Protocolos de sellado espacio-temporal: Mejorando su precisión y disminuyendo el nivel de confianza requerido

A. I. González-Tablas, B. Ramos, and A. Ribagorda

Universidad Carlos III, Leganés, SPAIN
aigonzal,benja1,arturo@inf.uc3m.es

Resumen Los servicios de sellado espacio-temporal son uno de los servicios de confianza propuestos más recientemente. Su objetivo es emitir evidencias digitales acerca de las condiciones espacio-temporales bajo las que se encuentra un documento o bajo las que una entidad realiza una acción sobre éste. Los protocolos de sellado espacio-temporal existentes en la literatura, en los que un tercero de confianza (TTP) genera las evidencias, presentan deficiencias en cuanto a la precisión con la que un tercero puede probar las condiciones espacio-temporales acreditadas en las evidencias. Además, la capacidad probatoria de las evidencias en los mencionados protocolos depende fuertemente de la confianza depositada en las TTP participantes cuando interesaría que esta confianza fuera menor. En este trabajo se presentan unos protocolos de sellado espacio-temporal que mejoran estos dos aspectos.

1. Introducción

Los avances en las técnicas de posicionamiento de dispositivos electrónicos a distancia y la integración cada vez más frecuente de la movilidad en las comunicaciones han permitido el desarrollo en la última década de los servicios basados en la localización (*Location Based Services* o LBS). En particular, las técnicas de estimación de la posición más utilizadas hoy en día son aquellas basadas en los sistemas satelitales de radio-navegación, como el sistema GPS [14], y aquellas basadas en las redes de comunicación celular móvil [17]. En [6] se puede consultar una clasificación de los sistemas de posicionamiento y un resumen de su estado de la cuestión. Los LBS se soportan en estas tecnologías y se definen como aquellos servicios de valor añadido que utilizan la posición geográfica de los usuarios para proporcionar este valor [4]. Los LBS han creado una gran expectación en diversos ámbitos. En la actualidad varios de estos servicios han sido implantados con éxito (véase, por ejemplo, el caso de los servicios de emergencia 112 europeo y 911 americano) y se prevé que otros muchos lo sean en un futuro próximo.

Por otro lado, ciertas actividades comerciales, gubernamentales, administrativas, financieras y legales se basan en la existencia de ciertos niveles de confianza entre las personas u organizaciones participantes en las transacciones. Los mecanismos utilizados tradicionalmente incluyen reuniones cara a cara, cartas de

recomendación, referencias, testigos, avales, etc. La implantación en la sociedad de tecnologías de comunicación remota utilizando medios electrónicos ha provocado que los usuarios exijan que dichas actividades puedan realizarse en este medio. Por ello, la comunidad académica de la seguridad de la información ha desarrollado mecanismos que permiten establecer y gestionar la confianza en este nuevo contexto. Los denominados servicios de confianza (*trust services* o SC) tienen este objetivo y habitualmente están provistos por entidades confiables o Terceros de Confianza (*Trusted Third Party* o TTP), que según la ISO/IEC se definen como '*una organización o uno de sus agentes que proporcionan uno o más servicios de seguridad, y en la que otras entidades confían para actividades relacionadas con estos servicios de seguridad*' [9].

Algunos de estos SC, los servicios de acreditación, dan fe sobre ciertas características de las entidades (como su identidad y los privilegios a los que tienen derecho [11]) o cualquier afirmación acerca de éstas en general, como en los sistemas de credenciales [3]. Otros SC, los servicios de notarización y sellado temporal, acreditan las características de documentos digitales (como su integridad, validez o su existencia en el tiempo [10]) o, en el caso de los servicios de no-repudio, que éstos han sido objeto de alguna acción (como su transmisión o recepción por una entidad [8]). Los servicios citados generan credenciales o evidencias, que suelen contribuir notablemente a la adecuada asignación de responsabilidades (*accountability*) ante las acciones realizadas por los sujetos implicados [1]. Esta situación es muy deseable si se desea llevar a cabo cualquier tipo de transacción electrónica. La capacidad probatoria de las evidencias determina en gran medida su capacidad para determinar responsabilidades de forma adecuada [13].

En los últimos años se han propuesto un nuevo tipo de servicio de confianza que acredita las condiciones espacio-temporales bajo las que existe un documento o bajo las que una entidad realiza una acción sobre éste. Los protocolos existentes en la literatura cuyo objetivo es proveer este servicio presentan ciertas deficiencias en cuanto a la precisión con la que un tercero puede probar las condiciones espacio-temporales acreditadas utilizando las evidencias, y el nivel de confianza que es necesario depositar en las TTP participantes en los protocolos. En este trabajo se presentan unos protocolos de sellado espacio-temporal que mejoran a los existentes en estos dos aspectos.

La organización de este documento es como sigue. En la Sección 2 se describen los servicios de sellado espacio-temporal y los servicios de acreditación espacio-temporal, estrechamente relacionados con los primeros. En la Sección 3 se describen los protocolos existentes en la literatura para proporcionar servicios de sellado espacio-temporal y en la Sección 4 se analizan los problemas que éstos presentan. Los protocolos que se proponen en este trabajo para abordar las deficiencias citadas se exponen y analizan en la Sección 5. Finalmente, la Sección 6 recoge las conclusiones de este trabajo.

2. Antecedentes

Como se ha comentado, recientemente se han propuesto los servicios de confianza espacio-temporal, cuyo propósito es *'proporcionar evidencias digitales acerca de las condiciones espacio-temporales de cierta entidad o documento de forma que estas condiciones sean verificables posteriormente por un tercero'*. En [16] se discute la naturaleza de estos servicios y algunos de los problemas que plantean; véase sin embargo [5] si se desea consultar un resumen reciente del estado de la cuestión de estos servicios y de los protocolos de autenticación de la localización (PAL) sobre los que aquellos se apoyan.

Entre estos servicios de confianza espacio-temporal se distinguen dos tipos según el objetivo específico que persiguen. El primer tipo contempla los *servicios de acreditación espacio-temporal (SAET)*, cuyo objetivo es acreditar las condiciones espacio-temporales de una entidad determinada S o *sujeto* de las evidencias. Habitualmente este sujeto (S) se corresponde con un *dispositivo* localizable (P), aunque a veces este término puede incluir además a la entidad *usuario* (U) que está controlando éste. Los SAET son similares a los servicios de certificación de identidad y atributos o los sistemas de credenciales. Las evidencias espacio-temporales (EET) generadas en los SAET se denominan credenciales espacio-temporales y se representarán como θ. Estas credenciales pueden utilizarse para controlar el acceso a servicios o para otorgar privilegios dependiendo de la posición actual o pasada del sujeto o del historial de esta característica. También pueden utilizarse para facilitar la asignación de responsabilidades en aplicaciones de seguimiento de recursos o entidades (por ejemplo, materiales de gran valor o peligrosos, trabajadores móviles, presos bajo libertad condicional o nodos en una red). En otros escenarios las EET pueden utilizarse para justificar la adaptación de las transacciones electrónicas o de su coste dependiendo del lugar-tiempo desde donde éstas se realizan o desde donde se utiliza un servicio.

El segundo tipo de servicios de confianza espacio-temporal lo suponen los *servicios de sellado espacio-temporal (SSET)*. En este caso su objetivo es acreditar que un determinado *documento* (M) existía en un lugar determinado en cierto momento temporal o que un *sujeto* S realizó determinada acción sobre dicho documento bajo ciertas condiciones espacio-temporales. Ejemplos de las acciones citadas podrían ser la firma, recepción o envío del documento. Los SSET son similares a los servicios de no repudio o los servicios de fechado digital. Las evidencias que se emiten en los SSET se denominan sellos espacio-temporales y se representarán como ϕ. Este tipo de servicios de confianza ya se sugería en la norma ISO/IEC 10181-4 [7] y tienen aplicación en los sistemas de votación electrónica, registro de patentes, transacciones legales, protección de la propiedad intelectual, establecimiento de impuestos dependientes de la localización en el contexto del comercio electrónico, y en la firma de contratos. Por otro lado, también se pueden utilizar para acreditar el lugar y tiempo de ocurrencia de eventos reales como graduaciones, bodas, reuniones, resolución de concursos, etc.

Habitualmente es un tercero de confianza (TTP) la entidad que toma el rol de *generador de las evidencias* (G_e), es decir, la entidad que emite las credencia-

les y los sellos espacio-temporales. En algunos casos, los propios sujetos pueden auto-localizarse a través de sus dispositivos y se puede asumir que el módulo en el dispositivo P encargado de esta tarea posee determinado grado de resistencia a manipulaciones. Entonces, el propio dispositivo también podría asumir el rol de G_e. Algunas veces, puede requerirse que exista otro TTP, denominado *verificador de las evidencias* (V_e), y que se encarga de verificar las evidencias espacio-temporales (EET) en nombre de los usuarios cuando éstos no lo pueden hacer por sí mismos.

En el caso de los SAET, G_e debe primero autenticar la localización del sujeto S y, una vez se ha asegurado de esta condición, acreditar ésta generando una evidencia. El mecanismo más utilizado para generar las EET es el de certificación basado en firmas digitales. La capacidad probatoria de estas credenciales se basa fundamentalmente en la confianza que terceras partes depositan en las entidades generadoras G_e para certificar las condiciones espacio-temporales de los sujetos y en que se pueda verificar que estas credenciales son auténticas (han sido generadas por G_e y no han sido alteradas) y válidas.

En el caso de los SSET, G_e debe verificar que una entidad S tiene bajo su poder un documento M mientras está situada en cierto lugar en determinado instante (de esta forma se verifica la existencia de M en ese lugar-tiempo). Por tanto, además de autenticar la localización de S, como se realiza en los SAET, G_e deberá comprobar que el sujeto S tiene bajo su poder M (o que S realiza cierta acción sobre M bajo ciertas condiciones espacio-temporales). En los SSET, igual que en los SAET, una alternativa para generar los sellos espacio-temporales es utilizar mecanismos de certificación basados en firmas digitales. Si este es el caso, la capacidad probatoria de estos sellos se basaría también en la confianza que terceras partes depositan en las entidades G_e y en que se pueda verificar que los sellos emitidos son auténticos y válidos. La diferencia es que, en el caso de los SSET, la confianza depositada en las entidades G_e es mayor comparada con los SAET, ya que no sólo se debe confiar en G_e para que autentique las condiciones espacio-temporales de S y acredite este situación en la EET, sino que también se debe confiar en G_e para que verifique la posesión de M por S (o la realización por parte de S de una acción sobre el documento) y para asociar correctamente estas informaciones en la EET.

3. Trabajos relacionados

Existen dos propuestas que se pueden encuadrar dentro de los servicios de sellado espacio-temporal. La primera de ellas es la propuesta de Kabatnik y Zugenmaier en [12]. En este caso, el sello espacio-temporal emitido ϕ trata de proporcionar una evidencia acerca de que un usuario U utilizando un dispositivo P generó una firma σ sobre determinado documento digital M (o sobre su resumen $H(M)$) en determinado lugar. El protocolo que se presenta inicialmente en [12] (véase el Protocolo 1) no especifica ninguna tecnología de posicionamiento en particular, aunque luego los autores exponen una particular implementación de éste para el caso de que los dispositivos fueran teléfonos móviles GSM y se

utilizasen éstos para localizar a los sujetos. El escenario del protocolo contempla un TTP encargado de generar los sellos (G_e) y un servicio de localización $STIS$ (*Spatial-Temporal Information Service*) que proporciona información de localización acerca del dispositivo P.

Protocolo 1 *(de sellado espacio-temporal de Kabatnik y Zugenmaier).*

1. $P \rightarrow G_e : H(M),\ ID_P,\ r$
2. $G_e \rightarrow P : Sig_{G_e}\{ID_P,\ N,\ H(M)\}$
3. $P \rightarrow G_e : \underbrace{Sig_U\{N,\ H(M))\}}_{\sigma}, \left[Cert(ID_P,\ SK_U^+)\right]$
4. $G_e \rightarrow STIS : ID_P$
5. $STIS \rightarrow G_e : l$
6. $G_e \rightarrow P : \underbrace{Sig_{G_e}\left\{\sigma,\ l',\ t,\ ID_{STIS}\right\}}_{\phi}$

En el paso 1, el usuario U a través del dispositivo P le envía a G_e un resumen $H(M)$ del documento sobre el que debe emitir el sello espacio-temporal, la identificación del dispositivo ID_P y la resolución r con la que quiere que se refleje la información de localización en el sello. En el paso 2, G_e le confirma a P el resumen y la identificación del dispositivo, enviándole estos valores firmados; además, le comunica un reto N (*nonce*) que U utilizará para autenticar la frescura de la firma en el siguiente paso. En el paso 3, U genera la firma digital σ sobre el resumen del documento $H(M)$ y el reto N enviado en el paso anterior. En este mismo paso 3, U puede enviar opcionalmente el certificado $Cert(ID_P,\ SK_U^+)$, que acredita que la clave privada SK_U^- utilizada para generar la firma (pareja de la clave pública SK_U^+) se encuentra alojada en el mismo módulo que contiene la clave secreta que permite al dispositivo con identificación ID_P autenticarse. Este es el mecanismo propuesto por Kabatnik y Zugenmaier para comprobar que la firma digital se genera en el mismo lugar que el dispositivo esté situado cuando se le localiza. El certificado permite a G_e verificar la firma σ y solicitar al $STIS$, en el paso 4, la localización del dispositivo P, sabiendo que esta información también corresponderá al usuario U que está controlando éste. Tras recibir la localización l en el paso 5, G_e genera el sello espacio-temporal ϕ como una firma digital sobre σ (la firma generada por U), l' (la localización del dispositivo expresada con la resolución r solicitada por el usuario), t (el momento temporal en el que se genera el sello) e ID_{STIS} (la identificación del $STIS$ que ha proporcionado la información de localización).

La otra propuesta de servicio de sellado espacio-temporal se presenta en [15], y tiene por objetivo acreditar que un documento ha sido transmitido por un dispositivo P que se encontraba en ese momento en cierto lugar. Aunque no se especifican los protocolos explícitamente, se plantean varios escenarios y se comenta cuál sería el proceso de generación del sello.

En algunos escenarios se asume que el dispositivo puede auto-localizarse. Una primera propuesta es que sea éste quien genere los sellos espacio-temporales utilizando firmas digitales. En segunda instancia se propone que el sello consista en el cifrado simétrico del documento y la localización con una clave compartida

entre P y una entidad confiable generadora de los sellos (G_e); posteriormente G_e podría generar un nuevo sello espacio-temporal firmando digitalmente ambas informaciones tras verificar su corrección o verificar la corrección del sello generado por el dispositivo si un tercero le presenta éste a G_e.

En otros escenarios de [15], se asume que el dispositivo puede ser localizado por un servicio de localización $STIS$. En este caso, se propone un proceso muy similar al de la propuesta [12]: se envía el documento a G_e, quien solicita la localización del dispositivo a $STIS$ y tras conocer esta información emite un sello firmando ambas informaciones. En una cuarta variante, se asume que el dispositivo puede ser localizado por el $STIS$ y que además P puede auto-localizarse. En este caso, se propone que P genere primero un sello y lo remita a G_e; entonces G_e comprueba que la localización reflejada en el sello es correcta solicitando la posición de P a $STIS$. Si ambas localizaciones coinciden, G_e aplica su firma digital sobre el sello enviado por P.

4. Descripción del problema

Como se ha visto en la sección anterior, algunas de las propuestas de SSET, como es el caso de algunas de las variantes en [15], se basan en dispositivos capaces de auto-localizarse. Para autenticar la información de localización que se incluirá en las evidencias utilizando este tipo de técnicas de posicionamiento, se requiere, entre otras condiciones, que los dispositivos presenten unas características de resistencia a y detección de manipulaciones demasiado ambiciosas para muchas aplicaciones. Un tercero debería confiar totalmente en estas características para convencerse de la veracidad de la evidencia espacio-temporal (EET) y esta situación en ciertos escenarios no es deseable, o lo que es peor, puede que ni siquiera se puedan garantizar estos requisitos. Por esta razón, en este trabajo no se considerarán este tipo de protocolos de sellado espacio-temporal.

La alternativa la suponen las propuestas de SSET donde se asume que el dispositivo va a ser localizado por un tercero confiable de forma correcta y que esta entidad va a asegurarse de la autenticidad de la IET, como el protocolo en [12] y algunas de las variantes descritas en [15]. Este tipo de protocolos suelen requerir una menor capacidad de resistencia a y detección de manipulaciones en el dispositivo, al menos en lo que se refiere a los procesos de posicionamiento del mismo. Supuesto un protocolo de sellado espacio-temporal, se han detectado dos deficiencias que se describen a continuación.

Por un lado, es deseable que los protocolos de sellado espacio-temporal proporcionasen evidencias que permitiesen a un tercero demostrar con precisión bajo qué condiciones espacio-temporales se han producido las acciones realizadas sobre los documentos. Las evidencias generadas por los protocolos propuestos en [15,12] no ofrecen estas garantías. En el caso de los protocolos en [15], ni se especifican éstos concretamente ni los contenidos de las evidencias que se generan durante su ejecución, por lo estas garantías no pueden ser ni analizadas ni aseguradas. En el caso de la propuesta [12], teniendo en cuenta que se confía en G_e para asociar el tiempo t de generación de la evidencia a ésta entre otras

cosas, un tercero que obtuviese un sello ϕ podría convencerse de que la firma σ del sujeto U sobre el documento M se realizó bajo ciertas condiciones espacio-temporales. Estas condiciones espacio-temporales harían referencia a que ésta se generó antes del momento t incluido en la EET y que en algún momento entre la generación de la firma y la emisión de la evidencia, el sujeto se encontraba en cierto lugar l'. Esta incertidumbre en las condiciones espacio-temporales puede ser inaceptable en determinadas aplicaciones donde se requiera conocer precisamente en qué lugar y en qué momento se ha realizado la acción acreditada en el sello (en este caso particular, la generación de una firma digital). Por tanto sería deseable proponer protocolos de sellado espacio-temporal que generasen sellos cuya capacidad probatoria con respecto a las condiciones espacio-temporales fuera precisa.

Por otro lado, en los SSET donde un TTP genera las evidencias, esta entidad (G_e) debe convencerse de que el sujeto de las evidencias(S) ha realizado cierta acción sobre el documento mientras estaba en cierto lugar en determinado momento. En los protocolos propuestos en [12,15] se debe confiar totalmente en la entidad G_e para acreditar esta acción, las condiciones espacio-temporales bajo las que ésta se produce y dar fe de todo esto en una evidencia. Al igual que no es deseable que la seguridad del protocolo dependa totalmente de las características de resistencia del dispositivo y su capacidad de detección de manipulaciones, tampoco es deseable que la seguridad del protocolo requiera depositar una nivel de confianza demasiado alto en las entidades G_e. Por tanto, sería aconsejable contar con protocolos de sellado espacio-temporal que disminuyesen el nivel de confianza que se requiere depositar en las TTP o que distribuyesen esta confianza entre distintas TTP para dificultar los comportamientos fraudulentos por parte de éstas.

5. Propuesta de protocolos de sellado espacio-temporal mejorados para la generación de firmas digitales

5.1. Objetivo, modelo y suposiciones

En este trabajo se aborda cómo mejorar los protocolos de sellado espacio-temporal según los aspectos comentados en la sección anterior. Se considera el caso concreto de los protocolos cuyo objetivo sea acreditar las condiciones espacio-temporales bajo las que cierta entidad S, la entidad firmante, genera una firma digital σ sobre cierto documento M (o sobre un resumen $H(M)$ de éste). Acreditar esta acción puede utilizarse posteriormente en la mayoría de las aplicaciones previstas para los SSET, así como para proporcionar pruebas acerca de la existencia de un documento bajo ciertas condiciones espacio-temporales.

Para lograr que los sellos permitan probar las condiciones espacio-temporales bajo las que se genera la firma con una mayor precisión, se propone acotar el rango espacio-temporal en el que S genera la firma e incluir en el sello evidencias demostrables acerca de estas cotas espacio-temporales. Se denominará *cota de apertura* a aquella que establece el comienzo del rango espacio-temporal y *cota*

de clausura a aquella que establece el final del rango espacio-temporal. La cota de apertura estará asociada al tiempo t_o y la cota de clausura al tiempo t_c. La generación de la firma se asociará al tiempo t_a. El rango espacio-temporal dentro del que se acota la generación de la firma estará determinado por el intervalo temporal $\mathcal{T}_t = [t_o, t_c]$ y una cierta área espacial conectada $\mathcal{L}_t$. Dado un sello espacio-temporal, éste debería permitir a un tercero probar que $t_a \in \mathcal{T}_t$ y que la entidad firmante estaba situada $\mathcal{L}_t$ en el momento t_a.

En la ejecución de los protocolos participarán una entidad G_e generadora de evidencias espacio-temporales y una autoridad de sellado temporal TSA. En algunos protocolos, la entidad G_e generará credenciales espacio-temporales (θ) y se denominará G_C. En otros casos, G_e generará sellos espacio-temporales (ϕ) y se denominará a esta entidad G_S. Se asumirá que G_C y G_S autentican las condiciones espacio-temporales de la entidad firmante antes de generar las evidencias espacio-temporales, y que éstas son infalsificables, intransferibles y válidas durante la ejecución de los protocolos. Para ilustrar los protocolos propuestos en este capítulo se asumirá que las entidades G_C y G_S generarán evidencias espacio-temporales utilizando mecanismos de certificación basados en firmas digitales, pero se podría utilizar cualquier otro mecanismo de generación que garantizase las propiedades mencionadas.

Por otro lado, la TSA emitirá sellos temporales de dos tipos: Anclas de tiempo confiables (γ) respecto a t y sellos de anterioridad (φ) de y respecto a t'. Los sellos de anterioridad φ proporcionan una evidencia acerca de que la información y fue creada antes de t'. Para generar estos sellos se pueden utilizar tanto esquemas de sellado temporal independientes como esquemas de sellado temporal enlazados. En el primer caso un sello de anterioridad para un documento M podría generarse según se muestra en el Protocolo 2.

Protocolo 2 *(de sellado temporal independiente - sello de anterioridad)*

1. $P \longrightarrow TSA : REQ(\varphi; H(M))$
2. $TSA \longrightarrow P : \underbrace{Sig_{TSA}\{H(M), n, t\}}_{\varphi}$

Las anclas de tiempo confiables γ son aquellos objetos digitales (*token*) que proporcionan una evidencia acerca de que cierto instante de tiempo t ya ha pasado. Usualmente interesa que este instante de tiempo t sea lo más cercano al instante actual. Estas anclas las puede emitir una TSA o se podrían construir utilizando información que sólo haya podido conocerse después de que ese instante haya transcurrido, e.g., el valor del barril de Brent para ese día, la combinación ganadora de un juego de azar nacional, etc. Un posible mecanismo para generar anclas de tiempo consistiría en la emisión de sellos de anterioridad para una información aleatoria. Por ejemplo, se podría generar un ancla de tiempo confiable para el tiempo t utilizando el Protocolo 2 de sellado temporal independiente si, en el paso 1, P enviase, en lugar de $H(M)$, un *nonce* N.

Para ilustrar los protocolos propuestos en este capítulo se utilizarán sellos de anterioridad y anclas de tiempo confiables basados en esquemas de sellado tem-

poral independiente, sin embargo se podrían utilizar igualmente sellos y anclas basados en esquemas enlazados.

Se asumirá que cada uno de los dispositivos P tiene una identificación única ID_P asociada a un secreto s. El conocimiento de este secreto s le permitirá probar su identidad a otras entidades. El secreto s se almacena en un módulo resistente a manipulaciones (TPM) de forma que todas las operaciones que utilizan s se realizan dentro de dicho módulo y se garantiza que s no puede ser filtrado al exterior.

Por otro lado, en el escenario planteado es muy probable que el sujeto S esté constituido por el dispositivo P y por una entidad usuario U que controle éste y sea quien realmente deba firmar el documento. Sería razonable asumir que el usuario U posee un objeto o TPM personal que contiene la clave privada SK_U^- del usuario y que este objeto le permite realizar operaciones criptográficas con ella de forma segura. Un ejemplo de TPM sería una tarjeta inteligente. Para utilizar la clave SK_U^-, y por tanto para generar la firma, el usuario debería autenticarse ante el TPM bien utilizando métodos biométricos bien probando su conocimiento de otro secreto compartido entre el TPM y el usuario. A su vez, el dispositivo P debería autenticar el módulo TPM y que ambos están próximos o en contacto directo. A pesar de estas afirmaciones, para simplificar la exposición de los protocolos, este problema no se abordará y se supondrá que es el propio dispositivo P quien debe generar la firma, es decir, P es la propia entidad firmante.

Por tanto, se asumirá que el dispositivo P es capaz de generar firmas digitales σ según un algoritmo $Sig_P(\cdot)$ utilizando un secreto SK_P^- conocido por éste. El secreto SK_P^- estará asociado intrínsecamente al secreto s que permite a P identificarse ante terceros, de forma que si se conoce uno, también se puede conocer el otro; por ejemplo, podría ocurrir que $s = SK_P^-$.

Así mismo, se asumirá que la velocidad del sujeto está acotada, es decir, que podrá alcanzar como máximo una velocidad v_{max}. Esta suposición no es muy descabellada ya que hoy en día una de las situaciones donde un sujeto en condiciones normales podría alcanzar una velocidad máxima sería cuando se encontrase a bordo de un avión comercial en vuelo, cuya velocidad de crucero no suele superar la velocidad del sonido.

Finalmente, se asumirá que existe una sincronización temporal fuerte entre las diferentes entidades confiables (TTP) participantes en el protocolo. Esta suposición es bastante razonable si todas las TTP que acreditan tiempos durante el protocolo toman como referencia el mismo tiempo o la misma cadena temporal. En el caso de la autenticación temporal absoluta (esquemas de sellado temporal independiente) suele utilizarse como referente el tiempo universal coordinado (UTC) o tiempos relacionados. En el caso de la autenticación temporal relativa (esquemas de sellado temporal enlazados) la propia cadena de tiempo formada por los documentos es el referente temporal; si participasen en el protocolo distintas TTP cada una con una cadena temporal diferente, se debería utilizar algún mecanismo que permitiese coordinar o establecer relaciones temporales demostrables entre las cadenas utilizadas (por ejemplo, entrelazando las cadenas o

estableciendo puntos en común asociados a otra cadena temporal de referencia). Estos mismos mecanismos o similares también deberían utilizarse si algunas de las TTP implicadas proporcionasen autenticación temporal absoluta mientras que otras proporcionasen autenticación temporal relativa.

5.2. Mejora de la precisión en los protocolos de sellado espacio-temporal

En esta sección se propone un protocolo de sellado espacio-temporal para la generación de firmas digitales que mejora la precisión con la que los sellos permiten probar las condiciones espacio-temporales bajo las que se genera la firma. El Protocolo 3 propuesto modifica ligeramente el Protocolo 1 de Kabatnik y Zugenmaier.

Protocolo 3 *(de sellado espacio-temporal - Variante 1).*

1. $P \longrightarrow TSA : REQ(\gamma; N)$
2. $TSA \longrightarrow P : \underbrace{Sig_{TSA}\{N, n_o, t_o\}}_{\gamma_o}$
3. *P verifica* γ_o *y genera* $\underbrace{Sig_P\{H(M), \gamma_o\}}_{\sigma}$
4. $P \longrightarrow G_S : REQ(\phi; ID_P, \sigma, H(M), \gamma_o, [Cert(ID_P, SK_P^+)])$
5. G_S *verifica el ancla confiable* γ_o *y la firma* σ*. Si la verificación no tiene éxito, se aborta el protocolo; en caso contrario se continúa.*
6. G_S *obtiene de forma auténtica la localización* l_c *del dispositivo identificado como* ID_P *en el momento* t_c*.*
7. $G_S \longrightarrow P : \underbrace{Sig_{G_S}\{ID_P, \sigma, l_c, t_c, v\}}_{\phi_c}$

La descripción del protocolo es como sigue. Primero P solicita a la TSA en el paso 1 la emisión de un ancla de tiempo confiable γ_o. Una vez P ha recibido dicha ancla en el paso 2, P genera la firma digital σ sobre un resumen $H(M)$ del documento y sobre el ancla γ_o en el paso 3.

Posteriormente, en el paso 4, P solicita a G_S un sello espacio-temporal sobre σ indicándole su identidad y enviándole también γ_o, M y opcionalmente $Cert(ID_P, SK_P^+)$, el certificado de clave pública que acredita que la pareja de claves (SK_P^-, SK_P^+) están asociadas a la entidad identificada como ID_P. Esta información permitirá a G_S verificar en el paso 5 la firma σ.

Si las verificaciones anteriores tienen éxito, G_S procederá a emitir un sello espacio-temporal ϕ_o sobre la firma σ generada por ID_P. Para ello, en el paso 6 G_S obtiene de forma auténtica la localización l_c del dispositivo en el momento t_c. Con esta información, G_S ya está en condiciones de generar el sello $\phi_c = Sig_{G_S}\{ID_P, \sigma, l_c, t_c, v\}$, por el que acredita que la entidad identificada como ID_P estaba en el lugar l_c en el momento t_c y que previamente a este instante esta entidad presentó la firma σ ante G_S. El valor v es el periodo de validez del sello.

Análisis del protocolo En el Protocolo 3, γ_o establece la cota de apertura en la generación de la firma σ. Debido a que P en el paso 3 incluye γ_o en dicha firma, ésta supone en sí misma una evidencia acerca de que la propia firma σ ha sido generada después de que existiera γ_o. Dado que se sabe que γ_o existe después de t_o, también podemos afirmar que σ existe después de t_o. Esto ocurre así porque habitualmente los algoritmos de firma actúan como funciones de un sólo sentido.

En el paso 7 G_S genera el sello ϕ_c que supone la cota de clausura. Con este sello G_S está emitiendo una especie de sello de anterioridad del documento σ respecto de t_c, ya que además de acreditar que la entidad P identificada como ID_P estaba en el lugar l_c en el momento t_c, el sello ϕ_c acredita que la entidad P presentó la firma σ ante G_S antes de ese instante. Este sello ϕ_c supone la cota superior espacio-temporal de la firma σ y v es la validez asignada al sello.

Por tanto, la firma σ ha debido generarse dentro dentro del intervalo temporal $\mathcal{T}_t = [t_o, t_c]$, donde $\mathcal{T}_t \neq \varnothing$ dado que se ha asumido que las TTP están sincronizadas temporalmente (y por tanto $t_c \geq t_o$).

Por otro lado, por haber asumido que P tiene una velocidad máxima v_{max}, la mayor distancia que puede haber recorrido P durante el intervalo temporal $\mathcal{T}_t$ es $d_{max} = (t_c - t_o) \times v_{max}$. Por tanto, la firma tuvo necesariamente que haberse generado mientras P estaba situado en el área $\mathcal{L}_t = \{l_t : l_t \in \mathcal{L}, d(l_t, l_c) \leq d_{max}\}$, donde $d(l_i, l_j)$ es una función que devuelve la distancia entre las posiciones l_i y l_j. La tupla $(\gamma_o, H(M), \sigma, \phi_c)$ permite a un tercero probar que la entidad identificada como ID_P generó la firma σ sobre $H(M)$ dentro del intervalo temporal $\mathcal{T}_t$ mientras estaba situada en el intervalo espacial $\mathcal{L}_t$.

5.3. Disminución de la confianza requerida en los protocolos de sellado espacio-temporal

En esta sección se presenta un protocolo que ofrece la misma precisión en la demostrabilidad que el Protocolo 3 pero que mejora a éste en cuanto a que se disminuye la confianza otorgada a las TTP participantes, así como se incrementa la privacidad de la entidad firmante gracias a la mayor modularidad del protocolo.

Protocolo 4 *(de sellado espacio-temporal - Variante 2).*

1. $P \longrightarrow G_C : REQ(\sigma; ID_P)$
2. G_C *obtiene de forma auténtica la localización* l_o *del dispositivo identificado como* ID_P *en el momento* t_o.
3. $G_C \longrightarrow P : \underbrace{Sig_{G_C}\{ID_P, l_o, t_o, v\}}_{\theta_o}$
4. P *verifica* θ_o *y genera* $\overset{\sigma}{\underbrace{Sig_P\{H(M), \theta_o\}}}$
5. $P \longrightarrow TSA : REQ(\varphi; \underbrace{H(H(M), \theta_o, \sigma)}_{H_\sigma})$
6. $TSA \longrightarrow P : \underbrace{Sig_{TSA}\{H_\sigma, n_c, t_c\}}_{\varphi_c}$

En este caso P solicita primero a G_C en el paso 1 la generación de una credencial espacio-temporal θ_o. Después, en el paso 2, G_C obtiene de forma auténtica la localización l_o de P (del dispositivo identificado como ID_P) en el momento t_o, para emitir una credencial θ_o sobre estas condiciones espacio-temporales y enviársela a P en el paso 3. Seguidamente, en el paso 4, P verifica la credencial θ_o y genera la firma digital σ sobre el resumen del documento $H(M)$ y la credencial espacio-temporal θ. En el paso 5 solicita un sello de anterioridad (o de tiempo) φ_c sobre H_σ en lugar de hacerlo directamente sobre $H(\sigma)$ para evitar ataques de falsificación del sello de anterioridad. En el paso 6 TSA genera el sello φ_c enviándoselo de vuelta a P.

Análisis del protocolo En este caso, la credencial θ_o es la cota de apertura en la generación de la firma σ. Dada θ_o un tercero puede probar que ID_P se encontraba en l_o en el instante t_o. Por incluir θ_o entre los datos de entrada en la generación de la firma σ, se puede probar que ésta se generó después de que existiese la credencial θ_o y, como se puede asumir que ésta existe después del instante t_o, se puede deducir que σ ha sido generada después de este instante.

El sello de anterioridad φ_c emitido en el paso 6 supone la cota de clausura. Con este sello φ_c se puede probar que H_σ fue presentado a la TSA antes del instante t_c y, por tanto, que existía antes de ese momento. Suponiendo que se utilizan funciones resumen de un sólo sentido, se puede deducir que σ fue también generada antes del instante t_c.

Por tanto al igual que en el Protocolo 3, la firma digital σ ha debido generarse en el intervalo temporal $\mathcal{T}_t = [t_o, t_c]$. Igualmente, la suposición de que la velocidad de P está acotada en v_{max} y el haberse acreditado que P estaba en l_o en el instante t_o, permiten deducir que, en el instante t_c, P puede haber recorrido como máximo una distancia $d_{max} = (t_c - t_o) \times v_{max}$. La firma σ tuvo necesariamente que haberse generado mientras P estaba situado en el área $\mathcal{L}_t = \{l_t : l_t \in \mathcal{L}, d(l_t, l_o) \leq d_{max}\}$. La tupla $(\theta_o, H(M), \sigma, \varphi_c)$ permite a un tercero probar que la entidad identificada como ID_P generó la firma σ sobre $H(M)$ dentro del intervalo temporal $\mathcal{T}_t$ mientras estaba situada en el intervalo espacial $\mathcal{L}_t$.

Sin embargo, a diferencia del Protocolo 3, se ha disminuido la confianza que es necesario depositar en la entidad G_C, pues ahora tan sólo debe acreditar las condiciones espacio-temporales de P y no está implicada en comprobaciones acerca del documento M ni acerca de que P haya generado una firma digital sobre éste. La confianza depositada en la TSA es la misma que antes, pues para esta entidad lo mismo da emitir el ancla confiable γ_o sobre un *nonce* que un sello de anterioridad φ_c sobre el valor resumen H_σ.

Pero además, por disminuir las tareas de G_C y no implicarla directamente en el sellado espacio-temporal del documento M, se incrementa la privacidad de la entidad firmante, pues G_C no tiene porqué conocer la finalidad de la credencial θ_o que emite, y tampoco esta finalidad trasciende durante la emisión del sello de tiempo φ_c (en los servicios de sellado temporal se suele enviar un resumen del documento a sellar y no directamente el documento). Esta privacidad sería

mayor si se utilizasen protocolos anónimos de acreditación espacio-temporal para emitir θ_o, como el propuesto en [2].

6. Conclusiones

Los servicios de sellado espacio-temporal (SSET) son uno de los servicios de confianza de más reciente aparición. Según se vayan implantando los servicios basados en la localización, la importancia de los servicios de confianza espacio-temporales se incrementará así como la necesidad de contar con servicios de este tipo con mayores garantías.

Actualmente existen algunas propuestas en la literatura cuyo objetivo es proporcionar servicios de sellado espacio-temporal. Sin embargo estos protocolos presentan, por un lado, ciertas deficiencias en cuanto a la precisión con la que un tercero puede probar las condiciones espacio-temporales acreditadas en las evidencias, por lo que su capacidad de asignar adecuadamente responsabilidades es menor. Por otro lado, su capacidad probatoria depende fuertemente de la confianza depositada en las TTP implicadas en los protocolos, dependencia que en la mayoría de las situaciones conviene disminuir.

En este trabajo se han propuesto dos protocolos de sellado espacio-temporal para la generación de firmas digitales que mejoran estos aspectos: Por un lado se acota el rango espacio-temporal bajo el que una entidad genera la firma digital y se incluyen en el sello evidencias demostrables acerca de esta acotación. Por otro lado, en el segundo protocolo, a la vez que se conserva la precisión conseguida con el primero, se limitan y distribuyen las responsabilidades de las TTP implicadas en los protocolos, provocando que se disminuya la confianza que es necesario depositar en éstas. Además, como resultado de la modularidad de este segundo protocolo, se mejora la privacidad de la entidad firmante.

Agradecimientos

La investigación presentada en este trabajo ha sido parcialmente financiada por la "Dirección General de Investigación del M.E.C." bajo el contrato SEG2004-02604: *'CERTILOC: Servicio de CERTIficación digital para la información de LOCcalización'*

Referencias

1. M. Burmester, Y. Desmedt, R.Ñ. Wright, and A. Yasinsac. Accountable privacy. In *The Twelfth International Workshop on Security Protocols*, April 2004.
2. L. Bussard. *Trust Establishment Protocols for Communicating Devices*. PhD thesis, Institut Eurécom, Télécom Paris, 2004.
3. D. Chaum. Security without identification: Transaction systems to make Big Brother obsolete. *Communications of the ACM*, 28(10):1030–1044, 1985.
4. G. M. Giaglis, P. Kourouthanassis, and A. Tsamakos. *Towards a classification framework for mobile location services*, pages 67–85. Idea Group Publishing, 2003.

5. A. I. González-Tablas, K. Kursawe, B. Ramos, and A. Ribagorda. Survey on location authentication protocols and spatial-temporal attestation services. In *Proc. of IFIP International Symposium on Network-Centric Ubiquitous Systems (NCUS 2005)*, 6-9 December 2005. (To be published).
6. J. Hightower and G. Borriello. A Survey and Taxonomy of Location Systems for Ubiquitous Computing. Technical Report UW-CSE 01-08-03, University of Washington, 2001.
7. ISO/IEC 10181-4. Information technology - OSI - Security frameworks in open systems - Part 4: Non-repudiation framework, 1997.
8. ISO/IEC 13888-1. Information technology - Security techniques - Non-repudiation - Part 1: General, 2004.
9. ISO/IEC 14516. Information technology - Security techniques - Guidelines for the use and management of Trusted Third Party services, 2002.
10. ISO/IEC 18014-1. Information technology - Security techniques - Time-stamping services - Part 1: Framework, 2002.
11. ITU-T. Recommendation X.509: Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, 2000.
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*, LNCS 2094. Springer, 2001.
13. R. Kailar. Accountability in electronic commerce protocols. *IEEE Trans. Softw. Eng.*, 22(5):313–328, 1996.
14. E. D. Kaplan, editor. *Understanding GPS: Principles and applications.* Artech House Publishers, 1996.
15. A. Lakshminarayanan, V. Singh, F. Bao, and K. P. Prabhu. Patent WO 03/007542. Method for certifying location stamping for wireless transactions, 2003. Publication date: 23/01/2003.
16. B. Ramos, A. I. González-Tablas, and A. Ribagorda. Sellado y Datación de Ubicación e Itinerario. In R. Menchaca et al., editor, *Actas del Segundo Congreso Iberoamericano de Seguridad Informática (CIBSI'03)*, pages 393–403, October 2003.
17. TS 23.271 Technical Specification Group Services and System Aspects; Functional stage 2 description of Location Services (LCS) (Release 7).