtener la evidencia del receptor en condiciones justas, evitando que el receptor pueda poseer la evidencia del origen sin haberse comprometido en la transacción. En [22] se propone el uso de firmas digitales condicionales como principio para el diseño de un protocolo justo. Otros artículos, y basándose en el concepto de firmas condicionales, proponen protocolos para poder revocar firmas digitales con el fin de no dejar en desventaja al firmante en caso de haber empleado un terminal malicioso [3-5].

Por otra parte se han propuesto diversos protocolos para el aseguramiento del intercambio justo de información dentro del contexto del comercio electrónico [2, 23].

Este artículo propone un protocolo de intercambio justo cuyos principios fundamentales se han extraído de la bibliografía existente al respecto hasta el momento, pero cuyo diseño es totalmente novedoso. El diseño del protocolo aquí propuesto se sustenta en lo que se conoce como Políticas de Firma [11], concepto que se detalla en el punto 3. Mencionar que el protocolo propuesto se centra en la fase de negociación de una transacción de comercio electrónico. Es decir, abarca únicamente las etapas de intercambio de información y sus evidencias correspondientes, quedando excluida la etapa de provisión del recurso comprado.

El resto del artículo se divide como sigue: el punto 2 define determinados conceptos referidos a lo largo del documento así como la notación empleada en la definición del protocolo. En el punto 4 se describe el protocolo y se realiza su evaluación. El proceso de resolución de disputas se detalla en el punto 5. Finalmente, se concluye el artículo en el punto 6.

2. Notación y conceptos básicos

2.1. Conceptos básicos

En este artículo se emplean determinados conceptos, los cuales conviene definir:

Firma digital

Datos que se añaden a, o una transformación criptográfica de, una unidad de datos y que permite al receptor de dichos datos conocer con certeza la identidad del origen de los datos además de prevenir frente a una modificación de los mismos por parte del receptor [19].

Firma electrónica

Datos en forma electrónica anejos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación [8].

Según se incorpore información adicional a la firma y se cumplan con determinados requisitos durante su generación, permite evitar el repudio de la información firmada.

No repudio de origen (NRO)

Firma digital realizada por el origen de la comunicación sobre determinados datos y que protege al receptor frente al falso rechazo por parte del origen de haber enviado dichos datos.

El origen, dentro del contexto de comercio electrónico, se correspondería con el comprador.

No repudio de recepción (NRR)

Firma digital realizada por el receptor de la comunicación sobre los datos recibidos y que protege al origen frente al falso rechazo por parte del receptor de haber recibido dichos datos.

El receptor, dentro del contexto de comercio electrónico, se correspondería con el vendedor.

No repudio de aceptación (NRA)

Firma digital realizada por un extremo de la comunicación sobre determinados datos recibidos y que protege al otro extremo frente al falso rechazo por parte del primero de haber tenido conocimiento de la existencia de dichos datos.

Protocolo de intercambio justo

Protocolo de intercambio de información que permite a los participantes interactuar sin que ninguno se halle, en ningún momento, en una situación de desventaja frente al otro.

Protocolo de intercambio justo finito en el tiempo

En cualquier etapa del protocolo, tanto origen como receptor pueden alcanzar, en un tiempo finito de tiempo, un punto donde parar el protocolo sin necesidad de intervención del otro participante, y sin que nadie quede en una situación de desventaja frente al otro.

Protocolo optimista de intercambio justo

Protocolo donde se supone que tanto origen como receptor actúan de buena fe, por lo que la intervención del Tercero de Confianza (TTP) solamente se produce en caso de conflicto. A este TTP se le conoce como TTP offline.

2.2. Notación básica

A continuación se presenta la notación empleada para describir el protocolo:

- P.F
  Política de Firma.
- X → Y : m
  Envío del mensaje m por la entidad X a la entidad Y.
- X ← Y : P.F.
  Obtención por parte de la entidad X de la política de firma localizada en Y.
- Sx (m, P.F.)
  Firma electrónica generada por la entidad X sobre el mensaje m, y en base a P.F.
- NRO = Sx (m, P.F)
  Corresponde al no repudio de origen.
- NRR = Sy ((m, NRO), P.F)
  Corresponde al no repudio de recepción, y es una firma electrónica paralela sobre m, pero posterior a NRO, y en base a P.F.
- NRA = Sx (Sy, P.F)
  Corresponde al no repudio de aceptación, y es una firma electrónica jerárquica sobre Sy, y en base a P.F.

3. Política de firma

3.1. Concepto

El concepto de política de firma fue introducido por ETSI [9], organismo europeo de estandarización, y posteriormente recogido por IETF [16], organismo de estandarización europeo.

Según [11], una política de firma (P.F.) es un documento donde se recogen las condiciones bajo las cuales puede asegurarse la validez de una firma electrónica que haya sido generada en base a dicha política. El documento puede ser meramente descriptivo (entendible por el hombre), siempre y cuando sea suficientemente claro y conciso, o procesable de manera automática (en formato ASN.1 [13] o XML [10]). Por tanto, una P.F define los procesos tanto de generación como de validación de una firma electrónica que desee adherirse a dicha P.F.

Normalmente, existen organismos que se conocen como entidades emisoras de P.F., los cuales abstraen a los sistemas de la creación y gestión de las políticas de firma. No obstante, es perfectamente viable que un sistema actúe a la vez como generador de firmas y como emisor de P.Fs.

A grandes rasgos, una P.F contiene lo siguiente:

- Identificador único (OID) de la P.F.
- Información sobre la Entidad Emisora de la P.F.
- El contexto de aplicación de la P.F: marco de negocio en el cual es aplicable, contexto transaccional, etc.
- Información de validación que debe estar presente en la firma electrónica con el fin de poder asegurar validez de la misma. Ej: sellos de tiempo [17], respuestas OCSP, CRLs [18], referencia a respuestas OCSP y/o CRLs, Certificado de clave pública, etc.
- Restricciones a la hora de la generación de la firma electrónica: uso de *smartcards*, uso y gestión de certificados de atributos, etc.
- Restricciones en la validez de las firmas electrónicas generadas bajo esta P.F.: periodo de validez de la firma generada, etc.
- Tipo de compromiso adquirido por el firmante en relación a los datos firmados. Ej: autenticación de origen, prueba de recepción (en firmas jerárquicas), compromiso legal, notaría (en firmas jerárquicas), testigo (en firmas jerárquicas), aprobación del contenido de los datos, etc.

Como puede verse, las políticas de firma ya contemplan los roles de origen y receptor, por lo que su empleo en un protocolo de intercambio justo parece bastante adecuado.

Importante destacar que la P.F. (o una referencia a la misma) es un atributo firmado dentro de la firma electrónica [14, 15], por lo que no es posible sustituir la P.F que se empleó durante la generación de la firma electrónica sin que ésta deje de ser válida.

3.2. Empleo de políticas de firma en contextos de negocio complejos

La información anterior está normalmente orientada al proceso de generación/validación de una única firma electrónica. No obstante, sucede en muchos casos que el modelo de negocio donde se aplican las firmas electrónicas es complejo, por lo que una única firma electrónica no cubre las necesidades existentes. Es por ello que aparecen las firmas electrónicas múltiples, las cuales permiten las siguientes posibilidades:

- Un mismo documento sea firmado electrónicamente por dos o más personas.
- Una firma electrónica sea firmada (autorizada) por otra o varias personas.

El primer caso se denomina firma en paralelo, pues las firmas generadas se realizan al mismo nivel sobre el documento en concreto. El segundo caso se refiere a firmas jerárquicas, pues la firma generada se lleva a cabo sobre la firma anterior, y no sobre el documento firmado.

Realizando una combinación de firmas en paralelo y firmas jerárquicas se puede abarcar todas las necesidades relativas a firmas electrónicas.

En [12] se extiende el modelo de P.F descrito en [11] para contemplar modelos de negocios complejos que necesiten el uso de firmas múltiples.

4. Protocolo optimista de intercambio justo basado en políticas de firma

El objetivo del protocolo es el intercambio justo de las evidencias de no repudio por parte de un origen y un receptor dentro del contexto del comercio electrónico. El protocolo consiste a su vez en dos protocolos y un conjunto de timeouts.

El protocolo principal, explicado en el punto 4.2, permite el intercambio de las evidencias de no repudio. Estas evidencias son firmas electrónicas generadas en base a una política de firma determinada. La política de firma es completamente dependiente del contexto de negocio concreto, aunque no obstante su contenido debe estar adaptado para cumplir con los requisitos impuestos por este protocolo.

Debido a la operativa del protocolo, se realizan firmas electrónicas múltiples [12], tanto en paralelo como jerárquicas, por lo que la política de firma a emplear se ha de ajustar al modelo extendido de políticas de firma descrito en el apartado 3.2.

El protocolo de recuperación, detallado en el punto 4.3, permite mantener las características de protocolo justo y finito en el tiempo en caso que no pueda llevarse a cabo una correcta ejecución del protocolo principal. Este protocolo, por tanto, sólo se ejecuta bajo determinadas condiciones, y es en el único punto donde entra en juego el TTP. Es por esto último que este protocolo se denomina protocolo optimista [1, 20].

Durante la ejecución del protocolo se hace uso de referencias temporales incluidas en las firmas electrónicas así como de timeouts definidos a nivel de política de firma para detectar, por ejemplo, si las entidades implicadas están actuando correctamente o si es necesario ejecutar el protocolo de recuperación. Dichas referencias temporales consisten en sellos de tiempo generados por otro TTP, más concretamente una Autoridad de Sellado de Tiempo (TSA, TimeStamping Authority) [17], y calculados sobre la firma electrónica.

4.1. Entidades del protocolo

Antes de detallar formalmente el protocolo, conviene definir la función de cada una de las entidades que intervienen:

- Origen (O)

  Es el extremo de la comunicación que envía los datos y que lleva a cabo la firma de los mismos, a modo de evidencia o prueba de envío (NRO). Espera obtener del receptor una prueba o evidencia de recepción de dichos datos.

  Como se verá más adelante en el protocolo, el origen también debe llevar cabo una firma sobre NRR, a modo de evidencia de aceptación (NRA).

- Receptor (R)

  Es el otro extremo de la comunicación. Recibe los datos y la firma del origen, tras cuya validación lleva a cabo la firma electrónica correspondiente como prueba o evidencia de recepción (NRR), enviándosela al origen.

- TTP-PF

  Es un tercero de confianza que actúa como entidad emisora y gestora de políticas de firma, acorde a [11]. Tiene configuradas determinadas políticas de firma accesibles tanto desde el origen como desde el receptor.

- TTP

  Es el tercero de confianza que interviene en el protocolo de recuperación. Actúa por tanto en modo optimista, es decir, sólo en caso que suceda una situación anormal en la ejecución del protocolo principal.

4.2. Protocolo principal

Este protocolo consiste en los siguientes pasos:

1. O ← TTP-PF : P.F
2. O → R : NRO, m
3. R ← TTP-PF : P.F
4. R → O : NRR
5. O → R : NRA

El origen accede al TTP-PF para la obtención de la P.F. adecuada. Posteriormente lleva a cabo la generación de la firma electrónica sobre los datos m (p.ej. el pedido y sus datos bancarios). Esta firma actúa como NRO de cara al receptor. La firma electrónica se realiza en base a los requisitos y procedimientos impuestos por la P.F.

Una vez que el receptor recibe el mensaje y el NRO correspondiente, debe obtener la P.F. referenciada. De esta manera puede llevar a cabo la validación de NRO. A continuación genera el NRR, llevando a cabo una firma electrónica paralela sobre los mismos datos (el NRR actuaría por tanto como justificante de recepción del pedido y los datos bancarios). El orden de este tipo de firmas paralelas sí importa, y puede y debe ser indicado en la P.F.

Cuando el origen recibe el NRR, debe validarlo acorde a la P.F. Tras la validación satisfactoria podrá realizar la última firma del protocolo, denominada NRA, y la cual es una firma jerárquica sobre el NRR. De esta manera se acepta por su parte la completitud del protocolo.

4.3. Protocolo de recuperación

Es posible que se dé la situación en la que el origen genere el NRA (paso 5 del protocolo) pero que no envíe dicha evidencia al receptor.

Para permitir al receptor poseer la evidencia es su completitud, se propone el siguiente protocolo de recuperación:

1. R → TTP : NRR, NRO
2. TTP → R : NRA
3. TTP → O : NRA

El primer paso consiste en el envío por parte del receptor del NRR y el NRO al TTP.

Tras la validación del NRR, el TTP genera un NRA sobre NRR.

Por último, el TTP envía el NRA generado tanto al origen como al receptor. El orden no es condicionante.

Consideraciones

Sólo el receptor puede iniciar el protocolo de recuperación. Para ello, debe cumplirse un tiempo determinado (t_0) desde el envío del NRR al origen. El valor de t_0 ha de estar estipulado en la P.F.

El certificado público asociado a la clave privada de firma empleada por el TTP ha de estar contemplado en la P.F. como certificado válido para la generación del NRA.

El TTP debe tener en cuenta el tiempo transcurrido desde la generación del NRO hasta la recepción del NRR y NRO en el paso 1. De esta manera se evita una posible situación de desventaja para el origen. Supongamos que el receptor, tras la generación del NRR en el protocolo principal, espera un tiempo suficiente de manera que provoca que el origen abandone el protocolo. El motivo de tal abandono puede ser que el origen piense que ha habido un error en la comunicación o que el receptor ha abandonado el protocolo. El receptor podría entonces iniciar el protocolo de recuperación, obteniendo sólo él el NRA del TTP.

Por tanto, si dicho tiempo transcurrido es superior a un valor determinado (t_1), que ha de estar recogido en la P.F., el TTP devolverá tanto al receptor como al origen un mensaje de Aborto.

Destacar que la referencia temporal es el momento de la recepción del NRR por parte del TTP, no el momento de creación del NRR. Esto evita la situación en la que el receptor genere el NRR una vez que el origen ha abandonado el protocolo por la espera provocada, pudiendo iniciar el protocolo de recuperación sin problemas. Para ello se supone que el TTP posee una fuente de tiempo fiable.

4.4. Análisis del protocolo

A continuación se realiza un análisis del protocolo en su completitud, contemplando tanto el protocolo principal como el de recuperación:

Interrupción del protocolo principal tras recepción de NRO

El receptor detiene el protocolo en el paso 2, por lo que el origen no poseería ninguna evidencia de recepción.

No obstante, debido a que P.F. dicta que para que NRO tenga validez es necesario NRA sobre NRR, el receptor no puede aportar NRO como evidencia de origen válida.

Interrupción del protocolo principal tras recepción de NRR

El origen detiene el protocolo en el paso 4, una vez que ha recibido el NRR. Por lo tanto, el receptor posee NRO y el origen NRR.

Por los mismos motivos que los anteriores, esta información no puede considerarse un NRR válido hasta que se lleve a cabo NRA sobre NRR.

Interrupción del protocolo principal tras generación de NRA

El origen detiene el protocolo en el paso 5, pero tras la generación de NRA. De esta manera el origen posee NRA, aunque no lo ha transmitido al receptor, el cual sólo posee NRO. Es decir, el origen posee ahora toda la información necesaria a modo de evidencia de recepción, mientras el receptor se encuentra en una posición de desventaja.

Para resolver esta situación el receptor debe iniciar el protocolo de recuperación una vez transcurrido un tiempo t_0.

Interrupción del protocolo de recuperación tras generación del NRR

Una vez obtenido el NRO, y transcurrido un tiempo tras el cual se supone que el origen ha abandonado el protocolo, el receptor genera el NRR y ejecuta el protocolo de recuperación. De esta manera el origen se encontraría en una situación de desventaja frente al receptor.

Este ataque se resuelve mediante t_1, descrito en el protocolo de recuperación.

Consideraciones

Es imprescindible que el origen, tras el envío de NRO, espere al menos un tiempo igual a t_1 antes de abandonar el protocolo. En caso contrario el receptor podría ejecutar y completar el protocolo de recuperación.

Así mismo, es necesario que t_1 sea mayor que t_0, para que la condición de inicio del protocolo de recuperación se pueda cumplir.

Por otro lado, y como consecuencia de t_1, puede suceder la situación siguiente:

En el protocolo principal, el origen genera NRO y espera t_1 antes de enviarlo al receptor. Una vez que ha generado el NRA en el paso 5, el origen abandona el protocolo. Cuando el receptor intente ejecutar el protocolo de recuperación, el TTP rechazará la solicitud de generación de NRA pues se habrá cumplido t_1.

Para evitar este ataque al protocolo, el receptor ha de comprobar que el tiempo pasado desde la generación del NRO hasta su recepción es mucho menor que t_1. En caso de no cumplirse esta condición el receptor deberá abandonar el protocolo.

5. Resolución de disputas

En caso que el origen rechace haber enviado el mensaje m, el receptor tendrá de presentar ante el juez las siguientes evidencias:

- NRA (NRR (m))
- NRO (m)

El NRA podrá haber sido generado tanto por el origen como por el TTP.

Si todas las firmas anteriores son correctas, en base a la P.F referenciada, entonces se ha probado que el origen ha transmitido el mensaje m.

Si es el receptor el que rechaza haber recibido la información, para probar lo contrario el origen deberá presentar ante el juez exactamente las mismas evidencias que en el caso anterior.

Las comprobaciones por parte del juez serán por tanto iguales en ambos casos.

6. Conclusión

El comercio electrónico es proclive a situaciones donde los compradores se encuentran en situaciones de desventaja respecto a los vendedores.

Para la resolución de esta problemática se han propuesto numerosos protocolos donde ni comprador ni vendedor pueden tomar ventaja sobre el otro durante la transacción electrónica. A estos protocolos se les conoce como protocolos de intercambio justos.

En este artículo se ha propuesto un protocolo de intercambio justo totalmente novedoso respecto a los anteriores, pues se basa en un concepto de reciente aparición: las políticas de firma. Una política de firma permite restringir la validez de una firma electrónica generada en base a dicha política, definiendo explícitamente los requisitos a cumplir durante su generación.

Una política de firma siempre está enfocada a un contexto de negocio concreto. Será el comprador el que decida confiar en la entidad que emite dicha política, así como aceptar los términos recogidos en ella. Una vez establecida esta relación de confianza, el protocolo asegura que al finalizar la transacción electrónica bien comprador y vendedor obtienen las evidencias necesarias para reclamar a la otra parte su responsabilidad en la compraventa bien ninguno de ellos posee información vinculante. Es por tanto condición imprescindible que la política de firma a emplear cumpla con los requisitos impuestos por el protocolo.

Por otra parte, el protocolo propuesto se engloba dentro de lo que se conoce como protocolos optimistas, pues el TTP solamente interviene en caso que alguna de las partes haya actuado de mala fe. De esta manera se evita crear un cuello de botella en el TTP, resultando en una mayor eficiencia del protocolo.

Finalmente, la existencia de estándares y recomendaciones internacionales respecto a firmas electrónicas y políticas de firma asegura que una solución basada en el protocolo presentado en este artículo podrá ser implementada de manera rápida y fiable así como interoperable con otros frameworks de comercio electrónico.

Referencias

[1] Asokan, N., Schunter, M. y Waidner, M. Optimistic Protocols for Fair Exchange. Proceedings of the 4th ACM Conference on Computer and Communications Security, T. Matsumoto, Ed. Zurich, Switzerland, 7-17. 1997.

[2] Bao, F., Deng, R. H. y Mao, W. Efficient and Practical Fair Exchange Protocols with Off-line TTP. Proceedings of the IEEE Symposium on Security and Privacy. Oakland, California. 1998.

[3] Berta, I. Z., Buttyán, L. y Vajda, I. Mitigating the Untrusted Terminal Problem Using Conditional Signatures. Proceedings of International Conference on Information Technology ITCC 2004, IEEE, Las Vegas, NV, USA. Abril 2004.

[4] Berta, I. Z., Buttyán, L. y Vajda, I. Privacy Protecting Protocols for Revokable Signatures. Proc. Smart Card Research and Advanced Application IFIP Conf. (CARDIS 2004). 2004.

[5] Berta, I. Z., Buttyán, L. y Vajda, I. A Framework for the Revocation of Unintended Digital Signatures Initiated by Malicious Terminals. IEEE Transactions On Dependable And Secure Computing, Vol. 2, No. 3. 2005.

[6] Coffey, T. y Saidha, P. Non-repudiation with mandatory proof of receipt. ACM SIGCOMM, 1996.

[7] Diffie, W., y Hellman, M. New Directions in Cryptography, IEEE Trans. Inform. Theory, 22, páginas 644-654. 1976.

[8] Directiva Europea 1999/93/EC aprobada por el Parlamento Europeo el 13 de Diciembre de 1999, para la aplicación de las Firmas Electrónicas dentro del marco europeo.

[9] European Telecommunications Standards Institute, ETSI. http://www.etsi.org

[10] ETSI TR 102 038 v1.1.1. TC Security – Electronic Signatures and Infrastructures (ESI); XML format for signature policies. Abril 2002.

[11] ETSI TR 102 041 v1.1.1. Signatures Policies Report. Febrero 2002.

[12] ETSI TR 102 045 v1.1.1. Electronic Signatures and Infrastructures (ESI); Signature policy for extended business model. Marzo 2003.

[13] ETSI TR 102 271 v1.1.1. Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies. Diciembre 2003.

[14] ETSI TS 101 733 v1.7.3. Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES). Enero 2007.

[15] ETSI TS 101 903 v1.3.2. XML Advanced Electronic Signatures (XAdES). Marzo 2006.

[16] Internet Engineering Task Force, IETF. http://www.ietf.org.

[17] IETF RFC 3161. Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). Agosto 2001.

[18] IETF RFC 3280. Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile. Abril 2002.

[19] ISO 7498-2: Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture. 1989.

[20] Kremer, S. y Markowitch, O. Optimistic non-repudiable information exchange. Biemond J (ed) 21st symposium on information theory in the Benelux, Wassenaar, The Netherlands. Werkgemeenschap Informatieen Communicatietheorie, Enschede, pp 139 – 146. 2000.

[21] Kremer, S., Markowitch, O., y Zhou, J. An Intensive Survey of Fair Non-Repudiation Protocols. Abril 2002.

[22] Lee, B y Kim, K. Fair Exchange of Digital Signatures using Conditional Signature. SCIS 2002, Symposium on Cryptography and Information Security. 2002.

[23] Ray, I. y Ray I. Fair Exchange in E-commerce. ACM SIGecom Exchange, Vol. 3, No. 2, Mayo 2002. Páginas 9-17.

[24] Zhou, J. y Gollmann, D. A Fair Non-repudiation Protocol. Proceedings of the IEEE Symposium on Research in Security and Privacy, páginas 55-61. Oakland, California. Mayo 1996.

[25] Zhou, J. y Gollmann, D. Observations on Non-repudiation. Lecture Notes in Computer Science 1163, Advances in Cryptology: Proceeding of Asiacrypt '96, págs. 133-144, Kyongju, Korea. Noviembre 1996.

[26] Zhou, J. y Gollmann, D. Evidence and Non-repudiation. Journal of Network and Computer Applications 20 (3). Páginas 267-281. 1997.