LA NECESIDAD DE REGULAR LA CERTIFICACIÓN DE LA LOCALIZACIÓN DE ENTIDADES EN EL ÁMBITO DE LAS COMUNICACIONES ELECTRÓNICAS

Ana Isabel González-Tablas Ferreres (Profesora Ayudante)
Benjamín Ramos Álvarez (Profesor Titular de Universidad)
Arturo Ribagorda Garnacho (Catedrático de Universidad)
Grupo de Seguridad de las Comunicaciones y las Tecnologías de la Información
Departamento de Informática - Universidad Carlos III de Madrid

I Introducción

Ha pasado más de medio siglo desde que apareció ENIAC, considerado como el primer ordenador de la historia, y dio comienzo la era en la que ahora vivimos, la era de la información. Tanto ha afectado este hecho a nuestras costumbres que denominamos a la sociedad en la que estamos inmersos como la sociedad de las tecnologías de la información. Estas tecnologías experimentan desde hace un tiempo y de forma continuada una gran evolución. El objetivo hacia el que se dirigen fundamentalmente es el proporcionar un acceso a la información de forma global, personalizada, en cualquier momento y desde cualquier lugar. Si, además, añadimos a estos requerimientos la característica de transparencia en el acceso obtenemos el paradigma de la computación ubicua, tan en auge en la actualidad.

Los dispositivos que proporcionan el acceso a la información y a los servicios asociados a ésta son los teléfonos móviles, los asistentes digitales personales (PDAs), los ordenadores portátiles, etc. Estos dispositivos convergen cada vez más en las funcionalidades ofertadas, y la característica común que destaca en todos ellos es la movilidad.

Los servicios y aplicaciones dependientes del contexto[1], y en particular dependientes de la información de localización, constituyen una de las áreas que más interés ha despertado dentro del marco de la computación ubicua. Se prevé que será uno de los mercados más importantes en los próximos años, ofreciéndose ya al usuario servicios de este tipo.

Desde el advenimiento de Internet, la seguridad y la privacidad se han planteado como una de las principales preocupaciones de la actual sociedad de las tecnologías de la información. Uno de los problemas más importantes que se presenta a la hora de implantar los servicios dependientes de la información de localización es precisamente la falta de esquemas y prácticas asentadas que otorguen seguridad y privacidad a esta información. A pesar de poder aplicarse las tecnologías y soluciones actuales de seguridad, no es suficiente ya que en este nuevo marco surgen necesidades y problemas distintos, para los que hay proponer nuevas soluciones.

Por supuesto, otro de los problemas que emergen es la falta de regulación que contemple la seguridad y la privacidad de estos datos de localización en todas sus facetas y que, a la vez, otorgue efectividad jurídica a estos datos de localización de forma que puedan utilizarse legalmente en el comercio y la Administración electrónicos.

II Servicios dependientes de la información de localización

Los servicios de localización (también denominados tecnologías de posicionamiento móvil) proporcionan información específica acerca de la información geográfica de terminales móviles, y, por ende, de los objetos o entidades a los que estén adjuntos o asociados aquellos, tómese como ejemplo el caso de una persona, un paquete o un vehículo.

Los servicios dependientes de la localización (nótese que los diferenciamos de los servicios de localización) ofrecen aplicaciones para el usuario, habitualmente basándose en la información de localización hallada a través del terminal móvil de aquél. Se puede acceder a estos servicios a través de un variado conjunto de dispositivos como teléfonos

[1] "Contexto: (...) 2. (m) Entorno físico o de situación, ya sea político, histórico, cultural o de cualquier otra índole, en el cual se considera un hecho. (...)". Diccionario de la Real Academia de la Lengua Española, 2001, versión electrónica: http://www.rae.es

El contexto al que aquí se hace referencia se podría definir como el conjunto de informaciones que pueden ser utilizadas para caracterizar la situación de una entidad. Entre estas informaciones se encontrarían la identidad de la entidad, la localización, la identidad de las entidades cercanas, el tiempo, las constantes biométricas, la velocidad en el caso de tratarse de una entidad móvil, los históricos de estas informaciones, etc.

móviles, módulos de rastreo para vehículos, etc. Además de la multitud de aplicaciones para el consumidor final, tienen una amplia aplicación en empresas e industrias. En estos casos se puede utilizar la información de localización en aplicaciones de gestión de relaciones con clientes (CRM), auditorías, planificación de redes, gestión de inventarios, servicios de campo, gestión de flotas, etc.

Como parte de los servicios dependientes de la localización encontramos los servicios de monitorización de la localización y seguimiento de entidades. Por un lado, estos servicios se utilizan cada vez más en entornos empresariales e industriales. Por otro lado, poco a poco se van venciendo los miedos ante la pérdida de privacidad de la entidad localizada y se van solucionando las trabas tecnológicas que permitirán que estos servicios de localización y monitorización se integren en el uso diario de ciudadanos. Posteriormente analizaremos la regulación existente que contempla el tratamiento de estos datos de localización.

La importancia de los servicios dependientes de la localización es tal que en el año 2000 Ovum[2] predijo que para el año 2006 existirían 182,3 millones de usuarios de este tipo de servicios con una tasa de penetración del 44%. Estas predicciones se pueden trasladar al año 2008[3] debido a la desaceleración que se ha producido recientemente en le mercado de las telecomunicaciones.

Por otro lado, dirigimos al lector interesado a las páginas web del Servicio de Información Comunitario sobre Investigación y Desarrollo[4] donde se puede apreciar el enorme esfuerzo que se está llevando a cabo en investigación relacionada con las tecnologías móviles y los servicios dependientes de la localización.

III Tecnologías de posicionamiento

Existen diversas plataformas y tecnologías para localizar un dispositivo (véase la Tabla 1), ya sea mediante redes de satélites, redes de telefonía móvil, radiofrecuencia, infrarrojos, ultrasonidos, o combinaciones de varias de estas tecnologías. Cada una de ellas ha adquirido diferente grado de madurez, precisión y estandarización.

[2] Ovum, “Mobile Location Services: Market Strategies”; Euroforum, Marzo 27-28, París (2000).

[3] EMILY.IST-2000-26040 Deliverable # 5 – User and System Requirements Report.

[4] Location Based Services cluster – LOBSTER http://www.cordis.lu/ist/ka4/mobile/proclu/c/lobster.htm
Dentro del V Programa Marco: http://www.cordis.lu/ist/so/mobile-wireless/home.html

A grandes rasgos las tecnologías de posicionamiento más utilizadas se pueden dividir en tres grandes bloques, dependiendo de cómo (y por quién) se calcula la información de localización:

- Soluciones basadas en la red (p.e. Cell-ID, TOA, etc.)

En este caso la posición del usuario se calcula en la red de comunicaciones y se transmite al terminal del usuario. Por supuesto, esta característica ha provocado una gran preocupación sobre aspectos tales como la integridad y la seguridad de los datos de localización del usuario ya que éste es localizado por la red. Por un lado, los mecanismos de posicionamiento están adecuadamente estandarizados y no es necesario modificar el terminal del usuario para utilizar estas soluciones. Por otro lado, son las soluciones con menor precisión[5] en el posicionamiento y sin cobertura global por el momento.

- Soluciones basadas en el terminal (p.e. GPS, Galileo, etc.)

La posición del usuario se calcula en el terminal utilizando señales provenientes de satélites o seudo satélites. Desde el punto de vista del usuario estas soluciones proporcionan mayor privacidad con respecto a los datos de localización, ya que es en el propio terminal del usuario donde se calcula la posición. La precisión del posicionamiento es bastante buena[6], y se puede considerar que se proporciona cobertura global si se incluye el uso de seudo satélites para interiores y áreas urbanas donde no alcanza a llegar la señal directa de los satélites. Una de las desventajas de estas soluciones es la necesidad de incluir un receptor específico en el terminal del usuario.

- Soluciones basadas en la proximidad (p.e. Bluetooth, etc.)

Estas soluciones están basadas en tecnologías de radio de corto alcance que no fueron diseñadas originalmente para localizar entidades. La cobertura que pueden proporcionar es muy limitada aunque, a cambio, la precisión se encuentra en un punto intermedio[7] entre la que se ofrece en las soluciones basadas en la red y la ofrecida por las basadas en el terminal.

Tabla 1: Una clasificación de las tecnologías de posicionamiento móviles[8].

ENTORNO DE	CATEGORÍA	PRINCIPALES

Dentro del VI Programa Marco: http://www.cordis.lu/ist/ka4/mobile/index.htm

[5] Desde 80 metros hasta 1 kilómetro o más dependiendo del tamaño de las celdas.

[6] Rangos de 0,1 a 1 metros si hablamos de GPS mejorado, y de 0,3 a 30 metros para GPS y A-GPS.

[7] Entre 3 y 300 metros.

[8] Fuente: mEXPRESS–IST-2001-33432 http://mexpress.intranet.gr/documentation.htm

APLICACIÓN		TECNOLOGÍAS
EXTERIORES	Basadas en la red (dependientes de la red de comunicaciones)	• Identificación de celda (Cell-ID) • Tiempo de llegada (TOA) • Diferencias entre tiempos de llegada (OTD)
	Basadas en el terminal (independientes de la red de comunicaciones)	• Sistema de Posicionamiento Global (GPS)
	Híbridas	• GPS asistido (A-GPS)
INTERIORES	Dependientes de la red	• Sensores infrarrojos • Tecnologías de ultrasonidos • Redes inalámbricas (WLANs) • Bluetooth • RF-ID
	Dependientes del terminal	• GPS interior (I-GPS)

IV Normativa acerca de los datos de localización en el ámbito de las comunicaciones electrónicas

La Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD) define los datos de carácter personal en su Artículo 3 apartado a) como

> "a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables".

La información de localización de una entidad identificada[9] podría considerarse por tanto un dato de carácter personal que debe ser protegido.

No es de extrañar que uno de las principales preocupaciones[10] de legisladores, empresarios, investigadores y ciudadanos sea proporcionar seguridad y privacidad a estos datos de localización sin que ello suponga dejar de disfrutar de las ventajas que se obtienen utilizando dicha información. Prueba de ello es la Directiva 2002/58/CE del

[9] Esto hace que se nos plantee la primera cuestión o reflexión acerca de la relación que se podría establecer entre la localización de un dispositivo móvil a nombre o cargo de una entidad identificable y la localización de dicha entidad, y más concretamente, en los efectos jurídicos de tal relación.

[10] Podemos citar como muestra de la preocupación existente el proyecto europeo PAMPAS IST-2001-37763 (Pioneering Advanced Mobile Privacy and Security) dentro del V Programa Marco, cuyo principal objetivo ha sido definir los retos y futuras líneas de investigación del VI Programa Marco en torno a la seguridad y privacidad de los sistemas y aplicaciones más allá de las redes de tercera generación (3G). Los servicios dependientes de la localización se tratan explícitamente en los documentos generados http://www.pampas.eu.org

Parlamento Europeo y del Consejo de 12 de julio 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), que hace referencia explícita a cómo deben tratarse los datos de localización de una entidad.

En la citada directiva se definen los "datos de localización" y los "servicios de valor añadido" que podrían hacer uso de aquellos; Artículo 2, apartados c) y g) respectivamente:

> "c) datos de localización: cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público;
>
> g) servicio de valor añadido: todo servicio que requiere el tratamiento de datos de tráfico o datos de localización distintos de los datos de tráfico que vayan más allá de lo necesario para la transmisión de una comunicación o su facturación;"

En el Artículo 4 se considera la seguridad que el proveedor de servicios de comunicaciones debe garantizar en los servicios que ofrece, así como el Artículo 5 hace referencia a la debida garantía de confidencialidad de las comunicaciones y los datos de tráfico generados. Sin embargo, el artículo más interesante para nuestros propósitos es el Artículo 9, donde se regula el tratamiento de los datos de localización, distintos de los datos de tráfico:

> "Artículo 9. Datos de localización distintos de los datos de tráfico
>
> 1. En caso de que puedan tratarse datos de localización, distintos de los datos de tráfico relativos a los usuarios o abonados de redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público, sólo podrán tratarse estos datos si se hacen anónimos, o previo consentimiento de los usuarios o abonados, en la medida y por el tiempo necesarios para la prestación de un servicio con valor añadido. El proveedor del servicio deberá informar a los usuarios o abonados, antes de obtener su consentimiento, del tipo de datos de localización distintos de los datos de tráfico que serán tratados, de la

> finalidad y duración del tratamiento y de si los datos se transmitirán a un tercero a efectos de la prestación del servicio de valor añadido. Se deberá ofrecer a los usuarios y abonados la posibilidad de retirar en todo momento su consentimiento para el tratamiento de los datos de localización distintos de los datos de tráfico.
>
> 2. Cuando se haya obtenido el consentimiento de un usuario o abonado para el tratamiento de datos de localización distintos de los datos de tráfico, el usuario o abonado deberá seguir contando con la posibilidad, por un procedimiento sencillo y gratuito, de rechazar temporalmente el tratamiento de tales datos para cada conexión a la red o para cada transmisión de una comunicación.
>
> 3. Sólo podrán encargarse del tratamiento de los datos de localización distintos de los datos de tráfico de conformidad con los apartados 1 y 2 personas que actúen bajo la autoridad del proveedor de las redes públicas de comunicaciones o de servicios de comunicación electrónicas disponibles al público o del tercero que preste el servicio con valor añadido, y dicho tratamiento deberá limitarse a lo necesario a efectos de la prestación del servicio con valor añadido.”

En la Ley 34/2002 de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico también se hace referencia en cierta manera a la forma en que deben ser conservados los datos de tráfico “necesarios para facilitar la localización del equipo terminal empleado por el usuario para la transmisión de la información [durante la prestación de un servicio de la sociedad de la información]”, haciendo referencia más adelante a que deben ser los imprescindibles para “identificar el origen de los datos alojados y el momento en que se inició la prestación del servicio” (Artículo 12).

Otra de las aportaciones de la citada ley a nuestra recopilación se desarrolla en el Artículo 29 de la misma:

> “Artículo 29. Lugar de celebración del contrato.

> Los contratos celebrados por vía electrónica en los que intervenga como parte un consumidor se presumirán celebrados en el lugar en que éste tenga su residencia habitual.
>
> Los contratos electrónicos entre empresarios o profesionales, en defecto de pacto entre las partes, se presumirán celebrados en el lugar que esté establecido el prestador de servicios."

V Planteamiento del problema

Desde hace siglos no resulta sorprendente el que un ciudadano haya debido confirmar que en un momento dado se hallaba en un lugar concreto, posiblemente para que su presencia en el sitio atestiguado le eximiera de alguna culpa. En la sociedad actual, demandante de servicios de seguridad y de cobertura jurídica, cabe igualmente esperar que una persona o un dispositivo electrónico necesiten acreditar su presencia[11] en el lugar exacto en el que sucede una acción de la que se deriva una comunicación o un documento digitales.

En operaciones tales como el comercio electrónico o el correo electrónico, los sujetos y los objetos involucrados exigen comprobaciones fidedignas de las partes implicadas (autenticación de entidades), discreción (confidencialidad) o prevención de negaciones (no repudio). En otras situaciones, como en trabajos de supervisión y reparación de estaciones de comunicación o en repartos de mercancías con tiempos y trayectorias preestablecidos, tanto los operarios como los artefactos utilizados precisan, en ocasiones, atestiguar su presencia en los lugares concretos de la maniobra (sellado de lugar adjunto a un registro, *location stamping*) e incluso del momento exacto de la estancia en el lugar de la operación (fechado de tiempo asociado a un documento, *time stamping*).

Supóngase que una persona se halla en un lugar concreto, determinado por unas coordenadas geográficas precisas, y necesita probar ante terceros (p.e. una entidad jurídica) que, en efecto, se encuentra en el lugar que dice estar. Esta obligación se la

[11] Con su controvertido proyecto TIA (*Total Information Awareness*, Conocimiento Total de la Información), la agencia de investigación DARPA (*Defense Advanced Research Projects Agency*), del Pentágono, se propone reunir toda la información sobre los movimientos, costumbres, etc. de una persona, para lo que perfecciona el programa LifeLog (literalmente "diario de vida").

impone en un momento en que, hallándose en el lugar, decide demostrar su estancia en el mismo. El rigor solicitado recuerda a la exigencia que se pide en el servicio de autenticación de entidades, es decir, que algún mecanismo logre demostrar de forma fehaciente que una entidad es realmente la que dice ser. ¿Se está demandando un servicio de autenticación de lugar? Más bien, parece que lo que se busca es el refrendo de que el personaje se halla en el lugar, corroborado éste como auténtico. Puede que transcurra un cierto tiempo sin que nada acontezca, la persona permanece inmóvil, y que el deseo probatorio incluya ahora el lugar y la hora, el individuo desee acreditar que se halla en un sitio concreto a una hora concreta. ¿Se está solicitando un servicio de autenticación de tiempo y lugar asociado a una persona? De nuevo, lo que se solicita es un refuerzo probatorio que certifique la estancia.

Sea ahora un dispositivo electrónico en manos de una persona que transita siguiendo una ruta, posiblemente preestablecida, de la que interesa saber si tal instrumento ha pasado por localizaciones concretas de ésta y, además, cuáles fueron los lugares anterior y posterior de cada localización. ¿Se trata ahora de autenticar el recorrido, es decir, acreditar los lugares por los que el dispositivo ha discurrido y el orden de la transición? Como en el caso del personaje, lo importante no es sólo el itinerario, sino asegurar que éste ha sido recorrido por una entidad reconocida y, además, certificar la asociación de la presencia de la entidad en cada uno de los puntos del trayecto, y quizá también del momento de la estancia.

Identificados los servicios de seguridad más demandados por las instituciones, y encontrados diferentes mecanismos que los consiguen, la sociedad digital, caracterizada por la creciente movilidad de sus individuos, y especialmente la comunidad dedicada al estudio de nuevos servicios de seguridad, se impone nuevos retos: certificar el lugar en donde sucede una cierta acción o en el que se halla una entidad determinada. Esta nueva necesidad obliga a definir claramente los elementos implicados, así como a tener en cuenta otros elementos de seguridad que pueden entrar en escena:

- fechado de tiempo (permite fijar la hora en que se produce el certificado de lugar),
- autenticación de entidades interventoras (imprescindible para el posterior uso del certificado),
- responsabilidad de identidades (para dirimir en caso de controversias), etc.

Por supuesto, uno de las tareas más importantes a las que se debe enfrentar nuestra sociedad es la de proporcionar un marco legal que regule la efectividad jurídica de los datos de localización hallados a través de los servicios de localización. También se

deberían regular los mecanismos y servicios de seguridad que permitan certificar esta información de forma que puedan esgrimirse como prueba legal ante terceras personas posteriormente.

En este punto queremos hacer notar al lector las diferencias existentes entre el concepto de "**certificado"**[12] tal como se define en la Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 por la que se establece un marco comunitario para la firma electrónica; Artículo 2, apartado g):

> "g) certificado: la certificación electrónica que vincula unos datos de verificación de firma a una persona y confirma la identidad de ésta;"

y las definiciones[13] de "certificado" y "certificado digital" que se proponen en el Glosario de Seguridad RFC 2828 del organismo de estandarización internacional para Internet (IETF[14]):

> "Certificado: [1. Definición recomendada para Internet] documento en el que se asegura la verdad de un hecho o la posesión de un objeto. [2. Definición recomendada para uso en seguridad] Véase: capacidad, certificado digital."

> "Certificado digital: [1. Definición recomendada para Internet] documento certificado en forma de objeto de datos electrónicos al que se adjunta el valor de una firma electrónica dependiente del objeto de datos (Véase: certificado de atributos, capacidad, certificado de clave pública)."

El concepto de "certificación" al que nos referimos los autores se acerca más al propuesto por el IETF, y no al "certificado" del marco de la firma electrónica europea que se restringe sólo a la acreditación de una clave pública a una identidad.

[12] "Certificación: 1. f. Acción y efecto de certificar. 2. f. Documento en que se asegura la verdad de un hecho." Diccionario de la Real Academia de la Lengua Española, 2001, versión electrónica: http://www.rae.es

[13] "**Certificate**: 1. (I) General English usage: A document that attests to the truth of something or the ownership of something. 2. (C) Security usage: See: capability, digital certificate. 3. (C) PKI usage: See: attribute certificate, public-key certificate." RFC 2828 , "Internet Security Glossary", May 2000.

"Digital certificate: 1. (I) A certificate document in the form of a digital data object (a data object used by a computer) to which is appended a computed digital signature value that depends on the data object. (See: attribute certificate, capability, public-key certificate.)" RFC 2828 , "Internet Security Glossary", May 2000.

En el propio documento RFC 2828 se aclara que las definiciones recomendadas para Internet se marcarán con "I" y los comentarios adicionales o de uso se marcarán con "C".

[14] The Internet Engineering Task Force (IETF) http://www.ietf.org

Esta certificación o acreditación electrónica del lugar o estancia de una entidad a la que hemos hecho referencia en los párrafos anteriores, sería necesaria en ciertas aplicaciones comerciales (*m-commerce*) o legales (firma de documentos o contratos electrónicos), realizadas a través de dispositivos móviles. La idea de sellar o certificar el lugar o la ubicación donde se encuentra una entidad fue expuesta por Kabatnik, Zugenmaier y Kreutzer en el año 2001. Su propuesta está enfocada a las redes GSM y consiste en certificar la información de ubicación de un usuario de la red o certificar que un usuario firma algún documento digital en algún lugar concreto, considerando opcionalmente la inclusión de un valor temporal o sello de tiempo. En su trabajo se destaca el impacto legal que podría tener este tipo de certificados, que ellos denominan sellos de lugar (*location stamp*), para el comercio o la firma de contratos electrónicos[15].

Una vez superado este envite, el siguiente desafío a afrontar es la certificación del itinerario[16] por el que va transitando una entidad móvil, de manera que se fije de forma indubitable cada uno de los lugares del recorrido, así como el orden secuencial de tránsito por los mismos. La necesidad de certificación de esta información se mantiene. Por ejemplo, esta necesidad de certificar un itinerario se plantearía en los siguientes casos:

- visitadores médicos, repartidores o comerciales, es decir, trabajadores itinerantes que hacen uso de las tecnologías de la información o *e-workers*, a los que se monitorizase su localización durante la jornada de trabajo, etc.
- transporte de mercancías peligrosas de acuerdo a determinada ruta preestablecida, etc.
- aplicaciones penales (prevención y protección de víctimas de malos tratos, monitorización de personas sujetas a libertad condicional), etc.

[15] Se pueden encontrar más detalles en el trabajo publicado por los investigadores M. Kabatnik y A. Zugenmaier, "Location Stamps for Digital Signatures: A New Service for Mobile Telephone Networks" ICN 2001, LNCS 2094, pp. 20-30, 2001, Springer-Verlag Berlin Heildeberg 2001; y en el trabajo de A. Zugenmaier, M. Kreutzer y M. Kabatnik, "Enhancing Applications with Approved Location Stamps" Intelligent Network Workshop IN 2001, Boston, MA, USA, IEEE 2001. En ellos se propone el concepto de **sello de lugar** (equivalente al certificado de lugar), y se describe una arquitectura y protocolo para la implementación de este servicio en las redes GSM.

[16] Este concepto de **certificado de itinerario** se ha propuesto en la ponencia de A. I. González-Tablas, B. Ramos y Arturo Ribagorda, "Path-Stamps: A Proposal on Enhancing Security of Location Tracking Applications", Ubiquitous Mobile Information and Collaboration Systems Workshop (UMICS 2003), CAiSE'03 Workshop Proceedings, June 16-17, 2003, Velden, Carinthia, Austria. En esta ponencia se presentan novedosas ideas acerca de las características y el funcionamiento de un sistema capaz de proporcionar este servicio de certificación de itinerarios.

En la publicación de B. Ramos, A. I. González-Tablas y A. Ribagorda, "Sellado y datación de ubicación e itinerario", Segundo Congreso Iberoamericano de Seguridad Informática (CIBSI'03), (pendiente de publicar en) Actas del Segundo Congreso Iberoamericano de Seguridad Informática (**CIBSI** '03), Octubre 28-31, 2003, Mexico D.F., México, los autores profundizan en las características de los servicios de seguridad que serían necesarios en los escenarios expuestos, así como en las entidades que deben proveerlos.

- aplicaciones comerciales (alquiler de coches con tarificación por recorrido o con servicios asociados a rutas de turismo personalizables), etc.
- aplicaciones para la administración (impuestos por el uso del coche -por contaminación-, cobro de tarifas de aparcamiento en entornos urbanos), etc.

Esta certificación de itinerarios también debería contemplarse en el marco jurídico al que se hace referencia anteriormente.

VI Sellado[17] y datación[18] de ubicación e itinerario

La idea de poder probar que algo o alguien estuvo en un lugar concreto no es nueva, se ha visto en suficientes litigios, casi siempre asociada a una hora precisa o a un intervalo temporal determinado. El mismo requerimiento probatorio puede aplicarse a un itinerario, en el que lo importante son los diferentes sitios por donde se ha pasado y el orden del recorrido, igualmente asociados casi siempre a un lapso de tiempo.

Lo que se anda buscando es una herramienta, un objeto, etc., que certifique la estancia, momentánea o perdurable, de la persona o el artefacto en el lugar, para que no quepa duda de que una u otro se hallan en el emplazamiento que manifiestan estar. En otro caso, la certificación de una ruta, el utensilio demandado actuará como garante de protección ante acusaciones de que la persona o el dispositivo no se hallaron en alguno de los sitios por donde realmente transitaron, o para dar fe del itinerario recorrido.

Las respuesta a las anteriores indagaciones pueden encontrarse enmarcadas dentro de una serie de nuevos servicios relacionados con la ubicación de una entidad móvil, a los que denominaremos Servicio de Sellado o Certificación de Lugar y Servicio de Datación de Lugar y de Itinerario, y a los que habrá que dotar de los elementos esenciales que les confieran la autoridad necesaria para la consecución de los fines perseguidos.

Los servicios de sellado de lugar ideados generan certificados de ubicación, los cuales asocian entidades con lugares, confirmando la presencia de una entidad en un lugar. La certificación exige de la doble autenticación de la entidad y el lugar. La certeza

[17] Sellar: Estampar, imprimir o dejar señalada una cosa en otra o comunicarle determinado carácter. Diccionario de la Real Academia de la Lengua Española, 2001.

[18] Datar: poner la data; Data: nota o indicación del lugar y tiempo en que se hace o sucede una cosa y especialmente la que se pone al principio o al fin de una carta o de cualquier otro documento; Datación: acción y efecto de datar. Diccionario de la Real Academia de la Lengua Española, 2001.

de la comparecencia, otorgada por el certificado, puede ser utilizada posteriormente en servicios de no repudio.

De igual manera, los servicios de datación de lugar y de itinerario ideados generan certificados de datación y certificados de itinerario. En el primer caso, éstos asocian entidades con una ubicación y un cierto momento temporal, exigiendo también autenticación del lugar y de la entidad. En el segundo caso los certificados generados aseveran que dicha entidad llevó a cabo un cierto itinerario o recorrido. Esta certificación exige de la autenticación del recorrido, es decir, el orden de los lugares por los que la entidad va transitando, además de la autenticación de la entidad y del conjunto de lugares.

Estos nuevos servicios, como los ya existentes en seguridad de la información, habrían de atenerse a normas[19], necesitarán de una estructura básica de funcionamiento (mecanismos y algoritmos criptográficos contrastados) y su uso se atendrá a políticas de seguridad establecidas en las organizaciones.

El objeto ideado para satisfacer el primero de tales empeños es el Certificado de Lugar, también denominado Certificado de Ubicación, generado por Autoridades confiables u obtenido mediante protocolos criptográficos. Si a esta información de ubicación, se añaden circunstancias temporales, se requerirá en su lugar de un Certificado de Datación. El tercer objeto ideado para el segundo empeño es el Certificado de Itinerario.

1. Entes implicados

A la hora de elegir las palabras[20] más acordes con las ideas expuestas, la riqueza de la lengua española ofrece más que suficientes, como se recoge en la XXII edición del DRAE, en el que han intervenido todas las Academias de la Lengua Española de América, Filipinas y España. A continuación se definen los elementos que participan en las diferentes fases del entramado propuesto.

- **Entidad**: Usuario o equipo físico que precisa probar su presencia en una ubicación debidamente reconocida.

[19] Por ahora no están contemplados con toda la profundidad requerida, en opinión de los autores

[20] Las siguientes tres entradas podrían igualmente haber sido elegidas como válidas para la propuesta. Estampar: Señalar o imprimir una cosa en otra. Estampillar: Marcar con estampilla. Estampilla: Especie de sello que contiene en facsímil la firma y rúbrica de una persona, o bien un letrero para estampar en ciertos documentos.

- **Demandante del certificado**: Entidad principal o subsidiaria que solicita el certificado para prevenir el no repudio, testimoniar una estancia, atestiguar un recorrido, etc.

- **Verificador**: Entidad que prueba la veracidad del certificado, pudiendo incluso utilizar para ello información no incluída en éste.

- **Proveedor de servicio de localización**: Entidad responsable de un servicio de localización, contratada por una entidad que demanda un certificado de ubicación o de itinerario, o por otras terceras partes como puede ser un proveedor de servicios de certificación.

  - **Ubicación**: Lugar, sitio o emplazamiento determinado por unas coordenadas (geográficas, simbólicas, ...) que lo sitúan de forma irrecusable.

  - **Itinerario**: Conjunto finito de lugares recorridos por una entidad, ordenado según la secuencia de transición por aquélla. En el conjunto, cada emplazamiento queda relacionado de forma unívoca con la pareja de lugares anterior y posterior, salvo, obviamente, los extremos del itinerario, primero y último.

  - **Sistema de localización**: Conjunto de técnicas y herramientas que permiten la identificación de un lugar con una precisión preestablecida.

  - **Servicio de localización**: Sistema que proporciona información de localización relacionada con una entidad ateniéndose a las políticas pertinentes.

- **Proveedor de servicio de certificación[21]:** Entidad responsable de un servicio de certificación; para el alcance de este trabajo se consideran servicios de certificación de lugar o de itinerario. Este servicio es contratado por una entidad que demanda certificados de ubicación o de itinerario.

- **Servicio de sellado o certificación de lugar o ubicación**: Servicio de seguridad que, mediante un certificado de ubicación, garantiza la presencia de una entidad en un lugar. Por tanto, el **certificado de ubicación** se puede definir como el documento que, avalado por una parte confiable o basado en técnicas criptográficas, confirma la presencia de una entidad en un lugar.

[21] Esta figura sería equivalente a la existente en la Directiva 1999/93/CE sobre “Prestador de servicios de certificación: la entidad o persona física o jurídica que expide certificados o presta otros servicios en relación con la firma electrónica;”, aunque teniendo en cuenta el significado que los autores atribuyen a los certificados.

- **Servicio de datación (de ubicación)**: Servicio por el que se certifica la presencia de una entidad en un lugar determinado a una hora determinada. El certificado emitido se denomina **certificado de datación.**

- **Servicio de datación (de itinerario)**: Servicio por el que se data cada uno de los emplazamientos de un recorrido y el propio recorrido o itinerario. Cada certificación parcial asocia a la entidad el emplazamiento, la hora y la información que se considere pertinente de los lugares anterior y posterior. El certificado generado se denomina **certificado de itinerario.**

- **Autoridad de certificación de ubicación**: Autoridad que certifica la estancia de una entidad (de la que se exige autenticación) en un lugar concreto (igualmente autenticado). Por tanto emite los certificados de ubicación.

- **Autoridad de datación**: Autoridad que atestigua la estancia de una entidad en un lugar concreto en una hora concreta o, también, acredita la presencia y hora de la entidad en cada uno de los sitios de un itinerario. Por tanto emite los certificados de datación y certificados de itinerario.

2. Esquema de relaciones

Definidas las entidades que pueden, o deben, considerarse en este escenario, se describen brevemente las relaciones que se dan entre ellas.

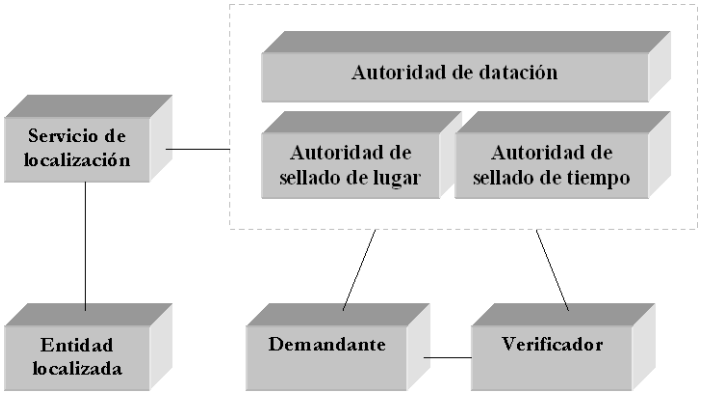

Figura 1: Esquema de relaciones entre las entidades involucradas

Las principales entidades son el *demandante* del certificado y la *autoridad de certificación de ubicación* (o la *autoridad de datación*). El demandante contrata los servicios de certificación al *proveedor* responsable del servicio ofrecido por dichas autoridades.

Por otro lado, el *servicio de localización* es la entidad que proporciona la información de ubicación de la *entidad localizada*. Esta información será solicitada por la autoridad de certificación según necesidad o cumpliendo la política de sellado aceptada tanto por el demandante como por el proveedor de servicios de certificación.

El *verificador* deberá ser capaz de comprobar o probar la validez del certificado, bien con los datos incluidos en el certificado o bien utilizando datos proporcionados por otras entidades, además del propio certificado.

VII Conclusiones

En este trabajo se ha resaltado en primer lugar la importancia creciente de los servicios dependientes de la localización, ofreciendo, a la vez, una visión de las tecnologías de posicionamiento más utilizadas para localizar entidades que demandan los citados servicios. Posteriormente, se ha presentado la importancia que los investigadores, las administraciones y los usuarios otorgan a la seguridad y la privacidad de estos servicios, y en concreto la asociada a los datos de localización. Esta preocupación también se refleja en las regulaciones ya existentes o en proceso de aprobación.

El objetivo de los autores al presentar estas reflexiones es doble:

1. Las aplicaciones relacionadas con la localización de lugares apenas disponen de medidas de seguridad, sobre todo en lo tendente a la autenticación (de sitios, estancias y entidades) y a la auditoría (histórico de transiciones de entidades por lugares). Los autores trabajan actualmente en la definición de un marco y un mecanismo que permita incorporar estos nuevos servicios de seguridad (sellado y datación de ubicación e itinerario) a los servicios dependientes de la localización. La propuesta supone una mejora basada en el poder probatorio de los certificados de ubicación y de la datación de itinerarios.

2. Cabe señalar que la normativa legal existente es insuficiente para cubrir las necesidades previstas en esta área. Se deberían resolver los siguientes interrogantes:

   - La eficacia jurídica que se otorga a los datos de localización obtenidos a través de un servicio de localización.
   - La normativa a la que un servicio de este tipo debe atenerse para que los datos de localización proporcionados sean reconocidos[22].
   - La provisión de normativas que regulen servicios de certificación y datación de ubicaciones e itinerarios.

Por supuesto, restan por aclarar muchos otros interrogantes relacionados con la configuración de los servicios y mecanismos de seguridad que se proponen. Y, obviamente, dada la poca madurez de las tecnologías implicadas surgen muchos problemas y obstáculos a resolver.

Para dar solución a la fortaleza que se presupone el disponer de un histórico de ubicaciones, se introducen los conceptos de datación de lugar y datación de itinerarios. Queda por investigar más a fondo lo que supone la incorporación del momento exacto de la presencia a certificar, es decir el sellado de tiempo asociado a una entidad en un lugar, lo que constituye la datación de lugar e itinerarios.

Por otra parte, un problema ya conocido por la comunidad científica se presenta cuando el proveedor de los servicios de certificación desaparece o deja de ofrecer el servicio. En este marco se debe considerar igualmente esta posibilidad, pudiendo asemejarse la solución a la que se aplica en el caso de otros tipos de certificados conocidos, la novación. Pero, además, se deben considerar otras extinciones, como la desaparición del tipo de coordenadas utilizadas o del propio lugar donde se ubicó la entidad con objeto de emitir el certificado. Lo lógico es aplicar de nuevo técnicas parecidas a la novación para mantener la vigencia del certificado.

Como conclusión final, y a pesar de las dificultades que se presentan, no debemos olvidar que los servicios dependientes de la localización son una realidad cada vez más presente y, más bien antes que después, la comunidad legislativa deberá proponer un marco que los regule.

[22] La utilización de este adjetivo, reconocidos, hace referencia al significado que se proporciona en la denominada firma electrónica reconocida (Directiva 1999/93/CE).