Servicios avanzados de seguridad para un sistema de emergencias

Helena Rifà Pous[1], Francisco Jordán Fernández[1], Javier Espinosa García[1], and Luis Javier García Villalba[2]

[1] Safelayer Secure Communications, S.A., Ed. World Trade Center (S-4), Moll de Barcelona s/n, 08039 Barcelona, Spain {hrifa,jordan,jespinosa}@safelayer.com
[2] Universidad Complutense de Madrid, Facultad de Informática, Dep. Sistemas Informáticos y Programación, Juan del Rosal 8, 28040 Madrid, Spain {javiergv}@sip.ucm.es

Resumen La recuperación de un desastre requiere la coordinación e interacción oportuna de todos los servicios de emergencias para poder hacer una valoración conjunta de los datos obtenidos y elaborar una respuesta rápida y efectiva.
En el presente trabajo se propone un sistema que permite el acceso, manipulación y transferencia de información sensible y urgente entre el personal de los organismos implicados. Los privilegios sobre los recursos están regulados mediante políticas de seguridad que permiten definir el comportamiento del servicio en función de la sesión o contexto temporal del solicitante. La arquitectura propuesta está basada en tecnología de redes ad hoc para el campo de operaciones, y una plataforma orientada a servicios en las sedes corporativas.

Palabras clave: redes ad hoc, emergencias, servicios web, seguridad.

1. Introducción

Una gestión eficaz de las emergencias y desastres es fundamental para asegurar la rápida recuperación de una crisis y evitar daños mayores. Una buena gestión implica que las organizaciones implicadas actúen de forma eficiente y coordinada intercambiándose los datos relevantes de forma segura y en tiempo real. Sin embargo, en una región en guerra, en una zona en situación catastrófica, en situaciones de rescate, ..., en general, cuando se tiene que dar respuesta a una emergencia, la principal carencia técnica es que no existe una infraestructura de red operativa en la zona del conflicto.

Las redes ad hoc móviles (MANET) son redes que no precisan de infraestructura, están formadas por dispositivos heterogéneos y tienen una topología dinámica. Son por lo tanto redes muy flexibles y adecuadas para zonas de emergencia donde la comunicación es un factor crítico.

Por otro lado, es necesario que la red de comunicaciones permita establecer un flujo de información entre el personal que está en la zona de operaciones y el

localizado en las sedes centrales de los organismos participantes. Estas conexiones se pueden establecer mediante enlaces radio o vía satélite.

Finalmente, el flujo de información de los servicios tiene que poder ser tanto horizontal (i.e. entre entidades) como vertical (i.e. entre los diferentes niveles jerárquicos de una organización) con propagación *push* y *pull*. Las entidades involucradas en solventar la situación tienen que interactuar estrechamente en varios niveles, unificando la información, almacenándola, procesando los datos en contexto y transformándolos en informes e instrucciones. La tecnología que mejor se adapta a estos requisitos son las arquitecturas orientadas a servicios (SOA), especialmente diseñadas para facilitar los procesos de integración y automatización.

Las arquitecturas SOA, generalmente implementadas sobre servicios web, proporcionan la flexibilidad, modularización y reutilización necesarias para acoplarse a los entornos de diferentes organismos que usan aplicaciones diversas para gestionar su trabajo. El acceso a los servicios se estandariza mediante un lenguaje común, basado en XML, que se utiliza para definir la localización, interfaz, funcionalidad, formatos, reglas, etc. que caracterizan el servicio sin entrar en detalles de implementación, esto es, cómo está desarrollado dicho servicio en los sistemas. La abstracción de la implementación del servicio es fundamental, y es la base de la integración.

En el presente trabajo presentamos un sistema de emergencias que combina las propiedades de disponibilidad en cualquier hora y cualquier lugar de una red ad hoc para monitorizar y actuar sobre una zona en conflicto, y los beneficios de integración y control de una arquitectura SOA para controlar, gestionar y coordinar una respuesta a la situación. El sistema ofrece servicios de seguridad multidominio y multinivel en entornos tácticos.

El resto del artículo está organizado de la siguiente manera. La sección 2 describe la plataforma de servicios web sobre la que se construye el sistema de emergencias. En la sección 3 se presenta la arquitectura del sistema. La sección 4 describe un caso de estudio y la solución propuesta. Finalmente, en la sección 5 se exponen las conclusiones.

2. Plataforma de servicios web

La plataforma de servicios web [3] que hemos implementado y sobre la que se desarrolla el análisis del artículo ofrece servicios de seguridad basados en infraestructuras de clave pública a través de la tecnología de servicios web (WS). Las tecnologías WS ofrecen una interfaz uniforme para acceder a los sistemas informáticos actuales a través de protocolos basados en XML. La plataforma utiliza los estándares de infraestructura SOAP -especifica un marco para la composición de mensajes de petición/respuesta a un servicio-, WSDL -permite disponer de una definición abstracta del servicio independiente del lenguaje de programación que se utilice para su implementación-, y UDDI -especifica el acceso a los registros de descripción, descubrimiento e integración de WS universales-.

[3] Omitido el nombre por revisión anónima

Los servicios que ofrece el sistema están diseñados para reducir los riesgos de seguridad asociados a los procesos de negocio que se realizan sobre medios electrónicos. Los servicios están basados en una PKI y en concreto pueden proveer las siguientes funcionalidades:

- *Firma Electrónica*. Permite la verificación y generación de firmas electrónicas. Se reconocen diferentes prestadores de certificación y se permite generar y custodiar las evidencias electrónicas que permitan la verificación de firmas a lo largo del tiempo.
- *Protección de datos*. Permite la protección de datos y su custodia, garantizando el mantenimiento y el acceso a éstos por las entidades autorizadas a lo largo del tiempo.
- *Gestión de claves*. Registro, revocación, consulta y verificación de las claves de las entidades.
- *Autenticación, Autorización y control de acceso*. Permite la autenticación, autorización y control del acceso de las entidades registradas haciendo posible el Single Sign-On (SSO) y federación en toda la plataforma (entre usuarios, Servicios Web y aplicaciones).
- *Gestión de objetos y entidades*. Proporciona un modelo de información uniforme basado en XML para todos los objetos y entidades de la plataforma, enmascarando totalmente formatos (XML, ASN.1, Tablas,...), fuentes de información (SQL, LDAP, ficheros,...), localizaciones (intranet, extranet, WAN,...), etc. Se ofrecen así funciones de registro, consulta y modificación de la información sobre entidades, en particular, información de identidad, configuración y auditoría.
- *Auditoría y Accounting*. Gestiona de forma centralizada y uniforme toda la información de traza (log) de todos los componentes de servicio de la plataforma así como la información de uso y/o consumo de los servicios. Mediante el acceso controlado a toda la información de actividad se pueden generar todo tipo de informes. Dichos servicios, a su vez, requieren los servicios avanzados de una o varias PKI que incluyan los servicios de sellado de tiempo y de verificación de los certificados digitales.

El acceso a los servicios de seguridad se realiza mediante protocolos estándares de WS: DSS [1] (firma digital), WSS [2] (integridad y confidencialidad de mensajes), SAML [3] (Single-Sign On), XACML [4] (autorización), Liberty ID-WSF [5] (federación), WS-Trust [6] (control de acceso) y XKMS [7] (gestión de claves). De esta forma se garantiza una infraestructura independiente de la tecnología empleada e interoperable con todos los productos del mercado que utilizan dichos estándares.

La plataforma de servicios de seguridad está formada por un conjunto de componentes que cubren la funcionalidad descrita anteriormente. Los componentes de servicio son los siguientes:

- *TWS-AA*. Servicio de autenticación y autorización con mecanismos de autenticación mediante nombre de usuario/contraseña, certificado digital (TLS/SSL), mecanismos WSS basados en firma digital, y mecanismos adicionales soportados a través de agentes especializados.

- *TWS-EP*. Servicio de gestión de información que uniformiza perfiles de objetos y/o entidades: usuarios, aplicaciones, servicios web, políticas, certificados, logs/auditoria, etc.
- *TWS-DS*. Servicio de firma electrónica de documentos que permite generar firmas básicas en los diferentes formatos reconocidos (PKCS7, CMS, PDF, XMLDsig/XAdES y S/MIME).
- *TWS-DR*. Servicio de firma electrónica avanzada que amplía con información de tiempo y revocación fiables documentos ya firmados, como base de firmas longevas.
- *TWS-DSV*. Servicio de verificación de firmas electrónicas (incluidas firmas avanzadas o longevas) independiente del prestador, del mecanismo de verificación de certificados y del formato de firma.
- *TWS-DE*. Servicio de cifrado y descifrado de documentos en formatos PKCS7, CMS y XMLEnc.
- *TWS-DEC*. Servicio de custodia de claves de cifrado de documentos garantizando su acceso a lo largo del tiempo.
- *TWS-DSC*. Servicio de custodia de firmas electrónicas de documentos que permite mantener su validez a lo largo del tiempo, implementando así firmas electrónicas longevas.
- *TWS-KM*. Servicio de gestión de claves para la generación, registro, consulta, verificación, etc.

2.1. Federación

Una de las características destacadas de la plataforma de servicios web propuesta es que ofrece servicios de federación, tanto a nivel de identidad como de confianza.

Los esquemas de federación de identidades permiten descentralizar la gestión de usuarios y se convierten en una solución para realzar la protección de los datos sensibles y administrarlos de forma única en el lugar más apropiado. Puesto que la federación de la identidad proporciona un mecanismo para intercambiar información sensible de un usuario a los proveedores de servicios situados en diversos dominios de seguridad, los usuarios pueden obtener de forma ubicua servicios destinados a ellos sin tener que volver a acreditar explícitamente su identidad, y los administradores de la información de identidad pueden controlar el acceso a la misma según el contexto de sesión del solicitante y la política de protección de los datos.

La primera propuesta de un esquema de federación de identidades global para servicios web fue diseñada por el grupo Liberty Alliace [5]. El objetivo principal era ofrecer servicios de Single-Sign On no solo dentro de una corporación o dominio, sino entre sitios web de diferentes dominios. La interfaz y la funcionalidad de los servicios de Liberty están basados en el estándar SAML [3], que se ha ampliado para soportar información del contexto de autenticación y la sesión del usuario. Por otro lado, también se han adoptado algunas ideas de Shibboleth en cuanto al acceso anónimo y auténtico a servicios web.

Otra de les especificaciones técnicas emergentes de gestión de identidades federadas distribuidas es la de WS-Federation, que se asienta sobre WS-Trust [6]. A diferencia de las otras propuestas, WS-Federation soporta delegación de autorizaciones a proveedores de diferentes dominios de seguridad, pero aún no permite una delegación de privilegios basada en el contexto de sesión.

La plataforma de servicios web presentada está basada y es compatible con los estándares de Liberty y WS-Trust, y extiende los objetos de federación a todos los perfiles consumidores de la plataforma (usuarios, aplicaciones y servicios).

Los esquemas de federación de confianza permiten definir vínculos de confianza entre diferentes sistemas gestionados bajo dominios y políticas diferentes. Los modelos de gestión y distribución de claves más prácticos y populares, y sobre los cuales está basada la plataforma de servicios web, son los basados en tecnología de PKI. El desarrollo de la confianza en esquemas de PKI se ha desarrollado típicamente en una estructura jerárquica dominada por una autoridad raíz. Debido a la inexistencia de una autoridad raíz global, el modelo ha derivado en agrupaciones aisladas e inconexas de confianza.

Un esquema de federación define las reglas de confianza entre los proveedores. Estas reglas, que se expresan en lenguaje XML, permiten determinar con un alto grado de granularidad la confianza depositada en las entidades externas para ofrecer diferentes servicios. Los servicios de confianza son accesibles para su composición, orquestación y consumo como otros servicios de negocio cualesquiera en el esquema SOA. El proveedor de servicios de confianza facilita al resto de componentes de negocio un servicio especializado de seguridad que estos podrán consumir, por ejemplo:

- Autenticación, Autorización y Control de Acceso unificado
- Federación de Identidad
- Federación de otro tipo de información acerca de entidades
- Gestión de claves criptográficas, sesiones seguras, single sign-on, etc.
- Generación y validación de firmas digitales
- Protección de la información
- Notarización de la información para su no-repudio

Uno de los principales valores aportados por un proveedor de servicios de confianza es el de uniformizar la gestión del dominio de confianza, esto es, la aplicación de las políticas de seguridad en un sistema.

2.2. Políticas

La gestión de la seguridad en la plataforma de servicios web propuesta está basada en políticas. Las políticas de seguridad son la solución más sencilla para gestionar de forma íntegra y flexible la creciente complejidad de los servicios de seguridad y confianza. Además, la reciente tendencia de separar la especificación de la política de la implementación del sistema permite la gestión dinámica de éstas para poder adaptarse a los cambios de estrategia del sistema.

La plataforma de servicios tiene tres tipos de políticas de seguridad: las de autenticación, las de autorización y las de servicio. Las dos primera constituyen

el modelo de control de acceso. Las políticas de servicio definen las acciones de la plataforma delante de una solicitud de servicio de seguridad, como generación de firma digital o verificación. En el caso de una verificación de firma, las políticas de servicio definen el marco de confianza con los proveedores de seguridad externos, el formato que debe tener la firma digital, el tipo de información que se debe devolver en la respuesta, etc..

Los modelos de control de acceso han ido evolucionando a lo largo de los años. El control de acceso basado en roles (RBAC) fue presentado por Sandhu en 1997 [8] y supuso una mejora sustancial en la gestión de la seguridad. En él se proponía que los permisos de acceso se asociaran a roles en lugar de a usuarios. A partir de aquí han surgido modelos más complejos basados en la misma idea de los roles: Temporal-RBAC [9], que introduce el tiempo en el control de acceso, [10] introduce condiciones de localización y estado del sistema, y GRBAC [11] que incorpora roles de sujeto, objeto y entorno en las decisiones de control de acceso. En [12] McDaniel clasifica las propiedades de seguridad de un contexto que pueden ser evaluadas en una política de autorización. Como en este último caso, el control de acceso a la plataforma de servicios de seguridad propuesta está basado en un contexto abierto, y las condiciones de acceso pueden ser descritas dinámicamente en tiempo de ejecución.

Un control de acceso basado en políticas está formado básicamente por dos módulos: el módulo de evaluación de la política (Policy Decision Point - PDP) y el módulo que hace cumplir la política (Policy Enforcement Poing - PEP). En nuestra plataforma el PDP está situado en el componente de servicio TWS-EP, y el PEP está replicado en cada uno de los componentes de servicio final. Los dos módulos, PDP y PEP, no necesitan estar forzosamente en el mismo servidor ya que la comunicación entre ellos es confidencial e íntegra.

Una infraestructura de políticas evalúa una política cuando se produce una solicitud de acción. La condiciones son evaluadas extrayendo el estado (posiblemente a través de una función parametrizada) de un fuente local o remota de información del usuario y el contexto. Este estado es interpretado o transformado por la infraestructura de políticas para llegar a un resultado de la condición. Las condiciones son funciones usadas para mesurar un contexto. Cada condición es una función de cero o más argumentos. Cada parámetro es un valor estático o variable (i.e. identificado por la infraestructura de políticas en tiempo de ejecución) y asumimos que retorna un valor booleano.

A continuación se listan los parámetros de las condiciones de las políticas de control de acceso: autenticación y autorización. La figura 1 muestra un ejemplo en XML de una política de autorización.

- Mecanismo de autenticación
- Dirección IP
- Roles
- Horario

Los roles de las entidades solicitantes de los servicios son asignados dinámicamente durante el proceso de autenticación. Los parámetros condicionantes para obtener un rol son los siguientes:

```
<AuthorizationRule active="true" name="urn:safe:tws:names:rules:ds:1">
    <Description>Autorización de la generación de firmas CMS/PKCS#7</Description>
    <Resource name="urn:safe:tws:resources:ds"/>
    <Actions>
        <Action name="urn:safe:tws:dss:1.0:profiles:cmspkcs7sig:1.0:sign"/>
    </Actions>
    <Allow>
        <Group dname="CN=Notario, O=Urgell, C=ES"/>
    </Allow>
    <AuthorizationConditions>
        <AuthenticationLevel>1</AuthenticationLevel>
        <TimePeriods>
            <TimePeriod>
                <DayRange from="Mo" to="Fr"/>
                <HourRange from="08:00:00" to="20:00:00"/>
            </TimePeriod>
        </TimePeriods>
        <NetFilters>
            <NetFilter>127.0.0.1</NetFilter>
            <NetFilter>192.168.55.0 - 192.168.55.255</NetFilter>
        </NetFilters>
    </AuthorizationConditions>
    <AuthorizationResults>
        <ActionPolicies>
            <ActionPolicy name="urn:safe:tws:aa:policies:generation:1"/>
        </ActionPolicies>
    </AuthorizationResults>
</AuthorizationRule>
```

Figura 1. Regla de autorización

- Mecanismo de autenticación y credenciales aportadas
- Pertenencia a grupos
- Información suplementaria del perfil de usuario
- Información del contexto
- Horario

Si el PDP no puede obtener toda la información necesaria para dar una respuesta de autorización (por ejemplo porque no tiene la información del contexto necesaria) puede colaborar con otros servicios, a los que llamamos agentes, sobre los que puede delegar determinadas funciones de recolección y evaluación de credenciales.

Así pues, la plataforma no tiene un único PDP centralizado y hermético sino que puede distribuir esta función a diferentes agentes especializados que pueden

evaluar características particulares y necesarias para ciertas aplicaciones o servicios. Si los agentes además de conseguir las credenciales de autenticación de los usuarios solicitantes realizan la evaluación y autenticación de las mismas, hablamos de agentes autoritativos. En este caso, las entidades finales tiene que confiar en estos agentes, que se convierten en autoridades de confianza intermediarias.

3. Arquitectura del sistema

El objetivo del sistema de emergencias es coordinar y dar respuesta a una situación excepcional de forma rápida y segura. Para ello es necesario disponer de la tecnología adecuada para poder colectar información sobre la zona afectada, analizarla, definir los requisitos básicos para solventar la situación, y enviar la ayuda y soporte necesarios.

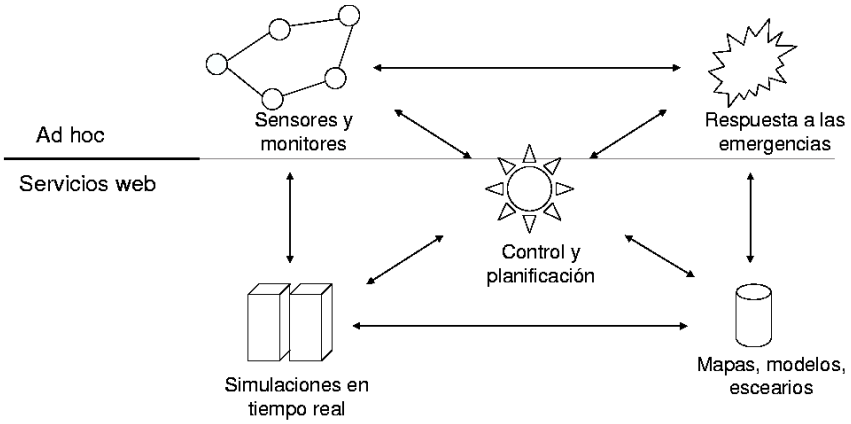

Figura 2. Flujo de datos en una situación de emergencias

La figura 2 muestra a alto nivel los componentes de un sistema de emergencias. Una red ad hoc da cobertura a la zona del conflicto y se encarga de dos funciones básicas: obtener información de la situación (a través de redes de sensores que monitorizan la zona o vía personas que envían informes de la situación con dispositivos móviles de mano) y transmitir las peticiones de asistencia a los cuerpos con las capacidades adecuadas. La red ad hoc por lo tanto, es el interfaz entre el mundo real donde hay la emergencia y el nivel estratégico y de coordinación.

Los servicios basados en tecnología web son necesarios para las funciones que requieren un entorno de comunicaciones rápido, acceso a información remota y máquinas apropiadas para procesos de cálculo. Desde un centro de planificación y control se tienen que gestionar las simulaciones en tiempo real, coordinadas

con los mapas, modelos y escenarios del lugar. El análisis de la situación requiere información de distintos sectores y las decisiones se tiene que tomar a diferentes niveles. La estructura jerárquica común en los modelos militares (adoptada por muchos sistemas de emergencias) está estructurada en un nivel estratégico, uno operacional, y uno táctico. Los agentes estratégicos realizan actividades de análisis y dirección, construyendo planificaciones con un de alto nivel del granularidad. Los agentes operacionales se encargan de las actividades de síntesis y control, refinando los planes producidos en el nivel superior a través de la programación temporal de sus recurosos y un adecuado balanceo de carga. Finalmente, los agentes tácticos están implicados en las tareas de ejecución.

En una situación de emergencia es fundamental tener un sistema de soporte de coalición multidominio y multinivel y por lo tanto, una tecnología que funcione de forma distribuida (grid o servicios web) es la más adecuada. El programa de investigación FireGrid [13] hace un estudio sobre la coordinación de agentes durante operaciones de rescate dentro de edificios. El proyecto es uno de los pioneros en estos sistemas e involucra a científicos, brigadas de bomberos, compañías aseguradoras, arquitectos, ingenieros, etc.. Está previsto que el despliegue sea sobre una red grid.

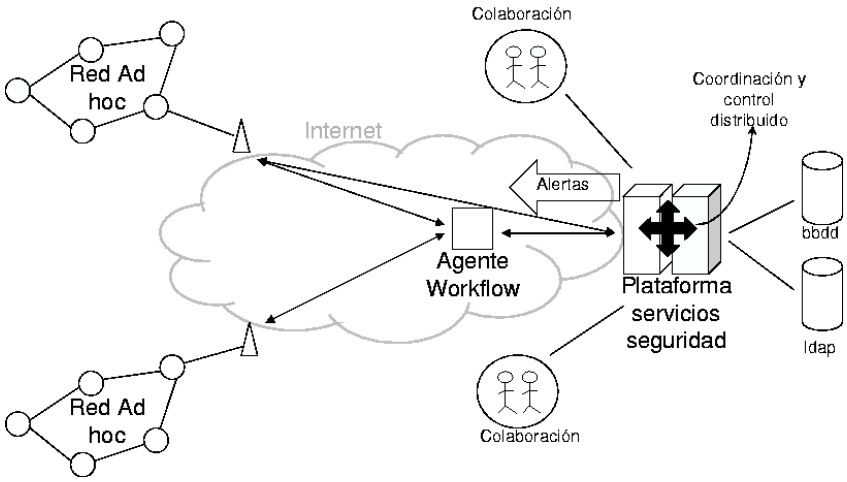

Figura 3. Arquitectura del sistema de emergencias

La figura 3 muestra la arquitectura del sistema. La red ad hoc está formada por terminales con tecnología IEEE 802.11 o IEEE 802.16, algunos de los cuales tienen conectividad a Internet u otras redes a través de GSM, UMTS o VSAT. El acceso a la plataforma de servicios de seguridad se realiza a través de un agente que controla todos los flujos de trabajo del sistema de emergencias.

A continuación se describe de forma más detallada cuales son las características de los dos módulos principales del sistema: la red ad hoc y la plataforma de servicios de web.

3.1. Redes Ad hoc

Una de las características principales de una red ad hoc es su funcionamiento multi-hop. En general, el campo de transmisión radio de un nodo no da cobertura a toda la red y, por lo tanto, la comunicación entre dos usuarios finales se tiene que realizar a través de una secuencia de nodos intermedios. La cooperación entre todos los nodos es esencial para poder formar una red funcional y para ello es necesario utilizar protocolos de encaminamiento (p.e. ARAN [14] o SAODV [15]) y transporte (p.e. SORI [16]) seguros que garanticen esta cooperación.

Los protocolos seguros de red asumen la existencia de un esquema de gestión de claves encargado de generar, distribuir, publicar y revocar, las claves usadas en la ejecución del protocolo. En un sistema de emergencias, las operaciones están gobernadas por convenciones internacionales y leyes y regulaciones nacionales. Las entidades y los perfiles de los participantes están predefinidos y no se admiten voluntarios civiles a menos que pertenezcan a una organización que que coopere en la operación. En un esquema de estas características, el esquema de gestión de claves más eficiente y seguro es el basado en un proveedor de confianza central.

El proveedor de confianza emite certificados para los miembros del grupo, que podrán autenticarse mútuamente. Además, también define una lista con las entidades federadas que son reconocidas y aceptadas para trabajar en el entorno ad hoc. El hecho de usar mecanismos de autenticación en los protocolos de red permite proteger a los usuarios de ataques externos y también hace la red más robusta delante de ataques internos, que son fácilmente detectables.

La red ad hoc está formada tanto por dispositivos de comunicación y soporte a funciones humanas (móviles, portátiles, agendas electrónicas, etc..), como por sensores de monitorización de las constantes de una región (sensores de temperatura, humo, movimiento..). La autenticación y el control de acceso sobre los primeros se hace no contra el dispositivo en sí mismo sino sobre la persona que lo usa. En cambio, en el caso de los sensores lo que se autentica es el dispositivo.

En general, la autenticación de clave pública no es adecuada para las redes de sensores debido a sus limitados recursos. La inicialización de estas redes con una clave simétrica predefinida tampoco es útil porque si un solo nodo de la red es comprometido, el adversario tiene acceso a todos los miembros. En estos casos proponemos un protocolo de pre-distribución de claves simétricas. Los protocolos de pre-distribución de claves permiten asignar a un sensor un subconjunto del conjunto total de claves simétricas de la red. La comunicación entre dos nodos se realiza con una de las claves simétricas que los dos tienen en común. El protocolo propuesto por Liu [17] utiliza el hecho que la mayoría de redes de sensores son estáticas. Cada sensor tiene una localización preestablecida y por lo tanto puede estar inicializado con un conjunto de claves de los que se supone serán sus vecinos.

3.2. Servicios web

El acceso a la plataforma de servicios de seguridad se puede hacer de forma directa, o a través de un agente de autenticación. En un sistema de emergencias es recomendable utilizar un agente por dos motivos:

- La definición de las políticas de autenticación puede adaptarse al contexto específico de trabajo ya que el agente tiene acceso al perfil del solicitante en el entorno de autenticación.
- En un sistema de emergencias interactúan muchos actores. Un agente que administre los flujos de trabajo del sistema (workflow) permite un mayor control de la emergencia.

La plataforma de servicios de web ha estado implementada sobre tecnología J2EE y soporta la administración a través del estándar JMX. A través de este protocolo se pueden programar las alarmas seguras necesarias para poner en estado de alerta a todos los organismos implicados en una emergencia en caso que ésta suceda.

Por otro lado, cabe destacar la gestión de logs que se realiza en la plataforma que permite obtener unas evidencias auditables de todos los actividades de los servicios web.

4. Caso de estudio

El caso de estudio sobre el que se desarrolla el sistema de emergencias presentado es el de unos Juegos Olímpicos (JJOO).

El comité organizador es el responsable de montar la infraestructura tecnológica para controlar y garantizar el buen funcionamiento de los eventos, pero cuenta con el soporte de organizaciones externas para resolver los pequeños conflictos eventuales, y sobretodo para combatir y superar situaciones excepcionales de riesgo, como ahora incendios, actos terroristas, accidentes civiles, evacuaciones, etc..

Suponemos un escenario formado por instalaciones deportivas, zonas de ocio y restauración, una villa olímpica, zonas de asistencia sanitaria, y edificios de seguimiento y control de las infraestructuras tecnológicas. Todas estas instalaciones están distribuidas dentro de un perímetro geográfico amplio y disconexo. El acceso físico a las zonas olímpicas requiere la autenticación mediante la verificación de datos biométricos (concretamente la huella dactilar) y una tarjeta RFID acreditativa. La tarjeta RFID contiene una clave privada y un certificado digital asociado generado por el proveedor de confianza de los JJOO.

Las tarjetas de acreditación a las instalaciones olímpicas son generadas por la organización olímpica a todos aquellos usuarios que se han registrado al evento para poder participar en él: espectadores, deportistas, personal de soporte técnico y logístico, periodistas, médicos y policías. Los certificados digitales les permiten acceder remotamente a la información relacionada con los eventos deportivos e incluso en algunos casos, y dependiendo del rol de cada usuario, modificar o

introducir informes del estado de desarrollo de determinadas operaciones en la zona de trabajo.

El personal acreditado por la organización olímpica es el único que puede acceder a las instalaciones en el transcurso normal de los eventos, pero en caso de producirse un incidente todos los cuerpos de seguridad y emergencia locales (o incluso nacionales e internacionales) tienen que unirse y coordinarse para establecer una solución común. La coordinación entre diversas organizaciones requiere procesos de federación que permitan que el personal designado a la misión pueda acceder de forma rápida y segura a la información necesaria para desarrollar sus funciones.

El cuadro 1 muestra un esquema de todos los grupos de usuarios, aplicaciones o servicios involucrados en unos JJOO y el proveedor de confianza que tienen asociado.

Grupos de usuarios	**Proveedor de confianza**
Espectadores	Organización JJOO
Deportistas	
Soporte	
Periodistas	
Sensores de monitorización	
Agentes de Autenticación	
Policía	Ministerio del Interior
Bomberos	
Militares	
Servicios médicos	Colegio de médicos

Cuadro 1. Grupos de usuarios

Se dispone de un sistema de directorio corporativo, accesible vía LDAP, con toda la información del personal interno. Del personal externo no se dispone de la información directa. Las relaciones de federación con las instituciones de soporte permiten crear grupos dinámicos formados por las personas que pertenecen a estas instituciones. El componente de autenticación y autorización de la plataforma de seguridad (TWS-AA) delega en un agente de autenticación la responsabilidad de recopilar los datos de federación para evaluar las condiciones de las reglas de control de acceso. En este caso, la función de PDP la realizan conjuntamente el agente y el TWS-AA.

Los JJOO tienen implantados tres mecanismos de autenticación:

1. Huella dactilar. La autenticación biométrica se utiliza para el acceso físico a las instalaciones de los JJOO.
2. Nombre de usuario y contraseña a través de ssl. Autenticación remota para el acceso a información de consulta.
3. Firma digital a través de los estándares WSS. Autenticación remota para el acceso a información sensible.

Las políticas de autorización definen los privilegios de los roles, que son asignados dinámicamente en el proceso de autenticación. La tabla 2 muestra un extracto de las políticas básicas de autorización.

Privilegio	**Rol**	**Condiciones**
Acceso a las instalaciones del los JJOO	Miembro acreditado	Acreditación del grupo organizador y autenticación física en el recinto
Información de los resultados deportivos	Miembro acreditado	Acreditación del grupo organizador
Publicación de resultados deportivos	Tribunal de los JJOO	Acreditación del grupo organizador, pertenencia al grupo de tribunal (información accesible vía TWS-EP) y autenticación física en el recinto
Informes de monitorización	Sensor	Acreditación del grupo organizador
Control de la información de los paneles informativos	Gestión	Acreditación del grupo organizador y pertenencia al grupo de gestión, o jefe de policía si hay situación de emergencia
Acceso a los informes de investigación de un suceso	Miembro de seguridad	Policía asignado a la misión. Mecanismos de autenticación con certificado
Acceso al historial médico de un paciente	Asistencia médica	Médico o policía asignado a la misión en caso de una emergencia. Mecanismos de autenticación con certificado

Cuadro 2. Políticas de autorización

Nótese que los roles no están asociados de forma estática a un usuario sino que depende del contexto de autenticación. Por ejemplo, un usuario que está acreditado como juez de un tribunal de una competición, no tiene el rol de miembro del tribunal sino se persona y autentica en el lugar del torneo en un horario determinado. De igual forma, un policía no adopta el rol representante de seguridad de los JJOO sino tiene unas credenciales que indiquen que ha sido asignado a la misión.

En general, los grupos de usuarios, roles y permisos se configuraran en el sistema antes del comienzo del evento. Si durante el transcurso de los JJOO se produce una situación excepcional, el contexto de autenticación cambia y los roles asignados a los usuarios también. La transición de un estado normal a un estado de alerta, riesgo o peligro es automática e inmediata.

La plataforma de servicios web de seguridad asigna unas políticas de acción de servicio diferentes según la política de autorización por la que se haya accedido al sistema. Así, un policía que necesite verificar un informe desde su terminal móvil conectado a través de una red ad hoc, obtendrá una información resumida y concreta de la verificación. Si la operación se realiza desde un terminal conectado a Internet, los detalles de la verificación pueden ser mucho más amplios.

Suponemos que en el entorno de unos JJOO la conectividad de todas las instalaciones mediante una red cableada está asegurada. En este escenario la red ad hoc no actúa como red principal para conectar el escenario del conflicto con los procesos de gestión y control de la información sino que forma parte de la red de respaldo. En caso de declararse una situación de emergencias, el respaldo de la red ad hoc es fundamental para el transporte de la información sensible y de control ya que en una región en la que la densidad de los nodos es alta, la redundancia de caminos de información hacen que la red ad hoc sea mucho más robusta que una red cableada o basada en un enlace GSM/GRPS/UMTS.

La validación del esquema propuesto se ha realizado a través del despliegue de la plataforma de servicios de seguridad sobre un PC de $3,8GHZ$ y con $1GB$ de memoria RAM. No se han valorado los retardos de la red ad hoc ya que los consumidores de los servicios se han simulado con nodos dentro de la propia red local del servicio.

Los resultados para una operación que engloba los servicios de autenticación, autorización, firma digital y auditoría sobre un canal SSL y usando certificados RSA de 1024bits, tienen una media de $40ms$ y un rendimiento de $40pet/s$. La verificación de firmas digitales tiene una media ligeramente superior ($50ms$) debido a los retardos por conexiones con las autoridades de validación externas.

5. Conclusiones

En el presente artículo se ha presentado un sistema de emergencias basado en una red ad hoc y una plataforma web de servicios de seguridad, se ha propuesto un caso de estudio sobre el esquema presentado y se han hecho pruebas de funcionalidad y rendimiento.

El despliegue del sistema ha permitido verificar la flexibilidad de las políticas de seguridad de la plataforma que posibilitan regular el comportamiento de la misma basadas en unas condiciones contextuales.

También se ha puesto de manifiesto la necesidad de usar políticas de federación de confianza para poder gestionar usuarios, entidades y recursos de diferentes dominios de seguridad. En un sistema de emergencias en el que la coordinación con diferentes organismos de asistencia, soporte y seguridad es básico, disponer de unas reglas de federación a nivel corporativo facilita la integración y evita los riesgos de que cada usuario asuma la federación a nivel individual.

Los resultados del rendimiento de la parte de servicios web han sido muy satisfactorios y se puede asegurar que los retardos en un sistema real vendrán determinados por los retardos de transmisión y propagación entre dominios.

Agradecimientos

Este trabajo ha sido financiado parcialmente por el Ministerio de Industria, Turismo y Comercio con el proyecto PROFIT FIT360000-2005-65.

Referencias

1. W3C: Digital Signature Service Core Protocols, Elements, and Bindings (2004)
2. OASIS: Web Services Security: SOAP Message Security (2004)
3. OASIS: Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) (2005)
4. OASIS: eXtensible Access Control Markup Language (XACML) (2005)
5. Project, L.A.: Liberty ID-FF Protocols and Schema Specification (2003)
6. IBM, Microsoft, Actional, BEA, Associates, C., 7, L., Oblix, OpenNetwork, Identity, P., Reactivity, Verisign: Web Services Trust Language (WS-Trust) (2005)
7. Hallam-Baker, P., Mysore, S.H.: XML Key Management Specification (XKMS) (2005)
8. Sandhu, R.S., Coyne, E.J., Feinstein, H.L., Youman, C.E.: Role-based access control models. IEEE Computer **29** (1996) 38–47
9. Bertino, E., Bonatti, P.A., Ferrari, E.: Trbac: a temporal role-based access control model. In: RBAC '00: Proceedings of the fifth ACM workshop on Role-based access control, New York, NY, USA, ACM Press (2000) 21–30
10. Covington, M.J., Long, W., Srinivasan, S., Dev, A.K., Ahamad, M., Abowd, G.D.: Securing context-aware applications using environment roles. In: SACMAT '01: Proceedings of the sixth ACM symposium on Access control models and technologies, New York, NY, USA, ACM Press (2001) 10–20
11. Covington, M., Moyer, M., Ahamad, M.: Generalized role-based access control for securing future applications (2000)
12. McDaniel, P.: On Context in Authorization Policy. In: 8th ACM Symposium on Access Control Models and Technologies (SACMAT), ACM (2003) 80–89 Como, Italy.
13. Berry, D., Usmani, A., Torero, J., Tate, A., McLaughlin, S., Potter, S., Trew, A., Baxter, R., Bull, M., Atkinson, M.: FireGrid: Integrated emergency response and fire safety engineering for the future built environment (2005)
14. Sanzgiri, K., Dahill, B., Levine, B., Belding-Royer, E.: A secure routing protocol for ad hoc networks (2002)
15. Guerrero Zapata, M.: Secure ad hoc on-demand distance vector (saodv) routing (2005) INTERNET-DRAFT draft-guerrero-manet-saodv-04.txt.
16. He, Q., Wu, D., Khosla, P.: SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad-hoc Networks. In: IEEE Wireless Communications and Networking Conference (WCNC 2004). (2004) 21–25
17. Liu, D., Ning, P.: Location-based pairwise key establishments for static sensor networks. In: SASN '03: Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, New York, NY, USA, ACM Press (2003) 72–82