Tarjetas de Datos Sanitarios con Circuito Integrado (Tarjetas Inteligentes)

Manual para los Profesionales de la Salud

Área de Tecnología y Prestación de Servicios de Salud
Unidad de Organización de Servicios de Salud
Organización Panamericana de la Salud
Oficina Sanitaria Panamericana, Oficina Regional de la
Organización Mundial de la Salud
Washington, D.C.

Tarjetas de Datos Sanitarios con Circuito Integrado (Tarjetas Inteligentes)

Manual para los Profesionales de la Salud

Área de Tecnología y Prestación de Servicios de Salud
Unidad de Organización de Servicios de Salud
Organización Panamericana de la Salud
Oficina Sanitaria Panamericana, Oficina Regional de la
Organización Mundial de la Salud
Washington, D.C.

Mayo 2003

Biblioteca OPS – Catalogación en la fuente

Rienhoff, Otto
Tarjetas de datos sanitarios con circuito integrado (tarjetas inteligentes): manual para los profesionales de la salud
Washington, D.C.: OPS, © 2003. 118 páginas

ISBN 92 75 32463 8

I. Título II. Rodrigues, Roberto J. III. Piccolo, Ursula
IV. Hernández, Antonio V. Oliveri, Nora

1. INFORMÁTICA MÉDICA
2. SISTEMAS DE INFORMACION
3. PROCESAMIENTO AUTOMATIZADO DE DATOS
4. ALMACENAMIENTO Y RECUPERACION DE LA INFORMACION
5. PERSONAL DE SALUD

NLM WA26.5.R557t

ISBN 92 75 32463 8

Otto Rienhoff

Profesor de Informática Médica
Director del Departamento de Informática Médica y director del Centro de Computación Hospitalaria, Georg-August-University, Gotinga, Alemania

Colaboradores

Roberto J. Rodrigues

Profesor adjunto del Programa de Ciencia, Tecnología y Asuntos Internacionales de la Escuela de Relaciones Internacionales, Georgetown University, Washington, D.C.
Consultor, The Institute for Technical Cooperation in Health Inc. (INTECH), Potomac, MD, EE.UU.

Ursula Piccolo

Asistente de investigación del Departamento de Informática Médica
Georg-August-University, Gotinga, Alemania

Antonio Hernández

Asesor regional de ingeniería clínica y mantenimiento
Organización Panamericana de la Salud
Oficina Regional de la Organización Mundial de la Salud
Washington, D.C., EE.UU.

Nora Oliveri

Presidenta y directora general
Fundación de Informática Médica, Miami FL, EE.UU.

Agradecimientos

Los autores agradecen a los siguientes profesionales que colaboraron en la preparación de esta publicación

S.Y. Chang

P. Debold

H. Doaré

U. Sax

J. Sembritzki

P. Wenzlaff

S. Dessi

Contenido

Prólogo

El siglo pasado ha sido testigo de avances significativos en la situación de salud en las Américas, pero la región confronta nuevos y complejos retos. Los gobiernos y la sociedad civil en conjunto son concientes de la necesidad de reducir la brecha existente entre el acceso a los servicios y la calidad de la atención de salud. La mayor movilidad de los ciudadanos, internamente en los países e internacionalmente, el proceso de integración regional y los nuevos modelos de la organización de los servicios de la salud caracterizado por proveedores múltiples públicos-privados han subrayado la necesidad de proporcionar atención con calidad y basada en la evidencia, independientemente de la ubicación de los servicios y del proveedor. Al mismo tiempo, la dimensión internacional de la salud pública y sus vínculos con las situaciones nacionales y locales, así como las consideraciones éticas y de privacidad, exigen nuevas formas para registrar, mantener y acceder las historias y datos clínicos de los usuarios de los servicios.

La simplificación y reducción del flujo de papeles y expedientes médicos tradicionales mediante el uso de soluciones de tecnologías electrónicas ofrecen una oportunidad para mejorar la gestión de la información clínica y administrativa. Por su portabilidad, el uso de "las tarjetas inteligentes" por pacientes y proveedores, pueden ser una solución eficaz para algunos de los problemas enfrentados en la búsqueda del mejoramiento de los sistemas de salud, el aseguramiento del acceso geográfico, cultural y financiero a los servicios de salud y la ampliación de los mecanismos de protección social. La introducción de "las tarjetas inteligentes" es un paso importante en la implementación del modelo centrado en la persona en los registros de salud y ha estimulado a muchos grupos de investigación para abordar el tema de la estandarización de lo datos clínicos y expedientes médicos. Los beneficios derivados del uso de de esta tecnología ya se han demostrado en la Comunidad Europea.

La convergencia de varias tecnologías digitales, la mayor capacidad y velocidad de las computadoras y la ubicuidad de las telecomunicaciones, el procesamiento de datos y la transferencia de

telecomunicaciones, el procesamiento de datos y la transferencia de datos, han facilitado un despliegue generalizado de aplicaciones computarizadas de información en el sector de la salud de América Latina y el Caribe. Sin embargo, mucho queda por hacer mientras continúe existiendo una discrepancia entre el deseo manifiesto de cambio y la incorporación real de tecnologías de la información en el sector salud.

De acuerdo con los mandatos de las Cumbres de los Presidentes y Jefes de Estado y Gobierno, la Organización Panamericana de la Salud ha enfatizado la importancia de la cooperación técnica para fortalecer la capacidad sectorial e institucional y para garantizar autosuficiencia, autonomía, excelencia y sostenibilidad. Es en este contexto que este texto introductorio, dirigido a los profesionales de la salud de las Américas, se concibió y preparó bajo la dirección de Prof. Rienhoff, de la Universidad de Goettingen, Alemania, un experto en el área de las tarjetas de salud.

Mirta Roses Periago
Directora
Organización Panamericana de la Salud

Resumen Ejecutivo

El presente informe resume quince años de la evolución internacional, el estado actual y las tendencias en la tecnología, y la utilización de dispositivos portátiles en formato de tarjeta para el almacenamiento y el transporte de datos sanitarios clínicos y administrativos.

El informe se centra en las tarjetas de datos "inteligentes", el dispositivo que más éxito ha tenido. Una "tarjeta inteligente" o "tarjeta chip" es un dispositivo de plástico del tamaño de una tarjeta de crédito al que se ha incorporado uno o varios chips semiconductores de circuito integrado (CI). Los chips CI almacenan y transfieren datos entre los usuarios de tarjetas. Los datos están relacionados con un valor monetario o clase de información, o ambos, y se almacenan y procesan en tipos específicos de tarjetas dentro del chip de circuito integrado, en la memoria de lectura-escritura o en el microprocesador de la tarjeta. Los datos de la tarjeta se transfieren mediante un lector de tarjeta, un dispositivo periférico conectado a un sistema informático independiente o en red. En la presente publicación se analizan varias cuestiones afines, como la relación de las tarjetas de datos con las redes de comunicación de datos, la identificación biométrica, la comunicación móvil, las cuestiones relativas a las aplicaciones así como los aspectos legales y la reglamentación relacionados.

Las tarjetas inteligentes aumentan sensiblemente la comodidad y la seguridad en cualquier transacción ya que proporcionan almacenamiento resistente a manipulaciones indebidas de la identidad, del registro del usuario y de los datos personales. Las tarjetas inteligentes pueden ser el módulo central en el control de la seguridad de sistemas en el intercambio de los datos distribuidos por la totalidad de cualquier tipo de red de comunicación electrónica. Las tarjetas protegen contra una amplia gama de amenazas a la seguridad, desde la custodia descuidada de contraseñas de usuarios hasta los sofisticados intentos de acceder ilegalmente a los datos almacenados. Las tarjetas de funciones múltiples pueden, además de servir de dispositivos de

acceso al sistema en red y usarse eficazmente para almacenar valor monetario y datos relativos a aplicaciones independientes.

El potencial de las soluciones inteligentes e innovadoras basadas en tarjetas se manifiesta mediante la multitud de aplicaciones fiables y seguras que pueden ejecutarse en una única tarjeta: identificación, series de datos, pagos, reservas, autenticación así como el acceso lógico y físico a sistemas de información, aplicaciones, bases de datos y servicios.

En la actualidad, las tarjetas inteligentes se están empleando con éxito para almacenar expedientes médicos de pacientes. La mayoría de las implantaciones de tarjetas inteligentes de salud se llevan a cabo en Europa, donde la tecnología ha logrado mayor desarrollo y aceptación. A los primeros proyectos de tarjetas de datos sanitarios iniciados a mediados de la década de 1980 les siguieron implantaciones y proyectos piloto de diversos alcances y envergadura en muchos países y entornos organizacionales. Varios países han implantado sistemas de tarjeta con diferentes niveles de éxito y continuidad. Desde entonces se han puesto en marcha proyectos de tarjetas de salud de diferentes tipos a nivel nacional, regional, o provincial con la inclusión de funciones que abarcan varias áreas sociales. Las tarjetas también han sido adoptadas ampliamente por el sector sanitario privado, diversas aseguradoras y numerosos programas industriales y municipales de higiene del trabajo.

El desarrollo técnico innovador de las tarjetas de datos y su vinculación a redes sanitarias están avanzando rápidamente. Aunque son escasos, los estudios sobre la repercusión económica realizados hasta la fecha han puesto de manifiesto los resultados positivos obtenidos en diferentes proyectos de implantación de tarjetas de datos sanitarios; los informes más espectaculares hacen referencia a la primera generación de tarjetas inteligentes puesta en circulación en Alemania a mediados de la década de 1990. El costo de implantación de estas primeras tarjetas se recuperó al cabo de dos años gracias al ahorro devengado en los gastos de administración del sistema del seguro. Se prevén resultados similares para la introducción en Alemania de un sistema de prescripción electrónica que a fecha de hoy (2003) se encuentra en fase de planificación. Se espera que los rendimientos económicos de otros proyectos de tarjetas y aquellos relacionados con

la implantación de la infraestructura de seguridad profesional basada en un modelo de tarjeta mucho más complejo (tarjetas de profesionales de la salud) produzcan resultados igualmente positivos de las inversiones.

Las tarjetas de datos deben considerarse como sólo un elemento de un proceso continuo de tecnologías de la información y la comunicación (TIC) que vayan a desplegarse en el contexto de una infraestructura o arquitectura nacional de informática de salud. Un examen completo de las experiencias comunicadas durante una reunión de trabajo celebrada en 1994 en Atenas y un análisis minucioso del Maryland Blue Cross Project realizado en 1996, pusieron de relieve que la implantación de tarjetas de datos sanitarios requiere contar con la existencia de varios requisitos indispensables para desplegar y usar con éxito la tecnología. Dadas sus especiales consecuencias, las tarjetas de datos deben considerarse en el contexto de una infraestructura general de sistemas de información para la salud y no pueden introducirse simple y económicamente como una solución independiente o aislada.

Cientos de proyectos pequeños de tarjetas de datos sanitarios no pudieron materializarse o fueron incapaces de superar las etapas iniciales en gran parte debido a que hicieron caso omiso de las lecciones aportadas por experiencias anteriores y de la condición de disponer de los requisitos indispensables antes referidos. A nivel nacional, el fracaso más sorprendente fue el ambicioso proyecto estadounidense de tarjeta de salud propuesto durante el gobierno de Clinton y nunca puesto en práctica.Más recientemente, hemos asistido a otro fracaso, esta vez en los Países Bajos, de un proyecto que no pudo sobrevivir a la fase piloto inicial, lo cual ha servido para subrayar la complejidad de tales proyectos y las dificultades existentes para alcanzar el uso generalizado.

Las tarjetas de datos sanitarios también han desencadenado intensos debates sobre la protección de datos, la privacidad, los derechos de los pacientes y las cuestiones relacionadas con el acceso a los datos personales, y los flujos de datos transfronterizos. Estos debates éticos, reglamentarios y legales se ven intensificados por la gran disparidad de mecanismos determinantes relacionados con la manera en que las diferentes sociedades regulan y perciben éticamente los datos. Además, antes de que se puedan implantar a nivel nacional

los sistemas de tarjetas con datos personales, se deben discutir, acordar y consolidar las definiciones relacionadas con la salud y las especificaciones tecnológicas de cuestiones éticas, reglamentarias y legales.

Las tarjetas forman parte de una infraestructura de tecnología de la información de atención sanitaria que va cambiando progresivamente. Los nuevos proyectos de tarjetas de datos sanitarios deben tener en cuenta las enseñanzas extraídas de las iniciativas desarrolladas en los últimos quince años y deben mirar al futuro analizando la variedad de las opciones tecnológicas del presente. Sin embargo, el éxito sólo podrá alcanzarse si se analizan de manera equilibrada ambas perspectivas, las experiencias anteriores y las oportunidades actuales, asociadas con el establecimiento de un entorno de proyecto que haga hincapié en el consenso entre los interesados directos, la normalización y la sostenibilidad financiera.

El futuro de la tecnología de tarjetas inteligentes en el ámbito de la salud se presenta prometedor. Existen probabilidades de que el despliegue de aplicaciones, las funcionalidades y la interactividad con aplicaciones relacionadas con otros sectores sociales aumenten en los subsectores sanitarios privado y público. Se prevé que las aplicaciones gubernamentales públicas centrales y federales se materialicen más lentamente que las aplicaciones locales, estatales y provinciales debido a los requisitos y las características diversos de los servicios que cada aplicación proporciona. En términos generales, los servicios gubernamentales centrales y federales tienden a demandar mayores niveles de seguridad, son más sensibles a las cuestiones de privacidad y son mucho más complejos y costosos de prestar. No obstante, los servicios gubernamentales centrales y federales parecen ser los que más necesidad tienen de las funcionalidades que proporciona la tecnología de tarjetas inteligentes.

La experiencia acumulada en el último decenio y medio recomienda que a la hora de diseñar, realizar y aplicar iniciativas de tarjetas de datos sanitarios, es necesario tener en cuenta los siguientes aspectos:

- Comparadas con los dispositivos de transmisión de datos convencionales como las tarjetas de banda magnética, las tarjetas inteligentes ofrecen una mayor seguridad y comodidad junto con ventajas económicas. Además, los sistemas de tarjetas inteligentes son sumamente configurables y permiten la adaptación a las necesidades individuales. Por último, la capacidad multifuncional que reúne en un mismo dispositivo funciones como almacenamiento, pago, aplicación e interconexión de redes, convierte a las tarjetas inteligentes en el interfaz perfecto para usuarios en una economía móvil e interconectada.

- Todo proyecto de tecnología de información y comunicación de la salud debe procurar la obtención de mejoras de la calidad en los procesos de atención sanitaria, una mayor eficacia y eficiencia de las operaciones y la atención individual, y certeza de rendimiento de la inversión.

- En cada implantación que se lleve a cabo, deben efectuarse los análisis detallados del volumen de trabajo y el estudio de viabilidad que analice los resultados esperados, las suposiciones y los riesgos, en estrecha cooperación con ciudadanos, pacientes, asociaciones profesionales, instituciones participantes, organismos reguladores, fuentes de financiamiento y profesionales de la salud.

- Las soluciones basadas en tarjetas inteligentes nunca deben considerarse como productos "listos para uso". Las tarjetas y las redes electrónicas son dos componentes de la misma idea por lo que ambas tecnologías deben ir de la mano. En concreto, las tarjetas de pacientes son más un elemento de una infraestructura de tecnologías de información y comunicación (TIC) integradas en el ámbito de la salud; el éxito de los proyectos depende de la matización de los objetivos, los recursos del proyecto, las funcionalidades, la interoperabilidad y las interfaces entre el subsistema de la tarjeta, los sistemas de información sanitaria y el sistema de salud en el que se emplearán las aplicaciones de tarjetas.

- Las implantaciones deben utilizar, en la medida de lo posible, los patrones técnicos, de interfaz y de interoperabilidad debidamente probados y que se hayan empleado íntegramente en las iniciativas exitosas. Existen numerosas publicaciones sobre las lecciones extraídas de los proyectos anteriores y los nuevos proyectos deben basarse en la evaluación y las pruebas de tales experiencias y no solamente en documentos unidimensionales de naturaleza puramente política.

- Los sistemas de tarjeta se componen de una mezcla de tecnologías TIC, procesos organizacionales y de personas. La motivación, la información y el adiestramiento son esenciales para manejar los nuevos volúmenes de trabajo controlados por tarjeta y cosechar todos los beneficios que puedan aportar.

- Cuánto más interoperables son estos sistemas, más complejos devienen los proyectos de tarjetas de datos. Esto no se debe a la tecnología de tarjeta *per se,* sino a la necesidad de crear un gran número de sistemas relacionados de aplicaciones médicas que sean interoperables.

- Aunque la experimentación es importante, debería limitarse a los proyectos de investigación desarrollados en un dominio cuidadosamente definido con variables de entorno bien controladas.

- A pesar de la recomendación de basarse en proyectos ya probados, hay que señalar que las tarjetas de datos, al igual que todas las demás áreas de aplicación de TIC, están en constante evolución. El ciclo vital de la tecnología digital y de telecomunicación es muy corto y, aunque casi siempre es difícil reconocer qué tecnología nueva va a sobrevivir, los proyectos deben intentar prever tales realizaciones en un plazo de 5 a 10 años y deben mirar imaginativamente más allá de las opciones tecnológicas actuales.

- Cuando las tarjetas de datos ya se estén empleando para la identificación personal, permisos de conducir de vehículos a motor, transacciones financieras o de créditos, etc., es conveniente investigar si tales implantaciones podrían compartirse con la planificada aplicación de salud siempre que se garantice la protección de datos al paciente y el proyecto siga siendo técnica y organizativamente controlable.

- La experiencia indica que la implantación de sistemas de tarjetas basados en el uso voluntario dan como resultado una utilización limitada y la imposibilidad de obtener todos los beneficios de la tecnología; la única manera de aprovechar tales ventajas es mediante el uso obligatorio. Esta estrategia puede entrar en conflicto con los temas relacionados la protección de datos personales y algunas cuestiones legales.

- La experiencia ha demostrado que los proyectos de tarjetas de datos sanitarios deben ser de considerable tamaño en orden a producir una repercusión significativa en un ambiente de TIC de salud determinado. Para crear y desplegar infraestructuras y aplicaciones de TIC de salud que funcionen óptimamente se necesita mucho tiempo, y una vez que son implantadas, ellas muestran una tendencia a continuar existiendo sin cambiar mucho y a oponerse a los realineamientos potencialmente desestabilizantes.

- Los proyectos de tarjetas de datos sanitarios requieren planificación financiera a largo plazo, una comprensión clara por parte de todos los interesados directos acerca de los costos de la inversión y de explotación previstos, las responsabilidades y el compromiso que cada participante en el proyecto debe asumir, y la concienciación de que en un plazo de tiempo relativamente corto puede ser necesario introducir actualizaciones o efectuar sustituciones de envergadura y de alto costo.

- Debido a la confidencialidad de los datos médicos y personales, la seguridad es un requisito indispensable para el despliegue de soluciones de tarjetas interoperables.

- Las tarjetas de datos que contienen datos médicos de pacientes requieren una infraestructura reguladora y legal que defina quién está autorizado a tener acceso a la información o a cambiarla (incluidos los derechos del paciente a acceder a datos personales y modificarlos).

- La implantación de infraestructuras de seguridad basadas en tarjetas de profesionales de la salud (TPS) y las infraestructuras de clave pública requieren gran cantidad de tiempo y recursos. Si no se dispone de estos, deben encontrarse otras soluciones alternativas de seguridad de datos que ofrezcan iguales garantías.

- Las soluciones transfronterizas (entre países, estados, provincias) son difíciles de aplicar y hacer cumplir, especialmente en lo que se refiere a las normas de definición de datos, la seguridad y las cuestiones de acceso a datos personales. Sin embargo, a largo plazo ofrecen beneficios considerables a los ciudadanos.

- El número de expertos y empresas con conocimientos avanzados y experiencia en esta área es todavía limitado.

1. Sinopsis de la tecnología de tarjetas de datos

Una "tarjeta inteligente" o "tarjeta chip" es una tarjeta de plástico con uno o varios circuitos integrados (CI) incrustados que almacenan y transfieren datos entre usuarios (figura 1). Los chips semiconductores de tarjetas inteligentes pueden estar conectados a dispositivos de lectura externos, terminales especializadas, o diferentes tipos de computadoras a través de puntos de contacto físicos o mediante comunicación de proximidad sin contacto, a través de antenas de interferencia.

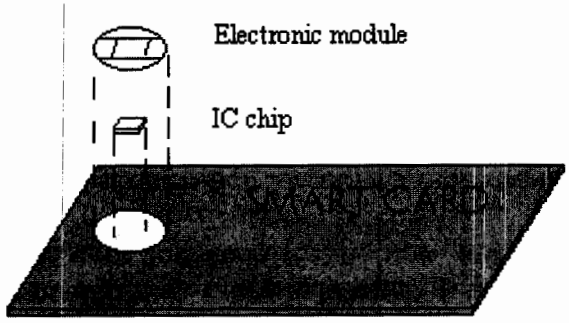

Figura 1. Una tarjeta inteligente ("smart card") es una tarjeta de plástico a la que se ha incorporado uno o varios chips de circuito integrado ("IC chip"). Según sea el tipo del chip o chips incrustados, las tarjetas inteligentes se clasifican en tarjetas de memoria, tarjetas con microprocesador, o con ambos tipos de chips.

Aunque cualquier tarjeta con circuito integrado incrustado puede denominarse tarjeta inteligente, la característica distintiva de una tarjeta inteligente es su uso para actividades personales. Por ejemplo, las tarjetas de ordenador personal del estándar conocido como PCMCIA (Personal Computer Memory Card International Association) tienen las mismas características tecnológicas que una tarjeta inteligente pero hacen las veces de dispositivos periféricos de ordenador tales como módems, dispositivos de almacenamiento o cartuchos de juegos. A estas tarjetas de PC nunca se las denomina tarjetas inteligentes ya que son dispositivos de extensión de hardware sin personalización. En este sentido, una tarjeta inteligente es una tarjeta dotada de un procesador que permite al usuario interactuar con otras personas digitalmente a fin de llevar a cabo transacciones y otras actividades relacionadas con datos personales.

Las tarjetas pueden tener sólo un chip de memoria o una combinación de chip de memoria y chip con microprocesador. Los datos asociados con un valor monetario, información, o ambos, se almacenan en los chips y, en el caso de tarjetas con microprocesador, se procesan dentro del chip. El chip microprocesador de una tarjeta es equivalente a la unidad central de procesamiento (UCP) de una microcomputadora y por consiguiente es capaz de realizar operaciones lógicas.

En las tarjetas con microprocesador, una parte del chip de memoria se usa para el almacenamiento de programas lo que permite que tales tarjetas puedan programarse transfiriendo algoritmos desarrollados apropiadamente a su área de memoria de sola lectura programable y borrable (EPROM o Erasable Programmable Read-Only Memory). Por lo general, los datos de la tarjeta de circuito integrado se transfieren a través de un lector que es un dispositivo periférico situado en un sistema de ordenador independiente o interconectado.

En 1979 la empresa francesa Bull lanzó la primera tarjeta operativa con microprocesador (tarjeta de dos chips). La Tarjeta CP8 albergaba un chip de memoria y un microprocesador provisto por Motorola (figura 2). El nuevo producto se basó en el monochip modelo 3870 y una EPROM (Memoria de Sólo Lectura Programable Borrable) modelo 2716 controlada a través de los puertos paralelos de entrada/salida del monochip. El ensamblaje se realizó según las nuevas

técnicas desarrolladas por Jacques Villières en la planta de Motorola en Toulouse.

Figura 2. La CP8 de Bull, la primera tarjeta comercial con microprocesador (1979).

A mediados de la década de 1990, se empezó a disponer de tarjetas que tenían hasta 2 KBytes (2.000 bytes o caracteres) de memoria de lectura y escritura y se registró un aumento repentino de proyectos en varios países. Desde entonces, la complejidad y la eficacia del diseño de tarjetas se han incrementado extraordinariamente. Hoy en

día las tarjetas pueden adaptarse a las necesidades de cada proyecto específico e incluso de procesadores determinados. Por ejemplo, en el caso de necesidades de criptografía avanzada pueden añadirse al sistema de circuitos de la tarjeta una serie de chips especiales. A continuación se exponen las ventajas más claras relacionadas con el uso de las tarjetas inteligentes con circuito integrado:

- En términos de identificación, las tarjetas inteligentes son más fiables que las tarjetas de banda magnética.
- Son capaces de almacenar bastante más información que las tarjetas de banda magnética.
- Son más difíciles de manipulación delictuosa que las grabaciones magnéticas.
- Pueden ser desechables o reutilizables.
- Pueden realizar múltiples funciones en una gama amplia de sectores.
- Pueden ser fácilmente compatibles con dispositivos electrónicos portátiles como teléfonos, asistentes digitales personales (PDA) y ordenadores personales.

1.1. Áreas de aplicación

Lanzadas primeramente en Europa hace dos decenios, las tarjetas inteligentes se introdujeron en el mercado como una herramienta de valor monetario almacenado para los teléfonos públicos con el propósito de reducir los robos de las monedas depositadas. En la actualidad los sistemas con tarjetas inteligentes se usan ampliamente en varias aplicaciones clave que abarcan sectores como la banca, el recreo y el transporte, y ya hay en uso miles de millones de tarjetas inteligentes. Europa occidental representa cerca del 70% del empleo actual de tarjetas inteligentes, seguida de América del Sur y Asia con cerca del 10% respectivamente, mientras América del Norte está a la cola con menos del 5%.

La mayoría de las tarjetas inteligentes expedidas son tarjetas de memoria con limitada capacidad de procesamiento. Alrededor del 75% de las tarjetas que se utilizan son tarjetas telefónicas. Muchos sectores han incorporado el potencial de las tarjetas inteligentes en productos tales como el Sistema Global para Comunicaciones Móviles (GSM), los teléfonos celulares digitales, los dispositivos del Servicio Radiofónico por Paquete (GPSR o General Packet Radio Service) y los descodificadores de televisión vía satélite. De un modo u otro, todas las aplicaciones pueden beneficiarse de las características y seguridad añadidas que proporcionan las tarjetas inteligentes.

En los Estados Unidos, a pesar de la escasa penetración, los consumidores han empleado las tarjetas con circuito integrado para todo tipo de actividades, desde la identificación segura, el control del acceso a instalaciones, operaciones bancarias, el préstamo bibliotecario, hasta la compra de productos alimenticios y entradas de cine. Varios estados tienen iniciativas de tarjetas chip en marcha para aplicaciones relacionadas con la administración como pueden ser el registro de vehículos a motor o la Transferencia Electrónica de Beneficios (EBT o Electronic Benedit Transfer).

Según Dataquest, el mercado mundial de tarjetas inteligentes alcanzó a finales de 2002 los 4,7 mil millones de unidades y los 6,8 mil millones de dólares de los Estados Unidos. Se incluyen los siguientes ejemplos de aplicaciones bien establecidas:

- Fidelidad y valor almacenado. Uno de los usos básicos de las tarjetas inteligentes es el valor monetario almacenado, en particular programas de fidelización que buscan y crean incentivos para generar clientes fieles. El valor almacenado resulta más cómodo y más seguro que el dinero en efectivo. Para los emisores de tarjetas, parte de la ganancia se genera a partir de los saldos no utilizados y los remanentes de saldos que nunca se usan. A los minoristas de cadenas de establecimientos que administran programas de fidelidad a través de muchos negocios y sistemas de puntos de venta (POS o Point of Sale), las tarjetas inteligentes les ayudan en la búsqueda

de datos. Las aplicaciones son numerosas y van desde el estacionamiento de vehículos y el servicio de lavandería hasta los juegos, sin olvidar todos los usos al por menor y en actividades de entretenimiento.

- Identificación y acceso. Numerosos negocios y organizaciones de todo tipo necesitan tarjetas de identidad sencillas para todos los empleados, trabajadores temporales, estudiantes, etc. A la mayoría de estas personas también se les concede acceso a determinados datos, equipo y departamentos según su posición. Las tarjetas inteligentes de funciones múltiples basadas en un microprocesador con y sin contacto (inalámbricas) incorporan la identidad junto con privilegios de acceso y también almacenan valor para ser utilizado en diversos establecimientos, como cafeterías y tiendas.

- Asegurar la información y el activo físico. Además de aportar seguridad de información, las tarjetas inteligentes pueden proporcionar seguridad física de alto nivel de servicios y equipo ya que la tarjeta restringe el acceso a todas las personas menos al usuario autorizado. El correo electrónico y las computadoras personales (PC) pueden bloquearse mediante una tarjeta inteligente, siendo la solución más discreta la tarjeta de proximidad sin contacto. Los sistemas de envío de información y programas de entretenimiento al hogar o al PC en forma de emisiones de vídeo digital están empleando tarjetas inteligentes que hacen las veces de claves electrónicas para asegurar la protección; controlan de este modo el desciframiento de las emisiones, el acceso de suscriptores individuales y la facturación por los servicios prestados. Las tarjetas inteligentes también pueden actuar como claves de acceso a espacios de maquinaria donde pueda haber equipo de laboratorio delicado y para los dispensadores automáticos de medicamentos, herramientas, tarjetas de biblioteca, equipo de gimnasio, etc.

- Caja de seguridad portátil. Las tarjetas inteligentes pueden funcionar como una especie de caja de seguridad para las claves de codificación y los algoritmos relacionados con las firmas digitales y la autenticación. Es más seguro llevar tales datos confidenciales en una tarjeta que en otros dispositivos portátiles como los ordenadores de bolsillo y los PDA.

- Cibercomercio. Las tarjetas inteligentes facilitan a los consumidores almacenar de manera segura información y dinero en efectivo para compras. Algunas de las ventajas son: la tarjeta puede incorporar una aplicación de contabilidad personal e información sobre el crédito y las preferencias de compra a la que se puede acceder con un simple clic del ratón en vez de rellenar formularios; las tarjetas pueden administrar y controlar los gastos con límites automáticos y notificación de los mismos; pueden utilizarse programas de fidelidad en Internet a través de múltiples vendedores con sistemas de punto de venta dispares; y pueden usarse como un depósito seguro donde almacenar puntos o premios y para efectuar "micropagos", es decir, para pagar gastos nominales sin tener que abonar las comisiones de transacción que normalmente se asocian a las tarjetas de crédito, o para cantidades demasiado pequeñas para pagarlas en efectivo o con tarjeta de crédito, como es el caso de los pagos en el uso de copiadoras.

- Finanzas personales. A medida que los bancos acceden a los nuevos mercados altamente competitivos que van surgiendo, como por ejemplo los corretajes de inversión, utilizan cada vez más diferentes aplicaciones destinadas a apoyar las transacciones seguras a través de tarjetas inteligentes. El resultado es un mejor servicio de clientes y la transferencia electrónica de fondos segura durante las 24 horas a través de Internet con costos reducidos ya que las transacciones que normalmente requerirían que un empleado de banca dedicase tiempo y trabajo

administrativo, pueden ser gestionadas electrónicamente por el cliente con una tarjeta inteligente.

- Atención de salud. El desarrollo experimentado por la práctica de salud multiprofesional y el crecimiento de los datos sobre atención sanitaria plantean nuevos retos con respecto al acceso a los datos generados por diferentes proveedores de asistencia sanitaria en muchos centros sanitarios y la importancia de integrar datos clínicos para aportar eficacia y eficiencia a la atención de pacientes al mismo tiempo en que hay la necesidad de proteger la privacidad en un entorno cada vez más interconectado. Las tarjetas inteligentes poseen el potencial para hacer frente a tales retos gracias a su capacidad para el almacenamiento seguro y la distribución de todo tipo de información, desde los datos de urgencias hasta la situación del paciente en cuanto a caracterización de derechos de asistencia y prestaciones, la identificación rápida de pacientes, la mejor atención, la comodidad de poder transferir datos entre sistemas o a centros sin sistemas, y la reducción de los costos de mantenimiento de registros.

- Trabajo a distancia y seguridad de la red empresarial. El uso de tarjetas inteligentes ayuda a mejorar las intranets B2B (Business to Business). Los usuarios pueden ser autenticados y autorizados para acceder a información específica con arreglo a ciertos privilegios predeterminados. Las aplicaciones complementarias incluyen el correo electrónico seguro y el comercio electrónico.

1.2. Tipos de tarjetas inteligentes (con circuito integrado incrustado)

Las tarjetas inteligentes se definen según el tipo de chip o chips con circuito integrado incrustados en la tarjeta y sus capacidades. Hay una gama amplia de opciones para elegir y mayores niveles de

capacidad de procesamiento, flexibilidad, funcionalidades de incremento de la memoria y obviamente de costos. Las tarjetas de función única son a menudo la solución más económica y se elige el tipo correcto de tarjeta inteligente para una aplicación específica haciendo una evaluación cuidadosa del costo frente a la funcionalidad y determinando el nivel de seguridad requerido (figura 3).

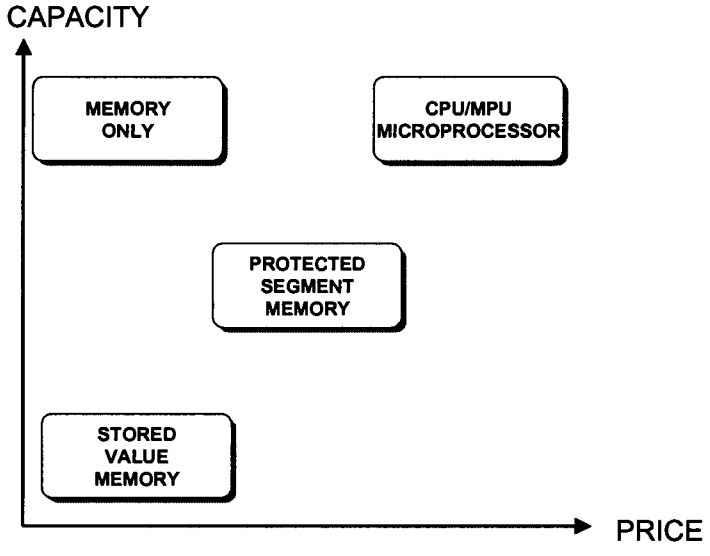

Figura 3. Funcionalidad y rendimiento de diferentes tecnologías de tarjeta con circuito integrado (CI). Capacidad y Precio de diferentes opciones en la arquitectura de los chips

Tarjetas de memoria

Las tarjetas de memoria no tienen capacidad de procesamiento o si lo tienen es de naturaleza poco compleja y también no pueden gestionar ficheros dinámicamente. Todos los chips de memoria se comunican con lectores mediante protocolos síncronos. Hay tres tipos básicos de tarjetas de memoria:

- Las tarjetas de memoria simple (Memory Only). Estas tarjetas sólo almacenan datos y no disponen de ninguna capacidad de procesamiento. Implican el menor costo por byte almacenado para la memoria de usuario. Deberían considerarse como discos flexibles de tamaños variados sin una función de seguridad. Estas tarjetas no pueden identificarse por sí mismas al lector, de manera que el sistema del servidor tiene que saber qué tipo de tarjeta está insertándose en un lector.

- Tarjetas de memoria segmentada protegida (Protected Segment Memory). Estas tarjetas tienen lógica incorporada para controlar el acceso a la memoria. A veces denominadas tarjetas de "memoria inteligente", son dispositivos que pueden ser ajustados para proteger contra escritura en parte o en toda el área de almacenamiento de memoria. Algunas de estas tarjetas pueden configurarse para restringir el acceso tanto a la lectura como a la escritura. Esto se hace generalmente mediante una contraseña o clave del sistema. Las tarjetas de memoria segmentada pueden dividirse en secciones lógicas si se desea obtener multifuncionalidad.

- Tarjetas de memoria de valor almacenado (Stored Value Memory). Estas tarjetas están diseñadas para la finalidad específica de almacenar valor monetario o fichas ("tokens"). Las tarjetas son desechables o recargables. La mayoría de las tarjetas de este tipo salen de fábrica con medidas de seguridad permanentes ya incorporadas. Estas medidas pueden incluir claves de contraseña y lógica que el fabricante coloca dentro del chip. Las matrices de memoria de estos dispositivos son configuradas como decrementos o contadores. Queda poca o ninguna memoria libre para otra función. Para las aplicaciones sencillas como es el caso de una tarjeta telefónica, el chip tiene 60 ó 12 celdas de memoria, una para cada unidad telefónica. Cada vez que se consume una unidad telefónica se despeja una celda de memoria. Una vez que todas las unidades de memoria se usan, la

tarjeta deja de tener utilidad y se desecha. Este proceso puede invertirse en el caso de las tarjetas recargables.

Tarjetas UCP/UMP de funciones múltiples con microprocesador

Estas tarjetas tienen incorporadas capacidades dinámicas de procesamiento de datos. Las tarjetas inteligentes de funciones múltiples asignan la memoria de la tarjeta a secciones independientes encargadas de una función o aplicación específica. Dentro de la tarjeta hay uno o varios microprocesadores o chips microcontroladores (Unidad Central de Procesamiento o Unidad Microprocesadora) que administran la asignación de memoria y el acceso al fichero interno. Este tipo de chip es similar a aquellos que se encuentran dentro de todas las computadoras personales, y cuando se incrusta en una tarjeta inteligente, gestiona los datos en estructuras de fichero organizadas, a través del Sistema Operativo de Tarjeta (COS o Card Operating System). A diferencia de otros sistemas operativos, este software controla el acceso a la memoria de usuario incorporada en la tarjeta.

Esta capacidad permite tener en la misma tarjeta funciones múltiples y aplicaciones diferentes, lo que posibilita a las empresas ofrecer y mantener una diversidad de "productos" a través de una única tarjeta. Un ejemplo de esta capacidad es una tarjeta de débito que también permite el acceso a un edificio de un campus universitario. Las aplicaciones que requieren un alto nivel de seguridad pueden tener a bordo un criptoprocesador específico responsable por el funcionamiento de rutinas de codificación.

Las tarjetas de funciones múltiples benefician a los emisores porque les permiten comercializar sus productos y servicios utilizando tecnología de transacción de vanguardia. En concreto, con esta tecnología se pueden efectuar actualizaciones de la información sin tener que sustituir la base de la tarjeta instalada, lo que ayuda a simplificar enormemente los cambios en el programa y a reducir los costos. Para el usuario de tarjetas, la multifunción equivale a mayor comodidad y seguridad, y en último término, a la concentración de múltiples tarjetas en unas cuantas que sirven para muchos fines.

1.3. Fundamentos de las comunicaciones por tarjetas, lectoras y terminales

El término "lectora" se usa para describir un elemento de hardware que comunica en forma de dispositivo periférico mediante interfaz con una computadora personal (PC) para la mayoría de sus requisitos de procesamiento. En cambio, una "terminal" es un dispositivo independiente de procesamiento de tarjetas. Tanto los lectores como las terminales leen y escriben en las tarjetas inteligentes. Las tarjetas pueden comunicarse con una lectora o terminal de manera independiente o combinada:

- Tarjetas inteligentes de contacto. La conexión se realiza cuando el lector o la terminal se pone en contacto con un área pequeña bañada en oro situada en la parte frontal de la tarjeta.

- Tarjetas inteligentes de proximidad o sin contacto. Estas tarjetas pueden establecer comunicación por frecuencia de radio (RF o Radio Frequency) mediante una antena, eliminando la necesidad de insertar y extraer la tarjeta en una lectora o terminal. Con una tarjeta sin contacto, lo único que se debe hacer es situarse cerca de una terminal inalámbrica especial, en este caso un "receptor", y la tarjeta empezará a comunicarse con este. Las tarjetas sin contacto pueden usarse en las aplicaciones en que la inserción y la extracción de tarjetas tal vez sean poco prácticas o en las que la velocidad sea importante. Algunos fabricantes están produciendo tarjetas que funcionan en ambas modalidades, con y sin contacto.

Ambas tecnologías presentan ventajas y desventajas. Mientras que las tarjetas de contacto tienen protocolos de transmisión y colocación de clavijas físicas internacionales estandarizados, las tarjetas de RF sin contacto todavía no son en general interoperables, aunque la solución MIFARE® de Philips, un producto comercial que cumple la normativa ISO 14443A, parece contar con una amplia aceptación y tiene una inmensa base instalada a nivel mundial. Esta plataforma ofrece una

amplia gama de tarjetas inteligentes sin contacto y circuitos integrados compatibles con lectoras de contacto, así como circuitos integrados de interfaz doble que proporcionan una conexión segura entre los mercados de tarjetas sin contacto y tarjetas de contacto.

Se espera que en un futuro no muy lejano, las funciones que todavía hoy están limitadas a las tarjetas de contacto, como por ejemplo las funciones de firma, también podrán realizarse con tarjetas sin contacto. Lo mismo puede decirse de las tarjetas con multiprocesador. Hace años sólo se podía incorporar un chip en las tarjetas; hoy en día una tarjeta puede albergar varios chips especializados. La tarjeta de datos con circuito integrado se está convirtiendo cada vez más en un diminuto sistema informático sumamente integrado y específicamente adaptado para cubrir necesidades funcionales bien definidas.

Los dispositivos lectores se presentan en muchos formatos y con una variedad amplia de capacidades. La manera más fácil de describir una lectora es utilizando el método que se emplea cuando se establece comunicación mediante interfaz con un PC. Las lectoras de tarjetas inteligentes están disponibles con conectores para comunicar por interfaz con el puerto serial RS232, el puerto USB, la ranura ("slot") PCMCIA, la ranura del disco flexible, el puerto paralelo, el puerto IRDA infrarrojo y los lectores de cuña del teclado. Otra diferenciación con respecto a los dispositivos lectores hace referencia a la inteligencia y las capacidades a bordo o la falta de estas. Existen grandes diferencias de precio y rendimiento entre un lector inteligente muy resistente que soporta una variedad amplia de protocolos de tarjeta y un lector de tarjeta de uso doméstico, que sólo trabaja con tarjetas microprocesadores y realiza todo el procesamiento de los datos en el PC. Las opciones existentes para las terminales son muy amplias y la mayoría de las unidades tienen sus propios sistemas operativos y herramientas de desarrollo de software. Generalmente, apoyan otras funciones como la lectura de bandas magnéticas, las funciones de módem y la impresión de transacciones.

Cada nuevo proyecto de tarjetas debe tener en cuenta las posibilidades tecnológicas existentes y futuras, y debe evaluarlas minuciosamente con arreglo a los objetivos y las necesidades del proyecto. Es evidente que los costos serán el factor determinante

principal a la hora de adoptar y desarrollar un modelo empresarial y que los costos de sistemas generales relacionados con las diferentes disposiciones de los componentes del sistema de tarjeta y su tecnología de interconexión son de importancia capital para decidirse por una u otra opción.

1.4. Normas

Al principio se dio cierto grado de conflicto entre el trabajo de normalización llevado a cabo por el Comité Europeo de Normalización (CEN), el organismo de normalización europeo, y la Organización Internacional de Normalización (ISO). La ISO comenzó a abordar los temas de normalización de informática médica y las tecnologías de información y telecomunicación mucho después que su equivalente europeo pero, poco después, ambos organismos iniciaron una estrecha colaboración y la ISO se hizo cargo de las principales actividades de elaboración de normas del CEN. Actualmente, ambas organizaciones están vinculadas a otras organizaciones y organismos afines nacionales dedicados al establecimiento de normas.

Numerosas organizaciones y grupos de investigación importantes han examinado e implantado normas para aplicaciones específicas. Algunos productos comerciales siguen usando normas patentadas pero hay una tendencia creciente hacia los sistemas abiertos y a ajustarse a las normas internacionales. Los sistemas abiertos para la interoperabilidad de tarjetas son aplicables en distintos niveles a la tarjeta misma, a las lectoras, las terminales de acceso, y a las redes y los propios sistemas de los emisores de tarjetas. Las organizaciones o grupos principales que actualmente se muestran activas en la normalización de tarjetas inteligentes son:

- Internacional Standards Organization (ISO). La Organización Internacional de Normalización Facilita la creación de normas voluntarias mediante un proceso de colaboración abierto a todas las partes interesadas. La ISO 7816 es la norma internacional para las tarjetas con circuito integrado que usan contactos eléctricos. Cualquiera que esté interesado en conocer las tarjetas

inteligentes desde una óptica técnica debe familiarizarse con dicha norma.

- U.S. National Institute of Standards and Technology (NIST). El Instituto Nacional de Normas y Tecnologías de los Estados Unidos publicó un documento denominado FIPS 140-1, "Requisitos de Seguridad para Módulos Criptográficos". Hace referencia a la seguridad física de un chip de tarjeta inteligente, definido como un tipo de módulo criptográfico.

- Especificaciones de tarjeta con circuito integrado para sistemas de pago de MasterCard, Visa y Europay. Estas especificaciones estás concebida para crear una base técnica común para la implantación de tarjetas y sistemas correspondientes para sistemas de valor almacenado. Las especificaciones de tarjeta con circuito integrado para sistemas de pago pueden obtenerse en cualquier entidad bancaria miembro de la red Visa, MasterCard o Europay.

- Especificación PC/SC. Fue propuesta por Microsoft como una norma para tarjetas y lectoras aplicable a las tarjetas con microprocesador Organización Internacional de Normalización que interactúan con plataformas de 32 bits basadas en Windows para computadoras personales. Actualmente, la PC/SC no soporta sistemas que no estén basados en Win32.

- CEN (Comité Europeo de Normalización) y ETSI (Instituto Europeo de Normas de Telecomunicación). Su trabajo se centra en las normas de telecomunicación, como el SIM de GSM para teléfonos celulares, el GSM 11.11 y la norma ETSI300045.

- OpenCard Framework. Se trata de una norma abierta que proporciona interoperabilidad de aplicaciones de tarjetas inteligentes a través de redes, terminales de punto de venta (POS), microcomputadores personales, computadoras portátiles y otros dispositivos digitales.

OpenCard promete proporcionar aplicaciones de tarjeta inteligente "puras" basadas íntegramente en Java. Las aplicaciones de tarjeta inteligente no suelen ser autónomas porque se comunican con un dispositivo externo y utilizan bases de datos residentes en otros dispositivos. OpenCard también proporciona a los desarrolladores de sistemas una interfaz a PC/SC para usar los dispositivos existentes en la plataforma Win32.

- eEurope Smart Cards initiative and the Open Smart Card Infrastructure for Europe (OSCIE). La iniciativa de tarjeta inteligente eEurope reunió a un extenso grupo de expertos del sector, usuarios, operadores y académicos con el objetivo de acelerar y armonizar la realización y el uso de las tarjetas inteligentes en toda Europa. Esta iniciativa dio como resultado la producción de un conjunto de especificaciones comunes acompañadas de normas, prácticas más adecuadas, especificaciones técnicas y requisitos para la acción política, legislativa y técnica.

Desde agosto de 1998, el Comité Técnico TC215 de la ISO y sus cinco Grupos de Trabajo son responsables por el trabajo de normalización en el área de la informática de salud y las tecnologías de información y telecomunicación. El Grupo de Trabajo 5 (Tarjetas de Salud) se estableció en abril de 1999. La ISO/TC215/WG5 se centra en la normalización de contenido y no en su tecnología fundamental. El Comité Técnico aborda los temas de normalización relacionados con las tarjetas procesables por máquina para uso en el ámbito de la atención sanitaria, incluidas las estructuras de datos dependientes de tecnología, la interoperabilidad y la compatibilidad, la comunicación de datos y el enlace de registros.

Los temas de normalización tecnológica son la responsabilidad de otros grupos, el más importante de los cuales es la ISO JTC1/SC17 (Tecnología de la Información, Tarjetas de Identificación y Dispositivos Relacionados), que entre otras produce la serie de normas 7816. Las normas de tarjetas inteligentes que cubren la ISO 7816-1, 7816-2 y 7816-3 rigen las propiedades físicas y las características de comunicación de los chips incrustados. El grupo de trabajo sólo tiene en

cuenta los dispositivos de tamaño de tarjeta de crédito [1]. Las especificaciones de la ISO 7816 abarcan varias áreas, algunas de las cuales son estables y otras son objeto de revisión. Es conveniente averiguar cuál es la revisión más reciente preguntando a la ISO o al Instituto Americano de Normas Nacionales (ANSI). La ISO 7816 consta de seis partes, algunas de las cuales ya se han completado mientras que otras se encuentran actualmente en fase de redacción preliminar:

- Parte 1: características físicas (ISO 7816-1:1987). Define las dimensiones físicas de las tarjetas inteligentes de contacto y su resistencia a la electricidad estática, la radiación electromagnética y la tensión mecánica. También describe la ubicación física del sistema de circuitos integrado, la banda magnética y el área de grabado en relieve.

- Parte 2: dimensiones y ubicación de los contactos (ISO7816-2:1988). Define la ubicación, la finalidad y las características eléctricas de los contactos metálicos de la tarjeta.

- Parte 3: señales electrónicas y protocolos de transmisión (ISO 7816-3:1989). Define el voltaje y las necesidades de corriente para los contactos eléctricos tal como se define en la Parte 2 y el protocolo de transmisión de caracteres en modo semidúplex asíncrono (T=0).Enmienda 1:1992 Protocolo tipo T=1, el protocolo de transmisión de bloque en modo semidúplex asíncrono. Las tarjetas inteligentes que emplean un protocolo de transmisión patentado incorporan la denominación T=14.Enmienda 2:1994 Revisión de la selección de tipos de protocolos.

- Parte 4: comandos para el intercambio entre diferentes usuarios (ISO 7816-4). Establece un conjunto de comandos para las tarjetas con microprocesador en todas las industrias para proporcionar acceso, seguridad y transmisión de datos de tarjeta. Dentro de este núcleo básico hay comandos para, por ejemplo, leer, escribir y actualizar registros.

- Parte 5: sistema de numeración y procedimiento de registro para identificadores de aplicación (ISO 7816-5:1994). Establece normas para los identificadores de aplicación o "Application Identifier" (AID). Un AID tiene dos partes: la primera es un Identificador Registrado de Proveedor de Aplicación (RID) de cinco bytes que es exclusivo para el proveedor mientras que la segunda parte es un campo de tamaño variable de hasta once bytes que los RID pueden usar para identificar aplicaciones específicas.

- Parte 6: elementos de datos intersectoriales (ISO 7816-6). Detalla el transporte físico de los datos del dispositivo y la transacción, la respuesta para "reset" (retorno a la condición inicial) y los protocolos de transmisión. Las especificaciones permiten dos protocolos de transmisión: el protocolo alfanumérico (T=0) o el protocolo de bloques (T=1). Una tarjeta puede soportar cualquiera de los dos pero no ambos. (Nota: algunos fabricantes de tarjetas no siguen ninguno de estos protocolos. Los protocolos de transmisión para tales tarjetas se describen con la denominación T=14).

1.5. Biometría

La biometría se basa en enlazar un protocolo de identificación a un atributo humano, algo que no puede ser robado, falsificado, o perdido. Varios mercados, organismos de seguridad nacional y militar, empresas de seguridad de aeropuertos, la banca y otros sectores fueron los primeros en adoptar la identificación biométrica; el hardware y el software necesarios se han desarrollado rápidamente y hoy en día la industria informática ofrece muchas opciones comerciales.

La biometría basada en la huella digital es la solución más común, principalmente porque el ambiente de implementación multi-terminal facilitan su uso, la tecnología tiene un precio asequible y los sensores necesarios son de pequeño tamaño. Los sensores de huella

digital óptica, la forma más extendida y desarrollada, utilizan una plantilla ("template") de la imagen de la huella para comparación. Una dificultad a la que se enfrentan los usuarios es que los cambios en la superficie de la piel producidos por suciedad, aceites, manchas y abrasiones pueden dar lugar a emparejamientos erróneos, aunque la corrección de errores, basadas en software inteligente, pueden reconocer y sanar la mayoría de esos errores.

Existen nuevas tecnologías, basadas en el ultrasonido y los sensores de silicio, que usan ondas sonoras de alta frecuencia o la frecuencia de radio combinada con la tecnología de vídeo y las matrices electrónicas para profundizar en la epidermis con objeto de captar el modelo de surcos único que se halla en la capa profunda de la piel y así evitar las anomalías de la superficie o resultantes de la colocación de un dedo torcido en el sensor.

El iris humano constituye el atributo biométrico más exacto al que se puede acceder fácilmente pero su uso generalizado se ha visto obstaculizado por el alto costo de las cámaras necesarias para captar las imágenes del iris. Hasta hace poco, la tecnología de reconocimiento del iris se usaba principalmente en aplicaciones de seguridad de alto nivel para acceso físico mediante el empleo de unidades instaladas en la pared junto a las puertas de acceso. La aparición de nuevas cámaras pequeñas con tecnología avanzada pero barata ha abierto el camino para el uso de la identificación a través del iris en todo tipo de aplicaciones.

La identificación biométrica ya está incorporándose en computadoras portátiles, dispositivos inalámbricos y dispositivos miniaturizados térmicos para la identificación de huellas digitales, y recientemente se han introducido en el mercado cámaras que caben en un teléfono móvil, computadoras de bolsillo y asistentes digitales personales (PDA). El sector sanitario se contempla como un mercado importante para la identificación segura y los dispositivos de control de acceso [2, 3].

1.6. Nuevas tecnologías

Actualmente, las tarjetas inteligentes tienen hasta 128 KBytes de memoria EPROM (Memoria de Sólo Lectura Programable Borrable). Se prevé que esta capacidad aumente. Como posibles competidores a largo plazo de las tarjetas están los nuevos dispositivos basados en USB (Bus Seriado Universal) que pueden conectarse directamente en cualquier computadora y, dado que los puertos USB son componentes omnipresentes estándar de entrada-salida de las computadoras de mesa y portátiles, su uso evitaría la necesidad de lectoras o terminales de tarjeta.

Los países europeos han adoptado la estrategia de establecer un modelo de cifrado común para la infraestructura de clave pública o "Public Key Infrastructure" (PKI) dentro del contexto de la ISO-7816, combinado con convenios intergubernamentales para la autorización mutua de clientes a pesar que hasta la fecha no existe una norma para las terminales. En Japón, el proyecto NICSS (Next Generation IC-Card System Study o Estudio de Sistemas de Tarjeta CI de Próxima Generación) está creando tarjetas sin contacto de aplicación múltiple para proteger las aplicaciones gubernamentales basadas en la Web. El enfoque del NICSS respecto de las interfaces es más riguroso que el Marco Europeo de Interoperabilidad General (GIF).

Las ofertas de comunicación inalámbrica más habituales en el mercado actual son compatibles con las LAN (redes locales) inalámbricas 802.11b (WiFi), capaces de proporcionar velocidades de Ethernet de hasta 10 MBytes/seg. También ofrecen un radio de acción de unos 100 metros desde un nodo de transmisor/receptor, según sea la construcción de las paredes y la configuración de la instalación eléctrica y del sistema de tuberías de un edificio. Se puede usar una tarjeta WiFi del tamaño de un sello de correos de bajo costo para proporcionar a un asistente digital personal (PDA) conectividad inalámbrica relativamente segura a una red local (LAN) de hospital configurada de forma apropiada.

Recientemente la disponibilidad generalizada de los teléfonos móviles ha planteado la cuestión de si pueden usarse más intensamente en el ámbito de la salud. En consecuencia, los teléfonos móviles se han

empleado como un componente de comunicación de los sistemas de monitoreo para asistencia ambulatoria o domiciliaria. Otra aplicación interesante es utilizar los teléfonos móviles para los procedimientos de pago sustituyendo las tarjetas de crédito por la propia tarjeta SIM (Módulo de Identificación de Suscriptores) del teléfono para establecer contacto entre un sistema de aplicación y un servidor que produce un pago autenticado por la "SIM Application Toolkit" (Caja de Herramientas de Aplicación SIM) y protegido mediante una aplicación de cifrado de teléfono móvil administrada por una infraestructura de clave pública (PKI).

Los teléfonos móviles también podrían obtener acceso a la Web a través de combinaciones de diversas tecnologías de teléfono móvil como el Protocolo de Aplicación Inalámbrica (WAP). A pesar de que estos proyectos son prometedores y que se está comercializando una variedad de dispositivos de TIC móviles y portátiles, aún sigue sin haber estudios exhaustivos de las ventajas y los inconvenientes de tales enfoques.

Los elementos de la economía de escala dependen en gran medida de las novedades comerciales sin las cuales es difícil prever las ventajas y la repercusión de estas soluciones. Para encontrar escenarios posibles y respuestas realistas será necesario investigar tales temas durante períodos prolongados en diferentes ambientes de implantación. La cuestión de la escala es particularmente importante para el sector de la salud; ya que existe la creencia generalizada de que las aplicaciones de salud sólo serán económicamente factibles cuando se adopten las tarjetas de funciones múltiples que puedan ser usadas por diferentes sectores (crédito, operaciones bancarias, licencia de conducir, etc.).

En las figuras 4 a 8 se muestran ejemplos de distintas generaciones de tarjetas de datos con circuito integrado. Los ejemplos mostrados ilustran las tarjetas de diferentes generaciones y diversas funcionalidades.

La figura 4 muestra un ejemplo de una de las primeras tarjetas inteligentes de pacientes implantada con éxito en 1993. La "DefiCard" se diseñó para los aproximadamente 70.000 pacientes existentes en

Alemania con desfibriladores implantados. Contenía datos relacionados con el dispositivo implantado seleccionado así como datos del paciente anteriores y posteriores a la operación, e información sobre la enfermedad de base e intervenciones terapéuticas. Esta tarjeta ya contenía el conjunto de datos de interoperabilidad G7, una serie estandarizada de información mínima sobre el paciente, y sirvió para allanar el camino a futuras aplicaciones interoperables en un entorno internacional.

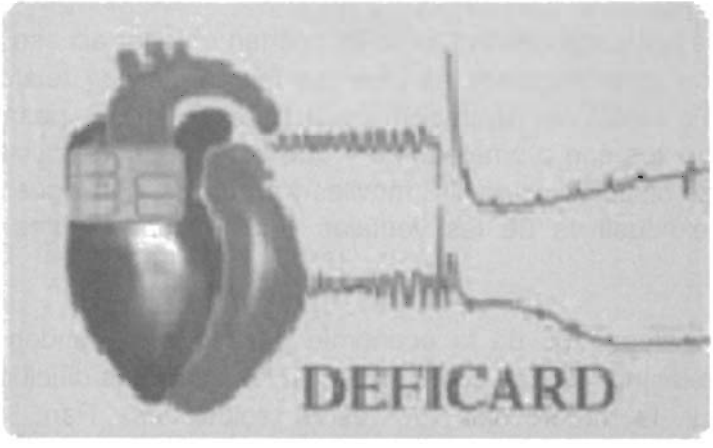

Figura 4. La DefiCard fue creada para los pacientes con desfibriladores implantados (1993).

La figura 5 ilustra la primera versión de una tarjeta de profesionales de la salud conforme a las normas internacionales sobre disposición y contenido. La foto y el holograma cumplen objetivos de seguridad. La tarjeta se interconecta con sistemas de TIC y funciona como una tarjeta oficial para la identidad de médicos. La figura 6 muestra la tarjeta de urgencia europea creada en 1996 por el proyecto CARDLINK dirigido por un consorcio de investigadores de Irlanda.

Figura 5. Una de las primeras tarjetas de identidad con circuito integrado para profesionales de la salud (1996).

Figura 6. Tarjeta de Urgencia Europea (CARDLINK) de 1996.

La figura 7 es un ejemplo de tarjeta sin contacto empleada por el personal del Hospital Universitario de Gotinga en 1999. Todas las funciones se cumplían mediante transmisión de frecuencias de radio (RF). El procesador y la antena estaban instalados en el interior de la tarjeta.

Figura 7. Tarjeta sin contacto del Hospital Universitario de Gotinga (1999).

La figura 8 muestra la tarjeta de estudiante de la Universidad de Gotinga (2002), un ejemplo de la flexibilidad de los sistemas modernos de tarjeta; se trata de una tarjeta sin contacto de tecnología mixta, mejorada con la incorporación de contactos y un chip independiente para firmas digitales y conexiones a numerosas aplicaciones de campus.

El diseño utiliza codificación por colores y distintos símbolos para identificar al estudiante y al personal, además de que puede portarse prendida en la ropa. Tiene un área actualizable y el reverso presenta un código de barras que sirve para conectar con el sistema bibliotecario alemán.

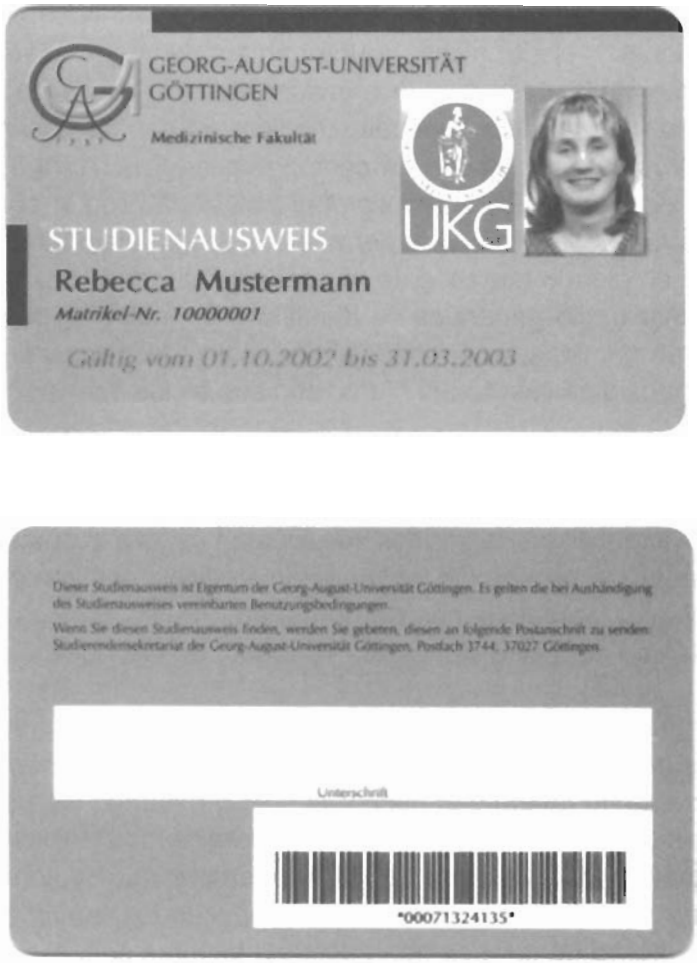

Figura 8. Uno de los sistemas de tarjeta moderna de funciones múltiples y tecnología mixta, la tarjeta de estudiante de la Universidad de Gotinga (2002).