Hacia una Caracterización de los Servicios de Datación Digital con respecto a otros Servicios de Terceros de Confianza

Ana Isabel González-Tablas, Benjamín Ramos y Arturo Ribagorda
Grupo de Seguridad de las Tecnologías de la Información y las Comunicaciones (STIC)
Departamento de Informática. Universidad Carlos III de Madrid
{aigonzal,benja1,arturo}@inf.uc3m.es

Resumen. La aparición de los servicios de sellado de lugar o datación digital, obliga a los mismos a caracterizarlos con respecto a otros servicios de TC cuyo objetivo es también emitir evidencias digitales acerca de distintas informaciones. En este artículo se presentan las principales propiedades de los modelos de estos servicios, así como su análisis comparativo para plantear la caracterización de los servicios de datación digital con respecto a éstos.

1. Introducción

Recientemente los servicios de seguridad basados en Terceros de Confianza o TC (*Trusted Third Parties*) han adquirido gran importancia pues son claves para desarrollar con éxito actividades tales como el comercio-e y la administración-e. Con el desarrollo de éstos surge la necesidad de trasladar a este entorno digital ciertas funciones, figuras o roles existentes en nuestra sociedad actual 'no digital' [15] para proporcionar evidencias digitales acerca de hechos o acciones acaecidos en este entorno (p.e. la participación en una comunicación, la firma de un documento electrónico o su fecha de existencia).

La comunidad académica del área de la seguridad de la información ha desarrollado una serie de modelos y protocolos como son, entre otros, los de certificación de identidad y atributos, no-repudio y fechado digital, que proporcionan evidencias acerca de la relación entre una clave pública y la identidad de su propietario o entre dicha clave pública y una serie de privilegios, la participación de una entidad en una comunicación y las características o circunstancias de un documento o mensaje, su firma o su transmisión.

Con el avance de nuestra sociedad y el despliegue de nuevas tecnologías surgen nuevos tipos de informaciones o acciones sobre los que sería necesario emitir dichas evidencias digitales. En concreto, en los últimos años se ha hecho realidad la posibilidad de localizar entidades móviles a través de dispositivos habilitados para ello. Esta información puede ser calculada bien por el propio dispositivo, p.e. GPS, bien por terceras partes, p.e. a través de los servicios de localización (*LoCation Services* o LCS) proporcionados por redes celulares de telefonía o redes de radio de área local. Los servicios dependientes de la información de localización (*Location Based Services* o LBS) utilizan esta información para ofrecer servicios de valor añadido y se sitúan como uno de los principales nichos de mercado del sector de las comunicaciones móviles en los próximos años [3].

En el escenario que descrito, la seguridad, e incluimos en este concepto la privacidad, es un requisito fundamental para el desarrollo de aplicaciones y servicios, fundamentalmente los orientados al comercio-e, la administración-e y el comercio móvil (o comercio-m). Recientemente [16] se ha señalado como reto de investigación el desarrollo de mecanismos de no-repudio y trazabilidad de las acciones, así como de auditabilidad de las entidades responsables de los servicios, en el marco de la seguridad y la privacidad de sistemas y aplicaciones móviles de última generación. Como particularización de este reto, varios investigadores [4, 12, 13, 17, 21] han señalado que en determinadas aplicaciones podrían requerirse evidencias digitales acerca de la información de localización, por lo que sería necesario desarrollar servicios y mecanismos con este objetivo concreto. Los servicios de emisión de evidencias digitales existentes no son válidos por lo que se han propuesto unos nuevos servicios que han sido denominados servicios de sellado de lugar o datación digital.

Kabatnik, Kreutzer y Zugenmaier [12, 21] han propuesto un modelo y un protocolo de

sellado de lugar para redes GSM. Simultáneamente, los laboratorios Kent Ridge Digital Labs [13] han patentado un método para la provisión de estos servicios en redes inalámbricas que es compatible con las dos grandes tecnologías de localización existentes hoy en día (basada en el terminal o en la red). Analizando estas propuestas [12, 13, 21] se pueden detectar diversas carencias como la falta de flexibilidad y automatización (de acuerdo a las tendencias y necesidades impuestas por los servicios dependientes de la localización), la falta de adecuación de los servicios y sus arquitecturas a las nuevas normativas, y, especialmente, el olvido de la emisión de evidencias digitales acerca de itinerarios (dado que este es un concepto muy utilizado en los servicios dependientes de la localización). González-Tablas, Ramos y Ribagorda [4, 17] han propuesto una extensión a los servicios de sellado de lugar para que sean capaces de emitir evidencias de itinerarios y de incorporar flexibilidad y automatización en el sellado. Pero sigue existiendo una falta de formalización en la especificación, el diseño y el análisis de los protocolos de sellado de lugar que requiere una revisión de éstos en ese sentido, así como una caracterización de estos servicios respecto a otros servicios de terceros de confianza.

El objetivo de este artículo es precisamente caracterizar los servicios de sellado de lugar o datación digital con respecto a otros servicios de Terceros de Confianza analizando los modelos de las propuestas existentes y comparándolos con los modelos desarrollados para otros servicios de TC.

La estructura del artículo se desarrolla en tres apartados principales. En el apartado 2 se describen brevemente los servicios de TC con respecto a los cuales se caracterizarán los servicios de datación digital, así como las tres propuestas existentes de éstos. En el apartado 3 se analizan las diferencias y similitudes existentes en los modelos expuestos con el fin de plantear una discusión sobre la caracterización de los servicios de datación digital. Se finaliza con las conclusiones en el apartado 4.

2. Servicios avanzados de Terceros de Confianza (TC) en el ámbito de la criptografía de clave pública

Existen multitud de servicios de TC basados en criptografía de clave pública. En este apartado se considerarán sólo aquellos cuyos objetivos sean emitir evidencias digitales, y entre los mismos, aquellos cuyos modelos puedan relacionarse con los de los servicios de datación digital.

2.1 Servicios de certificación digital de identidad

La idea de utilizar criptografía para emitir evidencias digitales con el fin de resolver posteriormente disputas fue propuesta por primera vez en el contexto de la criptografía de clave pública. Un certificado digital de identidad es un documento electrónico firmado digitalmente por una entidad en quien confiamos, es decir, un TC; este documento es una evidencia digital de la vinculación entre una clave pública y la identidad de su propietario. La entidad que acredita dicha relación mediante su firma electrónica se denomina habitualmente Autoridad de Certificación o AC. En la actualidad, las entidades encargadas de gestionar, emitir, distribuir y verificar las claves públicas y los certificados asociados conforman las Infraestructuras de Clave Pública o ICP (*Public Key Infraestructures* o PKI). Aunque existen varios modelos para gestionar la confianza entre estas entidades, en este documento nos referiremos fundamentalmente a la definida en el marco PKIX [6]. Este marco especifica una arquitectura y un conjunto de protocolos que determinan una ICP para Internet, y en la actualidad se sitúa en la base de la mayoría de los protocolos y tecnologías de seguridad para Internet.

Las principales entidades contempladas en el marco PKIX son las siguientes: **entidad final** (usuario de los certificados emitidos y/o el sujeto de éstos), **Autoridad de Certificación o AC** (emite, almacena y revoca los certificados), **Autoridad de Registro o AR** (sistema opcional al que la AC delega ciertas funciones de gestión como registrar a los usuarios),

repositorio (sistema, a veces distribuido, que almacena los certificados y las listas de certificados revocados o LCR, así como permite el acceso a los mismos), y **emisor de LCR** (sistema opcional en el que la AC delega la publicación de LCR). Las ICP también suelen comprender otros TC que ofrecen servicios avanzados como archivo y recuperación de claves, fechado digital, confirmación de envío y entrega de mensajes, certificación o notarización de contenidos, etc.

Un certificado digital de identidad básicamente contendrá los siguientes datos: información sobre el titular del certificado, la clave o claves públicas del titular del certificado, datos del emisor del certificado, un número de serie único, periodo de validez y fecha de expiración, y la firma del emisor del certificado sobre un resumen de los datos anteriores.

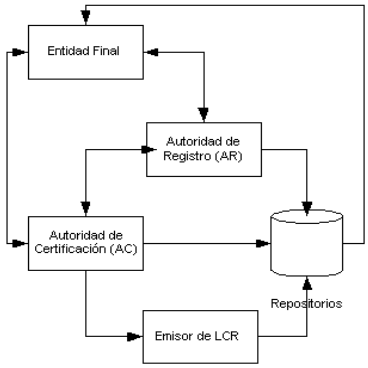

Figura 1: Principales entidades del modelo PKIX

2.2 Servicios de no-repudio

El objetivo general de un servicio de no-repudio se define como 'recoger, mantener, poner a disposición y validar evidencias irrefutables acerca de un evento o acción para resolver disputas sobre la ocurrencia de dicho evento o acción' [9]. Un servicio de no-repudio no previene (ni podría hacerlo) que una entidad repudie o niegue su participación en una comunicación [20]. En su lugar, el servicio proporciona evidencias o pruebas que pueden almacenarse y posteriormente presentarse ante un árbitro con el objetivo de resolver disputas que puedan surgir acerca de la ocurrencia del evento o acción. Se pueden encontrar en [14, 20] excelentes recopilaciones del estado de la cuestión de los protocolos de no-repudio, área donde aún quedan muchas cuestiones por investigar.

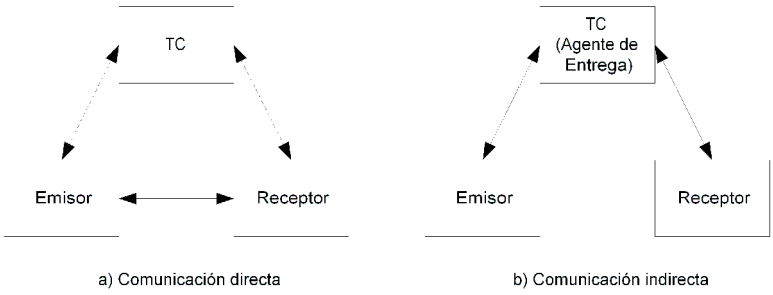

Figura 2: Modelos generales de no-repudio

Los objetivos concretos de un servicio de no-repudio dependen en gran medida de su tipo. El organismo internacional ISO define dos servicios básicos de no-repudio en su arquitectura de seguridad [8]: no-repudio con prueba de origen (proporciona una evidencia o prueba al receptor de los datos acerca del origen de éstos) y no-repudio con prueba de recepción (proporciona una evidencia o prueba a la entidad emisora de la información

acerca de que ésta ha sido recibida por el destinatario). Se reconocen además otros dos servicios de no-repudio referentes a una comunicación: no-repudio con prueba de envío o presentación y no-repudio con prueba de entrega.

En la norma ISO/IEC 10181-4 [9] se refina y extiende el concepto de servicio de no-repudio, así como se propone un marco para el desarrollo y provisión de estos servicios. En las tres partes que componen la norma ISO/IEC 13888 [10] se proporciona un modelo general para no-repudio y un conjunto de mecanismos de no-repudio basados en criptografía simétrica y asimétrica. El modelo de los servicios de no-repudio (Figura 2) habitualmente integra tres entidades [20]: **emisor** (envía el mensaje y respecto a quien se provee el servicio de no-repudio), **receptor** (recibe el mensaje y respecto a quien se provee el servicio de no-repudio) y **TC** (proporciona servicios de confianza al emisor y al receptor del mensaje). La comunicación de un mensaje desde el emisor hasta el receptor puede ser directa (el emisor y el receptor se comunican directamente entre ellos) o indirecta (la comunicación es a través de un TC que en este caso se denomina **Agente de Entrega**). Otros TC implicados en un servicio de no-repudio pueden ser [20] una **AC**, un **Fedatario** (asegura las propiedades de la información comunicada entre las entidades participantes en el protocolo), una **Autoridad de Fechado Digital** (AFD), y un **Árbitro o Juez** (resuelve las disputas). Las fases que se dan en un servicio de no-repudio que siga el modelo de la ISO se pueden ver en la Figura 3 [20], donde se utiliza el término de 'acción crítica' para referirse al acto de comunicación que es objeto del servicio de no-repudio.

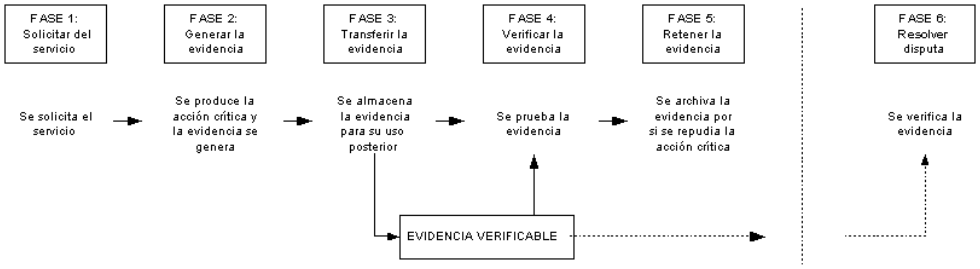

Figura 3: Fases en los servicios de no-repudio

Las evidencias de no-repudio deben satisfacer los requisitos de que el origen de la evidencia y su integridad puedan ser verificados por una tercera parte y que la validez de la evidencia sea innegable [20]. Dos de los mecanismos que se pueden utilizar para generar estas evidencias son los sobres seguros (*secure envelopes*) generados por un TC utilizando criptografía simétrica y las firmas digitales generadas por cualquier entidad utilizando criptografía asimétrica [10].

2.2.1 Servicios de notarización

Los servicios de notarización son un tipo de servicio de no-repudio un tanto especial por cuanto su significado no ha sido totalmente clarificado todavía. Habitualmente con este término se hacía referencia a la certificación del contenido o de otras propiedades de la información, es decir, su servicio sería prestado por la entidad Fedatario vista anteriormente como TC auxiliar en el modelo de no-repudio. Sin embargo últimamente es más común asimilar este término a los servicios electrónicos asociados a un notario humano [7]. Algunos autores han propuesto que los servicios de notarización electrónica, y las infraestructuras que los soporten, constituyan un concepto más amplio que comprenda la mayor parte de los servicios de TC habituales hoy en día [15].

2.3 Servicios de sellado de tiempo o fechado digital

Los servicios de sellado de tiempo o fechado digital proporcionan evidencias sobre la existencia de cierta información antes de un determinado instante de tiempo [1, 11]. En la mayoría de las aplicaciones prácticas, los servicios de fechado digital están a cargo de TC,

denominándose en este caso Autoridad de Fechado Digital (AFD) o Autoridad de Sellado de Tiempo. La AFD emite sellos de tiempo, que son aserciones electrónicas sobre la presentación de un documento ante la AFD en un cierto momento. Los servicios de fechado digital surgen por la necesidad de incluir de forma segura la dimensión temporal en el mundo digital y poder asegurar la existencia o la integridad de cierta información digital a partir de un momento dado [5]. Recientemente su importancia ha crecido considerablemente ya que son la clave para asegurar validez a largo plazo de los documentos digitales, especialmente de los certificados digitales o documentos sobre los que se ha aplicado alguna firma digital [2, 7].

A la vista de los objetivos de los servicios de no-repudio, los servicios de sellado de tiempo podrían tomarse como un caso especial de éstos, la evidencia en este caso no se referiría necesariamente a una comunicación o transferencia de un mensaje, sino a la existencia o la firma de un documento digital antes de un cierto momento o rango temporal. Tradicionalmente no se han considerado como tales sino como servicios de seguridad provistos por TC, y se consideran un soporte para los servicios de no-repudio, entre otros.

Los servicios de fechado digital han evolucionado en la última década, desde la utilización de esquemas simples donde la AFD firma el resumen del documento junto con un valor temporal absoluto (*hash-and-sign*) hasta los complejos esquemas acumulados con grafos autenticados que proporcionan certificados de tiempo. Las actividades de estandarización recogen parcialmente esta evolución [1, 11]. Desde el organismo IETF se ha desarrollado el RFC 3161 *Internet X.509 Public Key Infraestructure Time-Stamp Protocol (TSP)* [1], y desde el grupo JTC1/SC27 del organismo ISO/IEC se ha publicado un estándar compuesto por tres partes [11], basado en el anterior. En la parte 1 de esta norma se identifican los objetivos de una AFD, se describe el modelo general de los servicios de fechado digital y se definen los propios servicios así como los protocolos básicos de fechado digital. En las partes 2 y 3, se especifican una serie de mecanismos para producir sellos de tiempo independientes y enlazados.

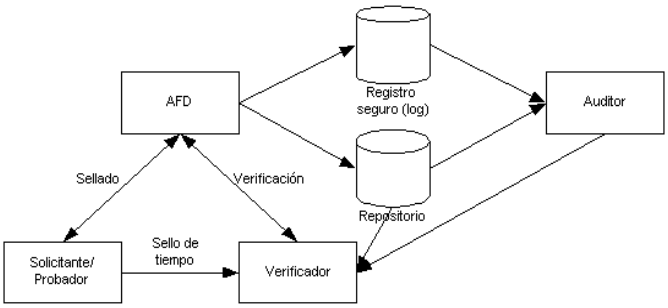

Figura 4: Modelo general de fechado digital [2]

Según ISO/IEC [11], los objetivos de un servicio de fechado digital son (1) enlazar de forma infalsificable un parámetro temporal a la información para proporcionar una evidencia digital sobre la existencia de esta información anteriormente a cierto instante de tiempo, y (2) tratar confidencialmente la información que va a ser fechada digitalmente. Otros investigadores realizan una aproximación más formal a la definición de los objetivos de un servicio de fechado digital [2].

El modelo de fechado digital propuesto por ISO/IEC [11] contempla la participación de las siguientes entidades (véase la Figura 4): **solicitante del sello** (solicita el sello de tiempo a un prestador de servicios de fechado digital), **prestador de servicios de fechado digital o Autoridad de Fechado Digital (AFD)** (acepta solicitudes de sellos de tiempo y los emite), **registro seguro** (donde se anotan las acciones que realiza la AFD), **repositorio** (directorio público para almacenar o publicar los sellos de tiempo), y **verificador del sello** (entidad que verifica la validez del sello). Algunos investigadores [2, 19] incluyen, además, otras

entidades en sus modelos: **Auditor** (audita el trabajo del prestador de servicios de fechado digital) y **Custodio de Evidencias** (almacena evidencias acerca de la integridad de los sellos emitidos por la AFD).

Un sello de tiempo contendrá habitualmente algunos de los siguientes datos, dependiendo del tipo de protocolo de fechado digital: la información a fechar digitalmente (habitualmente su resumen), la política de fechado digital, un número de serie, un valor temporal absoluto y su precisión, información de enlazado, y una firma digital sobre los elementos anteriores que estén contemplados en el protocolo que se esté aplicando.

2.4 Servicios de sellado de lugar o datación digital

En este apartado se van a describir brevemente las principales propuestas existentes para proporcionar servicios de sellado de lugar o datación digital, haciendo énfasis en la descripción del contexto en el que se enmarcan, los objetivos que persiguen y los modelos que plantean.

2.4.1 Propuesta de Kabatnik, Zugenmaier y Kreutzer: servicio de sellado de lugar para redes GSM

La idea de sellar la ubicación de una entidad localizada a través de un dispositivo móvil fue expuesta por Kabatnik, Zugenmaier y Kreutzer en el año 2001 [12, 21] como solución al problema de proporcionar una evidencia electrónica fiable sobre este hecho. Los autores toman como referencia los servicios de fechado digital para definir su modelo de sellado de lugar. La propuesta está enfocada a las redes GSM y el objetivo del servicio es proporcionar al usuario un sello de lugar que certificaría la ubicación del abonado, esto es, el sello de lugar podría servir como prueba (evidencia digital) de que el abonado asociado al dispositivo fue localizado en determinado lugar en un cierto momento con cierta resolución, o que aquél firmó un determinado documento digital en algún lugar concreto. La solución consiste en un TC integrado en la propia red GSM que mediante su firma emite la evidencia digital. Consideran opcionalmente la inclusión de un valor temporal o sello de tiempo, y 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-e o la firma de contratos electrónicos.

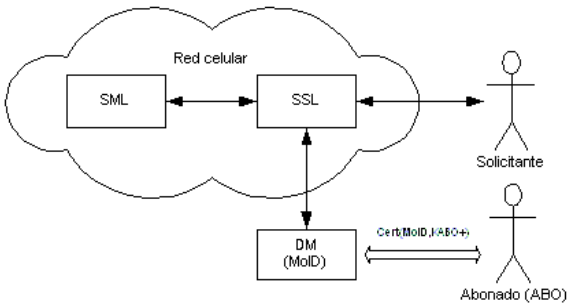

Figura 5: Modelo de sellado de lugar [12, 21]

Las entidades consideradas en el modelo son las siguientes (véase Figura la 5): **Sistema de Medida de la Localización o SML** (proporciona la información de localización), **Servicio de Sellado de Lugar o SSL** (TC encargado de recibir las peticiones de sellos de lugar y emitirlos), **dispositivo móvil o DM** (el dispositivo objeto de la localización), **abonado o ABO** (entidad abonada a la red celular y a la que está asociada el dispositivo móvil DM, un certificado asocia su clave pública con la identificación de DM), **solicitante** (entidad que solicita la emisión del sello de lugar sobre DM o ABO y que puede ser otro abonado de la red celular o una entidad externa como un LBS).

El formato del sello de lugar propuesto en [21] es el de un registro firmado digitalmente

conteniendo los siguientes campos: identidad del abonado, firma del abonado sobre un valor aleatorio no usado previamente (*nonce*), información de la localización incluyendo la resolución, nombre del prestador de la información de localización, sello de tiempo, firma del prestador del servicio de sellado sobre todo lo anterior, y, opcionalmente, los certificados correspondientes al abonado y al prestador del servicio. En su propuesta, Zugenmaier, Kreutzer y Kabatnik asimilan la localización del móvil a la localización del abonado que está manejando éste, sólo se emiten sellos bajo petición, que pueden solicitarse tanto por el abonado como por una entidad externa autorizada a través de una interfaz web, e incluyen varios mecanismos para garantizar la privacidad de la información de localización del abonado.

2.4.2 Patente de Kent Ridge Digital Labs: método para certificar sellos de lugar en transacciones móviles

En el año 2001 se presentó una patente a nombre de los laboratorios Kent Ridge Digital Labs [13] relacionada con los servicios de sellado de lugar, habiendo sido publicada como patente internacional recientemente (enero del 2003). En esta patente se propone un método para certificar información de localización relacionada con transacciones realizas a través de redes de radio, bien sea el dispositivo capaz de calcular su propia localización o bien sea necesario que una tercera parte la calcule por él. Para la certificación de la información de localización se utiliza de nuevo la firma de un TC.

Las entidades contempladas en el modelo son (véase la Figura 6): **dispositivo inalámbrico** (bien con localización basada en la red bien basada en el terminal; esta entidad, además de ser el objeto de la localización, puede solicitar la certificación de un sello de lugar), **solicitante externo** (mientras el dispositivo inalámbrico está realizando una transacción con una entidad externa, ésta puede solicitar la certificación de un sello de lugar referente al dispositivo), **Servidor de Certificación de Sellos de Lugar o SCSL** (TC que certifica los sellos de lugar mediante la aplicación de su firma), **Servidor de Determinación de la Localización o SDL** (calcula la posición geográfica de los dispositivos inalámbricos y realiza firmas digitales).

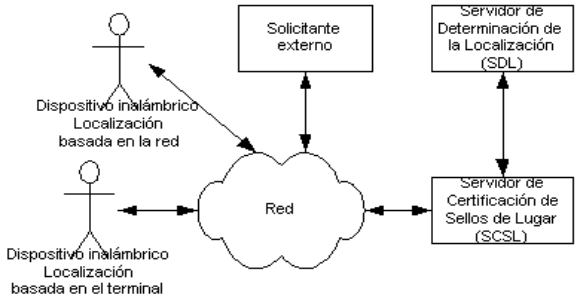

Figura 6: Modelo de sellado de lugar [13]

El proceso de certificación de un sello de lugar del método propuesto en [13] se presenta según distintas variantes dependiendo de si el propio dispositivo puede localizarse o no, o de si es el dispositivo quien solicita la certificación o lo hace una entidad externa, o si tiene capacidad de firmar digitalmente. Según los autores de la patente el sello de lugar emitido puede diseñarse de diversas incluyendo o no lo siguiente: información de identidad, información de localización, información auxiliar, información para su archivo y/o información criptográfica. Preferentemente los autores de la patente aconsejan que se incluya el tiempo en el que la localización fue determinada.

2.4.3 Propuesta de González-Tablas, Ramos y Ribagorda: servicio de datación digital

González-Tablas, Ramos y Ribagorda han propuesto [4, 17] una extensión a los servicios de sellado de lugar para que puedan emitirse evidencias acerca de itinerarios, y los autores han

denominando genéricamente el conjunto de servicios resultante como servicios de datación digital. Las razones que motivan esta decisión vienen dadas por el significado de los términos sellar y datar. Sellar tiene por significado "estampar, imprimir o dejar señalada una cosa en otra o comunicarle determinado carácter", y datar, "poner la data o 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" [18]. El término 'datación', por tanto, haría referencia a la consideración tanto de la localización como del tiempo; el término "sellado" más bien haría referencia a la consideración tan sólo de la localización (similar a lo ocurrido con los sellos de tiempo). Dadas las características de atemporalidad de la información digital, en este caso evidencias digitales, y de la necesidad de garantizar y poder verificar su validez, la consideración del tiempo simultáneamente a la localización es altamente recomendable. Por tanto, aunque algunos autores [12, 13, 21] emplean "sellado de lugar" y "certificación de sellos de lugar", los autores de [17] consideran más adecuado denominar al servicio con el término de "datación" si éste incluye el tiempo.

La extensión del mecanismo de datación digital propuesta por González-Tablas, Ramos y Ribagorda para emitir sellos de itinerario se basa en el enlazado de distintos sellos de lugar utilizando funciones resumen criptográficas (con lo que se obtiene autenticación temporal relativa entre éstos). Para añadir flexibilidad y automatización en la certificación y soportar la emisión de sellos de itinerarios, incorporan al modelo un marco para especificar y gestionar políticas de datación. Estas políticas de datación determinan en qué condiciones se debe solicitar la emisión de un sello de lugar, bien independiente bien de itinerario. El modelo (Figura 7) es similar al de las propuestas [12, 13, 21], pero la diferencia más importante es que incluye un **Agente Monitor de Políticas de Datación** vinculado a cada dispositivo móvil que active el servicio y que se encargará de que se emitan las evidencias digitales según la política de datación escogida, así como unos **repositorios** para la publicación de los sellos.

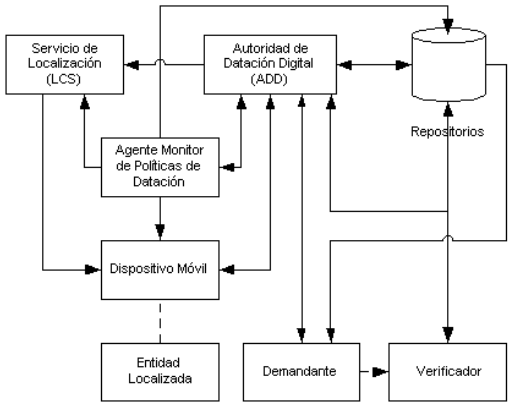

Figura 7: Modelo de datación digital [4, 17]

Los elementos básicos de los sellos emitidos en este modelo serán similares a los definidos en [12, 13, 21], y, en el caso de que se emita bajo una política de datación concreta, se debe incluir ésta. Si se trata de un certificado de datación se deberá incluir un sello de tiempo o un valor temporal, y si se tratar de un sello de itinerario se deberá incluir información de enlazado entre los distintos objetos generados para cada lugar incluido en el recorrido.

3. Discusión: Caracterización de los servicios de datación digital con respecto a otros servicios de TC

En general, todos los servicios vistos tienen como objetivo emitir una serie de evidencias

digitales acerca de determinados hechos o acciones. Todos incluyen la participación de al menos un TC que emite dicha evidencia habitualmente empleando el mecanismo de firma digital (aunque existen otros mecanismos posibles p.e. en no-repudio y en fechado digital). Los servicios de datación digital han sido descritos dentro de este marco como "similares a los servicios de fechado digital", y, efectivamente, entre ambos hay muchas características en común y unos son el modelo de los otros. Sin embargo, esta caracterización es claramente insuficiente y es necesario profundizar más para clarificar cómo se sitúan con respecto a los otros servicios de TC.

Podemos decir que existen unas entidades comunes a todas las propuestas de servicios de datación digital y de sellado de lugar:

- **Dispositivo móvil** con capacidad de ser localizado y **entidad localizada**. Son los objetos / sujetos a localizar. El dispositivo móvil puede tener capacidad de firma o no, y habitualmente sirve como instrumento para localizar a una persona (entidad localizada) que lo maneja; entre ésta y el dispositivo suele existir una relación verificable.
- **Tercero de Confianza** encargado de emitir las evidencias digitales acerca de la información de localización. Este TC tendrá asociado posiblemente un **repositorio** donde se puedan almacenar los sellos emitidos.
- **Servicio de Localización**, bien proporcionado a través de un tercero (proveedor de servicios de red inalámbrica) o bien integrado en el propio dispositivo (p.e. Receptor de GPS).
- **Demandante / solicitante**, entidad que solicita la emisión de la evidencia acerca de la ubicación o ubicaciones del dispositivo móvil o la entidad localizada.
- **Verificador**, entidad que verifica la evidencia digital, aunque el único modelo en el que se define explícitamente es en [4, 17], pues en [12, 13, 21] el rol del verificador es asumido por el demandante del servicio.

Comparando con los otros modelos de servicios proporcionados por TC, se echan en falta figuras o roles no tan inmediatos para la prestación del servicio, como son el Árbitro o Juez para resolver las posibles disputas que puedan surgir, el Auditor (junto con el Registro Seguro) y el Custodio de Evidencias. Esto puede se puede achacar a la relativa juventud de los modelos de datación digital en comparación con el resto, así como por no haber sido implantados para su uso público.

Si comparamos el servicio de datación digital con el modelo de certificación digital de identidad, podemos encontrar una similitud que en los otros servicios no se encuentra, o al menos no en los modelos más generales. Ésta es la situación en la que un TC emite las evidencias digitales (AC) y otro TC es quien verifica anteriormente la información a acreditar (AR), en este caso la relación entre la identidad y la clave pública. En los servicios de datación digital se identifican dos situaciones distintas dependiendo de qué entidad calcula la localización del dispositivo móvil / entidad localizada. Si esta información la proporciona un Servicio de Localización (integrado o no en un Proveedor de Servicios de Red), el modelo resultante es muy similar al de certificación digital de la identidad. Una de las diferencias que se presentan es que habitualmente la AR forma parte de la misma infraestructura que la AC, y tal como se está configurando el modelo de negocio para los servicios dependientes de la localización, es más probable que esto no ocurra así en este entorno. Si la información se calcula en el propio dispositivo, la situación es distinta porque dependiendo de cómo se diseñe éste (a prueba de falsificaciones y manipulaciones), se podría considerar como un TC independiente similar a un LCS. La situación que más nos interesa es claramente esta última, pues permitiría configurar un modelo coherente con ambos tipos de localización, pero implica resolver cómo integrar el módulo de localización de forma segura en el dispositivo.

Los objetivos y modelos de los servicios de datación digital son muy similares a los servicios de fechado digital. Una de las diferencias principales, que ya se ha comentado, es que habitualmente el TC que emite la evidencia de fechado digital es la fuente confiable de dicha información y en datación digital no va a ocurrir así habitualmente. La otra viene dada precisamente por la naturaleza atemporal de la información digital y la utilización de los servicios de fechado digital como mecanismo para imprimir esta cuarta dimensión en el entorno digital de forma segura. Esta característica hace que no se puedan asimilar ambos servicios directamente, pues provoca que los servicios de TC que tengan como objetivo emitir evidencias digitales deban marcar éstas temporalmente, por lo que en la mayoría de los casos se requiere la colaboración de una AFD o la integración de ésta en el TC del servicio considerado. Esto mismo ocurre en los servicios de datación digital. Sería muy interesante estudiar los modelos de fechado digital más complejos (enlazados y distribuidos, integrados con servicios de notarización o de archivo a largo plazo, etc.) para tratar de aplicarlos a los servicios de datación digital.

Por otro lado, en primera instancia los servicios de sellado de lugar o datación digital se podrían clasificar como servicios de no-repudio en su sentido más general si comparamos sus objetivos. Sin embargo, cuando se trata de integrar los modelos de datación digital en los modelos de no-repudio existentes uno encuentra que no es tan inmediato como podría parecer en un primer momento. La razón principal es que la investigación relativa a los servicios de no-repudio se basa en lo regulado por ISO/IEC, que se refiere exclusivamente al hecho de una comunicación o sus propiedades, y no a un evento o acción más general. Se podrían integrar los servicios de datación digital en los de no-repudio si la información de lugar se considerase como una propiedad más de una comunicación o de la transferencia de un mensaje; sin embargo, la emisión de evidencias digitales de ubicación con el significado de 'tal entidad estuvo en tal lugar en tal momento' no cabría en esta interpretación.

Es muy interesante por tanto la idea de un notario electrónico genérico [15] donde se pudiesen encuadrar todos estos servicios. El grupo LTANS del IETF [7] está actualmente trabajando en ello pero, tras publicar el primer borrador de requisitos para los servicios de notarización, parece que se van a decantar por el modelo de notario digital donde siempre existe una persona detrás. Se necesitaría por tanto definir todavía un modelo extensible que permitiese la colaboración y la gestión de la confianza entre distintos TC con el objetivo de emitir distintos tipos de evidencias digitales acerca de informaciones, eventos o acciones diversas.

Volviendo al caso particular de los servicios de datación digital, se plantea en ellos un problema que no aparece en el resto de servicios de TC. Este problema es la dualidad existente entre el dispositivo móvil y la entidad localizada. Sin el dispositivo la entidad no puede ser localizada, pero al ser entidades distintas aparecen multitud de problemas como la autenticación de la entidad, además de la del dispositivo, o la relación que se establece entre ellos y cómo gestionarla y verificarla. Esta área debería estudiarse también más a fondo.

4. Conclusiones

Los servicios de TC con el objetivo de emitir evidencias digitales son cada vez más necesarios para desarrollar con éxito el comercio-e y la administración-e. La comunidad científica del área de la seguridad de la información ha desarrollado diversos servicios y modelos con estos objetivos. Por un lado, estos servicios han sido desarrollados cada uno separadamente sin integrarlos en un marco común donde se pueda encuadrar a todos. Por otro lado, con la aparición de nuevas tecnologías y su integración en nuestras sociedades se requiere el desarrollo de nuevos servicios y mecanismos de este tipo, como ocurre con los recientemente propuestos servicios de sellado de lugar o datación digital. Entre los problemas por resolver que plantean estos servicios se encuentra el caracterizarlos con respecto a otros servicios de TC similares. El objetivo de este artículo ha sido iniciar esta

caracterización y plantear una discusión acerca de las similitudes y diferencias. Para ello se han descrito y comparado las características principales de los modelos de certificación digital de la identidad, no-repudio y fechado digital, así como de las diferentes propuestas existentes para servicios de datación digital.

La conclusión principal es que claramente los servicios de datación digital se encuentran entre los mencionados y tienen entidad propia entre éstos, pero haría falta desarrollar un marco de notarización general colaborativo y extensible donde pudieran encuadrarse todos estos servicios. Se necesita profundizar en este estudio y formalizarlo.

5. Bibliografía

[1] C. Adams, P. Cain, D. Pinkas, and R. Zuccherato. Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), August 2001.

[2] A. Ansper, A. Buldas, M. Saarepera, and J. Willemson. Improving the availability of time-stamping services. In *ACISP'2001, 6th Australasian Conference on Information Security and Privacy*, volume 2119 of *Lecture Notes in Computer Science*, pages 360–375. Springer-Verlag, July 2-4, 2001.

[3] CPS (Cambridge Positioning Systems), 2003.

[4] A.I. González-Tablas, B. Ramos, and A. Ribagorda. Path-Stamps: A proposal for enhancing the security of location tracking applications. *Ubiquitous Mobile Information and Collaboration Systems Workshop (UMICS03). CAiSE'03 Workshops Proceedings*, June 2003.

[5] S. Haber and W. Scott Stornetta. How to time-stamp a digital document. *Journal of Cryptology*, 3(2):99–111, 1991.

[6] IETF. IETF Working Group: Public-Key Infrastructure (X.509) (pkix).

[7] IETF. Long-Term Archive and Notary Services (ltans), 2003.

[8] ISO/IEC. ISO/IEC 7498-2. Information processing systems - Open systems interconnection - Basic reference model - Part 2: Security arquitecture, 1988.

[9] ISO/IEC. ISO/IEC 10181-4. Information technology - Open systems interconnection - Security frameworks in open systems - Part 4: Non-repudiation framework, 1996.

[10] ISO/IEC. ISO/IEC 13888. Information technology - Security techniques - Non-repudiation - Part 1: General, 1997. Part 2: Mechanisms using symmetric techniques, 1998. Part 3: Mechanisms using asymmetric techniques, 1997.

[11] ISO/IEC. ISO/IEC 18014. Information technology - Security techniques - Time-stamping services - Part 1: Framework, 2002. Part 2: Mechanisms producing independent tokens, 2002. Part 3: Mechanisms producing linked tokens, 2002.

[12] M. Kabatnik and A. Zugenmaier. Location stamps for digital signature: A new service for mobile telephone networks. In *Networking - ICN 2001, First International Conference*, Lecture Notes in Computer Science 2094. Springer, 2001.

[13] KRDL (Kent Ridge Digital Labs). Patente (PCT): WO 03/007542. Method for certifying location stamping for wireless transactions, 2003.

[14] S. Kremer, O. Markowitch, and J. Zhou. An intensive survey of non-repudiation protocols. *Computer Communications Journal*, 25(17):1606–1621, November 2002.

[15] J. López. Servicios de notarización electrónica. *SIC, Seguridad en Informática y Comunicaciones*, 25:I–V, Junio 2001.

[16] PAMPAS. Proyecto IST-2001-337763, Pioneering Advanced Mobile Privacy and Security, 2003.

[17] B. Ramos, A.I . González-Tablas, and A. Ribagorda. Sellado y Datación de Ubicación e Itinerario. *Actas del Segundo Congreso Iberoamericano de Seguridad Informática (CIBSI'03)*, pages 393–403, Octubre 2003.

[18] Real Academia Española. Diccionario de la Lengua Española. Edición del 2001.

[19] M. Une. The security evaluation of time stamping: The present situation and studies. Technical Report IMES Discussion Paper Series - 2001-E-18, Institute for Monetary and Economic Studies, 2001.

[20] J. Zhou. *Non-repudiation in Electronic Commerce*. Computer Security Series, Artech House, 2001.

[21] A. Zugenmaier, M. Kreutzer, and M. Kabatnik. Enhancing applications with approved location stamps. In *IEEE Intelligent Network 2001 Workshop (IN2001)*, 2001.