



DIGITAL CERTIFICATES

Applied Internet Security

Autores: Jalal Feghhi, Jalil Feghhi y Peter Williams
Editorial: Addison-Wesley - 1998 - 453 páginas
ISBN: 0-201-30980-7 - Incluye CD-ROM
http://www.diazdesantos.es

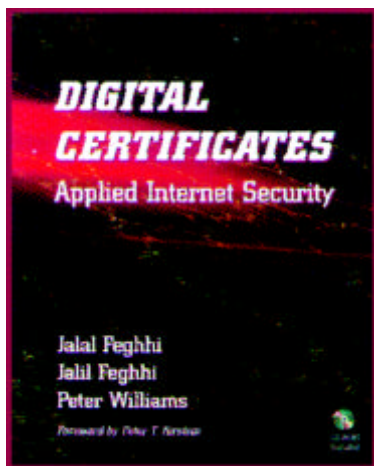
Por sus aplicaciones, más numerosas día a día, y soluciones que ofrecen a múltiples problemas de seguridad, no es razonable dudar que las tecnologías basadas en el mecanismo de cifrado de clave pública, y los protocolos de seguridad fundados en los certificados digitales, están destinados a ocupar una posición focal en la seguridad de las redes de ordenadores, Internet, Extranet, Intranet o simplemente RAL.

Algunas de estas aplicaciones tuvieron ya cumplido tratamiento en algunos libros aquí reseñados anteriormente. Es el caso del comercio elec-

trónico, inmejorablemente contemplado en el libro *Secure Electronic Commerce* (véase el número 32, de noviembre de 1998, de esta revista), que, como en su momento se vaticinó, ha devenido en un a modo de biblia del tema. Sin embargo, los usos de la clave pública, sus certificados y las Infraestructuras del mismo nombre, en adelante PKI (*Public Key Infrastructures*), lejos de inscribirse en el mundo del comercio, alcanzan en el presente aspectos tales como la mensajería electrónica segura, la autenticación de clientes y servidores, el control de acceso a Web y una numerosa estela de otras funciones que se ven incrementados día a día.

Por ello, parecía oportuna la recensión de alguna obra que tratase todas estas aplicaciones sin enfocarse en ninguna en particular, habiéndose elegido por su rigurosa y completa exposición el libro editado por Addison-Wesley, y publicado el pasado año 1999, **DIGITAL CERTIFICATES: Applied Internet Security**, cuyos autores son tres reputados expertos en certificados digitales (dos de ellos trabajando en Verisign): Jalal Feghhi, Jalil Feghhi y Peter Williams.

La obra se presenta en un amplio volumen de más de 450 páginas –y el añadido de un CD-ROM–, donde se recorre con mayor o menor pormenorización las ramificaciones de las tecnologías antedichas. Se estructura, muy atinadamente, en seis partes bien diferenciadas, cada una de ellas articulada en capítulos donde se han capturado numerosas y oportunas pantallas de Netscape y Explorer que ejemplifican los conceptos explicados. Todos estos capítulos concluyen con un resumen donde se sintetiza con precisión y escuetamente lo tratado, y una bibliografía acertada, aunque a menudo sucinta al menos para los manuales al uso. Así mismo, el estilo es claro y directo, lo que junto con las figuras e imágenes de pantallas –ya citadas– contribuyen a una lectura fácil y amena. Finalmente, cabe apostillar un logro más, no por último menos reseñable: el abundante muestrario de productos comerciales que ilustran los temas estudiados, que sin duda lo convertirá en una



obra de obligada referencia para todos aquellos que en el próximo futuro se vean involucrados en la implantación de soluciones de seguridad basadas en las tecnologías repetidamente mencionadas.

La primera de las partes citadas: *Security, Criptografía, and Digital Certificates*, explora sucintamente los principios de las comunicaciones en Internet y su protección, los fundamentos matemáticos de la criptografía, los tipos de cifradores y sus vulnerabilidades, para terminar con el capítulo más interesante de éstos –pues es de suponer al lector suficien-

temente familiarizado con los anteriores conceptos– *Digital Certificates, Certification Authorities, and Public-Key Infrastructures*, en el que se exponen el formato de los certificados –X.509 v.3– las funciones de la Autoridades de Certificación¹ (AC en adelante) y sus posibles conformaciones para conseguir el reconocimiento de sus certificados.

La segunda parte, de título *Applied Internet Security* y desglosada en cuatro capítulos, se detiene en el uso de los certificados en Internet. Así, se muestran en el capítulo cuarto los riesgos de la navegación por servidores Web desconocidos, y cómo protegerse frente a ello. Especial interés presenta la última sección, donde se estudia los sistemas de autenticación de *software* descargado de la red, centrándose en Microsoft Authenticode. El capítulo siguiente se enfoca a la mensajería segura, apoyándose en S/MIME y su empleo en Microsoft Outlook Express y Netscape Messenger. El capítulo VI se dedica a la seguridad de los servidores Web, incluyendo también un repaso trivial a los cortafuegos y *proxies*. Para concluir, el séptimo –que requiere de una lectura más reposada que todos los precedentes– expone todo un surtido de estándares de uso habitual en las PKI, singularmente los PKCS#7 y PKCS#10.

En la tercera parte, bajo el epígrafe *Security Management Practices*, se tratan diversos modelos de gestión de la seguridad en entornos corporativos usando PKI. Así, en el capítulo octavo se establece el marco de dicha gestión, ejemplificándose con diferentes productos comerciales de AC y PKI, mientras que en el noveno destaca la muestra de suministradores comerciales de servicios de certificación, y el décimo se consagra a las Autoridades Locales de Registro (o simplemente Autoridades de Registro, en adelante AR): su misión, funciones y, nuevamente, productos en el mercado que las instrumentan.

La parte cuarta, *The Trust Dilemma*, la más vaporosa de todas –como acontece siempre con los capítulos que se paran en los aspectos de gestión-

pero no menos interesante por ello, se concentra en cómo conseguir confianza en las PKI y los servicios que prestan. Con este objetivo, se estudian las políticas y prácticas a seguir en la emisión de certificados, capítulo undécimo, la distribución fiable de claves y las redes confiables, capítulo duodécimo, y en el siguiente –y último de esta parte–, la gestión de la seguridad de los ordenadores: Políticas de seguridad, acreditación de instalaciones, y centros de proceso de datos y dispositivos criptográficos fiables.

La siguiente, de nombre *Web Security and Certificates*, se conforma en dos capítulos, en el primero de los cuales se trata de cómo establecer un servidor Web seguro usando SSL, para a renglón seguido exponer tres posibles soluciones a la emisión del certificado del servidor: mediante el auxilio de una AC de confianza (no casualmente, dada la procedencia de dos de los autores, Verisign), a través de una AR (nuevamente Verisign's OnSite) o mediante un servidor de certificados propio (tomando como paradigma Microsoft Server Certificate), obviamente solución sólo válida en entornos de Intranet. El segundo capítulo, el décimoquinto de la obra, enfoca al otro extremo: el cliente, analizando la autenticación de éste, la obtención de certificados por el mismo y el uso de SSL. En resumen, una parte de general interés, dado lo generalizado –y mucho más en el inmediato porvenir– de los accesos a servidores seguros.

Para concluir, la parte sexta: *Microsoft Certificates Server*, se expone en ahondar conceptos, mecanismos, diseños, etc. abordados anteriormente, descendiendo a detalles de gran concreción y tomando como banco de ensayo el servidor de certificados de la marca citada. Para ello se estructura en cinco capítulos –del décimosexto al vigésimo– en los que se examina los componentes internos (la arquitectura), la programación de la política propia de seguridad (si se encuentra inadecuada la prevista en el *Policy Module*), la programación del módulo de salida (emisión, revocación de certificados, publicación de CRL, etc.), la programación del módulo de entrada (recepción de peticiones de certificados, recuperación de éstos, etc.), y la funciones de administración del servidor. Obviamente todo ello referido al correspondiente *software* de Microsoft.

El manual concluye con cuatro apéndices, dos acerca de la omnipresente notación ASN.1 y la estructuración de certificados X.509 para su uso con productos de Microsoft, respectivamente, y los restantes sobre el reglamento de certificación de Verisign y el punto de vista de ésta en la antinomia AR, servidores de certificados corporativos.

En resumen, nos encontramos ante una excelente y extensa obra, que será en lo sucesivo de referencia para los consultores o responsables de seguridad a los que sus empresas les enfrenten al reto de construir una PKI o asegurar sus conexiones a Internet mediante soluciones de clave pública. ■

¹ Denominados en la Directiva comunitaria, y en su correspondiente transposición a la legislación española –Real Decreto-ley 14/98 sobre firma electrónica–, Proveedores de Servicios de Certificación.

ARTURO RIBAGORDA
 Catedrático de la Universidad
 Carlos III de Madrid