Capítulo 7

Conclusiones y líneas futuras

7.1 Conclusiones

La evolución de los sistemas distribuidos ha dejado patente la necesidad de proporcionar mecanismos de seguridad de carácter descentralizado. No estamos frente al reto de proteger un gran sistema central de información administrado por un conjunto reducido de personas. Tampoco se trata de manejar comunidades reducidas y estáticas de usuarios, ni de controlar simplemente un sistema de ficheros compartido o una serie de periféricos. Por el contrario, en el entorno actual se encuentran involucradas grandes comunidades de usuarios, quizá geográficamente dispersas, que desean acceder a un número creciente de recursos de índole muy diversa, administrados de forma local por entidades que tienen la difícil tarea de enfrentarse a un problema de magnitudes muy superiores al existente años atrás.

En el fondo, todo podría considerarse como un problema de gestión de confianza, es decir, la necesidad de tener que plasmar en un sistema informático las distintas relaciones existentes tanto entre las entidades que conforman dicho sistema como entre el propio sistema y otros elementos externos al mismo. Como ya se comentó en el capítulo de introducción, para poder proporcionar los servicios básicos de seguridad es necesario realizar un proceso de identificación, autenticación y autorización que satisfaga los requisitos del sistema al cual pretende aplicarse. A lo largo de este trabajo de tesis, se ha mostrado cómo la certificación digital es una de las tecnologías capaces de proporcionar los mecanismos necesarios para poder llevar a cabo gran parte de las operaciones de seguridad relacionadas con la identificación y la gestión de privilegios.

Hemos visto cómo gran parte de las innovaciones científicas realizadas en torno a los certificados digitales han tenido como especial foco de actuación la provisión de técnicas ligadas a la gestión del ciclo de vida. Se ha comprobado que la aplicación de la certificación digital recae completamente en la existencia de sistemas que proporcionen las herramientas necesarias para su gestión, distribución e integración en entornos de aplicación concretos. Su éxito como herramienta de seguridad depende tanto de su fortaleza criptográfica y expresiva como de la disponibilidad y adecuación del sistema que los gestiona.

El análisis que se ha realizado acerca del estado del arte de las propuestas relacionadas

con la certificación digital, tanto de identidad como de autorización, ha mostrado múltiples aspectos a los que todavía no se les ha proporcionado una solución ampliamente aceptada. Se podría afirmar que tales carencias están asociadas a dos hechos muy concretos: por un lado, la falta de entornos reales de pruebas que permitan conocer las verdaderas necesidades del mercado y validar las distintas propuestas que se van formulando; por otro lado, la obsesión por mantener enfoques tecnológicos obsoletos e intentar adaptar los escenarios reales a las especificaciones existentes en lugar de buscar enfoques alternativos que se adecuen a la realidad en la cual nos encontramos inmersos.

El trabajo de tesis aquí presentado tiene en mente estos dos factores a la hora de proporcionar una solución completa al problema de la gestión y uso de los certificados digitales como herramienta básica de seguridad. En primer lugar, se ha realizado un esfuerzo analítico para encontrar enfoques alternativos al problema de la gestión de la confianza, y más concretamente a la gestión distribuida de la misma. Por otra parte, las propuestas realizadas han sido puestas en marcha y validadas en entornos de aplicación concretos con requisitos muy diversos.

La consecuencia es la especificación de una solución global formada por la composición de una infraestructura de clave pública basada en el estándar X.509 y de una infraestructura de autorización centrada en el uso de certificados SPKI. Ambos sistemas se encuentran claramente conectados, ya que el segundo toma al primero de ellos como punto de partida, y se complementan en la tarea general de etiquetar (identificar) y calificar (autorizar) a las entidades del sistema.

Una cuestión que ha resultado transversal durante el desarrollo de este trabajo ha sido mantener las políticas inherentes del sistema al mínimo, es decir, no definir una solución que conllevará la adopción de una serie de supuestos que pudieran no ser aconsejables en ciertos entornos y que por tanto limitaran su adopción. Por ejemplo, tanto la PKI como el sistema distribuido de gestión de credenciales han sido diseñados para soportar una amplia gama de prácticas de certificación y políticas de autorización. Esta filosofía también se puede apreciar en el diseño modular de muchas de las aportaciones realizadas, el cual tiene como objetivo clave favorecer la inserción o modificación de funcionalidad con el menor impacto posible sobre el resto del sistema.

Como conclusiones concretas en lo que respecta a las aportaciones realizadas en materia de certificación de identidad es posible afirmar que:

- La infraestructura proporciona una amplia gama de modos de acceso a los servicios proporcionados ya que la interacción con las entidades finales puede realizarse de forma directa o a través de las autoridades de registro. Además, al estar basado el diseño en estándares comúnmente aceptados, se favorece la interoperabilidad y se proporciona soporte a la mayor parte de sistemas operativos y aplicaciones.

- La gestión de los distintos componentes se realiza desde un punto de vista unificado. Varios de los aspectos técnicos de las prácticas de certificación se materializan en las denominadas políticas de PKI, las cuales constituyen un mecanismo extensible de especificación basado en la existencia de administradores especiales encargados

de introducir los criterios a seguir. Además, este mecanismo permite variar dinámicamente parte del comportamiento de la PKI, lo cual simplifica la adaptación de la infraestructura a entornos muy dinámicos.

- Se han introducido servicios avanzados en lo que respecta a la revocación y validación de certificados. Por un lado, al igual que sucede con otros esquemas de certificación de identidad, se proporcionan varias soluciones destinadas a permitir la autorrevocación de certificados digitales, lo cual permite agilizar el proceso de notificación de incidencias. Por otro lado, se ha introducido un sistema de validación de certificados basado en el refirmado de los mismos. Este último sistema está basado en la creación de sentencias positivas que permiten a cualquier aplicación validar el estado de un certificado en un instante dado sin tener que realizar ningún tipo de consulta externa ni conocer otras especificaciones en materia de validación. Además, se ha mostrado que, cuando el número de comprobaciones por usuario es elevado, el sistema ofrece mejor rendimiento que las propuestas basadas simplemente en OCSP.

Como ya se ha comentado en numerosas ocasiones, la PKI diseñada constituye el punto de partida del sistema de autorización, el mecanismo empleado para realizar la gestión de claves criptográficas y la generación de identificadores. Con el fin de definir el enfoque concreto de gestión de privilegios que se iba a seguir, se realizó un análisis exhaustivo de los distintos modelos de control de acceso surgidos en los últimos años. Fruto de dicho análisis, se determinó que tanto el control de acceso basado en roles (RBAC) como el modelo distribuido basado en delegación constituían las alternativas más apropiadas para el tipo de escenarios que se deseaba modelar, y que por tanto era necesario contrastar cuáles eran las posibilidades ofrecidas por las distintas especificaciones existentes en materia de certificados de credencial a la hora de implementar dichos modelos. La conclusión obtenida situaba a la especificación SPKI como las más acertada debido, entre otros factores, a su riqueza expresiva, su capacidad para absorber los modelos RBAC, la posibilidad de emplear delegación, la provisión de métodos genéricos de cálculo de autorizaciones y la existencia de implementaciones completas de la especificación.

Si bien hay gran multitud de propuestas que hacen uso de este tipo de certificados a la hora de implementar escenarios de aplicación concretos, la mayoría de estas iniciativas carecen de un sistema genérico de gestión de los certificados. Para subsanar esta carencia, se ha presentado el sistema DCMS, el cual proporciona un tratamiento completo a todas las cuestiones relacionadas con certificación de privilegios. Las principales conclusiones que podemos extraer a partir del diseño de DCMS son:

- El problema queda claramente dividido en 3 bloques conceptuales distintos: gestión de la pertenencia a roles y su jerarquía, gestión de la asignación de privilegios a entidades finales o conjuntos de entidades, y gestión de la reducción de autorizaciones. Esta división permite ver el sistema como una composición de subsistemas, los cuales pueden ser empleados de forma aislada dependiendo de las necesidades de autorización del escenario a modelar.

- Su diseño totalmente descentralizado, basado en delegación, permite adaptarlo correctamente a escenarios en los que la gestión de los privilegios se realiza por parte de entidades con escasa conexión entre sí.

- Se han definido todas las estructuras de datos necesarias para llevar a cabo el proceso completo de generación de credenciales. Por un lado, se ha especificado el formato de las solicitudes de nombramiento, autorización y reducción. Por otra parte, se ha definido el formato que deben tener las políticas de seguridad de las distintas autoridades participantes. Tanto el formato de las solicitudes como de las políticas está basado en s-expresiones, sin que haya necesidad de introducir nuevos formatos de codificación distintos a los empleados por los controladores a la hora de proteger sus recursos.

- Mediante las políticas de autorización es posible especificar conjuntos, posiblemente infinitos, de privilegios que pueden ser asociados a las entidades del sistema sin necesidad de tener que emitir los certificados previamente. El hecho de que la emisión se realice bajo demanda permite solventar algunos de los problemas de escalabilidad presentes en escenarios complejos.

- El mecanismo de reducción automática de certificados, junto con el uso de claves temporales, permite eliminar el enlace que pudiera existir entre la identidad de un usuario y sus privilegios. De esta forma, en escenarios en los que el anonimato está permitido o es un requisito, es posible ocultar la relación existente entre los certificados generados por la PKI y los del sistema DCMS. Adicionalmente, el servicio de reducción introduce mejoras en la eficiencia del tratamiento global de las autorizaciones ya que permite simplificar cadenas largas de certificación.

Las comunicaciones entre las entidades de DCMS se han basado en otra de las aportaciones principales de este trabajo de tesis, el marco AMBAR de intercambio de información relativa a autorización. Este marco fue diseñado para suplir la falta de soporte de certificados de credencial en los actuales protocolos de seguridad, lo cual implicaba que la responsabilidad de la transmisión de las solicitudes, políticas y credenciales debía recaer completamente en las aplicaciones finales. Mediante un diseño modular y estructurado, el marco aporta mecanismos de negociación de parámetros de autorización que le permiten adaptarse a distintos entornos, técnicas de optimización de solicitudes basadas en el establecimiento de sesiones, medidas para proteger la confidencialidad de la información que se está transmitiendo y una interfaz de programación que permite ocultar al desarrollador de aplicaciones muchos de los detalles de funcionamiento interno que le son irrelevantes.

Finalmente, dado que la puesta en marcha de un sistema de control de acceso basado en roles y delegación requiere una identificación muy concisa de los elementos participantes y de la relación entre ellos, la especificación de la metodología de definición de estructuras de gestión permitió averiguar que:

- La metodología ofrece un enfoque estructurado para resolver el problema de la puesta en marcha de un sistema basado en autorización. Se presentan conjuntos de

procedimientos específicos tanto para la gestión de pertenencia a roles como para la asignación de privilegios.

- Los procedimientos de la metodología se estructuran en niveles de gestión que tienen una relación directa con los mecanismos ofrecidos por el sistema DCMS, y más concretamente por las aplicaciones que conforman dicho sistema.

- Se distingue claramente entre las políticas de emisión de credenciales, también denominadas políticas de autorización y de nombramiento, y las políticas relacionadas con el reflejo de las estructuras de gestión en los puntos de acceso. En consecuencia, no sólo se proporcionan los medios para especificar el comportamiento de las autoridades sino que también es posible plasmar cuál va a ser la dinámica del sistema, es decir, cómo se van a producir las relaciones entre los distintos elementos participantes.

- Tanto la metodología como la infraestructura de autorización han sido aplicadas con éxito a escenarios concretos de aplicación. Esto ha permitido conocer la adecuación de estas dos propuestas a la hora de modelar dos entornos de autorización tan diversos como el control de acceso físico y la suscripción electrónica. Además, se ha mostrado cómo el uso de credenciales aporta ventajas adicionales respecto a la adopción de enfoques de carácter más centralizado.

Como conclusión global, es posible afirmar que el trabajo aquí presentado constituye un paso importante hacia la utilización de la certificación digital como herramienta fundamental en el diseño de servicios de autenticación y autorización. La composición de la PKI y de la infraestructura de autorización demuestra que la extensión y la mejora de tecnologías ya consolidadas mediante nuevos enfoques tecnológicos da lugar a la creación de nuevos modelos de gestión de sistemas distribuidos, los cuales se ajustan mejor al marco tecnológico actual.

7.2 Líneas futuras

Las aportaciones realizadas en el presente trabajo abren varias líneas futuras de actuación destinadas tanto a la extensión de las soluciones propuestas como a su integración en otros escenarios. Esto es especialmente importante en el campo de la certificación de privilegios, el cual presenta un gran abanico de posibilidades y desafíos que pueden ser resueltos.

En lo que respecta a la extensión de las soluciones aquí presentadas, algunas líneas de investigación futuras son:

- Analizar la problemática de la revocación de privilegios con el fin de dotar a las especificaciones actuales de certificados de credencial de las herramientas necesarias para poder llevar a cabo dicho proceso con las máximas garantías de seguridad y disponibilidad. Los esfuerzos realizados hasta el momento simplemente han intentado extrapolar las soluciones aplicadas en el campo de la identidad digital. Sin embargo,

la revocación de autorizaciones posee sus propias particularidades en lo que respecta a delegación, invalidación y propagación. Consecuencia de este análisis sería la integración en DCMS de un servicio de revocación de certificados SPKI.

- Estudiar lenguajes alternativos de especificación de políticas de autorización con el fin de poder modelar de forma más precisa tanto los requisitos impuestos por los controladores de recursos como por las autoridades. Por ejemplo, la notación basada en las s-expresiones SPKI podría extenderse para reflejar un conjunto más rico de condicionantes.

- Proporcionar al sistema DCMS de un mecanismo de almacenamiento y distribución de credenciales que satisfaga los requisitos de confidencialidad, disponibilidad y eficiencia vistos en la sección 4.4.4.

- Proporcionar implementaciones alternativas del marco AMBAR que sean independientes del mecanismo de transporte, por ejemplo haciendo uso de XML como lenguaje de especificación.

- Extender la metodología de autorización de forma que pueda reflejar los procedimientos necesarios para construir sistemas de control de acceso más complejos, como por ejemplo los basados en los modelos $RBAC_2$ y $RBAC_3$.

Adicionalmente, es importante recalcar la importancia de futuras líneas de actuación que tengan como objetivo tanto la comparación de las aportaciones realizadas respecto a los nuevos modelos que puedan ir surgiendo como su integración en otros escenarios de aplicación. En este sentido, se pueden identificar las siguientes vías:

- Revisión y comparación de los modelos propuestos por la ITU-T en relación con las infraestructuras de gestión de privilegios (PMI). El objetivo de esta línea es contrastar las posibilidades ofrecidas por la nueva versión del estándar X.509 respecto a la especificación SPKI. Para ello, sería necesario modelar un mismo sistema mediante ambas técnicas con el fin de extraer conclusiones a partir de los resultados obtenidos.

- Integración de la infraestructura de autorización en escenarios de acceso a recursos gestionados por controladores ampliamente distribuidos y con políticas de autorización específicas. Evaluar los resultados que pueden obtenerse de la aplicación en entornos de comercio electrónico inteligente (basado en agentes) o sistemas de computación distribuida basados en la composición de componentes software.

- Otra línea de investigación ya iniciada es la relacionada con el control de acceso a redes públicas, especialmente redes inalámbricas. Mediante este entorno, se pretende evaluar las ventajas que introducen las propuestas aquí realizadas a la hora de gestionar un aspecto tan de actualidad como es la movilidad. El objetivo principal será determinar los modelos de autorización que mejor satisfacen los requisitos relacionados con el uso de la red por parte de usuarios no habituales.

- Finalmente, y aprovechando los trabajos ya realizados por otros miembros del grupo de investigación, se está trabajando en la definición de un sistema de políticas de seguridad enfocado a la gestión de servicios telemáticos, como por ejemplo el establecimiento de redes privadas virtuales. La introducción del mecanismo de autorización tiene como finalidad mejorar el proceso de creación, actualización y revocación de políticas que llevan a cabo los administradores de los servicios.

En resumen, las aportaciones realizadas por este trabajo constituyen un punto de partida sólido que permitirá la definición de nuevas líneas de trabajo en la construcción de sistemas distribuidos. La extensión de los servicios de seguridad obtenidos como resultado de esta tesis representa el punto de partida de trabajos posteriores que forman parte del mañana más cercano.