



Tarjetas inteligentes

Autores: Juan Domingo Sandoval, Ricardo Breito y Juan Carlos Mayor

Editorial: Paraninfo - 1999 - 212 páginas

ISBN: 84-283-2602-9

Correo-e: itesparaninfo.pedidos@mad.servicom.es

De todos los dispositivos de seguridad con que la técnica nos depara, sin duda el más versátil (por sus múltiples aplicaciones), sencillo (por su fácil manejo), portable (por su escaso peso y volumen) y económico es la tarjeta, concretamente la adjetivada como inteligente. Usada originalmente -en el ámbito de la seguridad- como instrumento de autenticación y control de accesos físicos, devino posteriormente en un depósito de claves de cifrado y firma digital (clave privada del usuario) y, ya hoy en día, en el medio más prometededor de ejecución de la firma digital, lo que la hará transformarse en poco tiempo en el correlato de la pluma o bolígrafo para la realización de la firma autógrafa. Prueba de ello, es la presencia creciente de lectores de tarjetas en los ordenadores personales, sean empresariales o domésticos, crecimiento, por cierto, que se verá acompañado con la paulatina extinción de los lectores de disquetes, relegados por Internet y por los dispositivos ópticos de almacenamiento de datos.

Lo primero a destacar en el libro que nos ocupa, es que la obra no trata sobre aquellos aspectos de seguridad que se han visto o se ven influenciados por las tarjetas, sino de estas últimas. No obstante lo cual, no parece estrambótica su reseña en esta sección, dada la importancia de las tarjetas en la seguridad de la información, lo que hace obligado para numerosos profesionales de esta materia el familiarizarse con estos instrumentos. Por esto último, debemos celebrar la publicación que ahora reseñamos, única en su género, al menos en lo que nos consta, en nuestra lengua.

La obra se extiende a lo largo de más de 200 páginas, y se estructura en 13 capítulos, más otro de Bibliografía y un último de Apéndices, en los cuales se exponen tanto los aspectos lógicos, físicos y del *hardware* de las tarjetas como de sus equipos lectores. Además, en ocasiones se estudian otros aspectos vinculados sólo tangencialmente con estas herramientas, como por ejemplo un capítulo dedicado a la criptografía (por cierto, el más extenso, con diferencia, de todos: 40 páginas frente al promedio de los restantes que se sitúa en torno a las 10) introducido a contrapelo, parecería que más con fines de relleno que por su necesidad para la comprensión de las tarjetas y su mundo.

En general la exposición es clara y concisa,



aunque en ocasiones, que en su momento se irán exponiendo, se trasluce una redacción apresurada que hace a algunos apartados (pocos, eso sí) de difícil lectura. Finalmente, también se debe reseñar que la ordenación de los capítulos, salvedad hecha de los cinco primeros, parece hecha sin motivo, y así no se encuentra razón aparente para la posición del dedicado a la criptografía, ni de los dedicados a los terminales lectores, etc.

Entrando ya en sus capítulos, el primero, **Tipos de tarjetas**, es una muy concisa (de escasas

5 páginas de texto y figuras), clara y oportunamente ilustrada introducción a estos instrumentos. El siguiente, **Características físicas y eléctricas de las tarjetas**, repasa las dimensiones normalizadas de los distintos tipos de tarjetas y las coordenadas de sus puntos de contacto eléctrico -también normalizadas o en trance de ello- y las tensiones de alimentación correspondientes. El capítulo tercero, **La comunicación entre la tarjeta y los dispositivos externos**, de mayor calado que los precedentes, expone el protocolo de transmisión más importante de los contemplados por ISO, con detalles propios de un manual de especificaciones, que harán la delicia de los interesados en la construcción de tarjetas. El cuarto, **El sistema operativo de las tarjetas inteligentes**, repasa los tipos y características de los ficheros presentes en las tarjetas, y es seguido del titulado **El juego de instrucciones**, en donde se estudia una selección de las órdenes recogidas en las normas internacionales. El tratamiento extremadamente sucinto -tan sólo siete páginas-, junto con una redacción a veces embarullada -singularmente en los dos últimos apartados- hacen de esta sección una de las menos afortunadas de la obra.

Si los cinco primeros capítulos glosados se centraban en las características genéricas de cualquier tarjeta, los siguientes contemplan el mundo en el que éstas se desenvuelven, desde los servicios y aplicaciones en los cuales desempeñan un papel activo, a sus equipos lectores y grabadores, pasando por las técnicas de cifra. Así, el sexto, **Tarjetas para pagos en cabinas de teléfonos**, estudia detenidamente este tipo muy generalizado de tarjetas y sus lectores, incluyendo un apartado, el sexto, donde el lector interesado y aficionado a la electrónica (alguno con motivos poco confesa-

bles) aprenderá a diseñar y fabricar sus propias tarjetas.

Los dos siguientes, séptimo y octavo, se consagran al diseño de terminales lectores y las características de los existentes en el mercado. En el primero, nuevamente nos encontramos con una exposición amplia y clara, ilustrada con oportunos gráficos, que debería permitir al lector aficionado la fabricación de su propio lector, mientras el segundo, **Terminales lectores existentes en el mercado**, describe algunos lectores y *kits* de desarrollo de aplicaciones disponibles comercialmente. Lamentablemente, los autores no valoran ni comparan los productos que comentan.

El capítulo siguiente, singular en el contexto del trabajo, lleva por título: **Criptografía aplicada a las tarjetas inteligentes**, y realiza un rápido repaso a esta disciplina (a pesar de que la extensión suponga el 20% de la total del libro) y sus fundamentos matemáticos, lo que constituye un esfuerzo desproporcionado, aunque muy loable, habida cuenta de los objetivos del libro. El discurso es clásico y su aportación más significativa es la síntesis realizada, que ha permitido comprimir en 40 páginas la disciplina citada (incluyendo los conceptos matemáticos imprescindibles, algunos algoritmos notables de clave secreta y privada, otros de funciones *hash*, ídem de firma digital, etc.). Por el contrario, adolece de una cierta imprecisión en algunas definiciones, particularmente en el apartado de Matemáticas básicas, debido sin duda a los apremios editoriales.

El capítulo diez, **Monedero electrónico**, se detiene más -a pesar de su nombre- en el dinero electrónico que en las tarjetas que lo instrumentan. En particular, el apartado 10.3, dedicado a este medio de cambio, es una amplia introducción al mismo, frente al cual el resto de los apartados -preocupados por aplicaciones comerciales o proyectos de investigación- tienen un menor valor. El siguiente, **Integración de las tarjetas en la plataforma Windows**, presenta con gran concisión (en menos de seis páginas) los trabajos para normalizar la interfaz entre los lectores de tarjetas y los sistemas basados en ordenadores personales. Aunque interesante para los neófitos, dado su magro contenido sólo tendrá, para los más, carácter meramente informativo.

También escasa sustancia presenta la sección que sigue dedicada, según su título, a las tarjetas en el ámbito GSM, aunque se expone más en este último que en aquellas. Finalmente, la última, **Proyecto de tarjeta inteligente ULL**, es una memoria de la implantación de la tarjeta inteligente en la Universidad de La Laguna, sirviendo por ello de ejemplo práctico para aquellos que piensen instalar en sus empresas un sistema de gestión basado en estos dispositivos.

En resumen, una obra interesante, sobre todo por carencia de similares en nuestra lengua, y que servirá de ilustración a los interesados en la seguridad y, por ende, en este dispositivo, la tarjeta inteligente o de circuito integrado, tan útil para la misma. ■

ARTURO RIBAGORDA

Catedrático de la Universidad Carlos III de Madrid