CERTILOC: Análisis y diseño de un servicio de certificación espacio-temporal respetuoso con la privacidad

A.I. González-Tablas
Dpto. Informática
Univ. Carlos III de Madrid
aigonzal@inf.uc3m.es

J.M. Fuentes
Dpto. Informática
Univ. Carlos III de Madrid
100039302@alumnos.uc3m.es

J.C. Calvo
Dpto. Informática
Univ. Carlos III de Madrid
100070634@alumnos.uc3m.es

A. Orfila
Dpto. Informática
Univ. Carlos III de Madrid
adiaz@inf.uc3m.es

J. Gallo
Dpto. Informática
Univ. Carlos III de Madrid
100039293@alumnos.uc3m.es

J. Patter
Dpto. Informática
Univ. Carlos III de Madrid
100063891@alumnos.uc3m.es

Resumen

La certificación espacio-temporal respetuosa con la privacidad es uno de los retos que debe afrontar la comunidad académica ante el vertiginoso desarrollo de los servicios basados en la localización en los últimos tiempos. En este artículo se presenta el análisis y el diseño de CERTILOC, un servicio de certificación espacio-temporal que emite certificados basados en el estándar SAML y que es a la vez respetuoso con la privacidad de los usuarios al integrar mecanismos de control de acceso basados en políticas de privacidad espacio-temporales que especifican los propios usuarios.

1. Introducción

La última década ha sido testigo del desarrollo e implantación de los servicios basados en la localización (LBS), que se definen como aquellos servicios 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.

Uno de los retos que se plantean en el área de los servicios basados en la localización es la seguridad de dicha información [1]. Los principales requisitos de seguridad detectados son el establecimiento de confianza en la información de localización (autenticación y certificación) y la protección de su privacidad de dicha información. La comunidad académica ha propuesto diversos mecanismos para proporcionar los citados servicios, generalmente enfocados bien al establecimiento de la confianza bien a la privacidad de la información espacio-temporal, siendo pocos los trabajos que abordan ambos aspectos conjuntamente. Así mismo, dada la juventud de los servicios de seguridad específicos para la localización, es infrecuente la implementación de los mecanismos propuestos.

Este trabajo se realiza en el contexto del proyecto de investigación CERTILOC[†], que tiene por objetivos principales, primero, proponer un modelo para los servicios de certificación espacio-temporal que respete la privacidad de los usuarios y, segundo, implementar un demostrador de dicho modelo capaz de interactuar con varias tecnologías de estimación de la posición. Una vez desarrollado el modelo [2], se ha acometido su implementación. En este artículo se presenta el análisis y el diseño del demostrador de CERTILOC, así como los avances realizados en su implementación.

---

† El proyecto CERTILOC (Servicio de CERTIficacion digital de la LOCalizacion) está financiado por el M.E.C. (España) dentro del Plan Nacional de Investigación Científica, Desarrollo e Innovación Tecnológica 2004-2007 bajo el contrato SEG2004-02604.

2. Certificación espacio-temporal respetuosa con la privacidad

Los servicios de certificación espacio-temporal tienen por objetivo principal generar, recoger, mantener, proporcionar y validar certificados digitales sobre las condiciones espacio-temporales de un sujeto. Algunas de sus áreas de aplicación incluyen los servicios de control de acceso, los servicios de seguimiento y monitorización, y la facturación de servicios.

El amplio desarrollo que están sufriendo los servicios basados en la localización en los últimos años ha provocado que se considere actualmente dicha información como de carácter personal. De hecho, la privacidad de la información de localización ha sido abordada específicamente por los organismos legislativos de diversos países, complementando en la mayoría de los casos legislaciones ya existentes [3]. En la actualidad, los mecanismos más utilizados para proteger la privacidad de la información espacio-temporal son el control de acceso basado bien en políticas centralizadas bien en certificados de atributos, y la disociación de la información espacio-temporal de la identidad de los sujetos [4].

Durante la última década, se han presentado mecanismos para proporcionar certificación espacio-temporal que respetan en mayor o menor grado la privacidad. Zugenmaier, Kreutzer y Kabatnik proponen un modelo y un mecanismo para generar certificados espacio-temporales sobre subscriptores de la red de telefonía móvil GSM [5]. Los certificados son generados por una entidad confiable que asocia los atributos espacio-temporales con el subscriptor mediante su firma digital; la privacidad de los subscriptores se preserva con unas sencillas listas de autorizados y no autorizados (*opt-in*/*opt-out*).

Por otro lado, Bussard define un tipo de certificado privado basado en protocolos de conocimiento nulo que aplica a la notarización espacio-temporal [6]. A pesar de que este tipo de certificados protegen en gran medida la privacidad de los sujetos (ya que permiten mostrar la información espacio-temporal certificada de forma anónima), tienen la desventaja de requerir del sujeto la realización de complejas operaciones criptográficas, muchas de ellas interactivas.

2.1. Modelo propuesto en CERTILOC

Dentro del proyecto CERTILOC se ha propuesto un modelo general para la provisión de servicios de certificación espacio-temporal que considera la participación de varias entidades, tal y como se muestra en la Figura 1 [7]. En primer lugar, una entidad *RQ* solicita al generador de evidencias espacio-temporales G_e la generación de una evidencia sobre determinado sujeto *S*. G_e solicita la localización de *S* de forma segura al verificador de la localización V_{loc}; al recibir ésta, G_e genera un certificado espacio-temporal que es transferido al receptor de la evidencia *RC* o almacenado para su posterior descarga por éste. Posteriormente una entidad usuaria del certificado *CL* lo presentará ante cierto receptor confiado *RL* para que le proporcione determinado beneficio. Este modelo es más general que los propuestos por Zugenmaier *et al.* y por Bussard, siendo válido para representar estas propuestas.

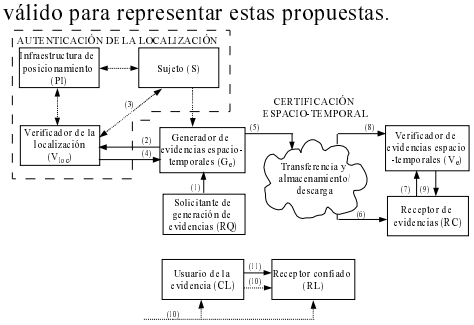

Figura 1. Modelo general para la provisión de servicios de certificación espacio-temporal

En CERTILOC se proponen dos formatos de certificado espacio-temporal basados en las especificaciones X.509 y SAML, los estándares de certificados de atributos más relevantes en la actualidad [7]. Estos formatos garantizan que se puede verificar la integridad de los certificados. Ninguna de las anteriores propuestas de Zugenmaier *et al.* y de Bussard especifica una estructura de certificado conforme a los mencionados estándares.

En CERTILOC la protección de la privacidad se aborda con un sistema de control de acceso basado en políticas [8]. Las políticas permiten a un usuario especificar los permisos, es decir, bajo qué condiciones autoriza la generación y la descarga de certificados espacio-temporales, así como la localización de los dispositivos de los que

el usuario es responsable, y asociar estos permisos a grupos personalizados de usuarios o roles-usuario. Un rol es una agrupación de usuarios (ejemplos de roles son 'empleado', 'compañero de trabajo', 'familiar', 'seguridad'…). Un rol-usuario es la asociación de un rol al usuario concreto al que el rol hace referencia ('amigo de…'). Los roles-usuario abstraen la finalidad con la que se utilizará la información espacio-temporal. Las políticas se definen en función de varios parámetros, los más importantes son el rol-usuario bajo el que el solicitante debe actuar, la acción solicitada y la información espacio-temporal del dispositivo (en el momento de la petición si se trata de localización o generación, o la reflejada en el certificado si se trata de descarga).

3. Análisis y diseño del demostrador de CERTILOC

El demostrador que implementa el modelo teórico de certificación espacio-temporal respetuoso con la privacidad propuesto en CERTILOC ofrece las siguientes funcionalidades generales:

1. Gestión básica de certificados espacio-temporales de dispositivos complementado con un servicio de localización en tiempo real.
2. Gestión de las preferencias de privacidad espacio-temporal por parte de los usuarios responsables de los dispositivos.
3. Administración de usuarios y dispositivos.

Adicionalmente, respecto a la seguridad y la privacidad, el sistema garantiza la confidencialidad de las comunicaciones realizadas con el sistema, el control de acceso a los servicios de forma complementaria al mecanismo de gestión de preferencias de privacidad basado en políticas, y el registro de acciones (*logs*) para posibilitar la exigencia de responsabilidades.

Respecto a la implementación, se ha exigido que el sistema interactúe con diferentes tecnologías de estimación de la posición. En particular, los dispositivos de CERTILOC pueden ser dispositivos móviles GSM, etiquetas RFID y asistentes personales (PDA) con receptor GPS. La inclusión de los PDA ha permitido adaptar el sistema a dispositivos de conectividad limitada.

Los usuarios de CERTILOC pueden acceder al sistema como clientes o administradores a través de una interfaz Web. Si un cliente es responsable de algún dispositivo podrá acceder a funcionalidades adicionales. Los dispositivos PDA ofrecen también algunas funcionalidades a través de su propia interfaz.

El entorno operacional del sistema se muestra en la Figura 2. Casi toda la funcionalidad se implanta en un servidor de aplicaciones Web excepto los módulos que se ejecutan en los PDA. CERTILOC interactuará con dos proveedores o servicios de información espacio-temporal (SIET) que le proporcionarán dicha información para los dispositivos contemplados y con un conjunto de PDAs que actuarán también como servicios de información espacio-temporal especiales gracias al módulo para PDA. Se asume que en caso de recibirse una petición a través de la interfaz web acerca de un PDA que implique la obtención de su localización, el sistema no puede contactar inmediatamente con el PDA para obtener dicha información. Por ello, este tipo de peticiones no se ejecutan en el mismo momento de la petición, sino de forma diferida. Son los propios PDA quienes se comunican de forma periódica con el sistema central para posibilitar la atención de las peticiones pendientes.

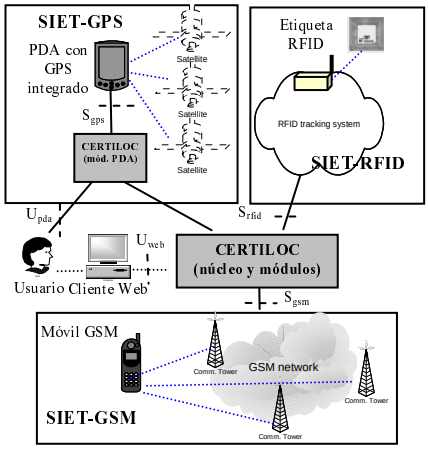

Figura 2. Entorno operacional de CERTILOC

3.1. Análisis

Las funcionalidades del sistema se representan en el diagrama de casos de uso de la Figura 3. Las funcionalidades se describen a continuación:

- **Localizar dispositivo**: el sistema solicita la información espacio-temporal de un dispositivo al proveedor correspondiente en el instante de la petición y se muestra dicha información al usuario. En el caso de que se solicite la localización de un dispositivo de conectividad limitada (e.g., un PDA) se comunicará al usuario un localizador que le permita reasumir la petición posteriormente. El usuario del PDA también puede acceder a la funcionalidad de localización de su propio dispositivo a través del interfaz del PDA.
- **Generar certificado**: el sistema genera y almacena certificados espacio-temporales (CET) acerca de dispositivos tras obtener su información espacio-temporal. Al igual que en el caso anterior, para dispositivos de conectividad limitada, se entregará al usuario un localizador. La funcionalidad de generar certificados también está accesible desde la interfaz del PDA para certificados acerca de sí mismo. Los PDA generan certificados espacio-temporales auto-firmados para todas las solicitudes (PDA e interfaz web). Este certificado previo generado por el PDA será posteriormente encapsulado en un certificado final por el sistema central.

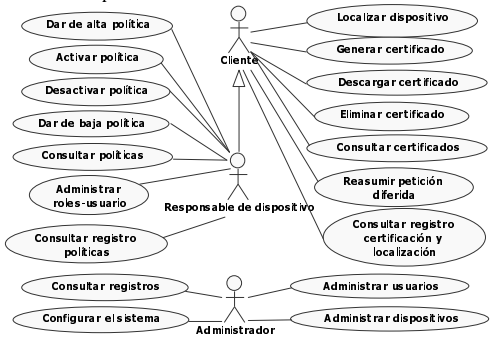

Figura 3. Diagrama de casos de uso de CERTILOC

- **Descargar certificado**: el sistema permite a los usuarios descargar certificados almacenados en el servidor.
- **Eliminar certificado**: el sistema permite a los usuarios eliminar del almacén de certificados uno determinado.
- **Consultar certificado**: el sistema devuelve por pantalla el contenido de un certificado.
- **Reasumir petición diferida**: el usuario puede reasumir una petición previa de localización o generación de certificado acerca de un dispositivo con conectividad limitada (e.g, PDA) proporcionando el localizador que se le entregó en la petición inicial al sistema.
- **Dar de alta una política**: el sistema permite a los usuarios almacenar en el servidor ficheros conteniendo sus preferencias de privacidad relativas a la información espacio-temporal de los dispositivos de los que el usuario es responsable.
- **Activar política**: el sistema permite que el usuario active políticas que hayan sido previamente dadas de alta en el sistema. La activación de una política tiene como consecuencia que las preferencias establecidas en ésta se comiencen a aplicar.
- **Desactivar política**: el sistema permite que el usuario desactive políticas activas.
- **Dar de baja política**: el sistema permite que el usuario dé de baja políticas no activas, eliminándose la política del servidor.
- **Consultar políticas**: el usuario puede seleccionar una de sus políticas dadas de alta en el sistema para que el sistema muestre sus contenidos por pantalla y su actividad.
- **Administrar usuarios**: el sistema permite que el administrador dé de alta o registre usuarios en el sistema, modifique los datos recogidos y dé de baja usuarios ya registrados. Los datos básicos que recoge el sistema para cada usuario son su identificador formal, su tipo (cliente o administrador), un identificador alternativo, su correo electrónico e información para su autenticación (como pueden ser certificado X.509 y/o autenticador).
- **Administrar dispositivos**: el sistema permite que el administrador dé de alta dispositivos en el sistema, modifique sus datos y finalmente los dé de baja. Además del identificador del dispositivo, se debe especificar cuál es su usuario responsable.
- **Administrar roles-usuario**: el sistema permite que los usuarios asocien los roles-usuario de su propiedad a otros usuarios, es decir, el usuario propietario de un rol-usuario tendrá potestad para gestionar las altas y bajas de otros usuarios en sus roles-usuario. Así mismo, los usuarios pueden consultar los roles-usuario de su propiedad.

- **Consultar registros**: CERTILOC pone a disposición de los usuarios administrador el registro de las actividades realizadas por los usuarios en el sistema.
- **Configurar sistema**: CERTILOC permite al administrador configurar parámetros básicos del núcleo del sistema (tiempo máximo de expiración de certificados, almacén de certificados a utilizar, clave con la que se firman los CET...). Así mismo, el usuario del PDA podrá configurar algunos parámetros, como el intervalo temporal para la conexión periódica con sistema central.

El modelo conceptual de datos utilizado en CERTILOC y que se utilizará como base para realizar el diseño se muestra en la Figura 4.

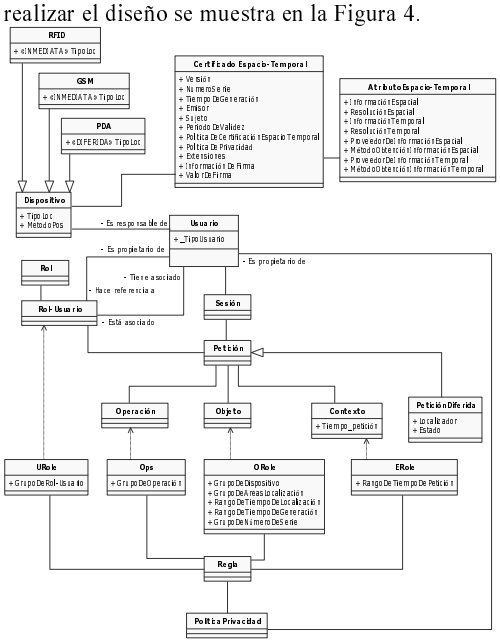

Figura 4. Modelo conceptual básico de CERTILOC

Los usuarios de CERTILOC tendrán asociado un tipo específico (cliente o administrador). Los clientes pueden tener asociado un conjunto de dispositivos de los que sean responsables. Cada cliente es propietario de un conjunto de roles-usuario basados en los roles establecidos en el sistema. Los clientes pueden asociar a sus roles-usuario otros clientes con el fin de gestionar sus propias preferencias de privacidad.

Los dispositivos localizables en CERTILOC se dividen fundamentalmente en dos clases: los que pueden localizarse en cualquier momento (cuyas peticiones de localización se resuelven de forma inmediata) y aquellos de conectividad limitada o esporádica (cuyas peticiones se resolverán de forma diferida).

El certificado espacio-temporal es el documento con el que se asocia la información espacio-temporal (contenida en el atributo espacio-temporal), con un sujeto determinado (un dispositivo). El certificado está firmado digitalmente por el sistema.

Los usuarios interactúan con el núcleo de CERTILOC por medio de sesiones, enmarcándose en estas sesiones las peticiones que realicen. Generalmente, una petición consiste en una operación que se llevará a cabo sobre un determinado objeto y bajo determinado contexto. La operación es la finalidad pretendida por la petición realizada, como puede ser la localización de un dispositivo. El contexto es el tiempo en el que se realiza la petición (fecha y hora). Los objetos hacen referencia a la entidad sobre la que se realiza la operación. Algunas peticiones consideran, además, el rol-usuario bajo el que el usuario actúa. Esta información permite comprobar los permisos asignados a este rol-usuario en las políticas de privacidad.

Las políticas de privacidad están compuestas por un conjunto de reglas. Cada regla especifica las condiciones bajo las que el usuario otorga su autorización definiendo un conjunto de roles-usuario (URole), un grupo de operaciones (Ops), un conjunto de objetos (ORole) que, en CERTILOC, se determinan en base a la información espacio-temporal o la contenida en los certificados espacio-temporales, y un rango de condiciones de contexto (ERole).

3.2. Diseño

En CERTILOC se obliga a que todas las peticiones de los usuarios tengan lugar dentro de una sesión válida. Por tanto, lo primero que debe hacer un usuario para acceder a los servicios del sistema es iniciar una sesión (véase la Figura 5). Las sesiones de aplicación se basan en sesiones SSL con autenticación del servidor ante el cliente para asegurar la confidencialidad de las comunicaciones. Para que un usuario pueda iniciar una sesión debe también autenticarse ante el sistema. La autenticación de los usuarios se

llevará a cabo empleando distintos mecanismos que difieren en los elementos que utilizados como base para la autenticación: contraseñas y certificados X.509 de usuario. El empleo de contraseñas determina la necesidad de generar un *token* de autenticación de sesión que debe presentar el usuario ante el sistema en cada interacción que realice con éste. La utilización de certificados X.509 para el servidor y los usuarios provoca que sea necesario contar con una PKI auxiliar plenamente operativa.

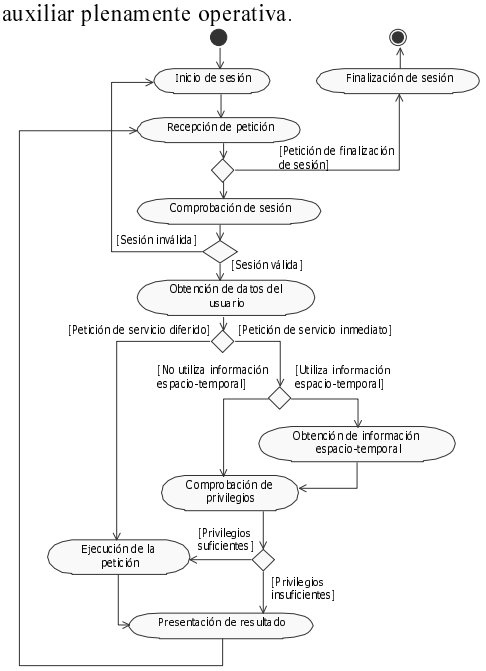

Figura 5. Funcionamiento simplificado de CERTILOC

Cuando el sistema recibe una petición de un servicio concreto, antes de pasar a atenderlo, comprueba que se ha realizado en el contexto de una sesión válida (usuario autenticado y sesión no caducada). Si la sesión es válida, el sistema primero obtiene del usuario la información necesaria para atender la petición. A partir de aquí el sistema se comportará de forma diferente según los siguientes casos:

1. Si se trata de una petición que puede atenderse de forma inmediata y que implica de alguna manera la utilización de información espacio-temporal (localización y operaciones con certificados), se obtiene dicha información, bien contactando con el proveedor de información espacio-temporal, bien recuperando dicha información de los certificados almacenados. A continuación, se comprueban los privilegios, y si estos son suficientes se ejecuta la petición. En cualquier caso se muestra al usuario el resultado.
2. Si la petición no implica el tratamiento de información espacio-temporal, se puede atender inmediatamente. Se ejecuta la petición si el usuario tiene suficientes privilegios. El sistema muestra al usuario el resultado.
3. Si la petición hace referencia a un servicio que se debe atender de forma diferida, el sistema proporcionará al usuario un localizador para que pueda reasumirse la ejecución de la petición más adelante.

Comprobación de privilegios. Cuando un usuario solicita la realización de un servicio, el sistema debe comprobar si éste tiene los privilegios básicos necesarios para llevarlo a cabo. La comprobación básica según unas políticas de control de acceso se realiza en base al tipo del usuario solicitante (administrador o cliente) y a la relación del usuario con el objeto sobre el que se solicita el servicio. Esta comprobación básica puede obtener un resultado positivo, negativo o indeterminado. Este último resultado puede darse si el servicio solicitado es localizar un dispositivo ajeno al usuario solicitante o generar/descargar un certificado que haga referencia a un dispositivo ajeno al usuario solicitante. En este último caso se recurre a las políticas de privacidad para comprobar los privilegios. Para ello se considera, además de la operación, el objeto y el contexto de la petición, el rol-usuario bajo el que el usuario desea actuar. El sistema comprueba entonces si el usuario tiene suficientes privilegios para realizar el servicio utilizando las políticas de privacidad establecidas por el usuario responsable del dispositivo al que la operación hace referencia. Para ello se recorren todas las reglas de las políticas definidas por el usuario propietario del dispositivo. Si se encuentra una regla que autorice peticiones con los parámetros de la petición actual, ésta se autorizará; si no, ésta será denegada.

Estructuras de datos basadas en XML. En CERTILOC se han representado mediante estructuras XML los certificados espacio-temporales y las políticas de privacidad espacio-temporal. En particular, el formato de los certificados se ha desarrollado ampliando el

estándar SAML [9]. SAML es un marco XML que estandariza el proceso de creación de aserciones acerca de la identidad, atributos y derechos de un sujeto y que especifica cómo transmitir esta información a otras entidades. En nuestro caso, el atributo que se crea dentro de la aserción contiene la información-espacio temporal del dispositivo y se especifica utilizando GML [10], un estándar de representación de información geográfica también basado en XML.

Las políticas de privacidad espacio-temporal utilizadas en CERTILOC se especifican según el estándar XACML [11]. Dicho estándar especifica una manera concreta de implementar sistemas de control de acceso utilizando el lenguaje XML. Los usuarios responsables de algún dispositivo que deseen dar de alta políticas, deben especificar las políticas y las reglas siguiendo el formato XACML. Cuando el sistema reciba una política en este formato, extraerá la información y la pasará a un sistema de gestión de datos para facilitar su manejo.

Funcionamiento en el caso de dispositivos de conectividad limitada. La relación existente entre el sistema central y los PDA podría modelarse en términos de cliente-servidor, pues se trataría de una comunicación típica en la que el sistema central enviaría peticiones de información de localización al PDA. Sin embargo, los PDA disponen de recursos computacionales, autonomía y conectividad limitados. Esto impide la implementación de un servidor tradicional en el PDA y motiva la aparición de un protocolo entre ambos comunicantes en el que el PDA establece una serie de conexiones periódicas con el núcleo. El módulo para PDA registrará con determinada frecuencia su propia información espacio-temporal (obtenida mediante un receptor GPS). Durante la ejecución del protocolo entre el PDA y el núcleo, éste enviará al PDA todas las peticiones de localización pendientes de resolución y recibirá como respuesta (por cada petición) un certificado preliminar sobre la información espacio-temporal del dispositivo. Dado que las peticiones estarán referidas a momentos anteriores, la información de localización corresponderá al momento registrado en el PDA más cercano al de la petición. De igual manera, el PDA aprovechará la comunicación con el núcleo para enviar certificados preliminares realizados por iniciativa del usuario que tiene el PDA bajo su control. En el sistema los certificados preliminares serán almacenados temporalmente hasta que el usuario reasuma la ejecución de la petición.

Diseño de la arquitectura según patrón MVC. El diseño del sistema se ha llevado a cabo según criterios ampliamente aceptados por la industria. En concreto, se sigue el patrón comúnmente conocido como MVC modelo 2 (MVC2), es decir, MVC adaptado a aplicaciones Web. En este modelo se definen tres entidades:

- (M)Modelo: Contiene la lógica de negocio, es decir la implementación de la funcionalidad del sistema. Normalmente es también el encargado de intercambiar información con unidades de almacenamiento persistentes como bases de datos. En CERTILOC el modelo está íntegramente realizado en Java.
- (V)Vista: Es el responsable de la presentación de información (generada por el modelo) al usuario. En CERTILOC la vista está compuesta por páginas JSP.
- (C)Controlador: los controladores son los encargados, por un lado, de gestionar los eventos del sistema (típicamente peticiones del usuario) y enviarlas al modelo; y, por otro lado, de preparar la información proveniente del modelo para poder ser representada por la Vista.

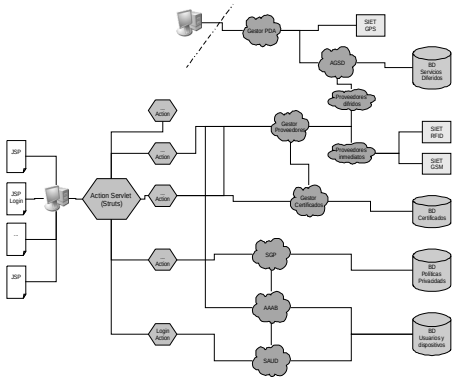

Figura 6. Arquitectura de CERTILOC

En CERTILOC se utiliza el marco Struts para implementar el patrón MVC. Struts está diseñado para ayudar en la construcción de aplicaciones Web complejas siguiendo el patrón MVC. Struts actúa como un puente entre el modelo de la aplicación y la vista, añadiendo entre otras las

siguientes características: configuración centralizada, validación declarativa (contiene rutinas que permite validación automática de los formularios Web), manejo global de excepciones, soporte para la internacionalización de la aplicación, etc. En la Figura 6, se muestra la arquitectura de CERTILOC.

4. Conclusiones y líneas futuras de trabajo

El desarrollo de los LBS para el público general en los últimos tiempos ha provocado que se haya incrementado el interés por idear y construir mecanismos de seguridad apropiados para estos servicios. En este artículo se aborda el análisis y el diseño de uno de los mecanismos mencionados, un servicio de certificación espacio-temporal respetuoso con la privacidad de los usuarios, estando en curso su implementación. Aunque el sistema que se presenta es muy completo, la implementación de algunas funcionalidades y características se ha pospuesto para las siguientes versiones.

Uno de los aspectos pospuestos es considerar sujetos duales, esto es, que los certificados no se emitan sólo para dispositivos, sino que también se considere al usuario que esté controlando éste. Por otro lado, los certificados se deben ampliar para que incluyan información sobre las condiciones de utilización establecidas por el usuario al que hacen referencia y se deben integrar mecanismos que permitan al usuario regular la granularidad de la información espacio-temporal que se incluye en el certificado.

El modelo de gestión de la privacidad que se implementa en esta versión del demostrador es una simplificación de un modelo más completo actualmente en desarrollo. En versiones posteriores, se deberá ampliar las funcionalidades del sistema para adecuarse al modelo completo. Así mismo, es recomendable que en un futuro se desarrolle un módulo que permita al usuario especificar las políticas de privacidad a través de la interfaz Web de forma fácil, en lugar de requerirse que el usuario dé de alta políticas con formato XACML.

Por último, dadas las implicaciones legales que podrían tener los certificados espacio-temporales, se deberá investigar cuál podría ser el marco legal por el que el usuario responsable/portador del dispositivo asumiría las consecuencias de su utilización salvo denuncia de sustracción.

Referencias

[1] Patterson, C.A.; Muntz, R.R. & Pancake, C.M. (2003), 'Challenges in Location-Aware Computing', *IEEE PervasiveComputing* **2**(2).

[2] González-Tablas Ferreres, A.I. (2005), 'Arquitectura y mecanismos para la provisión de servicios de acreditación y sellado espacio-temporal', PhD thesis, Universidad Carlos III de Madrid.

[3] 'Directiva 2002/58/CE', *Diario Oficial n° L 201 de 31/07/2002*, pp. 0037 - 0047.

[4] Görlach, A.; Terpstra, W.W. & Heinemann, A. (2005), 'Survey on Location Privacy in Pervasive Computing', *in Proc. of the Workshop on Privacy, Security and Trust within the Context of Pervasive Computing*.

[5] Zugenmaier, A.; Kreutzer, M. & Kabatnik, M. (2001), 'Enhancing Applications with Approved Location Stamps', *in Proc. of IEEE Intelligent Network Workshop*.

[6] Bussard, L. (2004), 'Trust Establishment Protocols for Communicating Devices', PhD thesis, Institut Eurécom, Télécom Paris.

[7] González-Tablas, A.G.; Ramos, B. & Ribagorda, A. (2007), 'Spatial-Temporal Certification Framework and Extension of X.509 Attribute Certificate Framework and SAML Standard to Support Spatial-Temporal Certificates', *in EuroPKI 2007*.

[8] Ramos, B.; González-Tablas, A.I. & Ribagorda, A. 'Legislación, ética y seguridad para la preservación de la privacidad de la información espacio-temporal', *in CISTI 06*.

[9] OASIS. 'Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) Version 2.0. OASIS Standard, 2005

[10] OGC (Open Geospatial Consortium Inc.). 'OGC 03-105r1: OpenGIS Geography Markup Language (GML) Implementation Specification', February 2004.

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