Comercio Electrónico basado en Servicios de Localización. Servicio de No Repudio

Benjamín Ramos, Ana I. González-Tablas, Arturo Ribagorda

Avenida de la Universidad, 30. 28911-Leganés

Universidad Carlos III de Madrid, España

{benja1, aigonzal, arturo,}@inf.uc3m.es

Resumen: En los últimos años han cobrado mucha importancia los servicios de localización y, consecuentemente, ha aparecido un numeroso tipo de negocios basados en ellos, entre los cuales merece citarse el comercio electrónico. Al estar basada tal actividad en las comunicaciones a través de telefonía móvil y redes informáticas, en especial Internet, la desconfianza en la seguridad de las transmisiones suele ser un impedimento para su desarrollo. Se precisa, por tanto, disponer de un mecanismo que proporcione diferentes servicios de seguridad destinados tanto a la empresa que usa los datos de localización del dispositivo móvil como al cliente que lo porta y al que se dirige la oferta publicitaria o las mejores condiciones de compra. CERTILOC, el mecanismo propuesto, certifica evidencias espacio-temporales asociadas al dispositivo móvil y a su portador, de forma que, además de garantizar comunicaciones seguras, los certificados emitidos serán de valiosa utilidad en casos de litigios posteriores. Se pretende, además, que las transacciones económicas asociadas al comercio electrónico dispongan del servicio de no repudio en origen y recepción.

Palabras clave: Comercio electrónico, Servicios de confianza, Servicio de No repudio, Servicios basados en la localización (*LBS*), Certificado espacio-temporal.

1. Introducción

En la última década se ha desarrollado un nuevo tipo de servicios en el que intervienen diferentes tecnologías y como consecuencia de los mismos han aparecido diversos tipos de negocio. Se trata de los Servicios de localización (*LS*, *Location Services*), de personas o dispositivos, y cuyo esquema suele consistir en detectar la presencia, en una zona determinada, del instrumento que porta un individuo que previamente ha consentido su localización bajo reglas pactadas entre él mismo y el Servicio de Localización (Hightower & Borriello, 2001). En algunos casos, el interés consiste en

obtener evidencias que acrediten el seguimiento de un itinerario concreto (Applewhite, 2002). Entre las situaciones más solicitadas merecen citarse, entre otras, el seguimiento de dispositivos móviles, el control de accesos a edificios o salas, la actividad de *m-commerce* mediante telefonía móvil, el rastreo de personas a través de sensores o chips, etc. De estos servicios de valor añadido (*LBS, Location Based Services*), muchos basan su oferta en la posibilidad de localizar al usuario demandante del servicio para proveerle de una información útil en un momento determinado, por ejemplo cuando se encuentra dentro de un área definida (Gajparia, Mitchell & Yeun, 2004).

Respecto del comercio electrónico, los sujetos y los objetos involucrados precisan de comprobaciones fidedignas de las partes implicadas (autenticación de entidades), discreción (confidencialidad), garantía del contenido (integridad) o prevención de negaciones en las transacciones (no repudio). La localización de un usuario puede ser utilizada en los servicios de acreditación y sellado espacio-temporal, un tipo reciente de servicios de emisión de evidencias digitales (evidencias espacio-temporales, EET) que certifican el lugar en el que se encuentra un individuo o un dispositivo móvil en un momento determinado (Directiva 2006/24/CE y Kabatnik & Zugenmaier, 2001).

Los servicios de confianza citados son similares a los de certificación de identidad y atributos o los sistemas de credenciales. Las credenciales pueden utilizarse para controlar el acceso a ciertos servicios o para otorgar privilegios asociados a la posición actual o pasada del sujeto o su historial de localizaciones. También pueden usarse para la asignación de responsabilidades en aplicaciones de seguimiento de recursos o entidades (por ejemplo, materiales peligrosos o de gran valor, trabajadores en rutas, presos bajo libertad condicional o nodos en una red). En otros casos las EET pueden usarse para justificar la aceptación de transacciones electrónicas o de su coste dependiendo del lugar-tiempo en que éstas se realizan o desde donde se utiliza un servicio (Davies & Gellersen, 2002 y Zugenmaier, Kreutzer & Kabatnik, 2001). Generalmente es un tercero de confianza (TTP) la entidad que adopta el rol de generador de las evidencias.

2. Trabajos previos y soluciones de aseguramiento

En la actualidad, los servicios de localización y seguimiento empiezan a reconocerse como uno de los pilares que sustentarán el comercio electrónico móvil, el *m-commerce*, detectándose gran número de aplicaciones orientadas tanto al usuario final como a las empresas. Respecto del usuario, pueden citarse algunos servicios para el consumidor, tales como las guías sobre el lugar de destino, los servicios de tráfico o las alertas climatológicas, la publicidad dependiente de la ubicación, los localizadores o

buscadores de menores, amigos o pertenencias varias (vehículos), la asistencia en carretera, etc. Respecto de las empresas, son habituales los servicios de navegación basada en sistemas GPS (en breve Galileo), la planificación de itinerarios, el control y la monitorización de flotas, las búsquedas en proximidad, el seguimiento de recursos o personas, etc.

Obviamente, uno de los retos más importantes en esta área consiste en dotar a las aplicaciones de los servicios de seguridad, confianza y privacidad requeridos. Hasta ahora, gran parte del trabajo realizado se ha centrado en preservar la privacidad de las personas implicadas, a la vez que se permite el disfrute a los usuarios de las ventajas de estos servicios de localización y seguimiento.

Desde el punto de vista de la seguridad, los servicios de certificación están cada vez más integrados en nuestra sociedad. Ejemplos cercanos de su aplicación se hallan en la declaración de impuestos a través de Internet, en novedosos sistemas de votación electrónica, y en general la cada vez mayor integración de la administración con las tecnologías de la información, la e-Administración, por no citar protocolos tan conocidos y utilizados como SSL o SET.

La mayoría de los servicios citados están sustentados por la tecnología de clave pública y, en concreto, están fundamentados en el mecanismo de certificación de identidad, de atributos o privilegios, o de otras informaciones. La infraestructura de certificación más reconocida en la actualidad es la definida por el grupo de trabajo *PKIX* del *IETF*, cuyo resultado se recoge en la normativa X.509 (*IEFT Working Group*). Un servicio relativamente nuevo, y que ya dispone de normas, ya sean integradas dentro del marco X.509 o bien definidas para un marco más general, se ofrece como referencia para los propósitos de este trabajo. Se trata del servicio de Sellado de Tiempo o *Time-Stamping* y está relacionado intrínsecamente con el mecanismo que aquí se expone. Otro servicio novedoso sobre el que en parte está fundamentado este trabajo es el servicio de Sellado de Lugar (*Location-Stamping*) para redes GSM propuesto conjuntamente por dos universidades alemanas durante el año 2001.

Por último, existe en la actualidad un gran número de proyectos en marcha (españoles, europeos, internacionales) para la creación de plataformas seguras en *e-commerce* en donde se buscan protocolos de no repudio justos[1], sea basados en el concepto de firmas digitales condicionales[2] o bien en políticas de firma[3].

---

1 Protocolo de no repudio justo: el que satisface el no repudio en origen y en destino

2 Firma digital condicional: aquella en la que se firma tanto los datos en sí como una condición, la cual supedita la validez de dicha firma al cumplimiento de la condición impuesta

3. Comercio electrónico

El comercio electrónico consiste en la compra, venta, marketing y suministro de información complementaria para productos o servicios a través de redes informáticas. La industria de la tecnología de la información podría verlo como una aplicación informática dirigida a realizar transacciones comerciales, mientras que una definición alternativa lo vería como una gestión de comunicaciones de negocios comerciales a través de métodos electrónicos. En la actualidad incluye actividades de compra de bienes y servicios a través de servidores seguros, con tarjetas de compra electrónica y con servicios de pago electrónico tales como autorizaciones para tarjeta de crédito. De las variantes en comercio electrónico (directo, indirecto, etc.) el que aquí interesa, de entre los más habituales, es el de ventas de empresa a consumidor. Las claves del éxito del comercio electrónico se encuentran asociadas al logro de los siguientes objetivos:

- Ofrecer productos que atraigan clientes potenciales a un precio competitivo, como en el comercio tradicional.
- Favorecer una compra amigable, interactiva, tal como se podría alcanzar en una situación cara a cara.
- Mostrar una página web atractiva.
- Incentivar a los consumidores con promociones, ofertas especiales, descuentos, publicidad, etc.
- Proporcionar una atención personal.
- Favorecer un sentido de comunidad entre vendedor y clientes compradores.
- Garantizar la seguridad (autenticación, integridad y no repudio) y la privacidad.
- Proporcionar una visión global de la relación con el consumidor.
- Poseer la experiencia total del consumidor.
- Optimizar los procesos de negocio.
- Dejar que los consumidores se ayuden a sí mismos.
- Ayudar a los consumidores a hacer el trabajo de consumir.
- Construir un modelo de negocio sólido.
- Crear una cadena de valor añadido en la que uno se orienta a un número “limitado” de competencias clave.
- Operar en o cerca del límite de la tecnología y permanecer allí mientras la tecnología sigue cambiando.

---

[3] Política de firma: documento donde se recogen las condiciones bajo las cuales se puede asegurar la validez de una firma electrónica que haya sido generada en base a dicha política

- Construir una organización con suficiente agilidad y sistemas de alerta para responder rápidamente a los cambios en el entorno económico, social y físico de una empresa.

Sin embargo, los intentos de muchas empresas en establecerse en este nuevo sistema de vender han resultado infructuosos, debido, en ocasiones, a soluciones tecnológicas mal resueltas (implementaciones inconsistentes o poco seguras) y en otros casos a no tener en cuenta algunos principios básicos del comercio tradicional. Algunas de las causas por las que comercio electrónico sigue sin acabar de triunfar, superadas las relativas a plataformas tecnológicas adecuadas, tiene que ver con la forma de ser y de sentirse el comprador, de su confianza en la tienda y el tendero, del intercambio tranquilizador de su dinero por su inmediato producto, etc. El cliente necesita sentirse amparado antes posibles disputas futuras con el vendedor. Para una buena aceptación del comercio electrónico, deberían desaparecer totalmente, o en buena medida, las siguientes lagunas:

- Preocupación sobre la seguridad. Mucha gente no utilizará las tarjetas de crédito en Internet debido a su recelo sobre un posible hurto o fraude. Además, comprador y vendedor se sentirán más tranquilos si el no repudio está asegurado para ambos.
- Falta de gratificación instantánea en la compra. Mucha recompensa obtenida por el consumidor en la compra reside en la gratificación instantánea que supone la utilización del producto. Esa recompensa no existe cuando la compra tarda en llegar días o meses.
- El problema del acceso a la web, particularmente para hogares pobres o en países subdesarrollados. Las tasas bajas de penetración de Internet en algunos sectores reduce el potencial del comercio electrónico.
- Aspecto social de la compra. Algunas personas les gusta hablar sobre el género con los dependientes o acompañantes: esta recompensa social de la terapia comercial no existe de igual forma en las compras *on line*.

4. Servicios de Certificación Espacio-Temporal

Las actividades comerciales, gubernamentales, administrativas, financieras y legales, entre otras, se han basado tradicionalmente en la existencia de niveles de confianza entre las personas y organizaciones participantes en las transacciones. Los mecanismos usados en estos casos incluyen reuniones cara a cara, cartas de recomendación, referencias, testigos, avales, etc. Con la aparición e implantación en nuestra sociedad de tecnologías que permiten las comunicaciones remotas usando medios electrónicos,

se ha requerido la traslación de tales actividades a este nuevo medio. Para que este proceso sea exitoso es necesario proporcionar mecanismos similares que permitan establecer niveles de confianza en el contexto de las comunicaciones electrónicas (Weiser, 1991). Los servicios de confianza, ya existentes en el contexto de las transacciones tradicionales, tienen precisamente ese objetivo (Burmester, Desmedt, Wright. & Yasinsac, 2004).

Los servicios de confianza son habitualmente provistos por entidades confiables o Terceros de Confianza (*Trusted Third Party* o *TTP*). Ejemplos de este tipo de servicios son, entre otros, los servicios de autenticación, autorización, confidencialidad, anonimato, cuantificación de los niveles de confianza, entrega y recepción garantizada (no repudio), archivo y notarización. La provisión de estos servicios se debe sustentar en marcos legales y en la definición de políticas públicas del servicio, en particular de seguridad y responsabilidad. Los servicios de acreditación y sellado espacio-temporal (SASET) se encuadran dentro de estos servicios de confianza provistos por *TTP*. Su propósito es precisamente proporcionar evidencias digitales acerca de las condiciones espacio-temporales de cierta entidad o documento, de forma que se permita posteriormente resolver disputas acerca de estas condiciones. La información espacio-temporal que se acredita en las evidencias se denotará como IET y las propias evidencias espacio-temporales como EET. Se distinguen dos tipos de servicios de evidencias espacio-temporales según el objetivo concreto que persiguen:

- El primero de ellos considera los servicios de acreditación espacio-temporal (SAET), cuyo objetivo es acreditar las condiciones espacio-temporales de una entidad denominada sujeto de la evidencia (S). Este sujeto suele ser un dispositivo localizable (D), aunque a veces este término puede incluir además a un usuario o controlador del dispositivo (DC) que esté controlando éste. Los SAET son similares a los servicios de acreditación o sistemas de credenciales.

- El segundo tipo lo componen los servicios de sellado espacio-temporal (SSET), en este caso el objetivo de estos servicios es acreditar que un determinado documento existía en un lugar determinado en cierto momento temporal o que cierta acción se realizó sobre éste. Los SSET pueden considerarse similares a los servicios de no repudio.

Una entidad de confianza, la entidad Generador de las Evidencias Espacio-Temporales (Ge), emitirá las credenciales y los sellos espacio-temporales que dan fe de estos hechos. Habitualmente es un tercero de confianza, *TTP*, el que toma este rol, aunque a veces puede serlo también un módulo confiable (*Trusted Platform Module* o *TPM*). En la provisión del servicio participa un Servicio de Localización (*Spatial-Temporal Information Service* o *STIS*) que aportará la información de localización del sujeto S.

5. Servicio de No Repudio

De entre las múltiples características que se pueden señalar de las transacciones seguras cabe destacar una nueva figura jurídica, el No Repudio. Dicha figura aparece cuando una determinada comunicación o mensaje electrónico adquiere fuerza vinculante o efectos jurídicos, ante el posible rechazo o reclamación de su no-existencia. A diferencia de la autenticidad y la integridad el no repudio consiste en la capacidad de probar a una tercera parte que una específica comunicación ha sido realizada, admitida y enviada a, o por, una determinada persona. Las normas civiles y usos de comercio han estado desde siempre preocupados por la búsqueda del no repudio. Las firmas, notarios, correo certificado y autoridades de registro son ejemplos de los mecanismos utilizados tradicionalmente para conseguir el no repudio del contrato (Ramos, 2003). La firma digital del mensaje por parte del emisor, si está correctamente implementada, se convierte en una prueba fehaciente de quién firmó (autenticación), qué datos son los que se firmaron (integridad) y, finalmente, consigue el efecto jurídico del no repudio.

Las comunicaciones, ya sean bilaterales o multilaterales, abarcan generalmente dos tipos de partes, el emisor y el receptor. De igual forma, el no repudio podría dividirse en dos formas o tipos: No repudio en origen y No repudio en destino. El no repudio en origen evita o resuelve posibles conflictos sobre la creación o no por una parte (el emisor) de un mensaje concreto en un momento determinado (inclusión del sello de tiempo). Este tipo de no repudio concede a los receptores de los mensajes una validez probatoria suficiente como para resolver futuros conflictos, como por ejemplo que el emisor niegue haber enviado un mensaje, o que el mensaje recibido es diferente de lo que el emisor dice haber enviado, así como la discrepancia de la fecha y hora de envío. En el ámbito del comercio electrónico seguro, los pasos necesarios para la consecución de un servicio de no repudio seguro incluyen las siguientes actividades (Ramos, 2003):

1. Solicitud del servicio: Para conseguir el efecto del "no repudio" es necesario que uno o varios de los participes en una comunicación estén de acuerdo antes de originar el mensaje y enviarlo, en utilizar los servicios del "no repudio". Por tanto, requiere que una de las partes o ambas realicen una solicitud de aplicación del no repudio a sus futuras comunicaciones. Dichos requerimientos o solicitudes no serán siempre necesarios, si bien suele ser una practica habitual en determinadas actividades ya sea por que la ley lo dice o porque los usos del comercio así lo establecen.

2. Emisión de una prueba. Dicha emisión hace referencia tanto a la emisión del mensaje como a su recepción, es decir en el repudio de origen corresponderá al emisor generar dicha prueba y en el repudio de destino será el receptor el encargado de generar dicha prueba. Para ello se acudirá a terceras partes de confianza o a

autoridades de certificación, o se usará la firma digital para obtener así la prueba deseada.

3. Transmisión de la prueba: una vez obtenida la misma, los generadores en cada extremo de la comunicación deben transmitir la prueba a las partes contrarias para que ésta pueda ser verificada. De esta forma, la siguiente actividad a desarrollar será:

4. La Verificación de la prueba: una vez transmitida la prueba corresponderá a su receptor verificar que dicha prueba se ha generado y transmitido correctamente conforme a lo pactado anteriormente. Aquí entrarían en juego las Autoridades de certificación, ya que el receptor debe verificar que efectivamente dicha parte es quién dice ser (autenticación) y que la firma electrónica del documento está actualmente vigente en el mercado. Esta fase es crucial, ya que los mensajes pueden ser firmados digitalmente pero ello no quiere decir que sean plenamente efectivos puesto que su firma puede no tener vigencia o fuerza vinculante por encontrarse revocada.

5. Finalmente, la Conservación de la prueba. No cabe duda de que para poder obtener los efectos pretendidos por el no repudio es imprescindible poder demostrar en el futuro que dicha comunicación existió y, por tanto, poder presentar ante el juez en caso de conflicto una prueba consistente que demuestre que lo que se aceptó, emitió y envió es jurídicamente vinculante.

Por otro lado la integridad de los datos evita que éstos sean modificados durante el trasiego telemático o para cumplir fines ilícitos de una de las partes. A pesar de que no se puede conseguir el no repudio sin la autenticación y la integridad de los datos, el no repudio consiste en algo más que la autenticidad o integridad, es la capacidad de probar a una tercera parte que una determinada comunicación ha sido originada, admitida y enviada a una determinada persona.

6. Mecanismo seguro para certificar las EETs

Se propone un mecanismo de certificación de la localización, CERTILOC, que proveerá de los servicios de seguridad que más adelante se enumeran y en el que participan las entidades que se muestran en la Figura 1. El mecanismo contempla diferentes tipos de certificados, sustentados en criptografía de clave pública y firma digital.

- Generador de EETs o Ge (*generator of spatialtemporal evidences*), entidad fundamental en CERTILOC: genera, almacena y pone a disposición de los usuarios las evidencias espacio-temporales.
- Repositorio de evidencias (*evidence repository*): almacena las EET generadas por Ge.

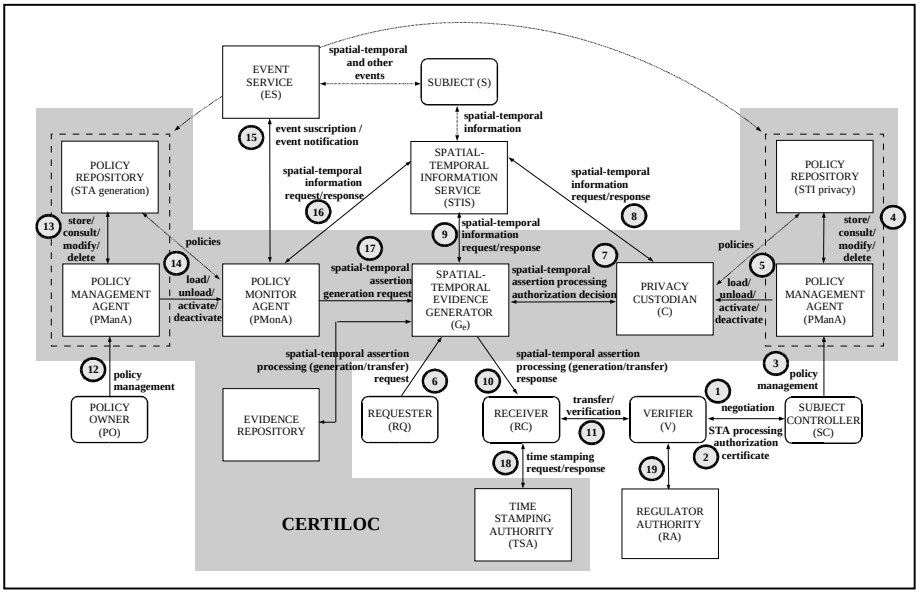

Figura 1 – Esquema de relaciones entre las entidades involucradas en CERTILOC

- Custodio de la privacidad de la información espacio-temporal o C (*custodian of spatial-temporal information privacy*): protege la privacidad de los sujetos.
- Agente monitor de políticas o *PMonA* (*policy monitor agent*): se encarga de solicitar la generación de evidencias según las políticas establecidas.
- Agente administrador de políticas o *PManA* (*policy administrator agent*): permite a los usuarios administrar las políticas de generación de CET y las políticas de privacidad de la IET.
- Repositorio de políticas (*policy repository*): almacena las políticas utilizadas.
- Servicio de información espacio-temporal (*STIS*, *spatial-temporal information service*): informa de la localización de los sujetos en un momento dado.
- Servicio de eventos o *ES* (*event service*): notifica la ocurrencia de eventos relacionados con las condiciones espacio-temporales del sujeto.

- Autoridad de sellado temporal o *TSA* (*time stamping authority*): genera sellos de tiempo y anclas de tiempo confiables.
- Autoridad reguladora o *RA* (*regulator authority*): puede auditar el comportamiento de las entidades de CERTILOC, así como el tratamiento que realizan los usuarios sobre las EET.

Por otro lado, los usuarios de CERTILOC son los siguientes:

- Sujeto o *S* (*subject*): es la entidad cuya información espacio-temporal se acredita en la evidencia.
- Controlador del sujeto (*SC, subject controller*): entidad responsable del sujeto.
- Solicitante o *RQ* (*requester*): solicita la generación o transferencia de evidencias espacio-temporales.
- Receptor o *RC* (*receiver*): recibe evidencias espacio-temporales.
- Verificador o *V* (*verifier*): verifica evidencias espacio-temporales.
- Propietario de políticas o *PO* (*policy owner*): configura políticas de generación automática de evidencias espacio-temporales.

Los servicios que proporciona CERTILOC son los siguientes:

- Acreditación espacio-temporal (SAET). Este servicio permite a los usuarios de CERTILOC solicitar la generación y la transferencia de nuevas credenciales espacio-temporales (CET). En CERTILOC se complementa con los de gestión de la privacidad de la IET (PIET) y de la generación automática de EET.
- Sellado espacio-temporal (SSET). Este servicio permite que los usuarios de CERTILOC obtengan sellos espacio-temporales (SET) que acrediten la información espacio-temporal bajo la que se generó una firma digital sobre algún documento en poder de los usuarios.
- Sellado temporal (SST). Los usuarios pueden solicitar la emisión de sellos temporales (ST) sobre documentos bajo su poder.
- Gestión de la PIET. Este servicio complementa el de acreditación espacio-temporal de CERTILOC. Permite que los usuarios configuren sus preferencias sobre la privacidad de su IET. Las preferencias podrán considerar, por un lado, bajo qué condiciones un usuario desea autorizar la generación o transferencia de una EET dependiendo de factores tales como quién lo solicita, con qué

finalidad y/o cuál es la situación espacio-temporal del sujeto y, por otro lado, qué condiciones de tratamiento de las EET desean asociar a éstas.

- Gestión de la generación automática de EET. Permite a los usuarios configurar sus preferencias con el objetivo de generar EET de forma automática dependiendo de las condiciones espacio-temporales del sujeto o de eventos.

7. Conclusiones

Se ha comenzado exponiendo la aparición relativamente reciente en la Sociedad de la Información de unos servicios de valor añadido, los servicios basados en la localización (*LBS*), capaces de obtener nuevos datos relativos a las personas, los que constituyen la Información Espacio-Temporal, y cuya cesión a terceros puede comprometer la privacidad y la intimidad de los individuos pero que, bajo compromisos mutuos entre empresas e individuos, facilitan una nueva modalidad de comercio electrónico.

La habitual desconfianza de los consumidores tanto en la recepción de mensajes a móviles como las transacciones a través de Internet, queda ahora despejada con la solución diseñada y expuesta, CERTILOC, un mecanismo que garantiza, mediante la certificación de evidencias digitales espacio-temporales y la correcta gestión de los certificados, las condiciones idóneas para el desarrollo de las actividades citadas en condiciones seguras. El marco de la certificación se engloba en una PKI habitual.

Finalmente, para paliar la desconfianza en las transacciones y aumentar la eficacia del *e-commerce*, se buscan soluciones para fortalecer el servicio de no repudio, demandado habitualmente entre vendedores y compradores.

Este artículo se enmarca dentro del Proyecto de Investigación CERTILOC, Servicio de CERTIficacion digital de la LOCalizacion, Ref. SEG2004-02604, concedido en el marco del Plan Nacional de Investigación Científica, Desarrollo e Innovación Tecnológica 2004-2007. Ministerio de Educación y Ciencia. España.

Referencias

Applewhite, A. What Knows Where You Are? Personal Safety in the Early Days of Wireless. *IEEE Pervasive Computing, 1:4* 4-8, 2002.

Burmester M., Desmedt Y., Wright R. N. and Yasinsac A.. Accountable privacy. *In The Twelfth International Workshop on Security Protocols,* April 2004.

Davies, N. and Gellersen, H.-W. Beyond prototypes: Challenges in Deploying Ubiquitous Systems. *IEEE Pervasive Computing 1:1* 26-35, 2002.

Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público.

ETSI TR 102 045 "Electronic Signatures and Infrastructures (ESI); Signature policy for extended business model". Marzo 2003.

Gajparia A., Mitchell C. J. and Yeun C. Y. Information Preference Authority: Supporting user privacy in location based services. *In To be presented at NordSec 2004, The 9th Nordic Workshop on Secure IT-systems*, November 2004.

González-Tablas, A. I., Ramos, B., and Ribagorda, A.: Path Stamps, A Proposal for Enhancing Security of Location Tracking Applications. *Proceedings of the Ubiquitous Mobile Information and Collaboration Systems Workshop (UMICS'2003)*, Klagenfurt/Velden, Austria, 2003.

Hightower, J. and Borriello, G. Location Systems for Ubiquitous Computing. *IEEE Computer, August 2001 57-66*, 2001.

IEFT Working Group: Public-Key Infrastructures (X 509), (PKIs).

ISO/IEC 13888-1:2004 IT security techniques - Non-repudiation - Part 1: General.

Kabatnik M. and Zugenmaier A. Location stamps for digital signature: A new service for mobile telephone networks. *In Proceedings of the First International Conference on Networking-Part 2* (ICN'01), LNCS 2094. Springer-Verlag, 2001.

Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico, 2002.

Ramos, B., González-Tablas, A. I., and Ribagorda, A.:CERTILOC: un mecanismo seguro para m-Marketing y Comercio electrónico basados en servicios de localización. *Actas del IV Simposio Internacional de Sistemas de Información e Ingeniería del Software en la Sociedad del Conocimiento (SISOFT2006)*, Cartagena de Indias, Colombia, 2006.

Ramos, F. Aspectos a tener en cuenta para implantar una solución de comercio electrónico segura y efectiva (séptima parte). *Legalia Abogados*, 2003.

Weiser, M. The Computer of the 21st Century. Scientific American, 265:3. 1991.

Zugenmaier, A., Kreutzer M., and Kabatnik M. Enhancing applications with approved location stamps. *In Proceedings of the IEEE Intelligent Network 2001 Workshop* (IN 2001), 2001.