Una arquitectura de seguridad jerárquica para entornos de trabajo inteligentes

Enrique de la Hoz de la Hoz, Iván Marsá-Maestre, Antonio J. De Vicente y Bernardo Alarcos
{enrique, ivmarsa, avicente, bernardo}@aut.uah.es
Departamento de Automática
Universidad de Alcalá
Edificio Politécnico – Crtra. N-II Km. 31,600 – 28871 Alcalá de Henares

Abstract. . *In the last years, there has been an increasing interest on security concerns in smart environments. In smart home environments the main goals are user comfort and easy deployment of new devices, so security is usually left apart or focuses mainly in transparency and privacy enhancement. Office security, however, has more rigorous security requirements due to the high number of potential users, devices and spaces, and the diversity of security roles. This paper presents a security solution for an agent-based architecture for the smart office. This security solution is potentially applicable to generic smart environments, but it suits particularly well to the smart office scenario, taking advantage of the particular characteristics of the environment to satisfy the security requirements.*

1 Introducción

El objetivo final de un entorno inteligente es liberar a los usuarios de las tareas cotidianas que normalmente realizan para cambiar su entorno de acuerdo a sus preferencias y para acceder a los servicios disponibles. Este objetivo se logra haciendo que el entorno sea capaz de adaptarse a las necesidades del usuario y de proporcionar interfaces personalizadas a los servicios disponibles en cada momento. Entre los diferentes enfoques tecnológicos posibles, proponemos construir un entorno inteligente basado en arquitecturas orientadas a servicios (SOA). Para la implementación, utilizamos un sistema multiagente, ya que los agentes software son especialmente adecuados para el desarrollo de sistemas distribuidos, inteligentes y autónomos.

En trabajos previos [1] hemos diseñado e implementado una arquitectura basada en agentes software para el hogar inteligente. Estamos extendiendo esta arquitectura para hacerla aplicable a otros entornos. En particular, estamos especialmente interesados en la personalización de servicios en el lugar de trabajo, ya que hay importantes desafíos en la automatización de este tipo de entornos debido al elevado número de usuarios potenciales y la diversidad de servicios disponibles.

Uno de los primeros desafíos que hemos tenido que enfrentar al cambiar del entorno del hogar digital de la oficina inteligente es el diseño de la arquitectura de seguridad. En una vivienda inteligente, los objetivos principales son la comodidad de los usuarios y la facilidad para desplegar nuevos dispositivos y servicios, por lo que la seguridad suele dejarse en un segundo plano. La seguridad de una oficina, sin embargo, presenta requisitos más rigurosos, especialmente si se trata de una organización de cierto tamaño, donde puede haber cientos, o incluso miles de empleados con diferentes necesidades de acceso y clasificaciones de seguridad. Este artículo analiza estos requisitos y sus diferencias respecto del hogar digital y propone una extensión a nuestra arquitectura basada en agentes para proporcionar servicios de seguridad en un entorno de trabajo inteligente.

El resto del documento se organiza como sigue. La sección 2 describe los aspectos más relevantes de nuestra arquitectura para espacios inteligentes, utilizando un caso de uso típico para ilustrarlos. La sección 3 resume los aspectos clave de la seguridad en entornos de trabajo inteligentes. La sección 4 presenta nuestra arquitectura de seguridad, describiendo la funcionalidad de los diferentes agentes que proporcionan los servicios de seguridad. Finalmente, la sección 5 resume nuestra contribución y plantea algunas líneas futuras de investigación sobre el tema.

2 Seguridad en computación ubicua

Desde un punto de vista funcional, el objetivo de la seguridad es valorar los riesgos presentes en un determinado entorno y desarrollar medidas que protejan al entorno y a sus usuarios de esos riesgos [2]. Algunos de los servicios clave que debe ofrecer una solución de seguridad son la confidencialidad e integridad de los mensajes intercambiados, la autenticación de las partes que se comunican, el control de acceso y la distribución de claves.

Por confidencialidad se entiende la protección de la información en el entorno ante accesos no autorizados. En espacios inteligentes, el término información adquiere una perspectiva única [3]. Los sistemas implicados son potencialmente capaces, como conjunto, de sensar prácticamente cada aspecto

de las interacciones de los usuarios con el sistema o entre los propios usuarios, y toda la información sensada puede ser almacenada, transmitida, consultada y repetida. En entornos como oficinas inteligentes, será necesario proteger parte de esta información por su sensibilidad relativa al negocio, pero otra gran parte de la información sensada por el sistema será información personal acerca de los usuarios. Por lo tanto, además de los aspectos relacionados con la confidencialidad normalmente presentes en los sistemas de información, aparecerán nuevas consideraciones con respecto a la privacidad de los usuarios [4]. Incluso aunque la información sensible se proteja empleando criptografía, puede obtenerse información sensible de un entorno inteligente (por ejemplo, en qué momento se está accediendo a un determinado servicio) simplemente analizando el tráfico de la red. Este riesgo se incrementa con el uso de tecnologías inalámbricas.

La integridad garantiza que la información del entorno sólo puede ser modificada por entidades autorizadas. Ejemplos de posibles modificaciones maliciosas pueden ser la alteración, repetición, eliminación o retraso de información almacenada o de mensajes intercambiados entre entidades. La integridad del código ejecutable debe protegerse también, especialmente en sistemas en los que se permita movilidad de código. Al igual que la confidencialidad, la protección de la integridad de la información almacenada o transmitida se alcanza tradicionalmente mediante el uso de técnicas criptográficas.

La autenticación de dispositivos en el entorno inteligente puede aprovecharse de las aproximaciones existentes para seguridad de ordenadores y redes de datos. La criptografía de clave pública o privada puede utilizarse para autenticar intercambios de información entre dispositivos, teniendo en cuenta las consideraciones acerca de las limitaciones de recursos que señalábamos más arriba. Sin embargo, dada la naturaleza altamente dinámica y descentralizada de los espacios inteligentes, el mayor problema que encontramos para proporcionar autenticación en estos entornos es la distribución de claves. Las soluciones que se sustentan en la conectividad a un servidor de autenticación y revocación, desde Kerberos a los certificados de clave pública, sólo pueden aplicarse a entornos inteligentes donde se pueda asumir una disposición jerárquica de principales, y donde la adición y eliminación de usuarios y servicios sea controlada. En [5] se emplea un enfoque centralizado para hogares inteligentes, y en la siguiente sección demostraremos su aplicabilidad a oficinas inteligentes. En espacios inteligentes donde los dispositivos se comunican a través de redes ad-hoc y donde se requiere añadir y eliminar dispositivos con facilidad, se emplean asociaciones seguras transitorias para proporcionar autenticación de forma distribuida [6].

El control de acceso pretende asegurar que sólo se permite ejecutar acciones sensibles desde el punto de vista de la seguridad a las entidades autorizadas para hacerlo. En los entornos inteligentes, las políticas de control de acceso pueden ser muy complejas debido a los diferentes roles que los usuarios pueden desempeñar, por ejemplo, en una oficina. Una solución para modelar esos escenarios es el control de acceso basado en roles o RBAC [7] o su extensión para tener en cuenta información de contexto definiendo roles de entorno o *environmental roles* [8]. Íntimamente ligados al control de acceso encontramos los mecanismos de delegación [9], que adquieren especial importancia en algunos entornos ubicuos como oficinas inteligentes.

3 La arquitectura de agentes SETH

La arquitectura de servicios presentada en este documento se despliega sobre nuestra plataforma SETH (Smart EnvironmenT Hierarchy), que es una extensión de la arquitectura iHAP architecture desarrollada para el hogar inteligente [1]. La descripción detallada de la arquitectura SETH va más allá del propósito de este artículo, y puede encontrarse en [10]. En esta sección se describen brevemente las características de la arquitectura que son más relevantes para la comprensión del artículo.

3.1 Espacios inteligentes en SETH

Nuestra arquitectura se basa en el concepto de espacios inteligentes (*Smart Spaces*, SS), que son localizaciones específicas y autocontenidas del entorno en el que se mueve el usuario. Desde un punto de vista funcional, un espacio inteligente A se caracteriza por un conjunto de dispositivos, un conjunto de servicios que pueden ser prestados en dicho espacio, y un determinado contexto. Es posible establecer una jerarquía de espacios inteligentes, si las características del entorno así lo requieren. Esta aproximación jerárquica nos permite proporcionar diferentes niveles de servicios, información de contexto y seguridad. En nuestro escenario de demostración consideraremos la existencia de un espacio inteligente que abarca una ciudad, y que incluye una vivienda, un restaurante y un lugar de trabajo, así como un entorno abierto: un monumento. El lugar de trabajo, a su vez, incluye el espacio Segunda Planta, en la que se encuentran un despacho y una sala de reuniones. La Figura 1 describe la jerarquía de espacios inteligentes del escenario descrito.

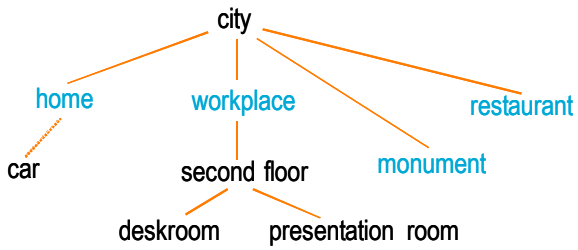

Figura 1: Ejemplo de jerarquía de espacios

En este tipo de escenarios podemos tener reglas de herencia que establezcan qué información de contexto, servicios y dispositivos procedentes de niveles superiores de la jerarquía están disponibles en un espacio concreto. También se pueden establecer reglas de agregación que permitan que un espacio inteligente exporte información de contexto, dispositivos o servicios a niveles superiores de la jerarquía. Las reglas de herencia y agregación pueden ser combinadas para permitir, por ejemplo, que un usuario que se encuentra en su espacio vivienda acceda mediante un proceso de herencia al servicio de reserva que se ofrece en el espacio restaurante y que se ha exportado al espacio ciudad mediante agregación.

3.2 Dispositivos en la arquitectura SETH

Para poder realizar sus funciones, la arquitectura que se propone en este trabajo se apoya en una serie de dispositivos distribuidos a lo largo de todo el entorno inteligente. La *Plataforma de agentes para el espacio inteligente* (*Smart Space Agent Platform –SSAP–*), obligatoria en cualquier espacio inteligente SETH, contiene la plataforma de agentes que permite la existencia del resto de los agentes en el espacio inteligente, y alberga los agentes de más alto nivel del sistema, así como aquellos que son necesarios para controlar dispositivos no inteligentes. Los *Dispositivos con Agentes* son sensores y actuadores con cierto grado de autonomía, generalmente proporcionada por agentes ejecutándose en una máquina virtual Java empotrada. Los *Dispositivos sin Agentes* son sensores y actuadores sin autonomía, controlados desde el SSAP. Además, cada usuario debe portar un *Dispositivo de Identificación*, que se utiliza para identificar al usuario ante el sistema y determinar su localización en el entorno. Finalmente, los usuarios pueden portar dispositivos móviles (teléfonos móviles, PDAs), que no sólo pueden proporcionar la funcionalidad de los dispositivos de identificación, sino también albergar los agentes necesarios para aprender, mantener y tratar de satisfacer las preferencias de los usuarios y para mostrar las interfaces adecuadas a los servicios en cada momento.

Para la implementación del sistema propuesto, nuestro grupo de investigación hace uso de la plataforma JADE[1], disponible como *open-source*. El hacer uso de una plataforma de agentes ya establecida nos libera de una serie de tareas de bajo nivel relacionadas con el ciclo de vida y funcionamiento el agente, así como el establecimiento de los mecanismos de comunicación entre los agentes. Por otro lado, la utilización de JAVA como lenguaje de desarrollo en esta plataforma garantiza la interoperabilidad de los sistemas y la posibilidad de desarrollo de sistemas de menores prestaciones en equipos más potentes, con menores problemas de implantación final. Por otro lado, la plataforma JADE cumple con los estándares de FIPA[2], una organización de estandarización de la IEEE Computer Society que promueve la tecnología basada en agentes y la interoperabilidad entre estos y con otras tecnologías.

3.3 Agentes software en SETH

Podemos encontrar diferentes tipos de agentes software en un espacio inteligente SETH. El *Agente de coordinación de entornos inteligentes –Smart Space Coordination Agent– (SSCA)*, que reside en el SSAP, proporciona descubrimiento de dispositivos y servicios a todos los usuarios o agentes que se encuentran en un espacio inteligente dado, y a los SSCAs de otros espacios. Los *Agentes de Dispositivo* proporcionan una interfaz unificada a los dispositivos, de manera que el sistema puede utilizarlos, independientemente del hardware que realice las funciones. Los *Agentes de Sistema*, como los agentes de contexto o los agentes de seguridad, proporcionan un nivel adicional de inteligencia por encima de los dispositivos que se encuentran en una ubicación concreta mediante mecanismos de coordinación y control. Los *Agentes Personales* (*Personal Agents*, PA) son, a todos los efectos, los representantes de los usuarios en el entorno y juegan un papel fundamental para alcanzar la percepción de "inteligencia" del entorno [11]. Finalmente, los *Agentes de Servicio* proporcionan servicios finales al usuario, y pueden ser *persistentes*, si siempre están activos en un determinado SSAP, o *no persistentes* o móviles, si son creados por el SSCA para cada petición de servicio, se mueven de un SSAP a otro cuando la localización del usuario cambia y se destruyen una vez que se ha prestado el servicio. Los servicios de interfaz, que son un caso particular de los agentes de servicio, y el uso de movilidad de agentes para permitir que los servicios "sigan" al usuario a través de diferentes espacios se cubren en [10]. El descubrimiento y acceso a servicios se describen en la siguiente sección.

La Figura 2 ilustra un caso típico de utilización de servicios en nuestro sistema. Alice entra en la sala de

[1] Java Agent DEvelopment framework (http://jade.cselt.it)

[2] Foundation for Intelligent Physical Agents (http://www.fipa.org)

presentaciones, y su agente personal llega a la sala siguiendo el proceso descrito en [11]. Los agentes de contexto notifican, tanto al Agente personal como al *SSCA_saladepresentaciones* que el usuario ha entrado (1). El agente personal sabe (a través de su agenda) que Alice tiene que realizar a esta hora una presentación haciendo uso de un documento de transparencias que se encuentra en el ordenador de su despacho. El agente personal solicita al *SSCA_saladepresentaciones* un agente que proporcione el servicio de presentación de transparencias (2). No se encuentra un agente persistente capaz de ofrecer ese servicio, por lo que *SSCA_saladepresentaciones* crea un agente de servicio de presentación no persistente (3) y devuelve su dirección al agente personal (4). El agente personal contacta al agente recién creado y le solicita que inicie una presentación con las transparencias que se encuentran en el ordenador de Alice (5). El agente no persistente contacta con el *SSCA_despacho* para solicitar un servicio que pueda proporcionarle el fichero necesario (6). El *SSCA_despacho* le devuelve la dirección de un agente persistente que presta servicio de transferencia de ficheros (7), con el que contacta el agente no persistente de presentación para obtener el fichero necesario (8). El agente de servicios de transferencia de ficheros obtiene el fichero del agente de dispositivo asociado al ordenador de Alice (9) y lo transfiere al servicio de presentación (10). Finalmente, el agente no persistente de presentación solicita al agente de dispositivo del proyector que realice la proyección de tas transparencias (11). Una vez que ha concluido la presentación, el agente no persistente de presentación de transparencias es destruido.

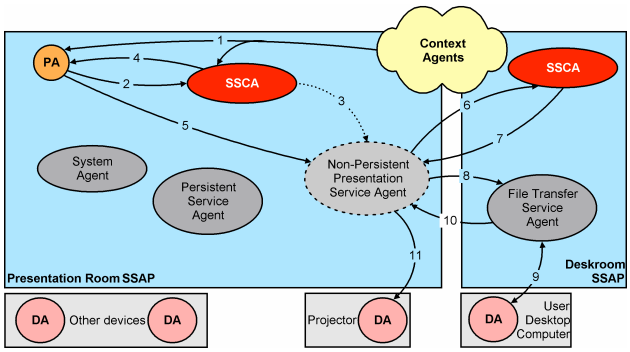

Figura 2: Caso de uso típico

Cualquier interacción típica como la descrita en el párrafo anterior puede necesitar que interactúen sistemas de descubrimiento de servicios en diferentes *SSAPs*, realizando solicitudes de servicio a través de dispositivos que pueden encontrarse en diferentes lugares. Esta flexibilidad del mecanismo de interacción, que es posible realizar de manera sencilla gracias a la arquitectura basada en agentes, tiene, sin embargo algunas consideraciones de seguridad que deben ser tratadas adecuadamente para asegurar que no se realiza un uso no deseado de la infraestructura del sistema.

4 Propuesta de seguridad

Por el momento, no existe una solución general para proporcionar seguridad en entornos inteligentes, ya que los requisitos de seguridad y las relaciones de confianza varían ampliamente en los diferentes escenarios con que podemos encontrarnos. Por ello, cada solución de seguridad debe establecer las condiciones bajo las que es aplicable y los objetivos de diseño que persigue. En el momento de escribir este documento, hemos desarrollado una solución para un escenario de oficina inteligente basado en la arquitectura propuesta. Se ha escogido como escenario la oficina inteligente por dos razones. En primer lugar, la seguridad en un entorno de trabajo puede suponer un desafío significativo, especialmente si se trata de una gran organización donde puede haber centenares, o incluso miles de empleados con diferentes necesidades de acceso y credenciales de seguridad. Por otro lado, debido al control de acceso físico, la presencia de personal de seguridad y la existencia de una jerarquía de poder, la aplicación de las políticas de seguridad en oficinas inteligentes es más fácil de garantizar que, por ejemplo, en entornos urbanos. Para nuestra arquitectura de seguridad para la oficina inteligente, asumimos que podemos confiar en el fabricante del núcleo de la arquitectura del espacio inteligente, y que todos los SSAP tienen conectividad a una autoridad de certificación centralizada a nivel de edificio (BCA), de forma que se pueda establecer una cadena de confianza desde la BCA al fabricante de cualquier agente de servicio o de sistema que se necesite para el funcionamiento básico de la arquitectura. Esta suposición no puede extenderse a los agentes de servicio no persistentes (puesto que son móviles) ni a los agentes personales (puesto que velan por las preferencias del usuario, y no por políticas de seguridad del sistema). Finalmente, asumimos que podemos considerar las máquinas sobre las que corren los SSAPs seguras. Dicha seguridad puede alcanzarse mediante el uso de Computación Confiable [12] u otras técnicas, como las propuestas en [13].

Además, establecemos como requisito para nuestra solución de seguridad que soporte la naturaleza dinámica del entorno (permitiendo la adición y eliminación flexible de usuarios y dispositivos), que sea escalable, que proporcione mecanismos de autenticación y control de acceso que puedan satisfacer las rigurosas consideraciones de seguridad de las oficinas inteligentes y que permita la existencia de dispositivos de diferentes capacidades en cuanto a administración de energía, ancho de banda y capacidad computacional.

Teniendo en cuenta estas suposiciones y objetivos, en este capítulo presentamos nuestra propuesta de seguridad para la oficina inteligente, describiendo la aproximación empleada para abordar cada una de las consideraciones de seguridad discutidas.

4.1 Autenticación, confidencialidad e integridad en las comunicaciones

La seguridad de los mensajes se proporciona habitualmente mediante el uso de técnicas criptográficas. La criptografía asimétrica proporciona una mayor seguridad a expensas de un mayor uso del ancho de banda y del tiempo de cómputo del sistema. En nuestra propuesta, asumimos que el uso de criptografía asimétrica es aceptable en los *SSAPs* y en los dispositivos personales (PDAs o teléfonos inteligentes) de los usuarios. Sin embargo, puesto que los dispositivos personales están alimentados con baterías, el uso de este tipo de criptografía debe minimizarse. Teniendo esto en cuenta, nuestra arquitectura de seguridad emplea criptografía asimétrica para acordar un secreto compartido entre las entidades que se comunican, empleando un protocolo de inicialización sencillo, que se describe con mayor detalle en [10].

4.2 Distribución de claves y dispositivos personales

Cada *SSAP* tiene su propio par de claves asimétricas, cuya clave pública se almacena en la *BCA*. Siempre que se añade un nuevo usuario al sistema, se generan pares de claves para su uso dentro del edificio. Si el usuario dispone de un certificado firmado por una autoridad de confianza, el sistema proporciona un mecanismo para que el usuario pueda generar de forma segura su propio par de claves y publicarlo en la BCA. Si no existe una prueba electrónica de la identidad del usuario, se requiere la intervención de un empleado de seguridad que verifique y registre su identidad para añadir el nuevo usuario al sistema y generar su par de claves.

El tipo de dispositivo empleado para almacenar el material criptográfico asociado al usuario puede variar dependiendo del modo en que el usuario vaya a interaccionar con el sistema. A los usuarios que no disponen de un dispositivo personal y a los visitantes ocasionales se les entrega una tarjeta inteligente que puede insertarse en los diferentes dispositivos de interfaz del edificio para acceder a cualquier servicio que requiera autenticación. Para los usuarios con acceso a personalización de servicios, se lanza un agente personal (PA, *Personal Agent*) en la plataforma de agentes de su dispositivo personal. Para que el agente personal pueda actuar en nombre del usuario para adaptar el entorno a sus preferencias, se genera un par de claves adicional. El hecho de tener dos pares de claves diferentes para el usuario y su PA permite al sistema distinguir entre peticiones automatizadas y peticiones directas del usuario, y permite también pedir confirmación al usuario (p.ej. una contraseña) para realizar tareas especialmente sensibles.

4.3 Autenticación de usuarios, dispositivos y agentes

La autenticación de usuarios se realiza por medio de certificados. El edificio tiene su propio agente de autoridad de certificación (BCAA, *Building-level Certificate Authority Agent*) que pueda expedir certificados de nivel de edificio (BCs, *Building-level Certificates*) para cualquier usuario que entre en el sistema. Un BC asocia la identidad del usuario a una clave pública y a un conjunto de roles, que se utilizan para distinguir, por ejemplo, a un empleado de un visitante desconocido. Estos certificados se utilizan para autenticar a los usuarios ante los agentes de coordinación de los espacios inteligentes (*SSCAs*) siempre que los usuarios entran en un nuevo espacio.

Cada *SSAP* tiene su propio par de claves asimétricas y su propio certificado de nivel de edificio asociado a su clave pública. Todos los agentes de sistema y los agentes de servicio persistentes que se ejecutan en un *SSAP* comparten este par de claves, y pueden utilizarlo para autenticarse ante usuarios, agentes personales y otros *SSAPs* y para intercambiar claves de sesión con ellos tal y como se describían en el apartado 4.1. Tal y como se establecía al inicio del capítulo, asumimos que el *SSAP* es seguro, y que los agentes de sistema y los agentes persistentes de servicio están firmados por el fabricante. Estos agentes se consideran los agentes propios del espacio controlado por el *SSAP*, y en este sentido vemos coherente que compartan una clave asociada a ese espacio.

No pueden aplicarse las mismas suposiciones de seguridad a otros dispositivos del espacio inteligente. No podemos garantizar la seguridad física de interruptores, lámparas o sensores de temperatura del mismo modo que garantizábamos la seguridad del *SSAP*, por lo que no es apropiado compartir el par de claves del *SSAP* con estos dispositivos y con los agentes que los controlan. Además, algunos de estos dispositivos pueden no tener la potencia computacional, el espacio de almacenamiento o la autonomía de batería necesarios para soportar el uso de criptografía asimétrica. Por ello empleamos criptografía simétrica para asegurar las comunicaciones con estos dispositivos, de un modo muy similar a la iniciativa del *Resurrecting Duckling* [6] En nuestra arquitectura, cada *SSCA* comparte una clave secreta con cada dispositivo dentro de su espacio inteligente asociado. Por medio de estas claves puede crear asociaciones transitorias seguras entre dispositivos, usuarios y agentes dentro del espacio inteligente asignando claves secretas temporales a pares de principales. El mismo enfoque es el que se emplea con los agentes de servicio no persistentes, ya que las consideraciones de seguridad asociadas a su movilidad hacen inaceptable que compartan el par de claves del *SSAP*. La Figura 3 ilustra este mecanismo con un ejemplo. El agente personal solicita un servicio de videoconferencia al

SSCA (1), utilizando una clave de sesión previamente acordada K_{S1}. Tras comprobar que la petición es legítima (trataremos la autorización con más detalle en el siguiente apartado), y puesto que no hay ningún agente activo capaz de atender la petición del usuario, se crea un agente de servicio no persistente (2) *improntado* al *SSCA* por medio de una clave secreta compartida K_{S2}. El *SSCA* genera entonces una clave temporal de sesión para la comunicación entre el PA y el agente recién creado, K_{S3}, y se la envía de forma segura a ambas partes (3), que pueden comunicarse a partir de ahora utilizando esta clave secreta compartida hasta que expire (4).

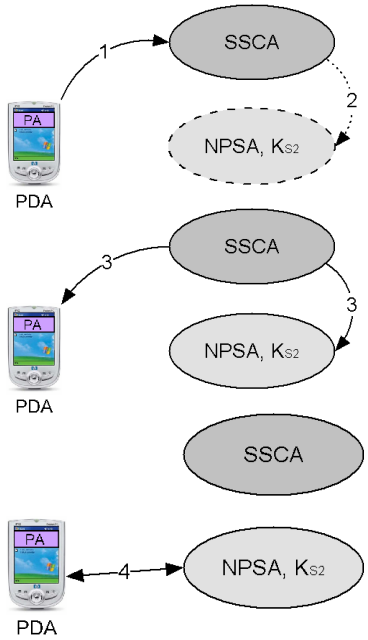

Figura 3: Comunicación segura con un agente de servicio no persistente

4.4 Autorización y delegación

Una vez que los usuarios, dispositivos y agentes se han autenticado y pueden establecer comunicaciones seguras entre ellos, el servicio de autorización se proporciona empleando un enfoque basado en credenciales. La idea básica es que a un usuario o agente se le permite efectuar determinada acción si pueden mostrar una credencial firmada por una autoridad de autorización válida. En nuestro sistema, esta autoridad se representa por medio de los agentes de autorización de los espacios inteligentes (*SSAA*, *Smart Space Authorization Agents*). Hay un *SSAA* por cada *SSAP*, y puede haber *SSAAs* asociados a grupos de *SSAPs* para proporcionar un árbol jerárquico de agentes de autorización. Podemos tener, por ejemplo, agentes de autorización para diferentes plantas que engloben a todos los *SSAPs* en cada planta. Normalmente, tendremos al menos un agente de autorización a nivel de edificio (*BAA*, Building-level Authorization Agent).

En la Figura 4 puede verse una secuencia típica de este mecanismo. El agente personal del usuario A quiere cambiar la música ambiental de un despacho para adaptarla a las preferencias del usuario. Una vez concluidos los procesos de descubrimiento de servicios y de autenticación, el agente PA realiza su petición (1) al correspondiente agente de servicio (pongamos, por ejemplo, un agente de servicio de música ambiental *AMSA*, *Ambient Music Service Agent*). El agente personal puede proporcionar cualesquiera credenciales necesarias junto con la petición si ya sabe que le van a ser requeridas (p.ej., si cada día hace uso del mismo servicio). Si no se proporcionan las credenciales adecuadas, el agente *AMSA* puede simplemente denegar el acceso al servicio o pedir las credenciales específicas necesarias para acceder al servicio (2). Si el agente PA no dispone de las credenciales adecuadas, puede pedírselas al agente *SSAA* correspondiente (3), que comprobará la política de seguridad y expedirá la correspondiente credencial si está de acuerdo con la política (4). Finalmente, el agente personal muestra las credenciales al agente AMSA (5), que puede entonces verificarlas y procesar la petición.

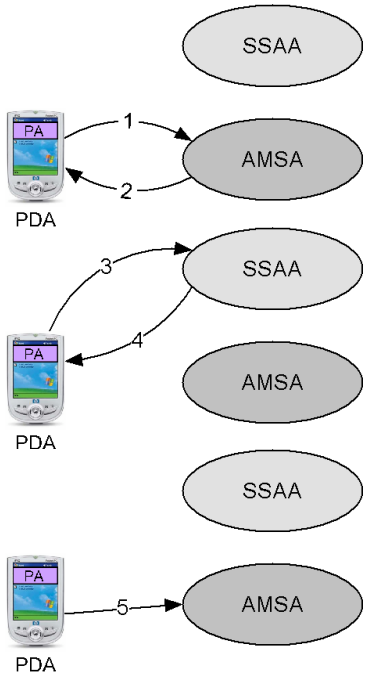

Figura 4: Autorización basada en credenciales

Existen ciertas consideraciones adicionales que deben tenerse en cuenta con respecto a la expedición de credenciales y a su distribución y almacenamiento. Las credenciales de nivel de edificio están asociadas generalmente a los roles de usuario, definiendo por ejemplo a qué espacios pueden acceder los visitantes o que servicios son accesibles a un empleado desde cualquier pasillo del edificio. De este modo se implementa una forma particular de RBAC [7]. Estas credenciales de nivel de edificio pueden incluirse en el certificado BC que se le da al usuario, evitando la carga de tener que solicitar una credencial específica para cada petición. Sin embargo, puede existir una

limitación para el almacenamiento de credenciales en los dispositivos personales de los usuarios. Además, para usuarios que no porten dispositivos personales con suficiente capacidad de cómputo o de almacenamiento, o aquellos que no dispongan de un agente personal actuando en su nombre, el protocolo descrito no es aplicable. Para estos casos, el sistema proporciona un mecanismo alternativo en el que son los propios agentes de servicio los que solicitan las credenciales del usuario a los agentes de autorización. Este será el escenario para visitantes desconocidos a los que se les proporciona una tarjeta inteligente para que accedan a ciertos espacios del edificio.

La delegación se aborda como un caso particular de autorización, donde la autoridad que expide una credencial para permitir a un principal A realizar una acción X no es un *SSAA*, sino otro principal B que tiene autorización para realizar dicha acción. Esto permite, por ejemplo, que un agente personal expida una credencial para permitir a un agente de servicio (por ejemplo, el agente que controla una pantalla de presentación) acceder a un fichero almacenado en el ordenador personal del usuario (que contenga, por ejemplo, una presentación de diapositivas).

Tanto la definición de políticas como la administración de credenciales se realiza utilizando una implementación de SPKI [14] basada en agentes, ya que esta infraestructura de clave pública se ha revelado como una solución fiable con un adecuado compromiso entre su potencia expresiva para la definición de políticas y credenciales y la carga computacional que impone al sistema.

4.4 Tratamiento de la movilidad de agentes

El empleo de agentes móviles plantea numerosas consideraciones de seguridad [15]. Por el momento, nuestra arquitectura sólo permite la movilidad a agentes de servicio no persistentes. Estos agentes son creados y lanzados por el *SSCA* ante una petición de un servicio proporcionado por esos agentes, lo que permite cierto control de la ejecución de código en el *SSCA*. Para aumentar la protección ante agentes maliciosos, el código de todos los agentes de servicio no persistentes está firmado por sus respectivos fabricantes, cuya clave pública se encuentra al alcance de los *SSAPs*. Cuando un agente móvil trata de migrar a otra plataforma, la firma del código se verifica en destino para asegurar que no ha sido maliciosamente alterado. Para proteger contra alteraciones maliciosas del estado de ejecución del agente, la petición que provoca la creación del agente es firmada por el *SSCA* que lo lanza y adjuntada con el agente en su migración, de forma que la plataforma destino pueda restringir las operaciones permitidas al agente en función de la petición firmada. Por último, siempre que un agente migra, el *SSAP* origen firma el estado de ejecución del agente, responsabilizándose de la generación de ese estado.

Puesto que los agentes móviles pueden viajar a través de diferentes *SSAPs*, e incluso a través de diferentes edificios, no deben compartir los pares de claves de los *SSAPs*. En su lugar, el SSAP en el que se ejecuta el agente genera claves simétricas temporales siempre que un agente móvil necesita comunicarse con otro principal. Estas claves se revocan si el agente móvil abandona el *SSAP*.

7 Conclusiones

Hay líneas de investigación muy diferentes acerca de la seguridad en entornos inteligentes. Aunque suelen partir de las mismas suposiciones generales, las estrategias que adoptan y la importancia que confieren a cada aspecto de la seguridad en entornos ubicuos varían ampliamente, de acuerdo con los diferentes escenarios a los que están dirigidos. Para abordar el problema de la seguridad en un entorno inteligente determinado, las suposiciones y requisitos específicos impuestos por el entorno deben ser sopesadas para determinar la arquitectura más adecuada para la solución. Como un primer paso, hemos escogido centrarnos en oficinas inteligentes, y hemos desarrollado una solución de seguridad adaptada específicamente a este escenario, aprovechando las características particulares del entorno considerado para satisfacer los requisitos de seguridad. Creemos que nuestra solución es adecuadamente equilibrada. Hemos extraído las ventajas de soluciones federadas para la seguridad en entornos ubicuos como Cerberus [16] y de soluciones distribuidas como Resurrecting Duckling [6] y las hemos aunado para obtener una solución jerárquica y basada en agentes que es suficientemente flexible y escalable para aplicarla a diferentes escenarios de oficinas inteligentes, desde negocios pequeños a grandes organizaciones.

Quedan numerosas líneas abiertas para futuras investigaciones. En este momento estamos implementando nuevos servicios en nuestros propios espacios de trabajo para comprobar si la arquitectura propuesta es suficientemente flexible para darles cabida. La seguridad de los agentes se trata de una manera muy restrictiva (firma de código), y pretendemos añadir a la arquitectura otros mecanismos de protección que permitan la adición flexible de nuevos servicios y dispositivos. Por último, debe abordarse el problema de la disponibilidad, que se ha dejado fuera de la propuesta por el momento.

Agradecimientos

Este trabajo ha sido realizado gracias a la financiación de los proyectos JCCM-PBC-05009-2 de la Junta de Comunidades de Castilla La-Mancha, y CAM-CCG06-UAH/TIC-0424, de la Comunidad Autónoma de Madrid.

Referencias

[1] Velasco, J.R., Marsá-Maestre, I., Navarro, A., López, M.A., Vicente, A.J., Hoz,E.d.l., Paricio, A., Machuca, M.: Location-aware services and interfaces in smart homes using multiagent systems. In: Proceedings of the 2005 International Conference on Pervasive Systems and Computing (PSC'05), Las Vegas, USA (2005).

[2] Nixon, P.A., Wagealla, W., English, C., Terzis, S.: 11. In: Security, Privacy and Trust Issues in Smart Environments. John Wiley & Sons (2005) 249–270

[3] Langeheinrich, M.: Privacy by design: Principles of privacy aware ubiquitous systems. In: UBICOMP 2001, Lecture Notes in Computer Science. Volume 2201. (2001) 273–291

[4] Campbell, R., Al-Muhtadi, J., Naldurg, P., Sampemane, G., Mickunas, M.D.: Towardssecurity and privacy for pervasive computing. In: Theories and Systems, Mext-NSF-JSPS International Symposium, ISSS 2002. Lecture Notes in Computer Science, Tokyo, Japan (2002) 1–15

[5] Al-Muhtadi, J., Anand, M., Mickunas, M., Campbell, R.: Secure smart homes using jini and uiuc sesame. In: Computer Security Applications, 2000. ACSAC'00. 16th Annual Conference. (2000) 77–85

[6] Stajano, F., Anderson, R.: The resurrecting duckling: security issues for ubiquitous computing. IEEE Computer 35(4) (2002) 22–26

[7] Ferraiolo, D., Kuhn, D.: Role based access control. In: 15th National Computer Security Conference. (1992)

[8] Covington, M., Fogla, P., Zha, Z., Ahamad, M.: A context-aware security architecture for emerging applications. In: Computer Security Applications Conference, 2002. Proceedings. 18th Annual. (2002) 249–258

[9] Na, S., Cheon, S.: Role delegation in role-based access control. In: Proceedings of the 5th ACM Workshop on Role-Based Access Control, Berlín, Germany (2000) 39–44

[10] Marsá-Maestre, I.: A hierarchical, agent-based architecture for smart spaces. Technical Report TR2006-101, Grupo de Ingeniería de Servicios Telemáticos, Universidad de Alcalá (2006) Available at http://www.it.aut.uah.es/ist/papers/TR2006-101.pdf

[11] Marsá-Maestre, I., López, M.A., Velasco, J.R., Navarro, A.: Mobile personal agents for smart spaces. In: Proceedings of the IEEE Internacional Conference on Pervasive Services 2006 (ICPS 2006), Lyon, France (2006) 299–302.

[12] Felten, E.W.: Understanding trusted computing. IEEE Security & Privacy 1(3) (2003) 60–66

[13] W. A. Arbaugh, D.F., Smith, M.: A secure and reliable bootstrap architecture. In: Proceedings of the IEE Symposium on Security and Privacy, IEEE CS Press (1997) 65–71

[14] Ellison, C., Frantz, B., Lampson, B., Rivest, R., Thomas, B., Ylonen, T.: Spki certificate theory. RFC 2693 (1999)

[15] Jansen, W., Karygiannis, T.: Mobile agent security. NIST Special Publication 800-19, National Institute of Standards and Technology (2000)

[16] Al-Muhtadi, J., Ranganathan, A., Campbell, R., Mickunas, M.: Cerberus: a context-aware security scheme for smart spaces. In: Pervasive Computing and Communications, 2003. (PerCom 2003). Proceedings of the First IEEE Internacional Conference on. (2003) 489–496