Mecanismo de certificación espacio-temporal basado en el estándar SAML

A. I. González-Tablas, B. Ramos, A. Ribagorda, and J. M. Estévez

Grupo de Seguridad de las Tecnologías de la Información y las Comunicaciones
Departamento de Informática - Universidad Carlos III de Madrid (España)
{aigonzal,benja1,arturo,jestevez}@inf.uc3m.es

Resumen El desarrollo de los servicios basados en la localización ha provocado la propuesta de un conjunto de nuevos servicios de seguridad adecuados a las necesidades que aquéllos plantean. Uno de estos servicios de seguridad, los servicios de certificación espacio-temporal, tiene por objetivo principal generar certificados digitales acerca de las condiciones espacio-temporales de una entidad. A lo largo de la última década diversos autores han propuesto mecanismos de certificación espacio-temporal. Una vez determinados los requisitos que las aplicaciones exigen a este tipo de servicios, se puede constatar que las propuestas existentes no cumplen satisfactoriamente éstos. En este trabajo se detallan cuáles son dichos requisitos y se propone un mecanismo de certificación espacio-temporal que sienta las bases para desarrollar un servicio de certificación espacio-temporal que satisfaga los requisitos mencionados. El mecanismo que se presenta se caracteriza por ser flexible y por utilizar el estándar SAML y otros estándares del contexto de los servicios de la localización en su implementación.

Palabras clave: Certificación espacio-temporal, estándares, SAML, servicios basados en la localización.

1. Introducción

La última década ha sido testigo del desarrollo e implantación de los servicios basados en la localización (*Location-Based Services* o LBS). Los LBS se definen como aquellos servicios de valor añadido que utilizan la posición geográfica de las entidades para proporcionar un valor añadido. El rango y la variedad de LBS es considerable, incluyendo, entre otros, servicios de emergencia y seguridad ciudadana, servicios de información y navegación, servicios de soporte al comercio electrónico, servicios de seguimiento de recursos y gestión de flotas, así como servicios de entretenimiento, ocio y proximidad [DB03,RM03].

Uno de los retos que se plantean en el área de los servicios basados en la localización es la seguridad de dicha información [TVM$^+$03,PMP03]. Los principales requisitos de seguridad detectados son el establecimiento de confianza en la información de localización y la protección de la privacidad de dicha información.

Desde la comunidad académica se han propuesto una serie de servicios de seguridad para abordar el establecimiento de la confianza en la información de localización, que en su conjunto se denominan servicios de confianza espacio-temporal. Los servicios de confianza espacio-temporal más relevantes son los que abordan la autenticación de la localización de una entidad en un momento determinado, la certificación (o acreditación) de la situación espacio-temporal de una entidad o su histórico y, por último, el sellado de documentos considerando sus circunstancias espacio-temporales. Es habitual y recomendable que los mecanismos para proporcionar servicios de certificación y sellado espacio-temporal se apoyen en los servicios de autenticación de la localización.

Recientemente, en [GKRR05], se ha publicado un estado de la cuestión acerca de este grupo de servicios, centrado principalmente en el de autenticación de la localización. Los mismos autores, en [GSRR05], presentan un modelo más detallado de los servicios de certificación espacio-temporal. Los servicios de confianza espacio-temporal posibilitan el desarrollo de aplicaciones de control de acceso dependientes de la información espacio-temporal de los sujetos y los recursos a los que se accede [DM98,SSW03], la asignación de responsabilidades con garantías en servicios de seguimiento y monitorización [ČBH03], la adaptación de transacciones electrónicas o la facturación de servicios según las condiciones espacio-temporales de las entidades [WLC03,Tol05], y la inclusión de la información espacio-temporal en los servicios de notarización [KZ01].

Respecto a la protección de la privacidad de la información espacio-temporal, pueden consultarse respectivamente en [Min04] y [GTH05] una discusión acerca de este asunto y un estado de la cuestión de los mecanismos que han sido propuestos para protegerla en el contexto de la computación ubicua.

Recientemente se han publicado una serie de propuestas con el objetivo de proveer servicios de certificación espacio-temporal ([ZKK01,WF03,Mic03,NNT03,Bus04]). El análisis de dichas propuestas a la luz de los requisitos planteados en las aplicaciones de los servicios de certificación espacio-temporal permite constatar que no los cumplen satisfactoriamente (véase la Sección 4). La investigación que se presenta en este trabajo se realiza en el contexto del proyecto CERTILOC[1] cuyo objetivo principal es precisamente diseñar y desarrollar un servicio de certificación espacio-temporal que satisfaga dichos requisitos. En particular, en este trabajo se determinan los requisitos mencionados y se propone el mecanismo que constituirá el corazón de CERTILOC. El mecanismo que se presenta define una estructura para representar los certificados espacio-temporales y los protocolos que permiten solicitar su generación y su transferencia. Se caracteriza por ser flexible y por utilizar el estándar SAML y otros estándares del contexto de los servicios de la localización en su implementación.

En la siguiente sección se determinan los requisitos que deberían satisfacer los servicios de certificación espacio-temporal y se presenta el modelo de provisión de dichos servicios. A continuación, en la Sección 3 se expone el mecanismo que se propone para proporcionar servicios de certificación espacio-temporal.

[1] Contrato SEG2004-02604 con el M.E.C: *'CERTILOC: Servicio de CERTIficación digital para la información de LOCalización'*

En la Sección 4 se presenta el análisis de los trabajos relacionados con esta investigación. Finalmente, en la Sección 5 se recogen las conclusiones alcanzadas y los trabajos futuros que se pueden derivar.

2. Los servicios de certificación espacio-temporal

En [GKRR05] se define que el objetivo principal de los servicios de certificación espacio-temporal es generar, recoger, mantener, proporcionar y validar certificados digitales sobre las condiciones espacio-temporales de un sujeto. Un conjunto representativo de aplicaciones de la certificación espacio-temporal incluiría los servicios de control de acceso, los servicios de seguimiento y monitorización, y la facturación de servicios. Para derivar el modelo de provisión de los servicios de certificación espacio-temporal y determinar qué requisitos deben satisfacer, se han tomado como referencia unos relatos de utilización de los servicios de certificación espacio-temporal en las mencionadas aplicaciones así como el análisis de las propuestas existentes en la literatura para proporcionar servicios de confianza espacio-temporal [GKRR05]. Los relatos se exponen a continuación.

El primer relato contempla la utilización de los certificados espacio-temporales para otorgar el **acceso a servicios o privilegios**. Por ejemplo, un centro comercial que ofrezca descuentos o privilegios a los clientes que visiten con cierta frecuencia las tiendas situadas en éste. Tanto a los clientes como al centro comercial les interesa que la información de las visitas sea correcta y que dicha información se refleje en algún documento acreditativo que pueda luego verificarse, e.g., un certificado espacio-temporal. El certificado deberá hacer referencia a un dispositivo que pueda ser localizado y que sea propiedad del cliente (e.g., un móvil o una PDA) o cedido por el centro comercial al cliente con este propósito (e.g., un dispositivo RFID). En el escenario descrito tiene sentido que sean los propios clientes quienes soliciten la generación de los certificados para preservar su privacidad. Tanto los clientes como el servicio de certificación espacio-temporal podrían conservar los certificados hasta que una oferta suficientemente sugerente del centro comercial motivase a los clientes a mostrarlos y revelar su historial de visitas. Otra posibilidad interesante consideraría que los certificados se solicitasen automáticamente o por el propio centro comercial tras detectar la presencia de los clientes en éste. Los requisitos de privacidad en este último caso son mayores, pues es una entidad distinta al cliente quien solicita el certificado. Una opción intermedia podría considerar que se permitiese al centro realizar dichas solicitudes pero que los certificados se enviasen a o se pusieran a disposición de los clientes. En todos los casos, una vez generado el certificado, es muy posible que los clientes deseasen restringir su utilización a determinados fines, e.g., obtención de la oferta, tal y como se promulga en la legislación actual.

El segundo relato se centra en los **servicios de seguimiento y monitorización** y puede tener como protagonista a un inspector y técnico de reparación de sistemas de refrigeración en grandes edificios. La empresa para la que trabaja incluye en sus políticas la localización de los trabajadores durante el horario de trabajo, tanto para gestionar eficientemente su flota como para monitorizar sus

actividades. A cambio de la presión que puede provocar en los trabajadores su localización continuada, la empresa les entrega unas primas mensuales, adicionales a su sueldo, en base a la eficiencia mostrada durante el mes. Además, la empresa se compromete a que no se localizará a los empleados durante la horario de comida, a pesar de que cada uno de ellos come a un horario diferente, dependiendo de las tareas que tiene asignadas diariamente cada trabajador.

El tercer relato aborda la **facturación de servicios** basados en la localización. Algunos ejemplos concretos de este tipo de aplicaciones son el cobro de peajes en autopistas, de impuestos en determinadas áreas geográficas (e.g., zonas urbanas altamente contaminadas y zonas naturales protegidas) o de tarifas por estacionamiento, en los que se realiza también un seguimiento de las entidades. En las aplicaciones de facturación de servicios es lógico que sea la entidad que proporciona el servicio quien esté interesada en solicitar los certificados para poder posteriormente exigir responsabilidades a los usuarios del servicio. Por supuesto, dichos usuarios deberán autorizar que su información espacio-temporal se utilice para este fin, en caso contrario los proveedores de servicios podrían exigir alguna tarifa estándar o 'plana'.

2.1. Modelo de provisión

En [GSRR05,GKRR05] se define también un modelo general de provisión de los servicios de certificación espacio-temporal. El modelo de provisión, que se resume en esta sección, especifica las entidades implicadas, las relaciones entre ellas y las fases en las que se provee el servicio (véase la Figura 1).

El sujeto S de los certificados debe ser un dispositivo con capacidades de localización, aunque adicionalmente puede considerar también a un usuario que controle el dispositivo. La entidad G_e es quien emite los certificados espacio-temporales. Típicamente el rol de G_e lo tomará bien un tercero de confianza (*Trusted Third Party* o TTP), bien un módulo confiable (*Trusted Platform Module* o TPM). En algunos casos, los usuarios podrán delegar la tarea de verificación de los certificados espacio-temporales a otra entidad confiable V_e. Por último, la entidad verificador de la localización (V_{loc}), en colaboración con cierta infraestructura de posicionamiento (PI), es quien obtiene de forma segura la información espacio-temporal sobre el sujeto. La diferenciación y separación de los diferentes roles en el modelo no implica que deban ser entidades distintas las que los tomen.

Por otro lado, los usuarios de los servicios de certificación espacio-temporal pueden tomar los siguientes roles: solicitante (RQ) de la emisión del certificado espacio-temporal; receptor (RC) de ésta tras su emisión; reclamante (CL) de su validez con el objetivo de obtener algún tipo de beneficio; y verificador (V), quien comprueba o hace comprobar la corrección y validez de la evidencia para otorgar el beneficio reclamado. Al igual que antes, y dependiendo de la aplicación concreta, una misma entidad podrá tomar varios de los roles descritos.

Las principales fases identificadas en la provisión de los servicios de certificación espacio-temporal son (1) la generación del certificado, (2) su transferencia y/o almacenamiento y recuperación, y (3) la verificación del certificado.

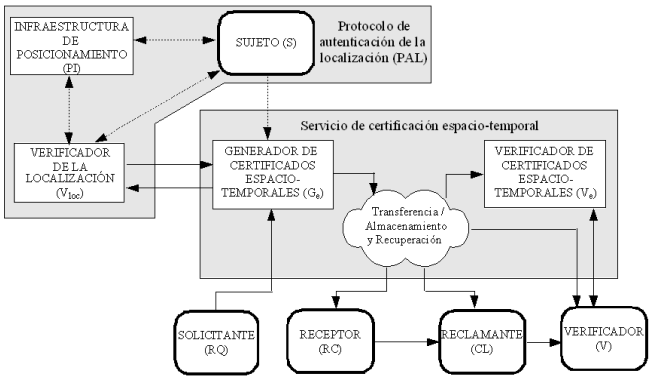

Figura 1. Modelo de provisión de los servicios de certificación espacio-temporal

2.2. Requisitos

Basándose en los relatos expuestos anteriormente, se pueden determinar una serie de requisitos que deben satisfacer los servicios de certificación espacio-temporal y que se presentan a continuación.

Establecimiento de confianza El objetivo principal de los servicios de certificación espacio-temporal es permitir que terceras partes (los usuarios) confíen en que cierta información espacio-temporal está asociada a una entidad concreta. Con este fin utilizan mecanismos de certificación con los que se generan certificados espacio-temporales. Un usuario debe poder asignar un nivel de credibilidad a dichos certificados utilizando los datos contenidos en éstos y, opcionalmente, datos externos. Para que esta confianza pueda establecerse deben cumplirse determinadas condiciones:

- Los certificados deben ser infalsificables (se debe poder comprobar su integridad y su emisor) y tener asignado un periodo de validez (se debe poder comprobar si son vigentes o han expirado).
- Los certificados deben ser intransferibles, es decir, un sujeto distinto al que está asociado el certificado no debe poder hacer uso de éste como si hiciera referencia a él mismo. Tampoco se deben poder utilizar para demostrar unas condiciones espacio-temporales del sujeto distintas a las acreditadas en los certificados.

Además, los usuarios deben confiar en que G_e utilizará para generar los certificados información espacio-temporal referente al sujeto auténtica. Dado que en el modelo propuesto es realmente la entidad V_{loc} quien obtiene dicha información espacio-temporal, los usuarios deberán confiar en que V_{loc} utilice mecanismos de posicionamiento del sujeto y de comunicación con G_e que garanticen la autenticidad de dicha información.

Privacidad Por otro lado, la información espacio-temporal, cuando está asociada de forma directa o indirecta a un individuo identificado o identificable, puede calificarse de dato de carácter personal, ya que su conocimiento permite construir perfiles sobre los hábitos, las preferencias y la vida personal de dichos individuos. Por esta razón, los servicios de certificación espacio-temporal se verán afectados por las diversas directivas y leyes elaboradas en la última década para proteger el derecho a la privacidad de las personas [Dir95,Dir02,Ley99,Rea05]. La mencionada legislación se fundamenta en especialmente en los principios de calidad de los datos, información, consentimiento y cesión a terceros.

Flexibilidad y personalización Las diferentes situaciones planteadas en los relatos permiten constatar que es necesario que los servicios de certificación espacio-temporal ofrezcan servicios independientes de generación y transferencia, permitiendo el acceso a estos servicios al conjunto completo de roles definidos en el modelo de provisión y permitiendo su utilización combinada.

Asimismo, las aplicaciones de los servicios de certificación espacio-temporal demandan que éstos ofrezcan mecanismos de personalización tanto para automatizar la generación y transferencia de certificados espacio-temporales como para gestionar la privacidad de la información espacio-temporal.

Utilización de estándares Los servicios de certificación espacio-temporal pueden ser utilizados en distintas aplicaciones y contextos y durante su provisión diversas entidades interactuarán con los mecanismos que implementen los servicios. Por esta razón, los mecanismos deberán esforzarse por utilizar estándares para definir los protocolos de interactuación entre las entidades participantes y representar los certificados.

Los estándares que podrían ser más apropiados para representar y gestionar los certificados espacio-temporales son el marco para certificados de atributos X.509 AC [IET02a] y el marco de aserciones de seguridad SAML [OAS05]. Sin embargo, X.509 AC no define un protocolo base para solicitar y recibir certificados, además de que es más fácil integrar SAML con otros estándares definidos en el entorno de los servicios de localización (GML y MLP), ya que en general utilizan XML para representar las estructuras de datos, al igual que SAML. Por estas razones se ha seleccionado SAML para implementar el mecanismo de certificación espacio-temporal propuesto en este trabajo.

SAML (*Security Assertion Markup Language*) es una especificación de la organización OASIS que define un lenguaje XML para representar e interpretar *aserciones de seguridad* así como un protocolo para permitir su intercambio [OAS05]. SAML especifica tres tipos concretos de aserciones - autenticación, atributo y decisión de autorización -, aunque también permite que los usuarios definan sus propios tipos de aserción. SAML define una estructura común para todos los tipos de aserciones que puede adecuar a cada tipo de aserción mediante la inclusión de determinadas *afirmaciones*. Las afirmaciones podrán ser de alguno de los tipos definidos en el estándar con este propósito - afirmaciones de autenticación, de atributo y de decisión de autorización -, o de nuevos tipos

definidos por los usuarios. Las afirmaciones de atributos son especialmente interesantes porque pueden utilizarse directamente en mecanismos de control de acceso basados en el estándar XACML [OAS04].

SAML define también un protocolo que considera dos tipos de mensajes, uno abstracto para solicitar aserciones y otro ampliable para recibir las respuestas a las peticiones. Los desarrolladores de aplicaciones deben derivar del mensaje abstracto de solicitud sus propios mensajes de solicitud. De igual forma deberán derivar del mensaje de respuesta definido en el estándar sus mensajes de respuesta en el caso de que necesiten ampliar lo establecido en éste. En [OAS05] se definen además algunos protocolos particularizan lo definido en el estándar para ciertas aplicaciones. Considerando el modelo de provisión de los servicios de certificación espacio-temporal interesa el protocolo definido para solicitar aserciones ya existentes, bien conociendo el identificador de las aserciones bien indicando el sujeto y el tipo de afirmación requerida, así como el mensaje de respuesta definido para estas solicitudes.

Aunque SAML proporciona una base para representar y gestionar certificados espacio-temporales, no especifica cómo representar la información espacio-temporal. Para este propósito la organización OGC (*Open GIS Consortium*) ha desarrollado el estándar GML (*Geographic Markup Language*) [OGC03]. GML es un potente y complejo lenguaje en XML diseñado para modelar, transportar y almacenar información geográfica mediante objetos que describen facetas, sistemas de coordenadas de referencia, geometría, topología, tiempo, unidades de medida, etc. El mecanismo que se propone utilizará elementos definidos en GML para representar la información espacio-temporal.

Por último, interesa conocer qué estándares podrían utilizarse para que G_e obtenga la información espacio-temporal de V_{loc}. En la actualidad, las propuestas existentes en la literatura para autenticar la localización de entidades no han especificado un formato concreto para proporcionar dicha información ni comparten una interfaz común, como se puede comprobar en el estado de la cuestión en [GKRR05]. En el marco más general de las tecnologías de posicionamiento, suelen existir estándares *de jure* o *de facto* particulares para cada tecnología. Sin embargo, se puede destacar la iniciativa del organismo OMA (*Open Mobile Alliance*) que tiene actualmente un papel principal en la estandarización de servicios móviles, aplicaciones y su interoperatividad. OMA ha desarrollado una norma que define un protocolo de localización móvil para redes inalámbricas (MLP o *Mobile Location Protocol*), con la intención de servir de interfaz común entre los servicios de localización (aquellos que proporcionan información de localización) y los servicios basados en la localización [LIF02]. Éste ha sido el protocolo elegido para la comunicación entre G_e y V_{loc}.

3. Mecanismo propuesto

Como se mencionó en la Sección 1, este trabajo se realiza en el contexto del proyecto CERTILOC. El objetivo final de CERTILOC es diseñar y desarrollar un servicio de certificación espacio-temporal que satisfaga los requisitos estable-

cidos en la Sección 2.2. En este trabajo se aborda el diseño del mecanismo que constituirá el corazón de CERTILOC según las siguientes directrices:

- Se debe garantizar que un tercero pueda establecer un nivel de confianza en la información contenida los certificados.
- Se debe facilitar la integración de mecanismos de control de acceso y autorización para preservar la privacidad de la información espacio-temporal, aunque no se abordará el diseño de estos mecanismos.
- El mecanismo ofrecerá flexibilidad suficiente para poder ser utilizado por las diferentes aplicaciones descritas en la Sección 2.
- Se utilizarán estándares existentes de las áreas de la seguridad de la información y los servicios basados en la localización.

3.1. Arquitectura

La arquitectura del mecanismo que se propone se basa en el modelo de provisión expuesto en la Sección 2. Las entidades que componen la arquitectura son las siguientes (véase la Figura 2):

- *Autoridad de Certificación Espacio-Temporal* (STCA), es un tercero de confianza que toma el rol de G_e. Cuenta con un *Repositorio* (R) donde almacenará los certificados espacio-temporales. Permite solicitar la generación de dichos certificados así como su transferencia si han sido emitidos previamente y se encuentran almacenados en el repositorio.
- *Sujeto*, equivale al sujeto del modelo de provisión.
- *Servicio de Información Espacio-Temporal* (STIS), abstrae las entidades V_{loc} y PI del modelo de provisión. Se asume que es capaz de obtener información espacio-temporal auténtica sobre el sujeto y de comunicarla de forma segura a la STCA. Para la obtención de la información espacio-temporal auténtica se deberán tener en cuenta las consideraciones realizadas en [GKRR05].
- *Usuario* (U), esta entidad toma el rol de RQ y RC del modelo de provisión.

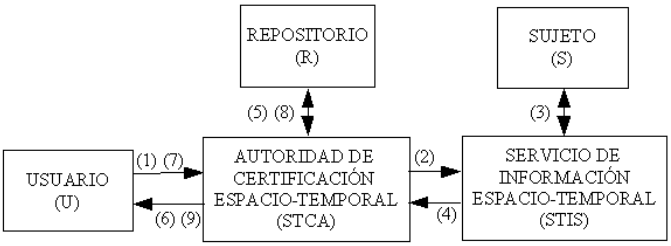

Figura 2. Arquitectura del mecanismo de certificación espacio-temporal propuesto

Se decide generar certificados digitales que los usuarios puedan verificar por sí mismos sin necesitar de la ayuda de un tercero de confianza, por lo que ninguna de las entidades de la arquitectura toma el rol de V_e. La fase de verificación se produce posteriormente fuera de la arquitectura propuesta y en el contexto de cada aplicación específica.

La provisión del servicio de certificación espacio-temporal transcurre según el siguiente flujo de mensajes:

(1) U envía a STCA un mensaje de solicitud de generación de certificado espacio-temporal, indicando el sujeto deseado del certificado y si una vez generado éste debe transferirse en la respuesta.
(2) STCA, utilizando el estándar MLP solicitará la información espacio-temporal relativa al sujeto indicado.
(3) STIS obtiene dicha información asegurándose de que ésta es auténtica.
(4) STIS comunica la información espacio-temporal solicitada a STCA utilizando también el estándar MLP.
(5) STCA genera el certificado espacio-temporal y lo almacena en el repositorio.
(6) Finalmente, STCA envía a U un mensaje de respuesta a la solicitud de generación, comunicándole el resultado de su petición y transfiriéndole el certificado si así lo solicitó y si éste fue generado con éxito.
(7) Posteriormente, el mismo usuario u otro distinto puede solicitar la transferencia de uno o varios certificados almacenados en el repositorio. Para ello U envía a STCA un mensaje de solicitud de transferencia de certificado espacio-temporal.
(8) STCA obtiene los certificados solicitados del repositorio.
(9) Por último, STCA envía a U un mensaje de respuesta a la solicitud de transferencia de certificados a U, comunicándole el resultado de su petición y, en su caso, los certificados solicitados.

La arquitectura propuesta permite satisfacer los requisitos planteados en los relatos de la Sección 2, pues al proporcionar ambos servicios de generación y transferencia de certificados tanto independientemente como combinados se cubren todas las situaciones posibles. Por otro lado, la definición de un usuario general que pueda tomar cualquiera de los roles RQ y RC, y posteriormente CL o V, supone una mejora con respecto al modelo general de provisión pues permite simplificar dicha provisión escondiendo la complejidad del modelo. La arquitectura propuesta ha sido diseñada de forma que sea posible su integración con el módulo de personalización para la generación de certificados espacio-temporales presentado en [GSRR05], por lo que este otro requisito sería también satisfecho.

En las siguientes secciones se expondrá la estructura de los certificados espacio-temporales y los protocolos de generación y transferencia de certificados espacio-temporales (mensajes 1, 6, 7 y 9) que se proponen y su implementación utilizando los estándares SAML y GML.

3.2. Certificado espacio-temporal

En primer lugar los certificados espacio-temporales deberán recoger la siguiente información:

(I1) Versión de certificado espacio-temporal bajo la que se han generado.
(I2) Número de serie que lo identifique unívocamente entre otros certificados emitidos por la misma autoridad.
(I3) Instante de generación del certificado.
(I4) Periodo de validez del certificado.
(I5) Entidad emisora del certificado.
(I6) Sujeto al que hace referencia el certificado.
(I7) Información espacio-temporal, es decir, cierta localización del sujeto y el instante temporal al que se corresponde. Se incluirá la resolución de ambos parámetros así como la entidad que ha proporcionado la información.
(I8) Extensiones que permitan asociar al certificado información referente a los usuarios que estarían autorizados a utilizarlos o bajo qué condiciones (finalidad, almacenamiento, distribución, etc.).
(I9) Firma digital de la entidad emisora sobre todo lo anterior.

Información	**Atributos y elementos de SAML**	**Nuevos atributos y elementos**
I1		`STAVersion`
I2	`ID`	
I3	`IssueInstant`	
I4	`NotBefore` y `NotOnOrAfter`	
I5	<`saml:Issuer`>	
I6	<`saml:Subject`>	
I7		<`SpatialTemporalStatement`>
I8	<`saml:Extensions`>	
I9	<`ds:Signature`>	

Tabla 1. Estructura de los certificados espacio-temporales como ampliación de las aserciones SAML

Para representar los certificados espacio-temporales se propone utilizar las aserciones de atributos del estándar SAML. En particular se define un nuevo tipo de aserción de atributos `SpatialTemporalAssertionType` derivado del tipo definido para las aserciones SAML. En la Tabla 1 se muestra cómo los atributos y los elementos de las aserciones SAML permiten representar la mayoría de las informaciones requeridas en un certificado espacio-temporal. El nombre de los elementos y los atributos XML se presentan con letra *TypeWriter*. Los elementos XML, además, se encerrarán entre corchetes y se prefijarán con el identificador del espacio de nombres al que pertenecen, en concreto, `'saml:'` para SAML, `'samlp:'` para el protocolo SAML y `'ds:'` para XMLDSig, el estándar de firma digital en XML [IET02b].

Los atributos y los elementos de las aserciones SAML que se utilizan en los certificados espacio-temporales son, en primer lugar, la versión (`Version`) de la especificación SAML utilizada, un identificador (`ID`) del certificado y su instante de emisión (`IssueInstant`). Además, el elemento (<`saml:Issuer`>) del

certificado contendrá la identificación de la autoridad de certificación espacio-temporal (ACET) que lo emitió. Los certificados incluirán una firma de la ACET sobre éste en el elemento (<ds:Signature>) y el sujeto (<saml:Subject>) del certificado espacio-temporal. El periodo de vigencia del certificado se especificará dentro del elemento SAML que permite determinar el conjunto de condiciones (<saml:Conditions>) bajo las que la aserción es válida (NotBefore y NotOnOrAfter).

En la Tabla 1 también se indica qué nuevos elementos se deben definir como ampliaciones de las aserciones SAML. El nuevo atributo STAVersion se define como una cadena de caracteres, al igual que Version. Además, se define un nuevo tipo de afirmación de atributos SAML para contener los elementos <SpatialTemporalStatement> de la siguiente forma:

```
<xs:element name='SpatialTemporalStatement' type='sta:SpatialTemporalStatementType'/>

<xs:complexType name='SpatialTemporalStatementType'>
<xs:complexContent>
<xs:extension base='saml:AttributeStatementType'/>
</xs:complexContent>
</xs:complexType>
```

Finalmente, se definen tres nuevos atributos SAML, <Location>, <Time> y <STIIssuer>, que permitirán precisar la posición del sujeto en un determinado momento temporal y la entidad que obtuvo esta información. Los elementos <Location> y <Time> se definen utilizando tipos abstractos del lenguaje GML[2] [OGC03] de posición y tiempo, permitiendo entonces que estas informaciones se puedan precisar de todas las maneras ofrecidas en este estándar. Además cada uno contiene un elemento para indicar la resolución con la que se expresa la medida, <SpatialAccuracy> y <TemporalAccuracy>, que también se definen utilizando elementos del lenguaje GML. La definición de estos elementos se muestra a continuación:

```
<xs:element name='Location' type='saml:AttributeType'/>

<xs:complexType name='LocationType'>
<xs:sequence>
<xs:element ref='gml:location'/>
<xs:element ref='sta:SpatialAccuracy'/>
</xs:sequence>
</xs:complexType>

<xs:element name='Time' type='saml:AttributeType'/>

<xs:complexType name='TimeType'>
<xs:sequence>
<xs:element ref='gml:_TimePrimitive'/>
<xs:element ref='sta:TemporalAccuracy'/>
</xs:sequence>
</xs:complexType>

<xs:element name='SpatialAccuracy' type='sta:SpatialAccuracyType'/>

<xs:complexType name='SpatialAccuracyType'>
<xs:choice>
<xs:element name='GeographicalAccuracy' type='gml:LengthType'/>
<xs:element name='SymbolicAccuracy' type='sta:SymbolicAccuracyType'/>
```

[2] Los elementos de este lenguaje se prefijarán con 'gml:'.

```
</xs:choice>
</xs:complexType>

<xs:complexType name='SymbolicAccuracyType'>
<xs:simpleContent>
<xs:extension base='xs:string'>
<xs:attribute name='AccuracySpace' type='xs:anyURI'/>
</xs:extension>
</xs:simpleContent>
</xs:complexType>

<xs:element name='TemporalAccuracy' type='gml:TimeIntervalLengthType'/>

<xs:element name='STIIssuer' type='saml:AttributeType'/>

<xs:element name='STIIssuer' type='saml:AttributeType'/>
<xs:complexType name='STIIssuerType'>
<xs:sequence>
<xs:element ref='sta:STInformationService'/>
</xs:sequence>
</xs:complexType>
```

El modelo propuesto de certificado espacio-temporal permite a un tercero establecer un nivel de confianza en la información contenida los certificados. La firma digital de STCA, si implementada correctamente, garantiza que los certificados son infalsificables. Por otro lado, cada certificado tiene asociado un periodo de validez que terceros pueden comprobar. Asimismo, al aplicarse la firma digital de la STCA sobre la identificación del sujeto y la información espacio-temporal asociada, el certificado es intransferible (está ligado a ese sujeto concreto) y no puede reutilizarse para demostrar unas condiciones espacio-temporales distintas a las reflejadas.

3.3. Protocolo de certificación espacio-temporal

El protocolo que se propone consta de dos parejas de mensajes que permiten solicitar respectivamente la generación de certificados espacio-temporales y su transferencia una vez han sido generados. Se basan en los protocolos definidos en SAML (para los tipos de mensajes mencionados, consúltese el estándar).

Solicitud/respuesta de generación de certificado espacio-temporal El usuario U necesitaría indicar el sujeto sobre el que solicita el certificado y si desea que éste le sea transferido en el mensaje de respuesta. Por ello se define `SpatialTemporalAssertionRequestType` un nuevo tipo de mensaje derivado de `samlp:RequestAbstractType` para especificar los mensajes de solicitud de generación (<`SpatialTemporalAssertionRequest`>):

```
<xs:element name='SpatialTemporalAssertionRequest'
type='stap:SpatialTemporalAssertionRequestType'/>

<xs:complexType name='SpatialTemporalAssertionRequestType'>
<xs:complexContent>
<xs:extension base='samlp:RequestAbstractType'>
<xs:attribute name='ReturnAssertion' type='xs:boolean'/>
</xs:extension>
</xs:complexContent>
</xs:complexType>
```

Para indicar cuál es el sujeto o los sujetos, se adjuntarán uno o varios elementos <`Subject`>, del mismo tipo que <`saml:Subject`>, dentro del objeto <`saml:Extensions`>.

Para representar el mensaje de respuesta a la solicitud de generación de certificado espacio-temporal se define un nuevo mensaje <`SpatialTemporal-AssertionResponse`> cuyo tipo se deriva del tipo `samlp:StatusResponseType`. Si se debe devolver el certificado espacio-temporal en este mensaje, se puede adjuntar dentro del objeto <`samlp:Extensions`>.

Solicitud/respuesta de transferencia de certificado espacio-temporal En este caso el usuario U está interesado en recibir uno o varios certificados espacio-temporales que hayan sido generados previamente y que fueron almacenados en el repositorio. Los mensajes <`saml:AssertionIDRequest`> y <`saml:Response`> del protocolo SAML permiten directamente contener solicitudes y respuestas de transferencia de certificados espacio-temporales, sin necesidad de ampliaciones. El usuario debe indicar los identificadores o números de serie de los certificados solicitados.

4. Trabajos relacionados

De las propuestas existentes en la literatura para proveer servicios de certificación espacio-temporal ([ZKK01,WF03,Mic03,NNT03,Bus04]), tan sólo las propuestas en [ZKK01] y [Bus04] son suficientemente robustas para garantizar el requisito de establecimiento de la confianza (consúltese [GKRR05] para más detalles sobre estos resultados).

Sin embargo, [ZKK01,Bus04] no cumplen satisfactoriamente los objetivos abordados al desarrollar el mecanismo de certificación espacio-temporal que se propone en este trabajo.

Bussard en [Bus04] plantea una situación demasiado específica que fuerza a descartar muchas de las aplicaciones descritas en los relatos de la Sección 2. Por otro lado, la propuesta en [Bus04] no define una implementación a bajo nivel del protocolo de certificación espacio-temporal que presenta, pero sí especifica un formato XML para los certificados. Desafortunadamente, no hace uso de un estándar sino que utiliza un marco de certificados de atributos propio [RBKKC03].

La propuesta en [ZKK01] sí permite solicitar a terceros la generación de certificados espacio-temporales, además de al sujeto de los mismos, pero no independiza la generación y la transferencia. Zugenmaier *et al.* proponen utilizar los servicios CAMEL, estandarizados para las redes GSM de telefonía celular, en la implementación del mecanismo de certificación. Sin embargo, no se puede calificar esta solución de general, ya que es específica a dichas redes, además de que tampoco especifican los autores un formato de certificado espacio-temporal basado en algún estándar.

5. Conclusiones y trabajos futuros

Desde la comunidad académica se han propuesto diversos servicios para establecer la confianza de la información de localización. La investigación que se presenta en este trabajo se realiza en el contexto del proyecto CERTILOC, que se centra en uno de los servicios mencionados, en particular en los servicios de certificación espacio-temporal. Recientemente se han publicado una serie de propuestas con el objetivo de proveer servicios de certificación espacio-temporal ([ZKK01,WF03,Mic03,NNT03,Bus04]). Sin embargo, el análisis de dichas propuestas a la luz de los requisitos planteados en las aplicaciones de los servicios de certificación espacio-temporal permite constatar que no los cumplen satisfactoriamente. CERTILOC tiene precisamente por objetivo principal diseñar y desarrollar un servicio de certificación espacio-temporal que satisfaga dichos requisitos.

En este trabajo se han determinado los requisitos mencionados utilizando una serie de relatos de utilización de los servicios de certificación espacio-temporal en el contexto de varias aplicaciones representativas. Además, se propone el mecanismo que constituye el corazón de CERTILOC y que aborda parcialmente dichos requisitos y sienta las bases para satisfacer el resto. El mecanismo presentado contempla la definición de una estructura para representar los certificados espacio-temporales y los protocolos que permiten solicitar su generación y su transferencia. Se caracteriza por ser flexible y por hacer un uso extensivo de los estándares existentes en las áreas de la seguridad de la información (SAML [OAS05]) y los servicios basados en la localización (MLP [LIF02] y GML [OGC03]). Estas características suponen un avance con respecto a las propuestas existentes en la literatura para proporcionar servicios de certificación espacio-temporal. Además, la utilización del estándar SAML facilita la futura integración de mecanismos de autorización y control de acceso implementados utilizando el estándar XACML [OAS04]. Adicionalmente, el mecanismo se ha diseñado de forma que es posible su integración con el módulo de automatización de la generación de los certificados presentado en [GSRR05].

La principal línea de continuación de este trabajo deberá abordar el diseño y la integración de mecanismos para proteger la privacidad de la información espacio-temporal de los sujetos. Una posible aproximación podría abordar esta necesidad combinando un sistema de políticas de autorización con certificados de atributos que permitiesen definir autorizaciones más específicas. Las políticas podrían definirse utilizando XACML y los certificados de atributos utilizando SAML de nuevo.

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

[Bus04] L. Bussard. *Trust Establishment Protocols for Communicating Devices*. PhD thesis, Institut Eurécom, Télécom Paris, 2004.

[ČBH03] S. Čapkun, L. Buttyán, and J. P. Hubaux. SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. In *the 1st ACM Workshop on Security in Ad Hoc and Sensor Networks*, October 2003.

[DB03] Thomas D'Roza and George Bilchev. An overview of location-based services. *BT Technology Journal*, 21(1):20–27, January 2003.

[Dir95] Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, 1995.

[Dir02] Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de Julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, 2002.

[DM98] D. E. Denning and P. F. MacDoran. Location-based authentication: grounding cyberspace for better security. In *Internet besieged: Countering cyberspace scofflaws*. ACM Press/Addison-Wesley Publishing Co., 1998.

[GKRR05] A. I. González-Tablas, K. Kursawe, B. Ramos, and A. Ribagorda. Survey on location authentication protocols and spatial-temporal attestation services. In *Proceedings of IFIP International Symposium on Network-Centric Ubiquitous Systems (NCUS 2005)*, 6-9 December 2005.

[GSRR05] A. I. González-Tablas, L. M. Salas, B. Ramos, and A. Ribagorda. Providing personalization and automation to spatial-temporal stamping services. In *Proceedings of the 1st International Workshop on Secure and Ubiquitous Networks*. IEEE Computer Society Press, 2005.

[GTH05] Andreas Görlach, Wesley W. Terpstra, and Andreas Heinemann. Survey on location privacy in pervasive computing. In *Proceedings of the Workshop on Privacy, Security and Trust within the Context of Pervasive Computing*. Kluwer, 2005.

[IET02a] IETF. *An Internet Attribute Certificate Profile for Authorization (RFC 3281)*, 2002.

[IET02b] IETF/W3C. *XML Signature Syntax and Processing*, 2002.

[KZ01] M. Kabatnik and A. Zugenmaier. Location stamps for digital signature: A new service for mobile telephone networks. In *Proceedings of the First International Conference on Networking-Part 2 (ICN'01)*, LNCS 2094. Springer-Verlag, 2001.

[Ley99] Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), 1999.

[LIF02] LIF (Location Interoperatibility Forum). *LIF TS 101 Mobile Location Protocol Specification, version 3.0.0*, June 2002.

[Mic03] N. Michalakis. Location aware access control for pervasive computing environments. Master's thesis, MIT, 2003.

[Min04] R. P. Minch. Privacy issues in location-aware mobile devices. In *Proceedings of the 37th Hawaii International Conference on System Sciences*. IEEE Computer Society Press, 2004.

[NNT03] K. K. Nakanishi, J. J. Nakazawa, and H. Tokuda. LEXP: Preserving user privacy and certifying the location information. In *Proceedings of the 2nd Workshop on Security in Ubiquitous Computing (UBICOMP 2003)*, October 2003.

[OAS04] OASIS. *Extensible access control markup language (XACML) Version 2.0 Committee Draft 04*, 6 December 2004.

[OAS05] OASIS (Organization for the Advancement of Structured Information Standards). *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) Version 2.0. OASIS Standard*, 15 March 2005.

[OGC03] OGC (Open GIS Consortium). *Geographic Markup Language (GML3.0)*, 2003.

[PMP03] Cynthia A. Patterson, Richard R. Muntz, and Cherri M. Pancake. Challenges in location-aware computing. *IEEE Pervasive Computing*, 2(2):80–89, April 2003.

[RBKKC03] Yves Roudier, Laurent Bussard, Roger Kilian-Kehler, and Stefano Crosta. Trust and authorization in pervasive b2e scenarios. In *Proceedings of the 6th Information Security Conference*, pages 295–309, 2003.

[Rea05] Real Decreto 424/2005 de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, 2005.

[RM03] Bharat Rao and Louis Minakis. Evolution of mobile location-based services. *Communications of the ACM*, 46(12):61–65, December 2003.

[SSW03] N. Sastry, U. Shankar, and D. Wagner. Secure verification of location claims. In *Proceedings of the 2003 ACM workshop on Wireless security*. ACM Press, 2003.

[Tol05] Toll Collect GmbH. Toll Collect service on the road. Available at: http://www.toll-collect.de/ (last access on October 2005), 2005.

[TVM+03] Aphrodite Tsalgatidou, Jari Veijalainen, Jouni Markkula, Artem Katasonov, and Stathes Hadjiefthymiades. Mobile E-Commerce and Location-Based Services: Technology and Requirements. In *Proceedings of the 2003 Scandinavian Research Conference on Geographical Information Science (ScanGIS'2003)*. Department of Surveying, Helsinki University of Technology, 4-6 June 2003.

[WF03] B. R. Waters and E. W. Felten. Secure, Private Proofs of Location. TR-667-03. Technical report, Princenton, Computer Science, January 2003.

[WLC03] C. Wullems, M. Looi, and A. Clark. Enhancing the security of Internet Applications using location: A new model for tamper-resistant GSM location. In *Proceedings of the 8th IEEE Symposium on Computers and Communications (ISCC 2003)*, 2003.

[ZKK01] A. Zugenmaier, M. Kreutzer, and M. Kabatnik. Enhancing applications with approved location stamps. In *Proceedings of the IEEE Intelligent Network 2001 Workshop (IN2001)*, 2001.