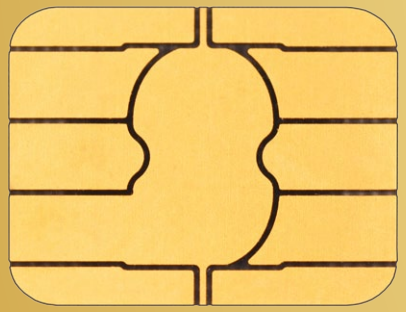


TARJETA CIUDADANA

Una visión de las tarjetas inteligentes y su aplicación en los Ayuntamientos

Junta de Castilla y León

red de municipios digitales de Castilla y León

AVISO LEGAL


TARJETA
CIUDADANA
Junta de
Castilla y León
red de municipios digitales
de Castilla y León

RESUMEN EJECUTIVO

El cambio que ha sufrido en los últimos años la sociedad gracias a la evolución de Internet y las tecnologías asociadas y el rápido despliegue que han tenido y que permite que el acceso a la red esté al alcance de cualquier ciudadano, ha provocado que se demande a las Administraciones Públicas servicios de calidad, que agilicen las tareas, favorezcan el acceso y simplifiquen los trámites administrativos por medios electrónicos, es decir, que faciliten la vida diaria a los ciudadanos.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, sentó las bases para poder implementar sistemas que permitan a los ciudadanos acceder a los servicios públicos por medios electrónicos.

En este contexto nace la idea de Tarjeta Ciudadana (aunque ciertos ayuntamientos llevan implementando estos sistemas desde hace más de una década). Este tipo de tarjetas permiten que un ciudadano pueda acceder a servicios ofrecidos por sus municipios de una manera sencilla, unificando en un mismo soporte servicios tan dispares como pueden ser el transporte urbano, el acceso a instalaciones deportivas y culturales, descuentos en las tiendas adheridas al proyecto, posibilidad de pago,...

La Tarjeta ciudadana es un tipo de tarjeta inteligente, es decir, la tarjeta puede realizar ciertas operaciones gracias a la inclusión de un chip en la misma. Las funcionalidades más comunes de este tipo de tarjetas son las siguientes:

- Identificación y acceso físico y/o lógico: la tarjeta permite identificar unívocamente a un cierto individuo, posibilitando su acceso tanto a instalaciones y edificios (acceso físico) como el acceso a las aplicaciones y sistemas mediante medios electrónicos (acceso lógico).
- Almacenamiento de información: las tarjetas permiten almacenar datos en la misma y tienen una mayor capacidad que una tarjeta de banda magnética, permitiendo ofrecen un número mayor de servicios.
- Medios de pago, bien como monederos electrónicos (donde es necesario realizar una precarga de dinero antes de poder utilizarlas) o como tarjetas financieras, que permitan el pago en el momento (hasta hace poco tiempo, la mayoría de las tarjetas financieras eran de banda magnética, pero una directiva europea obliga a que a partir del 1 de enero de 2011 todas las tarjetas incorporen el chip).

- Fidelización: permite ofrecer descuentos o promociones a los usuarios de ciertos servicios, que deberán presentar la tarjeta e identificarse.
- Control de asistencia / presencia, de manera automatizada.
- Otras funcionalidades, como pueden ser servicios de comedor, viajes, bonos,...

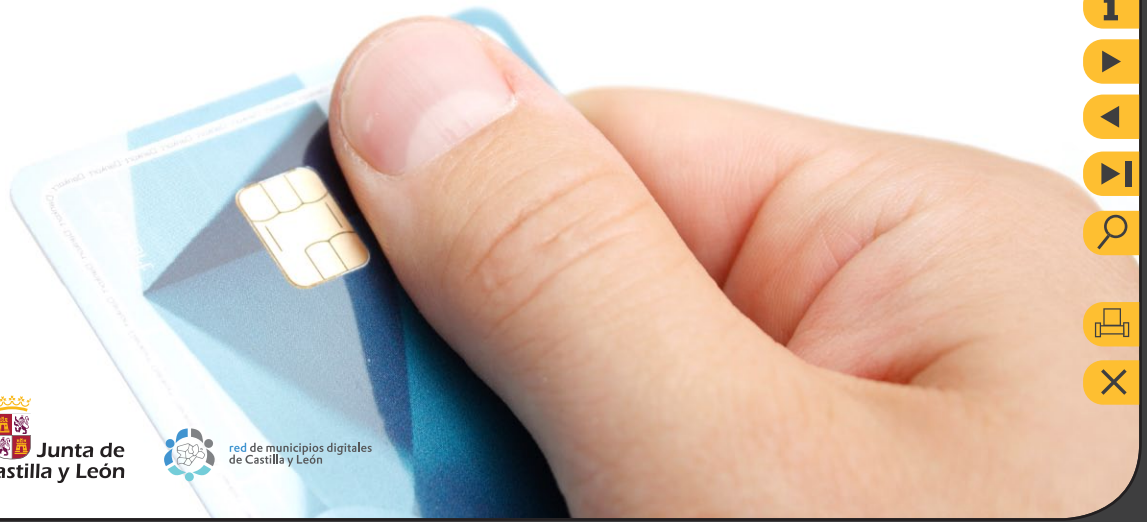
Como se observa por las posibles funcionalidades de estas tarjetas, se pueden unificar varios servicios en un mismo soporte, permitiendo a su vez, aunar los esfuerzos necesarios para desarrollar estos servicios en un mismo elemento, y que además, conlleva la simplificación de los procedimientos para los ciudadanos.

Pero que un elemento tecnológico de estas características permita realizar muchas funciones diferentes no asegura el éxito de su implantación, a no ser que implique ciertas ventajas y facilidades tanto para el usuario del mismo como para el prestador del servicio. Por ello, se hace necesario analizar las ventajas de la utilización de sistemas basados en Tarjeta Ciudadana, tanto desde el punto de vista del usuario, en este caso los ciudadanos, como desde el punto de vista del prestador de servicios, que serían las Administraciones Públicas y Entidades Locales.

Algunas ventajas para el ciudadano que presenta el uso de la Tarjeta Ciudadana son:

- Simplificación en los accesos a edificios, instalaciones y transportes públicos, de una manera rápida y sencilla.
- Adición o eliminación de nuevos servicios rápidamente, simplificando los trámites necesarios para llevarlos a cabo.
- Comodidad para el ciudadano, gracias a la unificación en una misma tarjeta de varios servicios para los que hasta ahora se necesitaban diferentes tarjetas (por ejemplo, el carné de la biblioteca, el carné para el uso de instalaciones deportivas, los billetes para el transporte urbano, las tarjetas de fidelización de museos y centros culturales, tarjeta monedero electrónico para las máquinas expendedoras en instalaciones oficiales,...).
- Agilidad a la hora de realizar pagos.

- Aumento de la seguridad en la identificación del usuario, gracias a las claves y las propiedades criptográficas de las tarjetas.
- Acceso a zonas personalizadas en las páginas web de los Ayuntamientos, que posibilitan la realización de trámites administrativos por medios electrónicos.
- Posibilidad de firmar electrónicamente documentos, de manera que sea equivalente a la firma manuscrita.
- Acceso a descuentos, promociones y tratos preferentes a los usuarios de la misma.
- Etc.



Pero las ventajas no se reducen sólo al usuario del sistema, sino que los Ayuntamientos que implementan estas soluciones también se ven beneficiadas por su uso:

- Facilitar al ciudadano los servicios a los que accede, repercutiendo en la imagen que estos tienen de los Ayuntamientos.
- Difusión de la imagen de la ciudad o municipio, puesto que las tarjetas presentan servicios propios de la localidad donde se emite, y pueden personalizarse gráficamente con imágenes y logos de la ciudad.
- Posibilidad de trazabilidad de los servicios, de manera que se obtengan feed-back, estadísticas y cuadros de mando que permitan tomar decisiones y realizar mejoras basadas en el uso que los ciudadanos realizan de los mismos.
- Integración de los sistemas asociados a los servicios prestados, de manera que se puedan intercambiar la información, sean interoperables y se agilicen los trámites.
- Agilidad en los trámites y unificación de criterios para acceder a los servicios.
- Reducción del coste asociado a las tarjetas (al unificar los servicios en una misma tarjeta, se necesita un número menor de tarjetas, mejores ofertas de proveedores de las mismas,...) y posibilidad de tener un único medio de gestión y distribución.
- Posibilidad de filtro de los servicios según ciertas características de los usuarios (jóvenes, tercera edad, discapacitados, desempleados,...).
- Etc.

Una vez desgranadas las funcionalidades asociadas a las tarjetas, y las ventajas que conllevan, es necesario detenerse un momento en los servicios que se pueden ofrecer si se implanta un sistema de estas características en una localidad. Como se ha comentado anteriormente, una misma tarjeta puede utilizarse para diversas funciones, de las que aquí presentaremos las más comunes y que presentan grandes ventajas:

- Acceso al transporte urbano, bien sea mediante un uso en el que es necesario recargar la tarjeta, que funciona como monedero electrónico, bien sea mediante bonos que se abonan mensualmente/trimestralmente/anualmente.
- Alquiler de bicicletas.
- Acceso a instalaciones deportivas, como pueden ser los polideportivos municipales, campos de fútbol, baloncesto, gimnasios, piscinas municipales, pistas de pádel o de tenis,...
- Bibliotecas, fonotecas, filmotecas: tanto para acceso físico a sus instalaciones, o a diferentes zonas de las mismas, como para el préstamo de los materiales que conservan.
- Aparcamiento en zonas de estacionamiento regulado o párquines públicos, para el pago en el caso de los no residentes, o identificación del vehículo para los residentes.
- Acceso en coche a las zonas peatonales para residentes.
- Acceso físico a centros culturales, museos,... También se podría incluir el pago de la entrada, o promociones, bonos y descuentos para sus usuarios.
- Acceso a los comedores, centros de día, centros de mayores,... y a cualquier centro de carácter social.
- Monederos electrónicos, para máquinas expendedoras en edificios e instalaciones municipales.
- Acceso a internet en zonas de Wifi que ofrezcan los municipios.
- Descuentos y promociones en tiendas y zonas comerciales que se adhieran al proyecto.
- Etc.

Como se puede observar, existen multitud de servicios que se pueden ofrecer a los ciudadanos mediante el uso de la Tarjeta Ciudadana, que presenta ventajas tanto para los usuarios como para las Administraciones que lo implementen. Este libro pretende dar unas nociones básicas sobre las tarjetas inteligentes, los servicios que se pueden ofrecer gracias a las mismas, las consideraciones que se deben tener cuando se inicia un proyecto de estas características y ejemplos de despliegues que se han realizado en España, de manera que las Entidades Locales se animen a implantar sistemas de Tarjetas Ciudadanas, con los conocimientos suficientes que permitan su funcionamiento y rápido despliegue.

Por último, sólo puntualizar que cualquier proyecto que suponga un cambio en la forma de actuar de los ciudadanos debe incluir un Plan de Difusión y Comunicación, puesto que es necesario explicar las ventajas que conllevan estos sistemas que justifiquen los cambios, además de ser una plataforma sensacional para dar a conocer la imagen de la localidad y el sentido de pertenencia a la misma, que crece y evoluciona igual que lo hace la tecnología.


1 INTRODUCCIÓN
Junta de Castilla y León
red de municipios digitales de Castilla y León

1. INTRODUCCIÓN

Las nuevas tecnologías están cambiando nuestra forma de interaccionar y relacionarnos con el mundo que nos rodea, permitiendo la comunicación mediante nuevos canales de fácil acceso. En este entorno nace el concepto de Administración Electrónica, refiriéndose al uso de medios electrónicos que permiten el desarrollo de servicios e interacción y comunicación entre las Administraciones Públicas y los ciudadanos.

Europa ha sido pionera en utilizar las nuevas tecnologías para mejorar esta relación con los ciudadanos, desarrollando nuevos servicios, simplificando los trámites administrativos, modernizando y ampliando los canales que permiten la comunicación entre los ciudadanos y las administraciones, de tal modo que sean percibidas como administraciones abiertas, eficaces en los servicios que ofrecen, receptivas con las opiniones de los ciudadanos, dinámicas, adaptándose a los cambios y pudiendo transformar rápidamente las necesidades de los ciudadanos en nuevos servicios.

La legislación española, donde destaca la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, y su normativa de desarrollo, está permitiendo que nos situemos entre los países más avanzados en el desarrollo de la Administración Electrónica. Esta Ley ha requerido que las Administraciones Públicas deban adaptar sus procedimientos, cambiando la forma de trabajar de sus empleados, de manera que se puedan prestar servicios a los ciudadanos de manera sencilla y eficaz, reduciendo las cargas administrativas e intentando reducir la burocracia a la mínima expresión.

Gracias a ello, los ciudadanos se han visto beneficiados por multitud de servicios que se pueden realizar de forma electrónica, a cualquier hora del día, sin tener que esperar colas ni desplazarse hasta las instalaciones de las administraciones, no siendo necesario entregar documentación que ya obre en su poder.

Adicionalmente a la implantación de la Administración Electrónica, se ha producido un gran avance tanto en la tecnología como en el uso de lo que se ha venido a denominar tarjeta inteligente, es decir, tarjetas que incorporan un chip, pueden procesar por sí mismas la información almacenada en su interior y, en algunos casos, permiten realizar operaciones criptográficas. Estas tarjetas se utilizan de modo habitual en nuestra vida diaria, con multitud de funcionalidades: tarjetas de crédito y débito (las entidades financieras han empezado a suministrar tarjetas con

chip, que sustituirán a las de banda magnética que se venían utilizando hasta ahora), tarjetas de fidelización (en comercios, hoteles, compañías aéreas,…), tarjetas de acceso (a los edificios de trabajo, a instalaciones deportivas,…), acceso al transporte urbano, …, y nuevos usos que se están empezando a desarrollar a medida que se generaliza su despliegue.

Las Administraciones Públicas no se han quedado rezagadas, viendo la oportunidad de aprovechar la funcionalidad de las tarjetas inteligentes como llave de acceso a los servicios de Administración Electrónica, y especialmente las Administraciones Locales, puesto que son las Administraciones más cercanas al ciudadano. La disposición de los elementos necesarios por parte de las Administraciones Públicas para asegurar la identificación y autentificación del usuario, la autenticidad y confidencialidad de las comunicaciones que se produzcan y la posibilidad de realizar firma electrónica es un paso imprescindible para que los ciudadanos puedan acceder a estos servicios y reforzar la relación entre los mismos y las administraciones.

El despliegue y uso del DNI electrónico (DNIe) y las tarjetas criptográficas, ejemplos de tarjetas inteligentes, ha permitido introducir este elemento como medio para acceder a estos servicios, firmar las solicitudes, escritos y comunicaciones y asegurar una comunicación segura con las administraciones. El DNIe proporciona esta seguridad adicional requerida. Asimismo, estas nuevas funcionalidades que plantean el uso de tarjetas inteligentes, permite que a medida que se universalice su despliegue, se amplíe el abanico de posibles aplicaciones y desarrollos que permitan el acceso a nuevos servicios.

Esta es la idea que subyace bajo el concepto de Tarjeta Ciudadana, una tarjeta inteligente que permita al ciudadano el acceso a los distintos servicios que ofrece la administración de una manera sencilla y segura, que simplifique los trámites, como el acceso a los transportes, el acceso y reserva de instalaciones deportivas, museos o centros sociales, e infinidad de nuevos servicios que se pueden ofrecer gracias al uso de la misma y que abordaremos a lo largo de este documento.

Este libro pretende servir como punto de partida para entender qué es una tarjeta inteligente, qué servicios se pueden ofrecer con las mismas, qué elementos son necesarios para poder ofrecer estos servicios en el ámbito municipal, cómo se debe llevar a cabo un proyecto de implantación de la misma, y mostrar algunos casos de éxito de implementaciones que se han llevado a cabo.

En el siguiente capítulo se explican las nociones básicas para entender el funcionamiento de las tarjetas inteligentes y el chip que integran, el ciclo de vida de las mismas, el tipo de seguridad que ofrecen y las características de los diferentes tipos de tarjetas que se utilizan.

En el capítulo tres, se detallan los elementos que se necesitan para poder hacer uso de estas tarjetas inteligentes: los terminales y lectores de tarjetas, y se realiza un estudio de su disponibilidad en el mercado nacional.

El capítulo cuatro explica las funcionalidades de la tarjeta, es decir, qué servicios pueden ofrecerse mediante el uso de las Tarjetas Ciudadanas: identificación, control de acceso físico/lógico, almacenamiento de información, etc., prestando especial atención a los servicios que se ofrecen desde las Administraciones Públicas.

Los pasos que hay que llevar a cabo para proyectos de implantación de Tarjetas Ciudadanas se detallan en el capítulo cinco, precisando las nociones básicas para su despliegue, integración con los sistemas ya existentes en las administraciones, el despliegue de la misma, y su viabilidad y sostenibilidad, teniendo en cuenta los tiempos actuales y la evolución de la tecnología y la legislación vigente.

Por último, se muestran algunos ejemplos de implantaciones que se han llevado a cabo con éxito en algunas administraciones españolas, como la Tarjeta Ciudadana de Ponferrada, la Tarjeta Ciudadana de Alcobendas o la Tarjeta sanitaria del País Vasco.

También se incluyen como anexos los estándares y especificaciones de tarjetas inteligentes, según los diferentes tipos definidos en el capítulo dos, detallando los tamaños y contactos de la tarjeta chip, y las características intrínsecas a las mismas. Esta información se complementa con los métodos de seguridad gráfica en la impresión de tarjetas, así como los criterios de evaluación de la seguridad.

Este documento se ha realizado en el marco de la Red de Municipios Digitales de Castilla y León. La Red de Municipios Digitales es una iniciativa de la Consejería de Fomento de la Junta de Castilla y León, enmarcada en la Línea “Municipios Digitales de Castilla y León” de la Estrategia Regional para la Sociedad Digital del Conocimiento (ERSDI) 2007-2013, que pretende impulsar la prestación de Servicios Públicos en Línea de Calidad en el entorno local a sus ciudadanos, empresas y organizaciones utilizando las TICs. La RMD, en la que están integrados los principales Ayuntamientos y todas las Diputaciones Provinciales de la región, coordina y apoya proyectos de Administración Electrónica y Servicios Públicos Digitales en el ámbito local.

Este documento está orientado, por tanto, a los responsables políticos, organizativos y al personal técnico de las Entidades Locales interesados en poner en marcha un proyecto de Tarjeta Ciudadana en sus municipios, enmarcado en sus planes de modernización municipal, con el objetivo de aportar unas nociones básicas que les permita conocer las múltiples aplicaciones y servicios posibles para ofrecer al ciudadano.

Desde la Red de Municipios Digitales queremos finalizar esta introducción agradeciendo al Ayuntamiento de Ponferrada su participación en la redacción, contenidos y recomendaciones de esta guía, sin cuya experiencia este documento no hubiera sido posible.


2 LA TARJETA CHIP
Junta de Castilla y León
red de municipios digitales de Castilla y León

2. LA TARJETA CHIP

Para comenzar, es necesario entender una serie de conceptos que nos permitan distinguir las tarjetas inteligentes de los demás tipos de tarjeta. Este capítulo pretende dar las nociones básicas que ayuden a la comprensión de los sistemas y servicios que se abordan a lo largo del libro.

2.1 QUÉ ES LA TARJETA CHIP

La tarjeta chip, tal y como su nombre indica, nació como una evolución de las tarjetas de cartón o banda, mediante la incorporación de un circuito integrado o chip a la tarjeta, el cual permite procesar la información que almacena y acceder a servicios a través de medios electrónicos. Actualmente, pueden incluir incluso un microprocesador con funciones criptográficas, que aporta una seguridad adicional en aplicaciones que manejan información sensible.

Las tarjetas chip que incluyen un microprocesador se conocen por diferentes nombres: tarjetas inteligentes, smart cards o tarjetas de circuito integrado (TCI o ICC, en su acepción en inglés), tal y como recoge la Organización Internacional para la Estandarización ISO. El tamaño de las tarjetas es fijo y viene determinado en las normas ISO (ISO/IEC 7816).

Los orígenes de la tarjeta chip se remontan a la década de los sesenta, cuando los alemanes Jürgen Dethloff y Helmut Gröttrup desarrollaron y patentaron un circuito integrado (chip) embebido en la tarjeta, cuya finalidad era servir de sistema de identificación, aunque desde la década de los cincuenta ya existían tarjetas de plástico, a las que se incorporaba una banda magnética que permitía ciertas funcionalidades.

La década de los setenta es realmente el inicio de lo que actualmente conocemos como tarjetas chip: en 1970, el japonés K. Arimura realiza, sobre el desarrollo de los alemanes, contribuciones importantes en la integración de lógica aritmética y almacenamiento en las tarjetas de circuito integrado. También es en estos años cuando se empiezan a desarrollar las primeras patentes: en 1974, el francés Roland Moreno patenta la primera tarjeta chip tal y como la conocemos actualmente, pero no es hasta el año 1978 que la empresa INNOVATRON, socia de Bull, a la que había vendido la patente, consigue un prototipo práctico, la primera tarjeta de circuito integrado.

A partir de este punto, se empiezan a desarrollar nuevos prototipos y servicios asociados:

- En 1983 aparecen las primeras tarjetas telefónicas, que incorporar un chip o circuito integrado.
- En 1984 se realizan las primeras pruebas de tarjetas de circuito integrado en el sector financiero para los cajeros automáticos.
- En 1987 aparecen los primeros estándares internacionales de tarjetas de circuito integrado, destacando la norma ISO/IEC 7816, donde se especifican los parámetros de fabricación de este tipo de tarjetas.

La década de los noventa supone el boom de las tarjetas, puesto que se empiezan a desarrollar servicios, funcionalidades y aplicaciones que permiten un uso generalizado de las mismas. Entre los mayores hitos que se producen en esta época, caben destacar los siguientes:

- El año 1990 fue un año muy prolífico, con numerosos avances en el desarrollo de las tarjetas y aplicaciones para las mismas.
- También en ese año se desarrolla la primera tarjeta criptográfica, la cual utilizará el algoritmo de encriptación RSA.
- En 1992, se fabrica la primera tarjeta SIM para la telefonía móvil, extendiéndose rápidamente su uso.
- El año 1994 es el de referencia para el estándar EMV: Europay, MasterCard y Visa (EMV) publican la primera versión de las especificaciones de interoperabilidad de las aplicaciones bancarias de las tarjetas inteligentes.
- En el año 1994, aparece la primera tarjeta monedero electrónico, Visa Cash, que no se distribuirá en España hasta un año después.
- La primera tarjeta criptográfica con procesador y algoritmo de encriptación RSA aparece en 1996, año en el que también se fabrica la primera tarjeta con chip basado en Java.

- En 1998, Francia inicia un proyecto piloto de tarjeta sanitaria.
- En 1999, Estados Unidos desarrolla los primeros proyectos de identificación y control de accesos lógicos y físicos basados en tarjetas inteligentes para empleados de las Agencias Federales.
- También en este año se desarrollan las primeras experiencias sobre tarjetas basadas en Java.

Aunque el concepto de tarjetas inteligentes es muy heterogéneo, comúnmente se denominan tarjetas inteligentes a las tarjetas que integran un circuito integrado (chip) con microprocesador, que permite procesar la información almacenada en la tarjeta. El chip puede incluir también módulos criptográficos que añaden un nivel de seguridad adicional, necesario para poder operar con ciertas aplicaciones o dispositivos que manejan información importante o sensible. La diferencia conceptual entre una tarjeta chip y una tarjeta inteligente es, por tanto, la inserción de un microprocesador, que la dota de capacidad de procesamiento de la información almacenada.

En los siguientes apartados se detallan las características del circuito integrado de la tarjeta y las ventajas e inconvenientes que presentan, antes de entrar a definir los tipos de tarjetas y su ciclo de vida.

2.1.1 El chip de la tarjeta

El elemento fundamental de una tarjeta de circuito integrado se encuentra en el chip, por lo que en este apartado se detallan las nociones básicas que permitan entender el funcionamiento de la tarjeta[1].

Según el uso al que se destine la tarjeta, existen varios tipos de tarjetas chip, dependiendo de los elementos que integren, aun cuando la ma-

1 En los anexos se enumeran y detallan los estándares y especificaciones que deben cumplir las tarjetas de circuito integrado según las normas internacionales.

yoría de las características son comunes, definidas por estándares internacionales: ubicación del chip, tamaño de la tarjeta, posición de los contactos de la tarjeta, características eléctricas y magnéticas, etc.

En general, los principales componentes del circuito integrado de la tarjeta son:

- Memoria: existen diferentes tipos de memoria:
  - *Memoria ROM (Read-Only Memory)*: la información que almacena este tipo de memoria es de sólo lectura, es decir, no se puede borrar, por lo que se utiliza para grabar el sistema operativo, el cual se incluye en la tarjeta en el momento de su fabricación. La capacidad de la memoria suele estar comprendida entre los 8 KB y los 32 KB, dependiendo del fabricante y el sistema operativo. En un primer momento, la mayoría de los sistemas operativos eran propietarios, por lo que era necesario realizar los desarrollos a medida, aunque esta tendencia se ha ido invirtiendo gracias a la estandarización y sistemas abiertos, que permiten desarrollos compatibles con las tarjetas de distintos fabricantes.
  - *Memoria EEPROM (Electrically-Erasable Programmable Read-Only Memory)*: en esta memoria se almacenan las aplicaciones que se incluyen en la tarjeta y sus datos asociados. Como bien indica su nombre, a esta memoria se puede acceder para grabar, extraer y borrar los datos y las aplicaciones. Su capacidad suele variar actualmente ente los 16 KB y 64 KB.
  - *Memoria RAM (Random Access Memory)*: esta memoria se utiliza para que el procesador pueda realizar sus funciones, es decir, cada vez que el procesador necesita ejecutar una orden, se utiliza esta memoria para realizar las operaciones. Esta memoria es volátil, lo cual indica que sólo almacena datos mientras haya alimentación. Si se extrae la tarjeta del lector, la memoria RAM se borra (aunque estuviera haciendo alguna operación y se hubiera quedado en la mitad del proceso). La capacidad de esta memoria es muy pequeña, puesto que sólo se utiliza para las operaciones que se realizan en el momento, y suele rondar los 256 bytes o 512 bytes.
- CPU (Central Processing Unit): es el procesador, o Unidad Central de Proceso, que ejecuta las instrucciones de las operaciones que se realizan sobre la tarjeta. El chip puede incorporar coprocesadores, utilizados generalmente para operaciones criptográficas, como encripta-

ción, firmas electrónicas o autenticación de usuarios. Hasta hace unos años, la mayoría de los microprocesadores eran de 8 bits y estaban basado en una arquitectura CISC con una frecuencia de reloj de 5 MHz. Actualmente, se utilizan también microprocesadores de 32 bits (por ejemplo, en tarjetas con sistema Java).

- I/O (puerto de Entrada/Salida, E/S): este puerto gestiona el flujo de datos entre el lector de tarjetas y la CPU, y consiste en un registro a través del cual se transfieren los datos.

La comunicación entre el chip de la tarjeta y el dispositivo lector se realiza a través de los contactos del chip.

La norma ISO/IEC 7816-1 define los posibles tamaños para una tarjeta inteligente y del circuito integrado, así como la posición de los contactos en el chip, tal y como se detalla en el Anexo I.

2.1.2 Ventajas e inconvenientes

Las tarjetas inteligentes conservan ciertas características de las tarjetas de banda magnética, pero el circuito integrado de la tarjeta las dota de una serie de nuevas funcionalidades, principalmente relacionadas con la capacidad de procesamiento que permite el microprocesador y el aumento del nivel de seguridad, mediante operaciones criptográficas.

A continuación se enumeran las principales ventajas e inconvenientes de este tipo de tarjetas.

- Ventajas de las tarjetas inteligentes:

  - Capacidad: son capaces de almacenar gran cantidad de información (en comparación con las tarjetas de banda magnética) y procesarla, gracias al microprocesador que incorporan en el chip que puede realizar operaciones dentro de la propia tarjeta, permitiendo de esta forma que no sea necesario conectarse online.

- Seguridad: la información puede ser protegida con claves contra lectura y/o escritura, gracias a la tecnología interna que integra, soportando operaciones criptográficas muy complejas, de manera que las posibilidades de copia que existe en las tarjetas de banda magnética se reduce, siendo difíciles de duplicar. Adicionalmente, la información que se transmite puede encriptarse con el fin evitar que se puedan producir robos de la misma.

- Una ventaja que se deriva de la anterior es la posibilidad de identificación y autenticación del usuario de la tarjeta, gracias a una clave o contraseña, evitando que otro individuo pueda realizar un uso indebido de la misma.

- Las tarjetas chip incluyen, entre los datos alojados en el mismo, un número de serie que la identifica unívocamente.

- Aunque, como se ha comentado, pueden trabajar offline, siguen conservando la posibilidad de comunicarse con ciertos sistemas mediante un lector de tarjetas.

- Al almacenarse la información en memorias tipo EEPROM, pueden actualizarse los datos contenidos en la tarjeta de una manera rápida y sencilla.

- Flexibilidad: gracias al microprocesador incorporado en el chip, las tarjetas pueden ser multi-aplicación, es decir, pueden realizar distintas operaciones según la aplicación elegida, adaptándose a las circunstancias y necesidades de cada usuario. Por ejemplo, la Tarjeta Ciudadana puede ser monedero electrónico, utilizarla para el transporte, acceso y reserva de instalaciones deportivas, trámites con las Administraciones,... Adicionalmente, se pueden desarrollar, almacenar o suprimir las aplicaciones en las tarjetas, puesto que para ello se utiliza la tarjeta EEPROM.

- Las tarjetas chip presentan mecanismos de autoprotección, tanto físicos, como lógicos y gráficos. En el apartado 2.2 y 2.3, se detallan estas características.

- Entre sus componentes integran memoria EEPROM, es decir, memoria no volátil. En la memoria ROM, donde se almacena el sistema operativo, los programas incluidos son inalterables, accesibles únicamente a través del sistema operativo, que garantiza la seguridad de la información mediante la encriptación de los datos (mecanismos de firma electrónica y algoritmos criptográficos).

- Las tarjetas chip presentan la posibilidad de nuevas funcionalidades que no se podían realizar con las tarjetas, gracias al microprocesador que incorporan, como por ejemplo, la tarjeta monedero electrónico.

- Inconvenientes de las tarjetas inteligentes:

  - Las aplicaciones deben estar programadas según el sistema operativo y el hardware que se utilice, aunque la mayoría de los procesos siguen estándares internacionales que permiten el funcionamiento de las mismas independientemente del fabricante de la tarjeta o del dispositivo lector.

  - Mayor coste de fabricación respecto de las tarjetas de banda magnética.

- Las tarjetas con contactos necesitan ser insertadas en un dispositivo lector de tarjetas para poder operar, puesto que su funcionamiento depende de la alimentación del chip.

- Mayor coste de la infraestructura necesaria para utilizarla (lectores, terminales de escritura, etc.).

2.2 CICLO DE VIDA DE LA TARJETA CHIP

El ciclo de vida de una tarjeta inteligente se inicia con la fabricación de la misma, puesto que dependiendo del tipo de hardware elegido, del tipo de tarjeta y del sistema operativo, la tarjeta tendrá ciertas funcionalidades y se deberán desarrollar las aplicaciones en lenguajes de programación específicos.

Las etapas principales del ciclo de vida de una tarjeta inteligente son las siguientes:

- Fabricación: dependerá del fabricante de tarjetas, y se inicia desde el momento de la fabricación del chip hasta el finalizado del mismo. Esta etapa se subdivide en las siguientes subetapas:

  - Fabricación del plástico: existen diferentes materiales que son utilizados para la fabricación de las tarjetas. En esta etapa se imprimen los fondos de las tarjetas, logos del fabricante, condiciones generales de la tarjeta, espacio reservado para la firma, y cualquier otro elemento que el fabricante quiere que aparezca en todas las tarjetas, independientemente de la personalización que se realiza después. Las normas internacionales definen los requisitos de seguridad que se deberán tener en consideración desde el punto de vista gráfico (tintas utilizadas, hologramas,... Dependiendo del material, la duración de las tarjetas y el coste de las mismas puede diferir. Los materiales más utilizados para la fabricación de las tarjetas son:

    – *PVC (policloruro de vinilo):* este material se utiliza para tarjetas con una vida corta, normalmente unos dos años. El PVC es grueso, y la lisura y el borde de la tarjeta tienen que ser de buena calidad para que no haya problemas con los colores durante la impresión. Es el

material más utilizado para la fabricación de tarjetas, debido al coste de su fabricación, pero es un material tóxico que se está intentando sustituir por materiales alternativos.

- *ABS (acrilonitrilo butadieno estireno):* es un polímero termoplástico con alta rigidez y dureza, baja absorción de humedad, alta resistencia térmica y muy resistente al impacto. La duración de las tarjetas fabricadas con este material suele rondar los cinco años. El proceso de fabricación deja pocos residuos, y garantiza un menor impacto medioambiental, mediante la eliminación del cloro, en contraste con el PVC.

- *Policarbonato (PC):* material de altas prestaciones, alta durabilidad, resistente a la fragmentación y ligero. Las tarjetas de policarbonato están destinadas para aplicaciones de seguridad, y su vida puede llegar hasta los diez años; esta es una de las razones por las que el DNI electrónico está fabricado con este material.

- *PET (Terephthalate de polietileno):* es un material biodegradable, flexible, resistente a elementos corrosivos o agresivos, con una la laminación que puede llegar a ser muy fina (entre 8 y 10 micras, mientras que la mayoría de las tarjetas tienen 30 micras de ancho). Las tarjetas fabricadas con este material pueden llegar a los ocho años de vida.

- *Otros materiales:* PVH, PETG (Glicol de Tereftalato de Polietileno), PLA (Ácido Poliláctico),…

• Fresado: se prepara el plástico de la tarjeta para insertarle el chip que se integrará posteriormente.

• Fabricación y obtención del chip: se corta el chip partiendo de una oblea de silicio, se incorpora la máscara (sistema operativo), se asignan los contactos del chip, se realiza el cableado de éste y se prueba. Este proceso es delicado y requiere un entorno libre de suciedad.

• Encartado: se integra el chip en la tarjeta. El chip incorporará el sistema operativo (máscara) y se asignan los contactos (en el siguiente apartado se detallan los mismos).

- Pre-personalización: una vez que la tarjeta está fabricada y se haya integrado el chip y la banda magnética, se necesita cargar el sistema de ficheros, ciertos programas y las rutinas básicas que permiten su posterior configuración y uso, mediante un programador de tarjetas inteligentes a través de los contactos del chip. Este proceso se debe realizar antes de personalizar la tarjeta para un usuario específico. En este momento se inhabilita el acceso físico a la memoria de la tarjeta donde se encuentra el sistema operativo. En esta etapa se introducen ciertos datos que no se podrán modificar, como el identificador del fabricante, el número de serie de la tarjeta y el código del emisor de la tarjeta.

- Personalización: en esta etapa se diseña la tarjeta según solicita el cliente, se programa la tarjeta con las aplicaciones y encriptación que sean necesarias y se entrega al usuario final. Se pueden distinguir varias fases bien diferenciadas:

  - Personalización gráfica de la tarjeta: según los requerimientos del cliente, se realiza el diseño de la tarjeta. Para ello existen herramientas de diseño gráfico que permiten generar pruebas según las imágenes y logos que se quieran estén presentes en la tarjeta. Cada fabricante de tarjetas o distribuidor exige unos formatos u otros y diferentes resoluciones, dependiendo del tipo de impresoras de tarjetas que se utilice. Habrá que prestar especial atención a la disposición de las imágenes, logotipos y textos que se quieren imprimir en la tarjeta, debido al chip que está integrado, con el fin de no tener problemas de pérdidas de imagen en zonas cercanas (normalmente se recomienda ampliar el espacio entre chip e imágenes). Una vez que se haya integrado todas las imágenes, se realizarán pruebas de color en imprenta para ver su resultado final (logotipos, imágenes, color, posición del panel de firma, banda magnética, hologramas,...).

  - Personalización eléctrica de la tarjeta: en esta etapa se graban la estructura de ficheros (bloques de definición de archivos) y los datos que irán almacenados en el chip de la tarjeta. Habrá que tener en cuenta el tipo de encriptación que es necesaria, los certificados que se van a incluir en la misma, y el momento de realizar la generación de claves, en la propia tarjeta o mediante un dispositivo hardware de claves seguro (HSM, Hardware Security Module). También en esta etapa se proporcionan los códigos de la aplicación, que otorgan los permisos para la lectura y escritura de los archivos de usuario que se almacenen en la tarjeta. Para resumir, la información que se necesita, sin tener en cuenta el diseño gráfico, es la siguiente:

    – Datos que requieran los estándares internacionales (ISO, EMV,...).

  - Datos de las aplicaciones que se almacenarán en la tarjeta, como, por ejemplo, el monedero electrónico.
  - Criptografía y claves (DES, RSA, elíptica,...).
  - Certificados a incluir en la tarjeta.
  - Configuración del comportamiento de la misma (perfiles de la tarjeta).

- Personalización magnética de la tarjeta: si se incluye una banda magnética, en esta etapa se graban los datos que se incluirán en la misma, según el uso o funcionalidades de la misma. La banda magnética puede ser grabada en 1, 2 ó 3 pistas, y cada pista codificada permite cierto número de caracteres:
  - Pista 1 – acepta 79 caracteres alfanuméricos y el formato de codificación es IATA *(International Air Transport Association).*
  - Pista 2 – acepta 40 caracteres numéricos y el formato de codificación es ABA *(American Bankers Association).*
  - Pista 3 – acepta 107 caracteres numéricos y el formato de codificación es TTS *(Thrift Third Standard).*

- Etapa de usuario: esta etapa se inicia una vez que el usuario tiene la tarjeta en su poder. Desde este momento, el usuario puede utilizar la tarjeta y la tarjeta estará asociada a ese usuario en particular, de modo que ningún otro usuario debiera utilizarla. La vida útil de la tarjeta se suele indicar en alguna de sus caras, y una vez se haya llegado a esa fecha, se deberá retirar y conseguir otra. Este proceso también será necesario si se ha producido un robo o extravío de la misma. A partir de este momento, dependiendo del tipo de tarjeta, de la infraestructura disponible y de la funcionalidad de la misma, se podrá utilizar para hacer las operaciones y servicios que tenga asociados ese usuario.

2.3 SEGURIDAD GRÁFICA

Las tarjetas chip permiten reforzar la seguridad, previniendo contra usos fraudulentos mediante la utilización de claves y la encriptación, pero eso no implica que se deba descuidar la seguridad gráfica de la misma, puesto que existen funciones y servicios en los que en la comunicación no interviene el chip (por ejemplo, si incluye banda magnética, tarjetas de radiofrecuencia, tarjetas sin contactos,...).

Esta seguridad gráfica se hace indispensable en documentos de identificación, como puede ser el DNI electrónico, puesto que la mayoría de las comprobaciones las realiza una persona mediante un examen visual del documento, debiendo asegurar la autenticidad del mismo.

De esta forma, queda patente la necesidad de evitar la falsificación de las tarjetas que se utilizan en la identificación, para lo cual existen diferentes procesos que dificultan la copia de la misma y afianzan la seguridad:

- Imágenes de seguridad visibles que cambian de color y/o intensidad dependiendo del ángulo de visión.
- Imágenes o patrones ocultos que sólo pueden observarse si se expone la tarjeta a cierto tipo de luz, como la luz ultravioleta.
- Imágenes retrorreflectantes, que son visibles bajo la luz directa.

En el Anexo II puede encontrar más información sobre las técnicas más utilizadas en la impresión de tarjetas.

2.4 TIPOS DE TARJETAS

Antes de iniciar la descripción de los diferentes tipos de tarjetas que existen, es preciso aclarar un concepto que normalmente crea confusión.

Como hemos visto anteriormente, el chip de la tarjeta no implica que ésta sea considerada una tarjeta inteligente. Las tarjetas inteligentes deben incorporar un microprocesador, que permita realizar cálculos complejos, almacenar información y utilizar las diferentes aplicaciones.

Las tarjetas de memoria, por ejemplo, incluyen un chip, pero el chip no las hace inteligentes, pues les falta el microprocesador que las permita procesar la información.

La clasificación de las tarjetas podría dividirse en dos grandes grupos: tarjetas de banda magnética y tarjetas chip. Las tarjetas de banda magnética incluyen una banda con propiedades magnéticas en su parte posterior, mientras que las tarjetas chip incorporan un circuito integrado. Aunque se haga esta diferenciación, no significa que no existan tarjetas híbridas que integren ambos elementos, la banda magnética y el circuito integrado, como por ejemplo las tarjetas de crédito, puesto que dependiendo del país se utilizará uno u otro método.

Las tarjetas chip se pueden clasificar a su vez en subgrupos, dependiendo de las características que se escojan para su distinción:

- Según el mecanismo de conexión / interfaz: la forma de conexión con los dispositivos lectores de tarjetas nos permite clasificarlas en tarjetas con contactos, si es necesario que la tarjeta se inserte en el lector o terminal para su funcionamiento, o tarjetas sin contactos, donde sólo es necesario acercar la tarjeta al dispositivo sin tener que entrar en contacto con el mismo, puesto que se comunican mediante señales de radiofrecuencia.

  Por supuesto, una tarjeta dual puede integrar ambas tecnologías, dependiendo de las necesidades del sistema y servicios que se quieran ofrecer: por ejemplo, una tarjeta puede incluir la tecnología sin contactos para control de accesos y la tecnología con contactos para acceder a servicios vía internet.

- Según los elementos del circuito integrado: si se observan los elementos del chip, las tarjetas se podrían clasificar en tarjetas de memoria o tarjetas con microprocesador. En este caso, no se puede considerar que existan tarjetas híbridas, porque en el momento en que incluyan el microprocesador, se consideran que forman parte de este último grupo.

  Las tarjetas con memoria, a su vez, se pueden clasificar en tarjetas de memoria libre y tarjetas de memoria protegida, dependiendo de si incluyen mecanismos de protección y seguridad para acceder a la información contenida en la memoria.

Las tarjetas con microprocesador, que son las únicas que pueden considerarse tarjetas inteligentes, también pueden distinguirse entre dos grupos: las tarjetas microprocesador sencillas, que únicamente incluyen un microprocesador, y las tarjetas criptográficas, que integran un segundo microprocesador que realiza las funciones relacionadas con la encriptación y criptografía.

Como se puede observar, dependiendo del tipo de característica que se tome en consideración para la clasificación, podemos distinguir entre los diferentes tipos de tarjetas, por lo que se interrelacionan entre las mismas:

- Una tarjeta sin contactos puede ser una tarjeta de memoria o una tarjeta con microprocesador.
- Una tarjeta con contactos también puede ser una tarjeta de memoria o una tarjeta con microprocesador. Generalmente, las tarjetas criptográficas son tarjetas de contacto, aunque la tecnología permite que puedan ser sin contactos.

La siguiente figura muestra gráficamente una posible clasificación de las tarjetas.

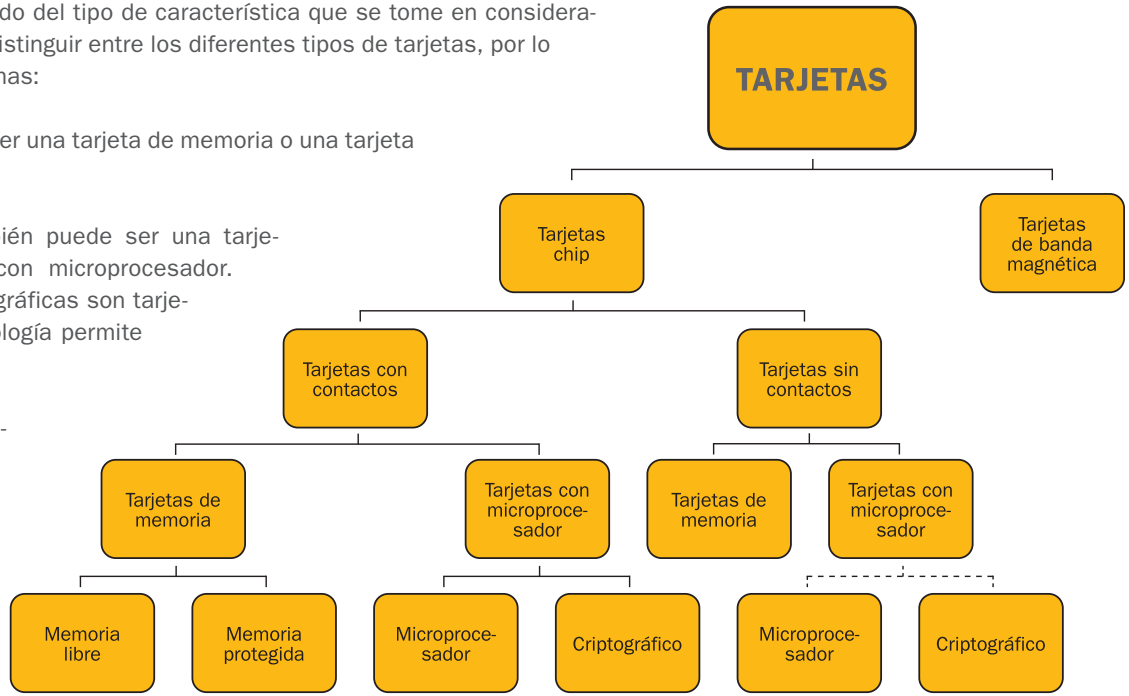


Figura 1
Clasificación del tipo de tarjetas

En los próximos apartados se detallan las características de cada tipo de tarjeta, sus ventajas e inconvenientes, y los usos y aplicaciones más habituales para las que se utilizan en la actualidad. No habrá de olvidarse en ningún momento que, aunque se haga esta distinción, las tarjetas pueden incluir varios elementos y tecnologías, no siendo excluyentes.

2.4.1 Tarjetas de banda magnética

Las tarjetas de banda magnética son aquellas tarjetas que presentan una banda, generalmente en su parte posterior, compuesta por partículas ferromagnéticas sobre una resina. Estas partículas, gracias a sus propiedades magnéticas, tienden a comportarse de un modo en el que se alinean en una misma dirección y sentido cuando se les aplica un campo magnético, de manera que al retirar el campo, estas regiones permanecerán alineadas, generando un campo magnético por su cuenta de cierta intensidad.

Las tarjetas de banda magnética fueron la evolución natural de las tarjetas con relieve (técnica de embosado), ya que permitían la personalización de la tarjeta para la identificación del individuo mediante un método sencillo y mucho más rápido que tener que “copiar” los datos incluidos en el relieve de la tarjeta.

Los datos son magnéticamente codificados en la banda de la tarjeta, aunque este tipo de tarjetas presenta una capacidad muy limitada de almacenamiento. Dependiendo del tipo de codificación y la necesidad de almacenamiento, la banda estará formada por hasta tres pistas de datos. En la siguiente tabla se muestran las características de cada pista:

Pistas	Tipo de codificación	Tipo de datos admitidos	Densidad de grabación (bits per inch)
Track 1	IATA (International Air Transport Association)	79 caracteres alfanuméricos	210 bpi
Track 2	ABA (American Bankers Association)	40 caracteres numéricos	75 bpi
Track 3	TTS (Thrift Third Standard)	107 caracteres numéricos	210 bpi

Figura 2 Características de las pistas de las tarjetas de banda magnética

Dependiendo de los materiales utilizados y sus propiedades, la banda magnética puede ser de baja coercitividad[2], LO-CO, debido a que utiliza elementos de menor resistencia, denominados ferromagnetos “blandos”, como el óxido de hierro, o de alta coercitividad, HI-CO, que utiliza ferromagnetos “duros” con mayor resistencia, como la ferrita de bario.

- Las tarjetas con banda magnética de baja coercitividad o LO-CO, generalmente de color marrón (aunque pueden ser de otro color), se caracterizan por la necesidad de una fuerza magnética menor para su codificación (300 oersteds). Habitualmente se suelen utilizar para aplicaciones que requieran su renovación cada cierto tiempo, debido a su menor resistencia y coste. Por ello, se suelen utilizar para tarjetas regalo, acreditaciones en eventos, etc.

- En cambio, las tarjetas de alta coercitividad o HI-CO necesitan una fuerza magnética superior (3600-6000 oersteds) para su codificación o borrado, pero presentan una vida útil prolongada. En un principio, la banda era de color negro; actualmente, puede ser de cualquier color. Estas tarjetas se utilizan en instalaciones en las que, por alguna causa, existan campos magnéticos fuertes, que podrían borrar la información.

La tarjeta puede estar fabricada con cualquier material, mientras este material no presente propiedades magnéticas, por lo que suelen ser de papel plastificado o plástico PVC, de manera que sean flexibles. La información se codifica en las pistas de la tarjeta alternando la polaridad de las partículas que están presentes en la banda magnética, utilizándose grabadores de tarjetas o impresoras con codificador magnético.

Las organizaciones internacionales de estandarización (ANSI e ISO) desarrollaron unas especificaciones, actualizadas puntualmente en base a nuevas necesidades o avances tecnológicos, que se deben contemplar en la fabricación de las tarjetas de banda magnética para su correcto funcionamiento independientemente del tipo de dispositivo lector utilizado. Las características, posición y técnicas de grabación y encriptado de las bandas magnéticas se describen en las normas internacionales ISO/IEC CR-80, ISO/IEC 7810 e ISO/IEC 7811, dependiendo de la técnica de codificación utilizada.

2 La coercitividad se entiende como la fuerza electromagnética necesaria para magnetizar la banda, y se mide en oersteds (Oe).

Las ventajas que presentan este tipo de tarjetas son las siguientes:

- Las tarjetas de banda magnética están muy extendidas.
- La tecnología está muy desarrollada y difundida.
- Presentan un coste bajo, respecto a su durabilidad, tanto la fabricación como el equipamiento necesario para su lectura y escritura.
- Son sencillas de personalizar.
- Se utilizan para aplicaciones muy variadas.

Los inconvenientes más destacados son:

- Materiales: es fácil que sufran daños por el uso habitual de la tarjeta, puesto que presentan la banda en el exterior (dependiendo del tipo, HI-CO o LO-CO tendrán una vida útil mayor o menor, respectivamente).
- Seguridad: son fáciles de duplicar y no ofrecen seguridad en el acceso y almacenamiento de la información.
- Memoria: capacidad bastante limitada de almacenamiento.
- Campos magnéticos: en zonas e instalaciones donde exista un campo magnético, puede producirse el borrado de los datos contenidos en la banda magnética, sobre todo, en las tarjetas de baja coercitividad.

Los ámbitos más habituales de uso son:

- Financiero: tarjetas de débito, crédito y tarjetas recargables (como pueden ser tarjetas monedero, tarjetas para las máquinas expendedoras,...).
- Transporte: tarjetas de tren, avión, metro, autobuses,...
- Identificación personal y control de acceso: tarjetas de acceso, tarjetas de socio, identificación de trabajadores, control de aparcamientos,...
- Fidelización: tarjetas de socio, tarjetas regalo.
- Hoteles: tarjetas de acceso para las habitaciones.
- Etc.

2.4.2 Tarjetas con contactos

Las tarjetas con contactos son tarjetas con un chip integrado en la misma, las cuales necesitan ser insertadas en un dispositivo lector para la comunicación entre ambos dispositivos, pues presentan una placa de contactos metálicos visible. Los contactos del chip se detallan en el Anexo I.

Las normas ISO/IEC 7816 e ISO/IEC 7810 definen los contactos del chip: su forma física, la posición de los conectores, sus características eléctricas, los protocolos de comunicación, el formato de los comandos, la dureza de la tarjeta, su funcionalidad,... Puede encontrar más información sobre estas normas en el Anexo I.

La ventaja de este tipo de tarjetas radica en su capacidad de procesamiento y almacenamiento de la información, incluyendo mecanismos de seguridad y acceso a la información que contienen.

Estas tarjetas presentan inconvenientes asociados al contacto de la tarjeta con el lector:

- La suciedad que se adhiere a la tarjeta por el contacto con el lector hace que se produzcan errores de funcionamiento de la tarjeta.
- Los contactos de la tarjeta pueden transmitir electricidad estática a los circuitos integrados del chip, lo que puede provocar su mal funcionamiento.

Su uso está extendido para infinidad de aplicaciones y servicios:

- Tarjetas bancarias de débito y crédito.
- Tarjetas prepago.
- Tarjetas monedero.
- Tarjetas de memoria.
- Tarjetas SIM para móviles.
- Máquinas expendedoras.
- Etc.

2.4.3 Tarjetas sin contactos

Básicamente, las tarjetas sin contactos son tarjetas chip que pueden tener el mismo uso y funciones que las tarjetas con contacto, pero utilizan distintos protocolos de comunicación con el dispositivo lector, puesto que presentan una antena para comunicarse con el exterior. Al no tener contactos, no existen errores asociados al desgaste o la suciedad de la placa.

La primera tarjeta de este tipo se empezó a desarrollar en el Instituto Arimura en 1978, debido a su utilidad en transacciones que debían realizarse con relativa rapidez, no siendo necesario introducirlas en un lector para su lectura, sino que la comunicación se realizaba por radio-frecuencia.

Los organismos internacionales han desarrollado estándares que definen las características de estas tarjetas: normas ISO/IEC 7816, ISO/IEC 14443, ISO/IEC 15693 e ISO/IEC 10536.

Dependiendo de las características que se utilicen para definirlas, se pueden clasificar según la distancia de aproximación al lector, según el tipo de alimentación de los circuitos y según la banda de frecuencias en las que operan.

Según el tipo de alimentación, o modo de aportar la tensión suficiente que permita su funcionamiento, se distinguen dos tipos:

- Mediante una batería interna junto al chip, que alimenta los circuitos. En este caso, el grosor de la tarjeta es de tres milímetros, por lo que no cumple el estándar ISO 7810.

- A través de una fuente de energía externa, por lo que es necesario que la tarjeta incorpore una bobina (hilo metálico incrustado en la tarjeta), que transforme la energía al someterse a un campo electromagnético variable, induciendo la corriente eléctrica necesaria.

Según el rango de utilización, es decir, la distancia de aproximación al lector, se pueden distinguir tres tipos:

- Tarjeta cercana, o “Close Coupled”: la tarjeta debe estar casi en contacto con el lector, a unos pocos milímetros, para que sea posible la comunicación. Este tipo de tarjetas se basan en el estándar ISO 10536, y generalmente deben insertarse en un terminal o posarlas sobre un lector.

- Tarjeta de proximidad o “Proximity Cards”: en estos casos, la distancia con el lector se acentúa hasta unos pocos centímetros, no siendo necesario que entren en contacto con el lector, y se basan en el estándar ISO 14443.

- Tarjeta lejana o “Vicinity Cards”: la distancia puede llegar hasta unos pocos metros, pero tienen la desventaja de que es necesario resolver problemas asociados a la concurrencia de tarjetas intentando dialogar con el lector. Se definen en el estándar ISO 15693.

Según la banda de frecuencias utilizada en la comunicación con el lector, se clasifican en tres tipos (la frecuencia que se puede utilizar viene determinada por las leyes y normativa vigente en cada país respecto a su espacio radioeléctrico):

- Baja frecuencia (BF): útil cuando la tarjeta no posee una batería y la velocidad de transferencia no es muy alta, se refiere a rangos de frecuencia inferiores a 135 KHz. El sistema RFID (*Radio Frequency IDentification*) utiliza dos frecuencias: 125 KHz. (el estándar original) y 134,5 KHz. (el estándar internacional).

- Alta frecuencia (AF): la frecuencia de funcionamiento es de 13,56 MHz. A diferencia de la baja frecuencia, no funciona cerca de los metales, por lo que se utiliza para la trazabilidad de productos o equipajes o control de accesos.

- Ultra alta frecuencia (UHF): comprende las frecuencias de funcionamiento en las bandas de 433 MHz, 860 MHz y 928 MHz.

- Microondas: este tipo de frecuencias permite, por ejemplo, el diálogo entre un terminal y un coche a gran velocidad. Las bandas de funcionamiento de estas tarjetas está en 2,45 GHz y 5,8 GHz.

Las tarjetas sin contactos presentan las siguientes ventajas:

- Bajo deterioro por la ausencia de contacto entre la tarjeta y el lector.
- Rapidez y comodidad de uso.
- Alta velocidad de comunicación entre tarjeta y terminal.

El principal inconveniente de este tipo de tarjeta es el método de comunicación por radiofrecuencia, puesto que si existen interferencias, la tarjeta no podrá utilizarse correctamente.

Los principales usos de esta tarjeta están asociados a controles de acceso o trazabilidad de productos:

- Acceso a edificios.
- Parkings.
- Transporte público.
- Llaves de los hoteles (acceso a las habitaciones).
- Movimientos de equipajes.
- Trazabilidad de animales y productos.
- Etc.

2.4.4 Tarjetas de memoria

Las tarjetas de memoria, también denominadas tarjetas sincrónicas, son el tipo de tarjetas más utilizado a nivel mundial y se utilizan para almacenar información (no existe un control de acceso a los datos, puesto que carecen de la seguridad propia de las tarjetas con microprocesador que se describen en el siguiente apartado).

Las tarjetas incorporan un chip integrado con una memoria de tipo EEPROM (*Electrically-Erasable Programmable Read-Only Memory*), es decir, memorias programables y que se pueden borrar eléctricamente. La capacidad de la tarjeta puede variar desde los 256 bytes hasta varios Kbytes, con una parte de memoria libre para poder almacenar información de forma segura, pudiendo ser con contactos o sin contactos. El estándar ISO/IEC 7816 define las características de las tarjetas de memoria.

Este tipo de tarjetas se puede diferenciar en dos grandes grupos:

- Memoria libre: estas tarjetas se disponen para el almacenamiento de información, pero carecen de mecanismos de protección y seguridad para acceder a la misma.
- Memoria protegida: presentan mecanismos de seguridad, de manera que son necesarias claves para poder acceder a la información que contienen, y utilizan técnicas de protección mediante algoritmos de cifrado de datos.

Las ventajas de este tipo de tarjetas respecto a las tarjetas de microprocesador son:

- Almacenamiento seguro de la información.
- Mayor espacio de memoria.
- Funcionamiento offline, puesto que se utilizan como tarjetas prepago.

Los inconvenientes de este tipo de tarjetas son:

- No son multiaplicación.
- No son tan seguras como puede ser una tarjeta con microprocesador.
- No se pueden realizar operaciones propiamente en la tarjeta, sólo almacenan la información.
- No son flexibles.

Estas tarjetas tienen infinidad de usos, como por ejemplo:

- Telefonía: es donde se ha visto un mayor desarrollo de las tarjetas, con las tarjetas prepago.
- Comercios: tarjetas de fidelización o socio.
- Control de accesos.
- Etc.

2.4.5 Tarjetas con microprocesador / chip criptográfico

Las tarjetas con microprocesador, también denominadas tarjetas asincrónicas, son las tarjetas chip que se conocen popularmente como tarjetas inteligentes, e igual que las tarjetas de memoria, pueden ser con contactos o sin contactos. Sus características se definen en los estándares ISO/IEC 7816 e ISO/IEC 14443. Estas tarjetas integran en el chip uno o varios microprocesadores, uno de los cuales puede ser criptográfico, permitiendo encriptación y firma electrónica, además de distintos tipos de memoria: RAM, ROM y EEPROM.

El microprocesador de la tarjeta permite un mayor control de acceso a los datos, mediante un conjunto de instrucciones que permiten el uso de claves de acceso para poder leer la información contenida en la misma, incluyendo capacidades criptográficas fuertes y almacenamiento de certificados digitales. Además, pueden realizar procesamiento de datos a nivel local y cálculos complicados, como los utilizados para la encriptación y el cifrado de datos, permitiendo sistemas avanzados de seguridad.

Estas tarjetas también poseen una capacidad de memoria alta. El microprocesador administra estas zonas de memoria (el sistema operativo, denominado máscara, se encontrará en la memoria ROM del chip, de manera que no sea modificable; la memoria EEPROM se utilizará para almacenamiento de los datos y las aplicaciones que contenga; la memoria RAM se utilizará en el momento del procesamiento de datos). La validación de la clave o contraseña, denominado PIN (Personal Identification Number o Número de Identificación Personal), la realiza el microprocesador mediante el uso de estas zonas de memoria.

Las tarjetas con microprocesador suelen ser utilizadas para aplicaciones que requieran un nivel de seguridad alto, que tengan múltiples aplicaciones en la misma tarjeta o para aplicaciones como monederos electrónicos. Su uso está muy extendido en tarjetas de crédito y débito, aunque en España se está empezando ahora con su despliegue.

Las ventajas de este tipo de tarjetas se centran en su capacidad de encriptación y procesamiento:

- Nivel de seguridad alto, puesto que pueden realizar el cálculo de los algoritmos de cifrado de datos.
- Multiaplicación, puesto que el sistema operativo únicamente contiene las instrucciones básicas, guardándose en la memoria del chip las aplicaciones. El microprocesador realizará las operaciones oportunas según el tipo de aplicación con el que interactúe.
- Almacenamiento de la información mediante el cifrado de datos, de manera que sea muy complicado acceder a los mismos.

Las tarjetas con microprocesador se están imponiendo al resto de tarjetas por la seguridad que conlleva su uso, por lo que se utilizan para todo tipo de servicios:

- Tarjetas de crédito / débito.
- Tarjetas Ciudadanas.
- Firma electrónica.
- Tarjetas monedero electrónico.
- Control de accesos.
- Tarjetas de identificación (DNIe, tarjeta de conducir,...).
- Tarjeta sanitaria.
- Etc.

Los sistemas operativos de los microprocesadores se graban en la memoria de sólo lectura (memoria ROM) del chip, de manera que no sea posible su modificación una vez finalizado el proceso de fabricación. Los sistemas operativos pueden ser de dos tipos:

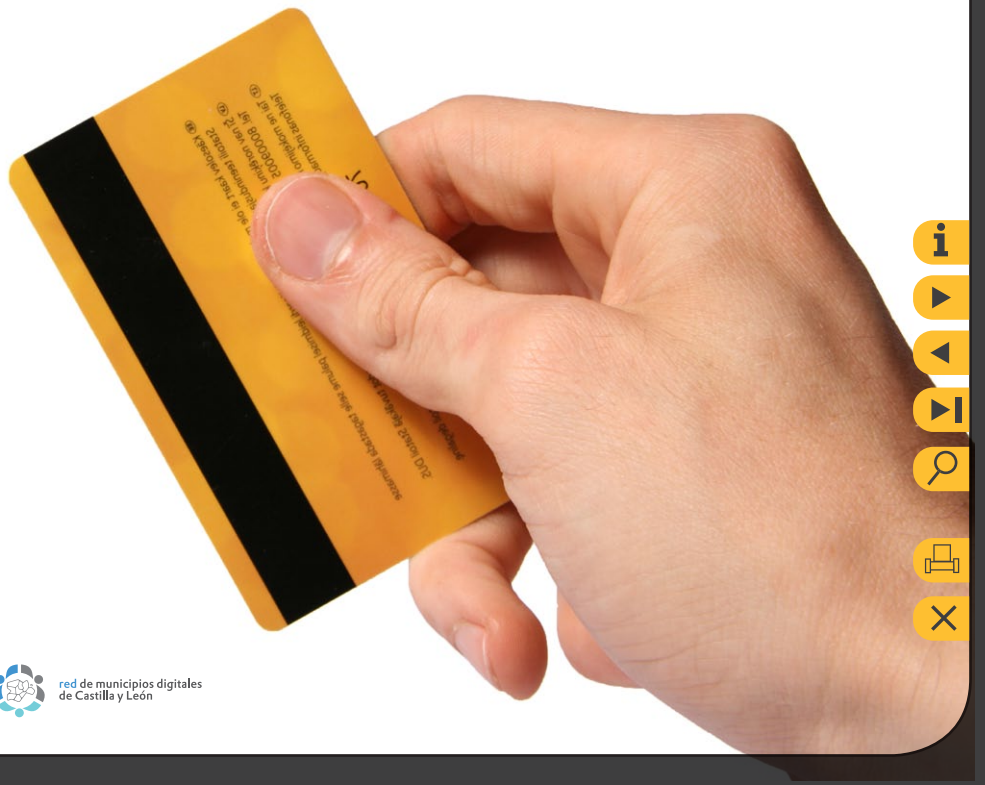
- Sistemas propietarios: dependen del fabricante del sistema, suelen estar respaldados por entidades financieras, compañías de servicios,.. y son muy seguros. Alguno de estos sistemas están creados específicamente para soportar aplicaciones de seguridad, como soporte de claves y certificados, o algoritmos biométricos. A continuación se enumeran alguno de los sistemas operativos (entre paréntesis se detalla el fabricante que lo utiliza).

  Ejemplos: WG10 (CEN), TIBC (SERMEPA), Criptonita/FN19 (FNMT), MMAR-PKI o TEMD (Microelectrónica), Starcos (G&D), Sealys eTravel (Gemalto), Criptoflex (antiguo Axalto, actualmente Gemalto después de su unión con Gemplus),...

- Sistemas abiertos: permiten fácilmente el desarrollo de aplicaciones, flexibilidad y la descarga de aplicaciones en la tarjeta.

  Ejemplos: JavaCard, Multos.

En el Anexo I se explica con más detalle alguno de los sistemas operativos que se pueden encontrar en el mercado actualmente.




3 LECTORES
Y TERMINALES
DE TARJETA CHIP
Junta de
Castilla y León
red de municipios digitales
de Castilla y León

3. LECTORES Y TERMINALES DE TARJETA CHIP

Las tarjetas necesitan dispositivos o terminales para comunicarse e interactuar con el mundo exterior, denominados lectores de tarjetas. Dependiendo del tipo de tarjeta se utilizarán unos lectores u otros. En el caso de las tarjetas inteligentes, aunque se les denomina igualmente lectores de tarjetas, la mayoría son capaces de leer y escribir.

En la tecnología de tarjetas de contactos, además de la función de comunicarse con la tarjeta, el lector debe alimentar el circuito integrado a través de uno de los contactos del chip.

Existen cantidad de lectores y terminales de tarjetas con múltiples formas y niveles de sofisticación mecánica y lógica, en función de las aplicaciones para las que se utilice la tarjeta y el lugar donde se instalen. Algunos ejemplos muy distintos son: lector de DNIe por USB, lectores de las máquinas expendedoras, lector de control de acceso físico a edificios, lector en autopistas, lector integrado en el teléfono móvil, lector integrado en cajeros automáticos o TPVs,…

El crecimiento y expansión del uso de tarjetas para aplicaciones cada vez más diversas y la estandarización que se ha realizado de las tarjetas a nivel internacional está permitiendo el continuo crecimiento del mercado, por lo que existen multitud de fabricantes, integradores y distribuidores de lectores y terminales de tarjeta. Un ejemplo de esta estandarización, la especificación PC/SC (*Personal Computer / Smart Card*), muy difundida a nivel mundial, permite el desarrollo de aplicaciones para cualquier lector de tarjetas chip que suministre los drivers PC/SC.

Precisamente, uno de los puntos más problemáticos es que la estandarización a la que están sometidas las tarjetas no ha sido continuada con una estandarización de los terminales y lectores de tarjetas. Hace unos años, este hecho causaba que los desarrolladores de los sistemas tuvieran que integrarse con diferentes lectores o terminales, según el tipo de lector y el fabricante del mismo. Finalmente, se están empezando a dar los pasos necesarios para la estandarización de los protocolos de comunicación como, por ejemplo, los lectores de tarjetas inteligentes financieras que cumplen el estándar EMV, de manera que no sea necesario desarrollar diferentes versiones del mismo sistema.

En el presente capítulo se intentará diferenciar entre los distintos tipos de lectores que se pueden encontrar en el mercado, según distintas características que permiten realizar varias clasificaciones de los mismos.

3.1 TIPOS DE LECTORES

Los lectores y terminales de tarjeta presentan una gran variedad de formas, tecnologías, elementos que los componen,..., dependiendo del uso y funcionalidad que tengan, del lugar en que se encuentren, de los usuarios que lo utilicen, etc.

Al existir tal variedad entre lectores y terminales, es necesario escoger alguna de las características más importantes inherentes a los mismos para poder realizar alguna clasificación que sirva de referencia. En este apartado se muestran varias categorías para el tipo de lectores en base a la tecnología para la que están diseñados, el tipo de interfaz de conexión del lector con un ordenador y los tipos de tarjetas que acepta.

Dependiendo del tipo de tecnología, los lectores se pueden clasificar en:

- Lectores de proximidad: los lectores de proximidad son sistemas fáciles de instalar y de usar, ya que lo único que hay que hacer es acercar la tarjeta al lector, normalmente a unos centímetros, aunque algunos todavía necesitan entrar en contacto con el lector. La tarjeta se conecta con el lector mediante ondas de radio a una frecuencia determinada. Dependiendo del tipo de tarjeta, la conexión de la tarjeta con el lector se produce a diferentes frecuencias (por ejemplo, según la ISO 14443, la frecuencia es 13,56 MHz, para las tarjetas de radiofrecuencia RFID, la frecuencia es de 125 KHz.,...). Estos lectores hasta ahora se utilizaban casi exclusivamente como control de accesos. Actualmente, gracias a la tecnología RFID (*Radio Frequency IDentification*), que permite transmitir la identidad de un objeto al lector, estos lectores se utilizan para identificación de animales, identificación de objetos en comercios, control de acceso en vehículos,... (dependiendo de la frecuencia a la que se utilicen, el coste, el alcance y las aplicaciones varían).

- Lectores de contactos: estos lectores son los más utilizados para las tarjetas chip debido a que el microprocesador necesita de alimentación para funcionar. Estos lectores incluyen unas patillas internas que se corresponden con los contactos del chip según se ha descrito en el apartado 2.1.2 El Chip de la tarjeta. Estos lectores soportan distintos estándares: PS/SC y USB CCID y se conectan al ordenador mediante el puerto serie, USB o PCMCIA. Además del lector, se necesitan los drivers del lector para poder utilizarlos.

- Lectores duales: estos lectores permiten leer las tarjetas con o sin contactos en un único dispositivo, siendo muy útiles cuando se utilizan

en entornos que permiten tarjetas de proximidad y tarjetas inteligentes. Esto permite que las tarjetas puedan ser utilizadas para un mayor número de funciones: control de accesos, firma digital, tarjetas monedero,...

- TPV (Terminal Punto de Venta): son sistemas compuestos por diferentes elementos que permiten el pago en comercios y puntos de venta, con la impresión del ticket o factura por los servicios o bienes adquiridos. Estos terminales están conectados con las entidades financieras que validan la operación, y suelen incorporar una pantalla donde introducir los datos, bien sea a través de un teclado o de la misma pantalla, que en este caso deberá ser táctil. La mayoría de los TPVs que existen en estos momentos en el mercado son un tipo especial de lectores duales, puesto que permiten la utilización de tarjetas de banda magnética y tarjetas chip.

Si se tiene en cuenta el interfaz mediante el cual se conectan con un ordenador, se podrán distinguir los siguientes tipos de lectores:

- Lectores USB: los lectores USB se conectan mediante un puerto USB al ordenador. El puerto USB es una interfaz de dispositivo que permite la comunicación entre el ordenador y el dispositivo. Las ventajas de esta interfaz son, entre otras, que sólo es necesario conectar el dispositivo y tener los drivers para su funcionamiento, sin tener que instalarlo o desinstalarlo (conexión y desconexión "en caliente"); la velocidad de transferencia es mayor respecto a los demás interfaces; y una de las más importantes, proporciona alimentación a través del propio puerto a los dispositivos conectados. Los lectores de tarjetas USB son los más comunes para su conexión a un ordenador, debido a la facilidad de su funcionamiento. Estos lectores, a su vez, pueden ser de distintos tipo:
  - Dispositivos externos con conector estándar USB.
  - Dispositivos internos.
  - Dispositivos integrados, como por ejemplo teclados con lector de tarjetas.
- Lectores serie: aunque estos lectores están casi *obsoletos*, todavía se puede encontrar alguno en el mercado. Utilizan el puerto serie para comunicarse con el ordenador al que están conectados, enviando la información bit a bit (en contraposición con el puerto paralelo, que envía

en paralelo los bits). El nombre puerto serie se suele utilizar para designar al puerto RS-232. Los lectores de tarjetas utilizan conectores DE-9, es decir, de nueve pines, ya que se ha generalizado su uso por ser más barato, cuando se conectan a través de una interfaz externa. Al igual que en los lectores USB, se puede distinguir entre:

- Dispositivos externos: utilizan los conectores DE-9.
- Dispositivos internos.

- Lectores PCMCIA (*Personal Computer Memory Card International Association*): es una interfaz de comunicación para tarjetas de memoria que amplían las funcionalidades del ordenador, destacando su uso en los ordenadores portátiles.

Por último, se puede realizar una clasificación más relacionada con los usos y aplicaciones de las tarjetas que se utilizan con estos lectores:

- Acceso a instalaciones: estos lectores y terminales se utilizarían para el control de acceso físico a edificios e instalaciones. Dependiendo de la tecnología de la tarjeta, podemos encontrar multitud de terminales diferentes: lectores de proximidad en los que únicamente es necesario acercar la tarjeta, lectores de proximidad o lectores duales donde es necesario introducir una clave PIN, lectores de tarjetas con técnicas biométricas, donde se comprobará alguno de los rasgos físicos que estén contenidos en la tarjeta (huellas dactilares, iris de los ojos, reconocimiento facial,...), etc.

- Transportes: generalmente son lectores de proximidad y tarjetas monedero electrónico (aunque también pueden ser tarjetas relacionadas con bonos mensuales o anuales, como las tarjetas para mayores de 65 años que se están empezando a distribuir en Madrid).

- Cajeros automáticos: los cajeros automáticos siempre integran un lector de tarjetas, en la mayoría de los casos dual, de manera que acepte tanto tarjetas de banda magnética como tarjetas chip.

- TPVs (Terminales de Punto de Venta): lectores de tarjetas que se utilizan en comercios y puntos de venta para el pago mediante tarjeta.

Estos lectores integran un PIN-Pad (teclado dispositivo que permite introducir la clave asociada a la tarjeta, denominada PIN, y que encripta esta clave en las transacciones que realiza) y pantallas para su utilización.

- Identificación: lectores que normalmente se conectan a un ordenador, para la identificación y autenticación mediante tarjetas inteligentes (el mejor ejemplo son los lectores compatibles con el DNI electrónico).

- Máquinas expendedoras: los lectores dependerán del tipo de transacción financiera que permitan, puesto que si la validación de la operación se realiza online, se podrán utilizar las tarjetas bancarias, pero si la validación es offline, será necesario utilizar las tarjetas monedero electrónico.

- Otros: existen otros muchos usos que se detallan en el apartado 4, como lectores de tarjetas en aparcamientos y autopistas, lectores para el préstamo de libros en bibliotecas,...

3.2 DISPONIBILIDAD EN EL MERCADO NACIONAL

En el mercado nacional se pueden encontrar multitud de fabricantes, integradores y distribuidores de terminales y lectores de tarjetas, por lo que dependiendo del tipo de aplicación para las que se utilice la tarjeta, el lugar donde se instalen, las necesidades de seguridad, y cualquier otro requerimiento adicional, se podrá elegir entre unos u otros.

La mayoría de los fabricantes distribuyen estos lectores a los integradores industriales o fabricantes de dispositivos (OEM, Original Equipment Manufacturer), que integran los terminales en sus dispositivos (máquinas expendedoras, cajeros automáticos, sistemas de control,...).

A continuación se enumeran alguno de los fabricantes más importantes que se pueden encontrar en el mercado nacional de lectores de tarjeta:

- C3PO (http://www.c3po.es): fabrica principalmente lectores de tarjetas para ordenadores personales y lectores para fabricantes de dispositivos (OEM).

- Bit4ID Ibérica (http://www.bit4id.com/espanol/): en su oferta de productos se pueden encontrar lectores de tarjetas de contactos, lectores de proximidad, lectores biométricos, lectores con PIN-Pad y pantalla,...
- Kalysis (http://www.kalysis.com): su catálogo de productos es muy diverso: lectores de tarjetas inteligentes para distribuidores y OEMs, teclados lectores de tarjetas, lectores de tarjetas de proximidad, lectores biométricos,...
- HID Global (http://www.hidglobal.com/espanol): fabrica y distribuye todo tipo de lectores: de proximidad, de contactos (OMNIKEY), duales,...
- Barcitronic (http://www.barcitronic.com/): empresa que importa y distribuye lectores de proximidad, lectores de contactos, lectores biométricos, teclados con lector integrado,...


4 FUNCIONALIDAD Y ENTORNO DE APLICACIÓN DE LA TARJETA CHIP
Junta de Castilla y León
red de municipios digitales de Castilla y León

4. FUNCIONALIDAD Y ENTORNO DE APLICACIÓN DE LA TARJETA CHIP

En este capítulo se pretende explicar las funcionalidades más comunes de las tarjetas inteligentes, haciendo hincapié en los servicios que pueden ofrecer las Administraciones Locales mediante la implantación de un sistema basado en Tarjetas Ciudadanas.

Aún cuando las funcionalidades de las tarjetas son las mismas, cada sector ha desarrollado sus servicios específicos, dependiendo de los requisitos del mismo, por lo que resulta interesante describir las experiencias de aplicaciones de tarjetas inteligentes en cada sector.

4.1 FUNCIONALIDADES DESTACADAS DE LAS TARJETAS CHIP

4.1.1 Identificación y acceso lógico / físico

La identificación de las personas para acceder a un lugar, bien sea físico o virtual, siempre ha sido una preocupación desde el punto de vista de la seguridad, llegando a ser uno de los quebraderos de cabeza actualmente, en un mundo tan globalizado donde la movilidad y el acceso a través de internet permiten acceder a infinidad de lugares físicos y virtuales. Con el objetivo de mejorar la seguridad y la confianza de los usuarios, se debe proveer de sistemas de identificación que sean seguros, proporcionen una verificación rápida y efectiva de la identidad del individuo y proteja la información de carácter personal.

Antes de entrar en detalle en la funcionalidad de la tarjeta, resulta necesario esbozar el concepto de identidad digital y los mecanismos de identificación, que permitan entender el uso que las tarjetas chip pueden ofrecer respecto al control de accesos, tanto físico como lógico.

La identidad digital, concepto análogo al de identidad personal, se le denomina al conjunto de rasgos o credenciales que caracterizan a un individuo mediante medios electrónicos. La identidad digital debe vincularse al individuo siguiendo un proceso que determinará el nivel de confianza.

El objetivo primordial de un sistema de identificación es estar diseñado para verificar que un individuo es quien dice ser. Hasta hace no muchos años, la mayoría de los sistemas de identificación se basaban en una persona de seguridad que cotejaba un documento oficial (DNI, carnet

de conducir, pasaporte, tarjeta de empresa,...) con los rasgos y credenciales del individuo que quería acceder, mediante una inspección visual y una serie de preguntas sobre el documento. Esta forma de identificación permitía el fraude muy fácilmente, mediante la falsificación de los documentos o el error humano en el cotejamiento de los mismos.

Actualmente, las transacciones electrónicas exigen que un individuo se tenga que autenticar para poder acceder a los servicios que proporciona el sistema. Este proceso genérico consta de tres pasos. El primer paso, la identificación, sería el proceso por el cual el individuo presenta estos rasgos o credenciales al sistema, que deberán ser verificados para determinar si se corresponden con los del individuo. Este proceso de verificación sería el segundo paso, y se conoce con el nombre de autenticación. Finalmente, el tercer paso consistiría en comprobar que el individuo tiene permisos suficientes para acceder a un determinado servicio, proceso denominado autorización.

Existen diferentes mecanismos de identificación/autenticación, según el nivel de seguridad que se necesite. Según el grado de "fortaleza" de los métodos, se pueden clasificar en:

- Mecanismos basados en "lo que sé": son los mecanismos más débiles, debido al problema de la custodia de los datos que se utilizarán para la identificación, una credencial que sólo conoce el individuo. Esta credencial se corresponde con una palabra secreta, que, adaptado al mundo digital y más concretamente a las tarjetas inteligentes, serían las claves o PIN de la tarjeta.

- Mecanismos basados en "lo que tengo": sería un mecanismo más fuerte que el anterior, puesto que el individuo dispone de algún elemento con el que identificarse para acceder a los servicios. En el ámbito electrónico, estos elementos permiten albergar o generar claves más complejas, por lo que aumenta la seguridad, pero al ser un objeto físico, pueden ser sustraídas. En nuestro caso, este elemento sería la tarjeta misma.

- Mecanismos basados en "lo que soy": serían los métodos de identificación más robustos, puesto que están íntimamente relacionados con el individuo, un rasgo o credencial que lo identifique unívocamente. Los elementos biométricos, es decir, los elementos que identifican los rasgos físicos o del comportamiento del individuo (huellas dactilares, reconocimiento del iris, reconocimiento facial,...), que se pueden incluir en las tarjetas (no todas las tarjetas permiten este comportamiento) componen los rasgos que se deberán comprobar en estos métodos.

- Mecanismos mixtos o híbridos: estos métodos utilizan varios de los mecanismos anteriores, complementándose, de manera que se habla de autenticación doble, triple o multi-factor, dependiendo del número de métodos que se combinen.

Si esto lo relacionamos con las tarjetas inteligentes como base de un sistema de identificación y acceso, se podría enlazar con los métodos detallados de la siguiente forma:

- Un primer paso para la mejora de la seguridad es el tecleo de una clave o PIN, mecanismo basado en "lo que sé". Aunque esto pueda parecer muy novedoso, el mecanismo es muy antiguo, pues es análogo a la petición de una contraseña ("santo y seña") que se hacía en la antigüedad cuando se quería acceder a un sitio protegido o secreto. El problema de este método es que una vez que se conozca la contraseña, clave o PIN, cualquier persona puede acceder al sistema.

- El siguiente paso para mejorar la seguridad sería utilizar un mecanismo basado "en lo que tengo". Gracias al avance de la tecnología, las tarjetas criptográficas permiten relacionar la clave o PIN con un certificado electrónico que se encuentra almacenado en la tarjeta, credenciales que identifican al individuo, garantizando un nivel adicional de confianza.

- Por último, se podrían utilizar técnicas biométricas asociadas a la tarjeta, mecanismo basado en "lo que soy". Estas técnicas consisten en verificar la identidad del usuario mediante rasgos específicos de los individuos, como pueden ser huellas dactilares, reconocimiento facial, reconocimiento del iris, reconocimiento de voz,... los cuales permiten discernir un individuo respecto del resto de individuos.

Las tarjetas inteligentes proporcionan una ventaja respecto a las demás tecnologías y elementos de identificación, puesto que permiten la salvaguarda de la información personal, proporcionando únicamente la información mínima necesaria para la comprobación correcta de las credenciales y requerimientos. Un ejemplo práctico podría ser el caso de la edad legal: si queremos comprar tabaco o alcohol, la ley obliga a verificar la edad del individuo, pero no es necesaria información sobre su nombre o domicilio, por lo que una aplicación de tarjeta inteligente podría proporcionar únicamente la información necesaria, en este caso, el año de nacimiento.

De esta forma, según el nivel de seguridad que se precise para cada sistema de identificación o control de accesos, se podrá solicitar una serie

de datos o credenciales u otros. La tarjeta se convierte precisamente en una representación confiable y verificable de la identidad del individuo, con la ventaja de la movilidad asociada, puesto que se puede guardar y transportar fácilmente.

Otra ventaja de la utilización de estas tarjetas para los sistemas de identificación es que es su facilidad para actualizar la información contenida en el chip. Por ejemplo, el cambio de alguno de los datos que contiene la tarjeta (domicilio, correo electrónico,...) se podrá modificar sin necesidad de tener que emitir una nueva tarjeta con los datos modificados (según el tipo de dato, puede ser igualmente complicado, pero la posibilidad existe y el coste asociado es menor).

La identificación es la aplicación más común de las tarjetas inteligentes para el control de accesos, tanto físico (instalaciones y edificios, transportes,...) como lógico (sistemas a través de diferentes canales: Internet, red interna, móvil, TDT,...). Y el mejor ejemplo del uso y posibilidades que ofrece este tipo de tarjetas es la implantación del DNI electrónico: es un sistema de identificación único, que se utiliza para múltiples aplicaciones de acceso, desde las relacionadas con las Administraciones Públicas, hasta el acceso a la zona de clientes de bancos y empresas de servicios a través de medios electrónicos.

Una aplicación de esta funcionalidad es el Documento Nacional de Identidad electrónico (DNIe). El DNIe es una tarjeta inteligente, criptográfica y personalizada, cuyo objetivo es proporcionar un mecanismo de identificación a los ciudadanos españoles, tanto física como electrónicamente, y permitir la firma electrónica para los trámites con las Administraciones Públicas. Al ser un documento con un nivel de seguridad mayor que el antiguo, se intenta fomentar la confianza de los ciudadanos para su uso en trámites administrativos por medios electrónicos, además de como medio de identificación.

El DNIe tiene impresos los datos del titular (apellidos y nombre, sexo, nacionalidad, fecha de nacimiento en el anverso, y lugar de nacimiento, nombre de los padres y domicilio del titular en el reverso) y una fotografía en blanco y negro, el número de DNI, la firma manuscrita del titular, el número de serie del soporte y la fecha de validez del documento, y caracteres OCR-B de lectura automática.

Figura 3 Anverso y reverso del DNIe. Fuente: “Guía de referencia básica” v2.1 (http://www.dnielectronico.es)

En el chip estarán almacenados los siguientes datos encriptados: de filiación del titular, las imágenes digitalizadas de la fotografía y la firma manuscrita, la plantilla de la impresión de la huella dactilar, los certificados electrónicos de autenticación, firma y de la autoridad emisora, y un par claves para cada certificado. Esta información está estructurada en tres zonas:

- En la primera zona, de acceso libre, estarán los certificados. El acceso a esta zona estará restringido mediante una clave personal de acceso (PIN).
- En la segunda zona, de acceso restringido a las Fuerzas y Cuerpos de Seguridad del Estado, se almacena la huella dactilar del individuo.
- En la tercera zona se encuentran los datos de filiación del ciudadano, y también será de acceso restringido.

Los certificados contenidos en la tarjeta permiten realizar las siguientes funciones:

- Certificado de autenticación, que permite acreditar la identidad del ciudadano por medios electrónicos.
- Certificado de firma electrónica reconocida, que garantiza al ciudadano poder firmar electrónicamente documentos, y acreditar la procedencia del documento y la identidad de firmante.

4.1.2 Control de asistencia / presencia

Aunque el control de asistencia o presencia es un método de control de accesos, que únicamente añade nuevos requerimientos, conviene dedicarle unas líneas a esta funcionalidad, asociada al desarrollo de nuevas aplicaciones y servicios, puesto que el funcionamiento de la tarjeta y el dispositivo lector es equivalente.

El control de asistencia o presencia podía resultar engorroso y sujeto a engaños, debido a los procedimientos que se utilizaban hasta ahora: generalmente, se identificaba al individuo y se solicitaba su firma, de manera que aseguraba su presencia. Después, era necesario comprobar las firmas de los asistentes y validarlas.

Con el uso de tarjetas chip es posible controlar la asistencia de una manera muy sencilla, solicitando que el participante pase su tarjeta por un lector cuando entra en las instalaciones o salas de reuniones. Con esta información se genera una base de datos de los asistentes al evento, evitando la identificación o acreditación previa. El nivel de seguridad se puede aumentar exigiendo al usuario que cada vez que se entre o salga de las instalaciones, deba utilizar la tarjeta. Este procedimiento depende casi exclusivamente de las aplicaciones que se desarrollen para utilizar los datos obtenidos del uso de la tarjeta.

En el entorno empresarial, se está generalizando el uso de tarjetas chip para comprobar que el empleado cumple sus horarios (además de otras funciones de la tarjeta) mediante el control de accesos, es decir, realiza la función de un control de presencia gracias a aplicaciones que calculan las horas de entrada y salida del empleado.

4.1.3 Almacenamiento de información

Las tarjetas chip tienen una capacidad de almacenamiento de información mucho mayor que las tarjetas de banda magnética, puesto que pueden incorporar varios módulos de memoria en el circuito integrado. Si además uno de estos módulos es una memoria EEPROM, es muy fácil la actualización o modificación de los datos contenidos en la tarjeta. Por esta razón, los principales emisores de tarjetas del mundo están paulatinamente incorporando el chip en sus tarjetas.

Como se ha comentado varias veces a lo largo del libro, las tarjetas chip además presentan la ventaja respecto a las tarjetas de banda magnética de poder proteger la información que contienen según diferentes niveles de seguridad, mediante la inserción de un microprocesador criptográfico en el chip.

A continuación se exponen los tipos de tarjetas más utilizados para el almacenamiento de información:

- Tarjeta SIM: este tipo de tarjetas son las que se utilizan en los teléfonos móviles. Básicamente, la tarjeta SIM es un tipo de tarjeta inteligente, en un formato físico más pequeño de lo habitual, pero con la misma capacidad de almacenamiento de la información, protección de acceso a esta información y gestión de los algoritmos criptográficos que permiten la comunicación segura. En la tarjeta se almacenan las características del operador de telecomunicaciones que ha vendido la tarjeta, los servicios asociados, además de tener un espacio para poder almacenar otros datos, como números de teléfono o mensajes sms.

- Tarjetas prepago: este tipo de tarjetas son las que se utilizan para el pago en máquinas expendedoras, el transporte, o anteriormente, para los teléfonos públicos (este uso cada vez es menor debido al despliegue de los teléfonos móviles). Estas tarjetas son tarjetas con memoria, sin microprocesador, puesto que lo único que necesitan es almacenar la información del dinero acumulado en la tarjeta, de tal modo que según se consume el dinero, se va actualizando esa información en la tarjeta. Otros datos que suelen almacenar esta tarjeta en su memoria son los datos del fabricante, el número de serie de la tarjeta, el identificador de la tarjeta,...

- Tarjetas de memoria (SD, MiniSD, MicroSD, MMC/SD, etc.): la función de una tarjeta de memoria es justamente el almacenamiento de la información. Estas tarjetas contienen memorias de lectura y escritura que permiten la salvaguarda de los datos en la tarjeta. El problema de este tipo de tarjetas es que generalmente no incluyen un microprocesador criptográfico, perdiendo la posibilidad de utilizar algoritmos criptográficos que aumenten el nivel de seguridad. El despliegue y uso de este tipo de tarjetas, cada vez más generalizado, está provocando que otros elementos utilizados para el almacenamiento de información, como CDs y DVDs, se estén quedando obsoletos.

4.1.4 Medios de pago

El sistema financiero fue uno de los pioneros en la utilización de tarjetas chip para aplicaciones de medios de pago. Las primeras tarjetas chip sólo permitían su uso como monederos electrónicos, es decir, era necesario realizar una carga de dinero en la tarjeta antes de poder utilizarla, y estaban dirigidas a aplicaciones en máquinas expendedoras, parkings, taxis, las primeras tarjetas universitarias,...

En los últimos años, gracias al estándar EMV, estándar internacional de interoperabilidad de tarjetas inteligentes para la autentificación de pagos mediante tarjetas de crédito y débito, se ha visto difundido su uso para cualquier tipo de pago. EMV es un acrónimo de "Europay MasterCard VISA", las tres compañías que inicialmente colaboraron en el desarrollo del estándar. Este estándar define la interacción y comunicación entre las tarjetas y los terminales de una forma segura[3].

El objetivo de la especificación es definir los procedimientos y acciones necesarias para la interoperabilidad segura entre tarjetas chip y terminales, definiendo los procesos que se deben llevar a cabo, es decir, una vez se introduce la tarjeta en el terminal (que debe ser compatible con dicho estándar) y se autentica (generalmente mediante el tecleo del PIN asociado a la tarjeta), se deberá comprobar la validez de la tarjeta y el titular de la misma, así como los permisos y servicios asociados a esta tarjeta e individuo, permitiendo un nivel mayor de seguridad respecto a las tarjetas de banda magnética, pero a un coste también mayor.

Las ventajas de utilizar tarjetas inteligentes en el sector de medios de pago son numerosas:

- Reducción del fraude, puesto que la falsificación de una tarjeta inteligente, debido a su seguridad gráfica y la seguridad lógica del chip (uso de algoritmos de cifrado), es mucho más complicado que la falsificación de una tarjeta de banda magnética (se necesitaría descifrar los algoritmos EMV de la tarjeta y duplicar los chips de la misma).

- Posibilidad de controlar de forma detallada la aprobación de transacciones off-line.

3 En el anexo III se explica con más detalle el estándar EMV.

- Unificación en una misma tarjeta de diferentes medios de pago: monedero, crédito, débito y otras aplicaciones no financieras (por ejemplo, las Tarjetas Universitarias).

- Nuevos canales financieros: internet, móvil, TV banking,…

- Sistemas de fidelización de clientes, a través de un programa de puntos o descuentos cada vez que se utilice la tarjeta.

Los inconvenientes de utilizar este tipo de tarjetas como medios de pago están relacionados con el coste (cambios en la infraestructura existente: sistemas, terminales, tarjetas chip, procesos de autorización, etc.) y el mayor tiempo de procesamiento que conlleva su uso, debido a los cálculos de los algoritmos criptográficos que pueden incorporar.

4.1.4.1 Monederos electrónicos

La operativa de las tarjetas monedero es el siguiente:

- Consumo: los pagos se realizan en el momento, sin necesidad de estar conectado a una red de comunicaciones que permita a una entidad financiera validar la transacción, puesto que el dinero con el que se realiza el pago está precargado, es decir, primero se carga en la tarjeta una cierta cantidad de dinero, y se puede utilizar la tarjeta mientras exista dinero en el mismo. Cuando una persona utiliza la tarjeta para pagar, se le resta esta cantidad del dinero que hay almacenado virtualmente en la misma. En el terminal de punto de venta, denominado TPV, se quedan grabadas las operaciones realizadas, de manera que se puede proceder de la siguiente manera:

  - *Mediante otra tarjeta inteligente*, que se suministra al comerciante, denominada de colecta o de comerciante, se acceden a los datos de las transacciones que estaban almacenados en el TPV, realizando una copia de los mismos. Una vez descargados los datos, se realiza una transacción con las entidades financieras para poder hacer el ingreso del dinero. Una vez realizado, se vuelve a insertar en el TPV para confirmar que la transacción con la entidad financiera ha sido correcta y se borran los datos almacenados.

- *Mediante conexión con la entidad financiera a través de una red de comunicaciones*, debido a que los TPVs están conectados directamente con la entidad financiera y se validan las operaciones en el momento del pago. Una vez realizada con éxito la operación, se borra la misma de la memoria.

- Carga: la carga se puede realizar en las propias máquinas, en cajeros automáticos, en puntos de venta,... dependiendo del sistema implementado para el pago de tarjetas, muy asociado con el tipo de usuarios al que van dirigidos. Por ejemplo, no es lo mismo una tarjeta prepago para máquinas expendedoras en una empresa que las tarjetas para el parking en zonas del centro de las ciudades.

Existen numerosas ventajas del uso de estas tarjetas monedero:

- Simplifica el trabajo del comerciante, puesto que las operaciones se almacenan en la tarjeta y reduce las operaciones de caja.

- El usuario no necesita llevar dinero en metálico para poder hacer uso de las máquinas, no necesita el dinero exacto cuando la máquina no tiene cambio.

- Al ser utilizado para cantidades pequeñas, no hay tantos problemas por robo o pérdida como puede suceder con una tarjeta de crédito / débito.

Según se deduce de esto, debería resultar fácil el despliegue de las tarjetas por las ventajas que proporcionan; sin embargo, este tipo de tarjetas no ha funcionado todavía a no ser en entornos cerrados (por ejemplo, máquinas expendedoras en empresas, o servicios de la universidad).

Los servicios en los que se utiliza este tipo de tarjetas monedero son:

- Máquinas expendedoras (vending).

- Parkings y zonas reguladas para el estacionamiento en ciudades.

- Comercios.
- Tarjetas universitarias.
- ...

4.1.4.2 Tarjetas financieras

El estándar EMV (desarrollado por Europay, MasterCard y VISA, aunque ahora EMVCo, grupo encargado del estándar, está formado por las empresas American Express, JCB, MasterCard y Visa) es un estándar que define la interoperabilidad entre tarjetas chip y terminales y lectores de tarjetas en operaciones financieras y la compatibilidad de los mismos, independientemente del fabricante. Esta compatibilidad no se reduce a los terminales actuales, sino que tiene en cuenta la posibilidad de utilizar nuevos instrumentos de pago, como el pago sin contacto o el pago mediante el teléfono móvil.

En este sentido, en España se está produciendo una sustitución progresiva de las actuales tarjetas de banda magnética por tarjetas EMV, debido a las directrices de la Comisión Europea y el Banco Central Europeo, los cuales fijan la fecha límite del 31 de diciembre de 2010 para migrar al estándar EMV todo el parque de tarjetas y terminales.

A fecha de 31 de marzo de 2010, en España únicamente el 26% de las tarjetas bancarias cumplían con el estándar EMV, en comparación al 98% de los cajeros automáticos y el 86% de los TPVs. A finales del pasado año 2010, todas las tarjetas que se emitían deberían ser tarjetas con tecnología EMV.

El mayor beneficio de utilizar las tarjetas EMV es el nivel de seguridad asociado a las mismas. Estas tarjetas realizan las operaciones de identificación y autenticación propias de las tarjetas financieras, pero añaden otras características que mejoran su seguridad en las transacciones entre el terminal o dispositivo lector y las tarjetas: uso de algoritmos criptográficos, uso del PIN de la tarjeta para medios de pago, validación del titular de la tarjeta, comprobación de las operaciones que se van a validar y el lugar desde donde se realizan,...

Además, el estándar define los procedimientos para poder controlar la aprobación de transacciones que se realizan de forma off-line, es decir, sin tener que estar conectadas a una red de comunicaciones para validar y verificar la identidad del individuo y las operaciones y servicios que puede realizar, y validar el riesgo de impago, según la información y aplicaciones que contenga la tarjeta.

Al utilizar sistemas criptográficos, estas tarjetas aumentan el tiempo necesario para el procesamiento de los datos respecto a las tarjetas de banda magnética, en las cuales las funciones de encriptación las realiza el terminal o dispositivo lector en el momento del envío de la información. Aún así, el uso de estos algoritmos incrementa exponencialmente el nivel de seguridad, que no significa que no se puedan producir pequeños resquicios por donde accedan los falsificadores (es decir, el fraude se reduce pero no se elimina completamente).

Por poner un ejemplo de fraude de tarjetas EMV, se expone un caso que sucedió en Reino Unido con un grupo de falsificadores. El ataque no estaba dirigido directamente a las tarjetas, sino a los terminales y lectores. De esta manera, decidieron modificar los terminales de venta EMV, acción que sólo podían realizar en el mismo momento de la fabricación, e introducirlos rápidamente en el mercado. Estos terminales modificados permitían la copia de los datos de la tarjeta y el PIN antes del cifrado de la información. Una vez conseguidos estos datos, se cifraban empleando las claves criptográficas de los usuarios y se enviaban a servidores remotos. En los servidores se descifraba la información, se accedía a los datos almacenados, y se disponía del PIN. Aunque este tipo de ataques es muy sofisticado, deja constancia de que cualquier proceso, por muy seguro que sea, deja algún resquicio, por lo que el objetivo debe ser reducirlos al mínimo posible.

4.1.5 Otros servicios

Gracias al despliegue de tarjetas inteligentes (como el DNIe, tarjetas sanitarias, tarjetas universitarias, tarjetas financieras que cumplan el estándar EMV,...) y la estandarización que se ha producido, actualmente existen multitud de aplicaciones y nuevos servicios que se pueden ofrecer. Estas nuevas funcionalidades parten de la base de que la tarjeta inteligente es un sistema de identificación más seguro que otros sistemas, y que adicionalmente permite proporcionar servicios de valor añadido según las características de las mismas (tarjetas de proximidad, tarjetas criptográficas, etc.).

4.1.5.1 Fidelización

Actualmente es uno de los servicios más demandados. Las compañías, sobre todo las empresas de servicios, calculan que el coste de conseguir un nuevo cliente es mucho mayor que el coste de mantenerlo, por lo que la mayoría de las grandes empresas están emitiendo tarjetas chip a sus clientes que permiten ofrecer nuevos servicios y ventajas o descuentos.

Los primeros sectores que empezaron a utilizar estas tarjetas fueron el transporte y los comercios, de manera que se acumulan puntos por cada compra o servicio que se solicite. El titular de la tarjeta puede canjear los puntos acumulados por nuevos servicios, descuentos o regalos, además de las ventajas asociadas a pertenecer a un club, con promociones exclusivas para los socios y derecho a servicios más exclusivos.

Adicionalmente, la mayoría de las tarjetas inteligentes (tarjetas EMV, tarjetas universitarias, Tarjetas Ciudadanas,...) proporcionan descuentos en comercios, cines, teatros,... Esto produce un efecto de retención de los usuarios, puesto que los usuarios se acostumbran a este tipo de descuentos y no es grato perderlos.

4.1.5.2 Servicios de comedor, viajes, bonos

Según la normativa vigente, las ayudas de comedor que algunas empresas e instituciones dan a sus empleados y beneficiarios deben estar controladas y sujetas a regulación, puesto que si un día no se trabaja o no se asiste al comedor, no se debería recibir la ayuda asociada. Esta es la razón de que se empiecen a utilizar tarjetas inteligentes que permiten el pago y control de estas ayudas de comedor, denegándole el uso para cualquier otro establecimiento u horarios que no sean los acordados o asociados a las ayudas.

Las Universidades han sido pioneras en la aplicación de estos servicios: las tarjetas chip universitarias se utilizan para el pago de servicios de comedor, puesto que es una manera sencilla para la universidad de llevar un control, y para el alumno, puesto que no tiene que llevar dinero “en metálico”.

En los centros de mayores y centros y comedores sociales se podría utilizar este tipo de servicios (comedor, viajes, bonos) que ofrecen las tarjetas inteligentes para agilizar los trámites y facilitar el acceso a los ciudadanos.

4.2 ENTORNOS DE APLICACIÓN DE LA TARJETA CHIP

El despliegue e implantación de sistemas que utilizan tarjetas inteligentes es cada vez mayor debido a sus múltiples ventajas, a la facilidad de las comunicaciones y a la seguridad y flexibilidad que ofrecen.

Este apartado pretende concretar los usos y aplicaciones de tarjetas chip, que se han ido desglosando a lo largo del libro, en varios sectores: sector público (Entidades Locales), sector financiero, sector educativo,...

4.2.1 Servicios orientados a Ayuntamientos

La modernización de las Administraciones Públicas y la aplicación de la normativa vigente, que pretende desarrollar el concepto de Administración Electrónica, está permitiendo ofrecer nuevos y novedosos servicios a los ciudadanos mediante medios electrónicos, que mejoran la relación entre las Entidades Locales y sus ciudadanos y les facilitan los trámites administrativos, mediante el uso de las nuevas tecnologías.

La implantación de sistemas de tarjetas chip, como la Tarjeta Ciudadana o el DNI electrónico, puede facilitar el acceso a los servicios que se detallan en este apartado.

4.2.1.1 Transportes

Uno de los primeros servicios en ofrecerse mediante el uso de sistemas que incorporen tarjetas inteligentes es el pago y acceso a los transportes públicos, puesto que facilita la utilización del transporte público y reduce las colas que se forman en el control de accesos de autobuses, metro, cercanías y tranvías.

El mecanismo de uso para el ciudadano es sencillo:

1. El primer paso es solicitar la tarjeta en los puntos de venta o emisión, normalmente en estancos, quioscos y en la red de transportes municipal.

2. Una vez solicitada, será necesario realizar la compra de un bono (normalmente mensual o anual, aunque en algunas ciudades se permite la carga de unidades de viaje o bonos de varios viajes), que permitirá el uso de la tarjeta durante un periodo de tiempo.

3. Para acceder a un medio de transporte que integre un sistema de tarjetas chip, se acerca o se inserta la tarjeta en alguno de los lectores que están visibles en la entrada del mismo, dependiendo de si es una tarjeta sin contactos o con contactos respectivamente, y se valida el acceso.

4. Cuando se agoten los viajes que se habían comprado o el periodo de tiempo por el que era válido, será necesario recargarla. Es decir, el titular de la tarjeta podrá utilizarla durante varios años (en general, cinco años) sin tener que tirarla y comprar otra nueva, simplemente acercándose a los puntos donde se emite o recarga.

Un ejemplo práctico de un sistema de tarjetas chip es el caso de la ciudad de Valencia. Desde hace varios años se viene utilizando la tarjeta Móbilis, tarjeta que permite el uso de la red de transporte público de la ciudad. Esta tarjeta ha ido evolucionando: de ser una tarjeta de banda magnética en los primeros años, actualmente se emite una tarjeta inteligente con chip integrado. Este cambio ha permitido que, en el caso de pérdida o robo, se puedan recuperar los viajes de EMT cargados y no disfrutados (con la tarjeta de banda magnética se perdían los bonos, aunque existen sistemas y procedimientos que podrían utilizarse para recuperarlos). También ha permitido mejorar el procedimiento de emisión, puesto que ahora se obtiene el carné en el mismo instante de la tramitación, sin tener que esperar a que te lo enviasen. Esto ha provocado que su difusión haya sido muy buena: en mayo de 2010, más de 350.000 valencianos disfrutaban de la tarjeta inteligente en los autobuses.

Existen varios casos prácticos de ciudades que, viendo la utilidad de este tipo de tarjetas (tarjetas inteligentes), están promocionando su uso o están desarrollando proyectos pilotos para llevar a cabo su implantación en una fase posterior.

4.2.1.2 Alquiler de bicicletas

El alquiler automático de bicicletas mediante tarjetas inteligentes está todavía en una fase inicial de implementación, aunque actualmente ya se pueden encontrar algunos ejemplos de integración de estos sistemas con el sistema público de transportes, mediante la incorporación de este servicio a la oferta de servicios que ofrecen las Entidades locales, por ejemplo, por medio de la Tarjeta Ciudadana. En cambio, se pueden encontrar más ejemplos de servicios de alquiler de bicicletas en el que se utilice una tarjeta chip para la identificación del usuario, sin ser un procedimiento automático. También existen ejemplos de sistemas de alquiler en el que se puede realizar el pago mediante la utilización de una tarjeta monedero electrónico.

Una ventaja de implantar un sistema de tarjetas chip para el alquiler automático de bicicletas es que no hace falta un operario que esté atendiendo al público para poder hacer uso de la bicicleta o devolverla, por lo que pueden estar funcionando veinticuatro horas al día. El sistema funciona de la siguiente manera: el usuario introduce su tarjeta en un lector instalado en los puntos de recogida de bicicletas; las órdenes de operación se centralizan y se transmiten a cada punto de anclaje donde están las bicicletas, de forma que lo libera o bloquea, dependiendo de si se quiere recoger la bicicleta o devolverla; el usuario se comunica mediante una pantalla táctil o un teclado que existirán en estas zonas.

El problema radica en que los sistemas automáticos requieren una inversión inicial grande en infraestructuras y tecnología, aunque permiten un mayor control e información para el análisis posterior (tarifas, lugares donde montar un punto de bicicletas, descuentos,...), pudiendo prevenirse el robo y vandalismo.

Según la “Guía metodológica para la implantación de sistemas de bicicletas públicas en España”, editada por el Ministerio de Industria, Turismo y Comercio, este sistema es ideal para ciudades de tamaño grande o mediano, con una demanda elevada.

Existen varias experiencias de este tipo en Holanda, Francia, Bélgica, Noruega,..., donde es más común el uso de bicicletas. En Londres se ha lanzado un proyecto en el verano de 2010 con cuatrocientas estaciones y unas seis mil bicicletas.

En Barcelona existe un sistema público de bicicletas, siendo necesario registrarse para conseguir la tarjeta de usuario con un abono anual. Una vez obtenida, el usuario se puede acercar a un punto-bici, alquilar una bicicleta y dejarla en otro punto de la ciudad. Si se encuentra una estación donde están todos los sitios ocupados, se acerca la tarjeta por al lector, puesto que es una tarjeta sin contactos, y se obtienen diez minutos más de tiempo extra, y un mapa con las direcciones de los puntos-bicis más cercanos donde puedes devolverla. Otras ciudades de España están empezando a implantar sistemas similares, como Gijón, Ponferrada,..., aunque su implantación es lenta por conllevar una inversión inicial grande, tal y como se ha comentado en este apartado.

4.2.1.3 Acceso a zonas peatonales / restringidas

El centro, o casco antiguo, de la mayoría de las ciudades tienen restringido el paso de vehículos excepto para residentes. La tarjeta inteligente puede proporcionar un servicio que permite el acceso a estas zonas en condiciones especiales, cumpliendo una serie de requisitos.

Por ejemplo, para los residentes con plaza de garaje se les puede permitir el paso, y a los residentes sin plaza de garaje, se les puede permitir el aparcamiento en superficie.

El Ayuntamiento de Ponferrada, mediante la Tarjeta Ciudadana, ofrece este servicio a personas residentes en las zonas peatonales que quieran solicitarlo.

4.2.1.4 Administración pública: e-government

La Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (en adelante LAECSP) establece la necesidad de adaptar los procedimientos de la Administración Pública a los medios electrónicos, representando el marco general en el que se desarrolla la Administración Electrónica en España:

- La Ley fija el derecho de los ciudadanos a relacionarse con las Administraciones Públicas (Administración General del Estado, Autonómica y Local) por medios electrónicos.

- La Ley define la configuración de los aspectos básicos en el ejercicio de la actividad administrativa a través de medios electrónicos o telemáticos.

- Los principios para la cooperación e interoperabilidad entre Administraciones en el impulso de la Administración Electrónica.

Efectivamente, la progresiva utilización de medios electrónicos para comunicarse con la Administración implica, no ya la necesaria adaptación de ésta a una nueva forma de relacionarse con los ciudadanos, sino también la adecuación de sus formas de actuación y tramitación de los expedientes y, de manera genérica, la adaptación de sus procedimientos a la realidad que imponen las nuevas tecnologías, tal y como se recoge en la exposición de motivos de la citada norma.

Las tarjetas inteligentes son parte fundamental en esta adaptación, destacando cuatro tipos de tarjetas inteligentes que se utilizarán para acceder a estos servicios:

- El DNI electrónico: el DNI electrónico es un tipo de tarjeta inteligente, que incorpora un pequeño circuito integrado (chip). Su uso, adicionalmente al tradicional del DNI, sigue una doble vertiente:

  - Por una parte autentica electrónicamente y de forma inequívoca la identidad de la persona titular, de forma que permite operar en entornos digitales no presenciales con la misma certeza que en el mundo físico.

  - Por otra parte, aporta firma electrónica reconocida, acreditando la voluntad del titular de firmar digitalmente documentos, con la misma validez jurídica que si se hubieran firmado físicamente, de forma manuscrita (Ley 59/2003 de Firma Electrónica y RD 1553/2005 de regulación del DNI y sus certificados de firma electrónica).

- La Tarjeta Ciudadana: el objetivo de la Tarjeta Ciudadana es facilitar los servicios y mejorar la experiencia del usuario cuando los utiliza. La Tarjeta Ciudadana se puede utilizar para ingresar en la Oficina Virtual y autenticarse mediante la clave (por ejemplo, la Tarjeta Ciudadana del Ayuntamiento de Gijón).

- La tarjeta de empleado público: la Ley 11/2007 desarrolla un nuevo concepto, el certificado de empleado público. Estos certificados pueden incluirse en una tarjeta criptográfica, permitiendo la identificación del empleado, acceso a instalaciones y sistemas, funcionalidades asociadas a su cargo, así como acceso a otros servicios asociados a su condición de empleado de la Administración. El empleado siempre podrá utilizar su DNI electrónico en lugar de la tarjeta.

- Las tarjetas criptográficas (PSCs): los proveedores de servicios de certificación (PSCs) llevan años suministrando tarjetas inteligentes con capacidades criptográficas que incluyen los certificados que emiten. Estos certificados pueden utilizarse para acceder a servicios de Administración Electrónica. En general, la mayoría de las administraciones permiten el uso de un certificado emitido por la FNMT; este certificado suele suministrarse en formato software, aunque siempre existe la opción de comprar una tarjeta e introducirlo en la misma. La aceptación y validación de certificados que emiten otros PSCs dependerá del organismo con el que se realiza el trámite.

Los trámites administrativos que se pueden realizar mediante el uso de estas tarjetas quedan fuera del alcance del presente libro, y dependerán de los tipos de servicios prestados por cada Administración Pública.

El reto que se plantea ahora es traspasar las barreras de la reticencia todavía existente en la ciudadanía y guiar a los ciudadanos para que comiencen a aprovechar las múltiples ventajas de este tipo de tarjetas. Para ello, el primer paso es dar a conocer la oferta de servicios actualizada de las Administraciones Públicas.

4.2.1.5 Monederos para adquisición de servicios municipales

Las tarjetas monedero fueron los primeros desarrollos que se realizaron para sistemas de tarjetas inteligentes, debido a su capacidad de almacenar información y procesarla. El procedimiento de uso para el ciudadano es sencillo:

1. Se solicita la tarjeta monedero (dependiendo de los casos, esta tarjeta puede llevar otros muchos servicios asociados, como pueden ser las tarjetas universitarias o las Tarjetas Ciudadanas).

2. En puntos adecuados para ello, como cajeros automáticos, TPVs u otros puntos de servicio, se carga la tarjeta con una cantidad de dinero. Estos lectores de tarjetas pueden estar conectados con las entidades financieras para facilitar la recarga, o con operadores de medios de pago.

3. A partir de ese momento, la tarjeta funciona como si fuera dinero en efectivo, pudiendo utilizarla para el pago de servicios en donde se permita y exista un terminal de pago. El valor del dinero en la tarjeta se actualiza cada vez que se realice una transacción.

Estas tarjetas suelen permitir el pago de pequeños importes, puesto que su función es ser una tarjeta monedero. La comodidad y seguridad del sistema y el coste de la transacción, el cual es nulo puesto que las entidades bancarias no intervienen el momento de realizar el pago por compra de servicios, permiten que este servicio se haya extendido rápidamente entre los servicios de los que se benefician los usuarios de estas tarjetas.

4.2.1.6 Acceso / reserva de instalaciones deportivas

Las instalaciones deportivas siempre requieren un control de accesos para permitir únicamente a los individuos que tienen contratado algún servicio acceder a las mismas. El uso de las tarjetas inteligentes como sistemas de control de acceso y monederos está permitiendo que cada vez un mayor número de centros utilicen este sistema.

El uso de las tarjetas para instalaciones deportivas públicas se inició en las Universidades, mediante el carné universitario. En una primera fase, los servicios desarrollados sólo permitían la reserva de las instalaciones, pudiendo consultar la disponibilidad de los mismos y en su caso, proceder a realizar la reserva. En varias universidades españolas ya se utiliza como sistema de acceso a las instalaciones, puesto que permite identificar si un individuo es usuario y tiene contratado el servicio, así como realizar el pago de cursos, actividades deportivas, alquiler de las instalaciones,...

En la actualidad, mediante el despliegue de Tarjetas Ciudadanas que se está realizando en diferentes ciudades de España, se están empezando a desarrollar estos servicios, entre los que se incluyen la reserva y el acceso a piscinas, gimnasios, pistas de tenis, campos de fútbol, y cualquier instalación deportiva.

4.2.1.7 Acceso a museos y centros sociales

Mediante las tarjetas se pueden conseguir descuentos sobre las entradas a los museos o se pueden utilizar como identificación para poder acceder al mismo de forma gratuita o con reducción del precio de la entrada. Estos servicios están en fase de implantación en ciertas ciudades donde existen sistemas de tarjetas.

Las tarjetas también se están empezando a usar en otras instalaciones, aunque todavía son muy pocas las Entidades Locales que ofrezcan servicios basados en estos sistemas:

- Bibliotecas: para el acceso a las mismas, préstamo de libros, consulta de catálogos, y cualquier servicio que se ofrezca.
- Centros de mayores: para acceso a los centros, comedores, actividades que se realizan, viajes, etc.

4.2.2 Otros Sectores

Además de su aplicación para servicios ofrecidos por Administraciones Públicas, las tarjetas chip llevan muchos años utilizándose en otros sectores, que se explican brevemente en el presente apartado.

4.2.2.1 Sector educativo

Las universidades llevan varios años implementando servicios relacionados con la Tarjeta Universitaria.

Las tarjetas universitarias son tarjetas inteligentes desarrolladas por las Universidades, generalmente en colaboración con entidades financieras, que identifica a los miembros de la Universidad (alumnos, docentes y personal administrativo) y permite el acceso a servicios e instalaciones (deportivas, laboratorios, zonas de seguridad,...). El único requisito que se suele exigir es estar matriculado en ese año académico en alguna de las carreras que ofrece la universidad.

Los servicios más representativos que se ofrecen a través de la tarjeta en las Universidades son:

- Identificación y autenticación en la Universidad (por ejemplo, para exámenes).
- Pago de matrículas y tasas y acceso a servicios online, como consulta del expediente académico, matriculación,...
- Control de acceso a bibliotecas y préstamo de libros (Proyectos Fin de Carrera).
- Control de acceso a instalaciones deportivas.
- Control de acceso a laboratorios, aulas informáticas,...
- Control de acceso a los aparcamientos de la universidad.
- Monedero electrónico: para pagos en cafeterías y comedores, servicios de reprografía, máquinas expendedoras,...
- Ventajas y descuentos en cines, comercios, museos, teatros, transportes urbanos,...

Algunas Universidades ofrecen adicionalmente la posibilidad de convertir la tarjeta universitaria en tarjeta financiera (tarjeta de débito), que permite realizar las mismas funciones que si la hubieses emitido alguna entidad financiera, con el aliciente de que es gratuita. Para poder ofrecer este servicio, se necesita la colaboración de alguna entidad financiera.

La solicitud de emisión de la tarjeta se suele realizar mediante formulario web, y todas las operaciones relacionadas con la misma (renovación, sustitución por robo o extravío, cambio de PIN, regeneración de PIN,...) también se podrán realizar a través de la página de la Universidad (sede electrónica). La recogida de la tarjeta suele realizarse en alguno de los puntos de la universidad donde se pueda ofrecer este servicio (en general, en las secretarías de las facultades y escuelas).

Se muestra a continuación unos ejemplos de estas tarjetas, específicamente, la de la UNED y la de la Universidad Politécnica de Madrid.

Figura 4
Ejemplos de Tarjetas Universitarias. Tarjeta Universitaria de la UNED y Tarjeta Universitaria de la Universidad Politécnica de Madrid

Algunas Universidades han dado un paso más y han utilizado una tarjeta criptográfica, que incorpora certificado de usuario, y permite acceder a los servicios prestados por las Administraciones Públicas, autenticación electrónica y sistemas de firma electrónica avanzada.

La mayoría de las tarjetas incorporan los datos del usuario y una fotografía reciente.

Cabe resaltar en este apartado que dentro del Proyecto SCANet (Sistema de Codificación Académica Normalizado en Red), que se está encargando de desarrollar normas de aplicación para los servicios de intercambio de datos de gestión académica, de manera que se pueda conseguir una convergencia de gestión entre las universidades del espacio europeo, se ha desarrollado una norma para la Tarjeta Universitaria Inteligente Homologada (TUIH). La norma 6.02/04E-TUIH define el formato de las Tarjetas Universitarias, la identidad gráfica, el contenido del mismo y la estructura del chip de la tarjeta, unificando los dos tipos de tarjetas que se venían utilizando (TIBC, Tarjeta Inteligente de Bancos y Cajas, y la WG10).

La caducidad de las tarjetas dependerá del tipo de tarjetas y del colectivo al que pertenezca el titular. Algunas Universidades desactivan el chip al iniciar un nuevo curso académico, y se debe actualizar de una manera sencilla, generalmente es suficiente con realizar una consulta en los terminales de información de la universidad.

4.2.2.2 Sector financiero

El sector financiero es un gran consumidor de este tipo de tarjetas. En España, la mayoría de las tarjetas que existen son de banda magnética, pero desde hace unos años, esta tendencia está empezando a cambiar. El coste de fabricación de las tarjetas con chip integrado se ha reducido, y los beneficios de su uso han provocado que las nuevas tarjetas que se suministran sean de este tipo. A este hecho ha ayudado el estándar EMV, descrito en apartados anteriores.

Esto, unido al cambio provocado por la irrupción de nuevos canales, que posibilitan la realización de las operaciones por medios electrónicos, ha permitido que también se generalice el uso del DNI electrónico para el acceso y autentificación en las áreas de clientes de sus páginas en Internet.

El sector financiero abarca tres grandes áreas de actuación bien diferenciadas:

- Comercio electrónico.
- Seguros.
- Medios de pago.

El área que en los últimos años ha sufrido un cambio tecnológico importante son los medios de pago, los cuales han debido de transformarse para poder aceptar el pago electrónico securizado por Internet mediante el uso de tarjetas inteligentes. Esto ha provocado que existan grandes retos en el sector, puesto que resulta necesaria la renovación de las infraestructuras requeridas para proporcionar correctamente los servicios ofrecidos a través de Internet.

La obligatoria implantación de tarjetas y dispositivos lectores que cumplan el estándar EMV para cumplir con la legislación vigente, también ha permitido la transformación del sector, de manera que se sustituyan las antiguas tarjetas de banda magnética, por tarjetas híbridas, es decir, tarjetas inteligentes que incorporan la banda magnética.

4.2.2.3 Sector empresarial

Las empresas valoran la seguridad en sus centros de trabajo. La información y los datos que mantienen es uno de sus recursos más importantes, siendo necesario protegerla frente a posibles amenazas. Las amenazas pueden provenir desde fuera de los centros de trabajo, mediante ataques y robos de contraseñas, o desde los propios centros, mediante robos de ordenadores, portátiles, llaves de memoria,..

Para atajar el problema de la seguridad, las empresas exigen a sus empleados el uso de contraseñas fuertes en sus sistemas y aplicaciones, que sean difíciles de descifrar (incluyendo números, letras en mayúsculas y minúsculas, símbolos,...), cambios cada cierto tiempo,... Pero el peligro del uso de estas contraseñas proviene de los propios usuarios, que suelen intentar utilizar contraseñas que recuerden; puesto que si no son fáciles de recordar, se suele acabar apuntándolo en algún lado y la seguridad queda amenazada.

Las tarjetas inteligentes pueden ayudar a aumentar este nivel de seguridad en sus dos vertientes, puesto que proporcionan una identificación y autenticación robustas:

- Seguridad física: mediante control de accesos físicos.
- Seguridad lógica: mediante encriptación de la información.

Para ello, se pueden utilizar tarjetas duales (con contactos y sin contactos), criptográficas, que incluyan medidas de seguridad gráficas y banda magnética en su reverso. Esta integración permite su uso tanto para aumentar el nivel de control de accesos a los edificios e instalaciones de la empresa, como para el acceso a sistemas y terminales (ordenadores, portátiles, servidores,...).

En empresas que deban cumplir con normas de seguridad estrictas, se pueden incluir sistemas biométricos que permitan la identificación del usuario por sus rasgos únicos (huellas dactilares, iris, reconocimiento facial,...).

Este tipo de tarjetas presenta ventajas tanto para el empleado como para la empresa:

- Desde el punto de vista del empleado:
  - Autenticación fuerte mediante certificados digitales.
  - Comodidad y sencillez de uso.
  - Una única tarjeta puede sustituir a la mayoría de contraseñas que se utilizan para los diferentes sistemas y aplicaciones, con lo cual es más fácil de recordar.
  - Control de acceso seguro a edificios e instalaciones.
  - Posibilidad de cifrado de la información.
- Desde el punto de vista de la empresa:
  - Multiaplicación: una tarjeta puede ser utilizada para múltiples funciones, como el acceso a edificios e instalaciones, acceso a los sistemas,... Es decir, presenta las características de acceso físico y acceso lógico seguros.

- Modular: los sistemas de tarjetas permiten diseñar módulos independientes que interaccionen entre ellos, por lo cual se recomienda la utilización de arquitecturas SOA, que nos permitirá integrar fácilmente los distintos sistemas de forma escalonada, práctico tanto a nivel económico (puesto que permite la integración con otras tecnologías existentes, como la banda magnética o el código de barras) como organizacional (la gestión del cambio suele ser problemática si no se realiza con cuidado y en un periodo aceptable de tiempo).

- Refuerza la imagen de seguridad en la empresa: si la empresa empieza a tomarse el nivel de seguridad en serio, y es capaz de transmitírselo a sus empleados, estos prestarán mayor atención a cumplir estas normas. La tarjeta facilita este sentimiento, puesto que es algo tangible.

- Imagen corporativa: el uso de tarjetas personalizadas con logos e imágenes de la empresa, o con los datos del propio usuario, permiten mostrar una imagen corporativa fuerte, que se toma la seguridad muy en serio.

4.2.2.4 Sector sanitario

El sector sanitario es un sector que está en plena revolución respecto a las tarjetas inteligentes. En este sector se vienen utilizando tarjetas desde hace muchos años en la identificación del ciudadano para el acceso a los servicios sanitarios.

Las nuevas tecnologías están permitiendo que todo el papel que se utilizaba hasta este momento (historial clínico, resultados de las pruebas, radiografías,...) se digitalice, así como las recetas que se suministran a los ciudadanos. La digitalización de estos elementos permite una mejor gestión de la información, que podrán consultar los médicos, independientemente de dónde se haya tratado al ciudadano, y los propios ciudadanos.

Pero la digitalización exige un nivel de seguridad muy elevado, puesto que estos datos están protegidos por la Ley Orgánica de Protección de Datos, en la que España es uno de los países más avanzados. Para alcanzar este nivel de seguridad es necesario introducir nuevos elementos en el sistema, que permita asegurar la protección de los datos y la salvaguarda de la intimidad de los pacientes.

La única forma para asegurar la protección de los datos es el uso de una infraestructura de clave pública (PKI), y uno de los elementos necesarios para ello es la utilización de certificados digitales. Por supuesto, la seguridad se verá aumentada si estos certificados están contenidos en una tarjeta criptográfica, que permita el acceso a la información pero que no permita exportar las claves privadas del usuario.

Por ello, ha sido necesario crear estándares específicos para las comunicaciones en estos entornos. Dentro de estos estándares, la Smart Card Alliance identifica varios servicios en los que la tarjeta inteligente ayudará a simplificar trámites y facilitar la vida al usuario y el trabajo a los médicos y personal sanitario, con una gestión de la información centralizada, y medidas de seguridad fuertes:

- Consulta de los historiales médicos, que se convertirán en la Historia Clínica Electrónica, por lo que habrá que exigir un almacenamiento de la información seguro.
- Controles de acceso, tanto físicos como lógicos, de pacientes y profesionales sanitarios a los sistemas e instalaciones sanitarias.
- Información de médicos y ambulatorios, enfermedades,...
- Receta electrónica, para lo que se utilizará el soporte de la tarjeta sanitaria.
- Histórico de prescripciones.
- Identificación segura, tanto de los pacientes como de los profesionales sanitarios.
- Control de horarios.
- Pago de servicios: cafeterías, comederos, televisión en las habitaciones,...

En este sentido, en España algunas comunidades han iniciado, o está en pleno desarrollo, el despliegue de una tarjeta sanitaria, criptográfica, que se utiliza para la identificación del titular, autenticación, modificación de los datos, solicitud de citas médicas,... Entre las Comunidades que han realizado un esfuerzo mayor en este sentido, se encuentran Andalucía y Baleares.


5 PROYECTO DE IMPLANTACIÓN DE TARJETA CIUDADANA
Junta de Castilla y León
red de municipios digitales de Castilla y León

5. PROYECTO DE IMPLANTACIÓN DE TARJETA CIUDADANA

Antes de iniciar un proyecto de estas características en un Ayuntamiento, es necesario estudiar y evaluar la viabilidad del mismo. Para ello, será necesario realizar un análisis exhaustivo de los tipos de servicios que se quieren ofrecer, elementos y sistemas necesarios para ofrecer estos servicios, posibilidad de integración con los sistemas de que se disponen actualmente, tipos de tarjeta a distribuir, personalización requerida, público objetivo, procedimientos de emisión de las tarjetas a los ciudadanos, difusión del proyecto, etc.

A continuación se intentará dar unas nociones básicas de las necesidades que se deben tener en cuenta para realizar la implantación de un sistema de Tarjeta Ciudadana en Ayuntamientos.

5.1 ANÁLISIS DE SITUACIÓN Y PLANIFICACIÓN

El primer punto para iniciar un proyecto de estas características y envergadura en un Ayuntamiento es el análisis de la situación actual, que permita determinar los servicios que se prestan actualmente mediante el uso de tarjetas y la infraestructura desplegada para estos servicios. Con estos datos se podrá realizar una evaluación de la viabilidad del proyecto respecto al coste asociado a la prestación de los servicios que se quieren ofrecer.

En este sentido, se recomienda realizar los siguientes estudios de análisis de la situación actual como paso previo en los proyectos de implantación de una Tarjeta Ciudadana y la planificación posterior de las tareas asociadas:

- Análisis de los servicios actuales sobre los que se quiere implantar un sistema basado en tarjetas inteligentes: se analizarán los servicios, la forma en que se prestan, la tecnología asociada a los mismos, y los elementos, sistemas y arquitectura necesaria para que la prestación del servicio se realice correctamente. Si estos servicios hacen uso de tarjetas, también se analizará la tecnología de las mismas, el aspecto gráfico y la personalización, el mapa de datos de la tarjeta, etc.

- Análisis de los proveedores de cualquier elemento necesario para el servicio: se analizarán las características técnicas de los sistemas im-

plementados suministrados por los proveedores, mediante cuestionarios y entrevistas personales: arquitectura, sistemas, comunicaciones, funcionalidades y procedimientos operativos.

- Análisis de las tecnologías existentes de tarjetas inteligentes disponibles actualmente en el mercado, y la arquitectura necesaria para implementar estos sistemas. Para ello, se deberán analizar diferentes características: seguridad, tanto física como lógica, interoperabilidad, continuidad, proveedores, interfaces de usuario, y cualquier otro requisito que obligue o favorezca la elección de una tecnología en concreto.

- Análisis de la infraestructura existente que puede ser reutilizada para la prestación de los servicios mediante el uso de tarjetas. Cuando se habla de infraestructura, se debe tener en cuenta cualquier elemento, es decir, servidores, redes de comunicación, ordenadores, routers, dispositivos lectores de tarjetas, etc.

- Análisis de los costes de los elementos que forman el sistema, teniendo en cuenta la integración con la infraestructura existente y poniendo especial cuidado con los costes asociados a tarjetas (a las inicialmente emitidas habrá que añadir un porcentaje de reserva para emitir en caso de pérdida o robo), elementos físicos de las mismas (panel de firma, banda magnética, panel de firma, seguridad gráfica,…) y personalización (impresoras y consumibles). En el caso de elementos físicos, hay que prestar atención a la posible obsolescencia de cualquiera de sus elementos, que haga necesario tener un stock suficientemente preparado para cualquier eventualidad, en el cual se almacenen las piezas de repuesto.

- Definición del alcance del proyecto: una vez se tenga una idea general de todo lo expuesto anteriormente, se estará en posición de poder definir el alcance del proyecto, es decir, el tipo de solución de Tarjeta Ciudadana, elementos necesarios (teniendo en cuenta la infraestructura existente), planificación de las fases y posible evolución del sistema a corto y medio plazo para poder agregar nuevos servicios.

5.2 INTEGRACIÓN CON INFRAESTRUCTURA EXISTENTE

En cualquier estudio de viabilidad de un proyecto de implantación, el primer paso es realizar un análisis de la situación actual. En el caso de un proyecto de Tarjeta Ciudadana, se deberán analizar los servicios que se pretenden ofrecer, los sistemas, infraestructuras y elementos que se utilizan, y las posibles soluciones que existen en el mercado.

En muchas ciudades existen actualmente servicios que ya utilizan tarjetas, como pueden ser los transportes públicos o las zonas de aparcamiento regulado, el acceso a instalaciones deportivas,... En este caso, se debe analizar la posibilidad de reutilizar alguno de los elementos de estos sistemas para abaratar el coste del despliegue, teniendo siempre en cuenta los servicios más demandados y que su implantación suponga beneficios para los ciudadanos. La unificación de servicios en una misma tarjeta implicará un despliegue más rápido, sobre todo si se basa en un sistema ya existente y que los ciudadanos utilizan (el caso más claro es el del transporte público).

Los elementos a tener en cuenta en caso de que exista ya algún servicio que se ofrezca mediante la utilización de tarjetas son los siguientes:

- Tipo de tarjetas: dependiendo de los servicios que se quieran ofrecer, se deberá elegir el tipo de tarjetas que son necesarias para prestar dichos servicios. Normalmente, la primera elección versará sobre la utilización de una tarjeta con contactos, una tarjeta sin contactos o una tarjeta dual, puesto que dependiendo de esta elección, se utilizarán un tipo de sistemas u otros. También se deberá decidir si es necesario que la tarjeta provea de funciones criptográficas (en la mayoría de los casos).

  Una vez se haya elegido el tipo de tarjeta, se analizará la posibilidad de reutilizar las tarjetas que se suministran para alguno de los servicios del Ayuntamiento, si reúnen las características requeridas para las nuevas aplicaciones, y las posibilidades que ofrecen los proveedores actuales y los contratos de suministros actualmente adjudicados.

  Por poner un ejemplo, en el transporte de viajeros se impone el uso de tarjetas sin contactos, característica a tener en cuenta si existe actualmente alguna implementación de un sistema de este tipo.

- Tipo de dispositivos lectores de tarjetas: dependiendo del servicio que se ofrezca y del tipo de tarjeta que se haya elegido, se necesitarán distintos tipos de lectores. Como ya se ha indicado anteriormente, los lectores de proximidad son adecuados para control de accesos, mientras que los lectores de contactos están más indicados para los sistemas de pago o monederos electrónicos.

  Al igual que en el caso de las tarjetas, se analizará la viabilidad de reutilizar los dispositivos y terminales que ya están en funcionamiento.

- Memoria de la tarjeta: aunque en el análisis se encuentre un servicio que emite tarjetas que se podrían reutilizar para los nuevos servicios, es importante conocer la memoria que incluyen y las necesidades de memoria de las tarjetas, dependiendo de los servicios, información contenida en la tarjeta y tipo de aplicaciones que se cargarán en su memoria (el precio de la tarjeta varía en función de la capacidad de la misma).

- Infraestructuras de los sistemas: con este punto se quiere llamar la atención sobre la infraestructura necesaria según la arquitectura del sistema, es decir, redes de comunicaciones, servidores, ordenadores, routers y cualquier elemento de la arquitectura de sistemas. Aunque sea necesario cambiar el sistema y las aplicaciones, puesto que el funcionamiento sea distinto, se debe analizar la posibilidad de reutilizar todos estos elementos, puesto que el mayor coste suele proceder de la infraestructura.

- Puntos de venta, información y tramitación: es importante para el despliegue de la tarjeta reutilizar los puntos de venta o suministro para minimizar los costes. Dependiendo de los servicios ofrecidos y de los grupos de ciudadanos a los que se impacte con su implementación, se deberá escoger el sistema que permita un mayor despliegue a un menor coste. Por ello, además de tener en cuenta el lector, es necesario conocer si la actualización o modificación del firmware de los puestos permiten la reutilización del mismo. También se debe valorar la posibilidad de reutilizar los lectores/grabadores de tarjetas que existan en los puestos de emisión y gestión, así como las características de los puestos, es decir, las características del terminal u ordenador utilizado para estas funciones.

- Impresoras de tarjetas: dependiendo de la imagen de la tarjeta, de los acuerdos con los fabricantes y de la personalización de la misma con los datos del usuario, y de la calidad y tipo de impresión, se necesitan unos tipos de impresoras u otros.

  Si actualmente se cuentan con impresoras de tarjetas, se debe valorar la posibilidad de reutilización de las mismas para la emisión y personalización de las tarjetas.

5.3 IMAGEN DE LA TARJETA

Una vez se decida dar el paso para la implantación de la Tarjeta Ciudadana, es preciso empezar a pensar en el diseño de la propia tarjeta. Esta decisión debe tener en cuenta que según los requerimientos que se exijan, el nivel de seguridad que requieran los sistemas, y los servicios que se ofrezcan, se establece el tipo de tarjeta, la seguridad gráfica necesaria y los sistemas que se deben utilizar.

Para el diseño de la imagen de tarjetas existe software especializado, como por ejemplo, Fortuna, pero cualquier programa de diseño como Adobe InDesign, Adobe Photoshop, Adobe Ilustrator, Freehand, QuarkExpress,... puede utilizarse para ello.

En el diseño se tendrá en cuenta el material que se utiliza para la fabricación de la tarjeta, el tipo de personalización que se requiere, el tipo de impresión y la seguridad gráfica necesaria. Una vez realizado el diseño, en el que se incluirán el fondo, los logos de la Entidad Local y del proyecto, las imágenes y los datos, se podrá proceder de dos formas diferentes:

- El proveedor de tarjetas suministra una tarjeta en blanco, y mediante impresoras de tarjetas se personaliza en el propio Ayuntamiento o Entidad Local o en las oficinas que se utilicen para la emisión de tarjetas al ciudadano.

- Se establece con el proveedor de tarjetas el diseño de las mismas, de manera que se suministran con la imagen ya grabada. Esto no implica que no se puedan personalizar a posteriori con ciertos datos de los usuarios mediante impresoras de tarjetas.

La elección de un sistema u otro dependerá del coste asociado (la impresión de las tarjetas implica la compra de impresoras, consumibles para las impresoras y persona encargada de realizarlo, por lo que dependiendo de las ofertas de los proveedores, es más barato la personalización por el proveedor o por la administración pública en cuestión) y de la seguridad gráfica necesaria para la tarjeta, puesto que las impresoras de tarjetas varían:

- Impresión por sublimación térmica.
- Impresión por retransferencia térmica.
- Impresión indirecta.
- Impresión láser.

La segunda fase de personalización está relacionada con los datos del usuario. Primero es necesario analizar los datos que deberían aparecer en la tarjeta. Los datos más usuales son nombre y apellidos y número de usuario o de DNI, aunque dependiendo de las implementaciones y del tipo de proyecto, también es conveniente que incluya la foto de la persona.

Cuantos más datos del usuario se inscriban en la tarjeta, más aumentará el coste y la dificultad del proceso de personalización. En el momento de iniciar el despliegue, se deberá tener en cuenta esta personalización: no se necesitan los mismos procedimientos para el suministro de tarjetas sin datos o con poca información del usuario que para la implantación de tarjetas personalizadas, que incluya la foto del ciudadano.

Si se elige la personalización de la tarjeta con los datos del usuario, se deberá estudiar con detalle los procedimientos de emisión de las tarjetas, y escoger entre un suministro de forma centralizada o de forma distribuida, con puntos de emisión a los que se les facilite impresoras de tarjetas para realizarlas en el momento. Si se realiza de una forma centralizada, se debe tener en cuenta el procedimiento para suministrar la tarjeta al usuario.

Cada personalización exigirá que las imágenes y datos que se quieren imprimir se presenten según unos determinados baremos de calidad para que la impresión sea adecuada. Los requisitos a tener en cuenta, como mínimo, serán los siguientes:

- Formatos de las imágenes: dependiendo de la calidad de la imagen y de la imprenta o impresora, será necesario suministrar las imágenes en unos formatos concretos.

- Modelo de color de las imágenes: cuando se realiza un diseño, muchas veces el color que se muestra en pantalla no es el mismo que el de impresión. Esto se debe al modelo de color elegido: RGB, CMYK, o parámetros vectoriales.

- Resolución: dependiendo de la calidad exigida y del tamaño de la imagen, existirán unos requisitos de resolución para las mismas. Además, habrá que tener en cuenta la limitación de resolución de la impresora (plotter).

- Fuentes y tipos de letra: al hacer las pruebas de impresión, puede suceder que el tipo de letra no sea el adecuado o que haya que hacer modificaciones, por lo que se deben suministrar las fuentes para poder realizar las correcciones pertinentes que permitan un nivel determinado de calidad. Si las fuentes se suministran en formato vectorial, no se podrán realizar modificaciones.

Es importante tener en cuenta la disposición de las imágenes en la tarjeta, prestando especial atención a la disposición del chip para no tener problemas al realizar la impresión.

5.4 PROCEDIMIENTOS OPERATIVOS

Para llegar a cabo la implantación de la Tarjeta Ciudadana, será necesario definir los procedimientos operativos que conlleva. Desde el punto de vista de la distribución de las tarjetas a los usuarios, los procedimientos que habrá que definir son los siguientes:

- Emisión de las tarjetas: las tarjetas se suministrarán a los ciudadanos en los puntos de gestión. Dependiendo de la personalización de las mismas, estos puntos deberán tener impresoras de tarjetas para realizar la personalización definitiva. Al ser una tarjeta inteligente, se

solicitará al usuario su identificación en el momento de emisión, mediante la documentación que se considere conveniente. Este sistema se implanta para mejorar los servicios, por lo que se recomienda pedir la menor documentación posible, tal y como se describe en la Ley 11/2007, puesto que cualquier documento que esté en poder de la administración no se debería solicitar. Por ello, el procedimiento más adecuado es conectar el sistema con el padrón (o cualquier otro registro que englobe al grupo de usuarios al que se va a dirigir los servicios de Tarjeta Ciudadana) para comprobar que el usuario puede solicitar la tarjeta, y la forma de identificación sería por DNI, de forma que la mayoría de los datos se cumplimentan automáticamente.

Una vez que el usuario se identifica, se realiza la personalización final de la tarjeta:

- Personalización gráfica de la tarjeta: como ya se ha comentado, la tarjeta estará personalizada por la Administración que las emite, con una imagen y/o logos de la Entidad Local. Se recomienda que esta personalización ya se realice en los puntos de emisión o gestión de las tarjetas, es decir, que lo único que tenga que realizar la persona encargada de emitir la tarjeta es la personalización de la misma pero respecto del usuario. En este caso, la personalización consistiría en imprimir cierta información en la misma con los datos del usuario. Los datos más comunes son los siguientes:
  - Nombre y apellidos del usuario.
  - Número del DNI.
  - Fecha de nacimiento del usuario (si el precio de los servicios difiere según los tramos de edad, por ejemplo, para jóvenes o personas mayores).
  - Fotografía del usuario.
  - Número de la tarjeta y fecha de caducidad.
  - Etc.

Se pueden incluir todos los datos que se quieran, pero es importante tener en cuenta que a mayor número de datos, el proceso de emisión es más lento y el coste asociado es mayor (tipo de impresoras, consumibles de las impresoras,...). Adicionalmente, si una tarjeta no se imprime correctamente, esta tarjeta deberá ser invalidada en el momento.

- Personalización eléctrica de la tarjeta: en este proceso se graba en el chip los datos del usuario y de las aplicaciones con las que deba interaccionar la tarjeta. Normalmente, las tarjetas vendrán con una clave o PIN predefinido, por lo que es necesario el cambio de PIN para activarlas, según los procedimientos de seguridad que se recomiendan. En este proceso, además, se asignará en el sistema la tarjeta al usuario, de manera que un usuario no pueda tener varias tarjetas activas. Debido a que la información que se almacena en el chip de la tarjeta puede modificarse, se recomienda que este proceso se lleve a cabo previamente a la personalización física de la tarjeta, puesto que si existe algún error en el momento de la impresión, se deberá prestar especial cuidado en que no se conserve información del usuario almacenada en la tarjeta si la tarjeta es inválida.

  Una vez se termine la personalización de la tarjeta, el usuario estará dado de alta en el sistema y se le podrá suministrar la tarjeta. Dependiendo del tipo de servicios, se le pedirá la activación de la misma, normalmente mediante el cambio de PIN (por ejemplo, cuando las entidades financieras envían las tarjetas que sustituyen a las tarjetas antiguas, se pide que se active utilizándola o llamando a un número de teléfono). En general, en el momento de emitir la tarjeta, ésta se activará para los servicios que presta el Ayuntamiento mediante su uso.

- Renovación de la tarjeta: siempre habrá de tenerse en cuenta que la emisión de las tarjetas conlleva el procedimiento de renovación. La renovación de la tarjeta se puede producir por múltiples causas: fecha de caducidad de la tarjeta, pérdida de la misma, deterioro o mal funcionamiento, robo,... Este proceso se deberá realizar en los mismos puntos que la emisión de la tarjeta, puesto que se deberá volver a emitir una nueva. En el caso de que el ciudadano conserve la tarjeta antigua, se deberá entregar en el momento de la renovación, puesto que es más sencillo obtener los datos de la antigua tarjeta y transferirlos a la nueva (los datos serán los mismos, excepto el número de tarjeta asociado al usuario y la fecha de caducidad de la misma). Si la renovación de la tarjeta se produce por deterioro, robo o pérdida, el procedimiento a seguir será el mismo que para el de una emisión de una nueva tarjeta, no pudiendo duplicar la información contenida en la misma.

Será necesario comunicar al ciudadano que el proceso de renovación se lleve a cabo antes de que la tarjeta caduque, puesto que una vez que alcance la fecha de caducidad, la tarjeta dejará de funcionar.

- Desbloqueo del PIN de la tarjeta: como la mayoría de las tarjetas inteligentes, si se introduce el PIN erróneamente un número de veces (en la mayoría de los casos sólo se permite introducir el PIN tres veces), la tarjeta se bloqueará para su uso en aplicaciones que necesiten este PIN. Para su desbloqueo, será necesario acudir a un punto de gestión de tarjetas, donde se insertará en el lector/grabador de tarjetas y se desbloqueará el mismo. Se recomienda que en este caso se obligue al usuario al cambio del PIN de la tarjeta por motivos de seguridad.

- Robo o pérdida: en este caso será necesario emitir una nueva tarjeta al ciudadano, con el procedimiento indicado antes, y proceder a la anulación de la anterior. Para ello es importante crear los mecanismos necesarios para que el usuario pueda anular su tarjeta, puesto que aunque esté protegida por una clave de seguridad, puede ser utilizada para otros servicios, por lo que es necesario que la comunicación sea fácil y rápida. La primera opción a disposición de los ciudadanos sería la posibilidad de comunicar vía telefónica la pérdida, aunque es necesario disponer de otros canales, como puede ser un correo electrónico, un formulario web y por supuesto, presencialmente en alguna de las oficinas de gestión o en la propia Oficina de Atención al Ciudadano del Ayuntamiento.

Otros procedimientos operativos estarán más relacionados con el suministro e instalación de los lectores:

- Se deberá crear un procedimiento para la sustitución de los lectores de tarjetas en los lugares donde sea necesario. Este procedimiento de cambio debe ser suficientemente ágil, para afectar lo mínimo posible al funcionamiento de los servicios. Este tipo de sustituciones se deben sobre todo a actos vandálicos, y en menor medida, a las condiciones meteorológicas (en el caso de lectores que están en el exterior a la intemperie, como lectores para las zonas de aparcamiento regulado) y a su deterioro por el uso del mismo (la mayoría de los servicios que se ofrecen desde un principio utilizan lectores sin contactos, por lo que el desgaste por el uso es mucho menor). En el sistema de gestión que se utilizará estarán de alta todos los elementos del sistema, por lo que cualquier cambio o sustitución se deberá reflejar en dicho sistema para su control.

Por último, existirán procedimientos operativos asociados a la administración y gestión de los sistemas que se utilizan para ofrecer correctamente el servicio:

- Administración y gestión de usuarios: es necesario tener una base de datos actualizada en todo momento que relacione las tarjetas suministradas con el usuario para el que se ha emitido. En este caso, habrá de tenerse en cuenta los procedimientos de emisión, renovación, sustitución y anulación, por robo o pérdida, de las tarjetas suministradas, y el procedimiento de altas, bajas y modificaciones de usuarios y datos asociados en los sistemas y puestos de gestión.

- Administración y gestión de dispositivos lectores: tal y como se ha explicado en el punto anterior, es necesario gestionar los dispositivos lectores de las tarjetas: funcionamiento, sustitución, reparación, stock, obsolescencia,..., para lo que es necesario una gestión de los mismos, con procedimientos definidos para las altas, bajas y modificaciones de los datos.

- Administración y gestión de incidencias: independientemente de la solución, siempre surgen incidencias en cualquier sistema de información, que pueden estar asociadas a elementos tan dispares como la introducción de los datos necesarios para emitir las tarjetas en un punto de emisión como la necesidad de cambiar un lector por mal funcionamiento. Por esta razón, es conveniente contar con un sistema de gestión de incidencias que asegure la calidad del sistema.

5.5 DESPLIEGUE

El despliegue de la tarjeta dependerá de los servicios que se ofrezcan, de las infraestructuras y sistemas que se reutilizan de servicios ya existentes, si cabe la posibilidad, y de la difusión del proyecto de implantación.

Para el despliegue se deberá tener en cuenta las siguientes etapas o fases:

- Fase piloto: primero es necesario realizar un proyecto piloto sobre un número pequeño de ciudadanos. En este piloto se deberá tener en cuenta los servicios que se van a ofrecer y el público objetivo al que se dirigen estos servicios. Por ejemplo, el sistema de transporte público

lo utilizan todo tipo de personas, por lo que en la fase piloto se deberá incluir personas de todas las edades, a diferencia de un sistema para un centro de mayores, en el que el público objetivo es un grupo muy específico.

- Suministro e instalación de lectores y terminales de tarjetas: se deberán suministrar los dispositivos de lectura de las tarjetas e instalarlos en todos los lugares donde sean necesarios. Es el primer paso a realizar en el despliegue, después de las pruebas preliminares. En la mayoría de servicios ofrecidos el despliegue de lectores y terminales podrá ser gradual, no así en el caso de los transportes públicos, cuyo despliegue deber ser completo para cada sistema de transporte, es decir se deberán instalar a la vez en toda la flota del transporte, y posteriormente, si así se decide, ampliar el uso de la tarjeta ciudadana a nuevos sistemas de transporte de la ciudad.

- Sistema de gestión: este sistema se puede implementar paralelamente al despliegue de los lectores, para la gestión de altas, bajas, y modificaciones de todos los elementos del sistema (lectores, tarjetas, usuarios, servicios), de manera que puedan interaccionar unos con otros mediante una red de comunicaciones que permita procesar las transacciones, y que sean interoperables. La comunicación entre los diferentes elementos del sistema no tiene que ser en tiempo real, sino que puede utilizarse sistemas que permitan la descarga de las operaciones cada cierto tiempo, mediante el uso de tarjetas, memorias flash USB, o cualquier otro tipo de interfaz.

- Emisión de tarjetas: una vez que el sistema se haya implantado y se hayan realizado las baterías de pruebas suficientes y una experiencia piloto, se estará en posición de poder realizar el despliegue de las tarjetas. Este despliegue deberá tener en cuenta varias de las elecciones que se hayan tomado respecto al sistema:

  - Personalización de las tarjetas: dependiendo del tipo de personalización deseada, el despliegue de las tarjetas cambiará: si las tarjetas no están personalizadas, el despliegue se podrá realizar en cualquier punto de la ciudad, puesto que sólo será necesario un ordenador y un lector/grabador de tarjetas para poder almacenar los datos del usuario y los servicios en el chip de la tarjeta; en cambio, si la tarjeta incluye datos del usuario impresos, se deberá suministrar en puntos de emisión con impresora de tarjetas (la elección de la impresora dependerá del tipo de impresión que se requiera y de los datos de la misma, por ejemplo, si se incluye foto del usuario o cualquier otra imagen o no, o si los datos son monocromos o en color, como se ha comentado anteriormente).

- Servicios ofrecidos: según los servicios ofrecidos, los puntos de emisión y gestión de tarjetas pueden variar. Cuanto más puntos de emisión existan, más rápido se realizará el despliegue pero a un coste mayor. Si la emisión de tarjetas es centralizada, el ahorro de costes es grande pero supondrá más molestias para el usuario, puesto que se tendrá que presentar en unas oficinas concretas, por lo que la generalización de su uso puede verse afectado.

- Estrategia de comunicación y difusión: es importante definir un plan de difusión y comunicación del proyecto, puesto que aunque el sistema presente muchas ventajas, se facilite y agilice el acceso a los servicios y se implementen nuevas aplicaciones, el éxito del proyecto dependerá del uso que hagan los ciudadanos del mismo. Existen varias experiencias que no han funcionado precisamente por este punto. Un ejemplo claro son las tarjetas monedero, que aunque presentan muchas ventajas respecto al pago de servicios, sólo se ha conseguido implementar en entornos cerrados.

5.6 VIABILIDAD, SOSTENIBILIDAD Y COSTE

La viabilidad del proyecto irá ligada al coste del proceso de implantación más el coste del proceso de despliegue de la misma, es decir, también dependerá de cuán rápido se quiere realizar la implantación del sistema.

A continuación se mostrarán los elementos a tener en cuenta en el proyecto de viabilidad, que conllevan asociados un coste:

- Tarjetas inteligentes: como se ha comentado en apartados anteriores, el coste irá asociado al tipo de tarjeta que se necesite para ofrecer servicios (con contactos o sin contactos), a la memoria que se necesite para las funcionalidades deseadas, y sobre todo, a la personalización de la misma (diseño de la imagen de la tarjeta, impresión de los datos, necesidad de personalización respecto al usuario, impresoras de tarjetas,...).

- Lectores/grabadores de tarjetas: en los puestos de emisión existirán lectores/grabadores de tarjetas que permitan su funcionamiento. Normalmente estos lectores irán conectados a un ordenador desde donde se tramite su emisión. También serán necesarios lectores en

todos los elementos de los servicios que se quieren suministrar mediante el uso de la tarjeta (autobuses, instalaciones deportivas, zonas de estacionamiento regulado,...). En este punto, habrá también un coste asociado a la instalación de los mismos.

- Impresoras de tarjetas: dependiendo de la personalización requerida, del tipo de impresoras, de la forma de distribución (centralizada o distribuida) este concepto puede variar mucho. El coste menor sería un sistema centralizado de tarjetas, de manera que se imprimen la imagen de la tarjeta en el mismo lugar, y una personalización respecto del usuario inexistente. También es necesario valorar el coste de los consumibles de las impresoras y cada cuánto es necesario cambiarlo.

- Actualización de los sistemas y hardware existente: si se quiere reutilizar los sistemas de los que ya se dispone, se deberá analizar, como se ha detallado anteriormente, la posibilidad para los nuevos servicios. El coste asociado dependerá del tipo de actualización y modificaciones necesarias, y de la integración e interoperabilidad entre los sistemas, por lo que es muy difícil de calcular sin un análisis pormenorizado de la situación actual.

- Sistemas de gestión y control: será necesario el desarrollo e implantación de sistemas interoperables, que puedan comunicarse con otros sistemas para un mayor rendimiento, por lo que se recomienda que se utilicen sistemas con arquitecturas modulares, interoperables, que hagan distinción entre el interfaz del usuario y el desarrollo del servicio.

- Puestos de administración, gestión y control: se deberá tener en cuenta los puestos físicos de emisión de las tarjetas y de gestión de los sistemas, es decir, el lugar o instalación donde

se encontrará, el personal necesario y los elementos que necesita para el cumplimiento de sus funciones (ordenador, accesorios, impresoras, puesto de trabajo,...). Si la distribución de las tarjetas no es centralizada, existe un coste asociado adicional (por ejemplo, envío de las tarjetas a los usuarios mediante correo ordinario o certificado).

- Infraestructuras: redes de comunicaciones, servidores, y cualquier otro elemento necesario para el correcto funcionamiento de los sistemas de administración y gestión, el almacenamiento de la información y la comunicación entre los diferentes sistemas.

- Sistema de incidencias: además de los puestos de gestión y control, debe existir un sistema de incidencias, orientado a cualquier problema que puedan causar las tarjetas y dispositivos lectores, las aplicaciones o los sistemas implementados. Se recomienda que la comunicación por robo o pérdida de la tarjeta se pueda realizar por varios canales (telefónico, presencial, internet,...).

La implantación y despliegue de un sistema de Tarjetas Ciudadanas deberá evaluar ciertos riesgos, que permitirán la elección de los diferentes elementos del sistema y su sostenibilidad:

- Seguridad: es necesario evaluar el nivel de seguridad necesario, tanto física como lógica:

  - Seguridad física: orientada a los dos elementos más vulnerables, las tarjetas y los lectores de tarjetas:

    – Las tarjetas deberán poseer cierto tipo de seguridad para que no puedan ser falsificadas, para lo que se utilizan las técnicas de seguridad gráfica que se han comentado en el apartado anterior.

    – Los lectores de tarjetas, que dependiendo de si son para exteriores o interiores deberán poseer ciertos mecanismos de protección frente al vandalismo.

  - Seguridad lógica: la seguridad lógica está relacionada con los sistemas de las tarjetas. Dependiendo el nivel de seguridad requerido, se elegirán unas tarjetas u otras, que incorporen algoritmos de seguridad más fuertes o tarjetas criptográficas.

- Durabilidad de los elementos del sistema frente al uso e inclemencias del tiempo, si son lectores o terminales de exteriores. En las tarjetas se deberá tener en cuenta el desgaste de las mismas dependiendo del material con el que están fabricadas y su utilización, según los servicios que se presten, y el tipo de tarjetas (existen diferencias de desgate entre las tarjetas de contactos y sin contactos, puesto que la inserción en lectores provoca un desgaste mayor, y en las tarjetas sin contactos el chip está protegido por el plástico de la tarjeta y su durabilidad es mayor).

- Obsolescencia de alguno de los elementos: parece ser que estamos en un punto donde la estandarización de las tarjetas y lectores permite asegurar su funcionamiento a medio plazo. El uso de estas tecnologías permiten que fabricantes de tarjetas, terminales y lectores puedan desarrollar nuevos elementos que interactúen. El elemento más importante a tener en cuenta es la tarjeta y los algoritmos de seguridad que incorporen, debido a que se pueda "romper" el algoritmo y la información contenida en la tarjeta sea vulnerable. Pero los algoritmos de encriptación actuales permiten asegurar que son inquebrantables a medio plazo.

- Ampliación de los servicios: la ampliación de los servicios puede provocar que se necesiten tarjetas con características específicas, por lo que se debe escoger el tipo de tarjeta en base a las funcionalidades no únicamente presentes, sino las que se le pueden ir añadiendo en un futuro. Los sistemas deberán ser desarrollados de manera que sea fácil su integración e interoperabilidad, de forma modular, con una arquitectura que permita desarrollar de forma sencilla nuevos servicios.

Por último, cabe destacar que la viabilidad del proyecto no implica el éxito del mismo, dependiendo en gran medida de la aceptación y utilización de estos sistemas por parte de los ciudadanos. Una buena campaña de comunicación y difusión, que explique a los usuarios las ventajas, las funcionalidades y los procedimientos operativos que hay que realizar para poder acceder a los servicios que prestará el Ayuntamiento en cuestión, es vital para un rápido despliegue. Si los ciudadanos entienden que el uso de las tarjetas les puede facilitar el acceso a servicios, las probabilidades de éxito aumentarán de forma significativa.


6 EJEMPLOS SIGNIFICATIVOS DE APLICACIÓN DE TARJETAS INTELIGENTES
Junta de Castilla y León
red de municipios digitales de Castilla y León

6. EJEMPLOS SIGNIFICATIVOS DE APLICACIÓN DE TARJETAS INTELIGENTES

A continuación se muestran algunos ejemplos de implantaciones de tarjetas inteligentes que han realizado algunos Ayuntamientos. También se incluye un apartado sobre la tarjeta sanitaria del País Vasco, puesto que es otra forma de integrar servicios a partir de una tarjeta y su despliegue es muy sencillo pues la mayoría de los empadronados en el municipio deberán poseer una tarjeta sanitaria para poder acceder a los servicios médicos.

6.1 TARJETA CIUDADANA DEL AYUNTAMIENTO DE PONFERRADA

La Tarjeta Ciudadana que suministra el Ayuntamiento de Ponferrada es una tarjeta chip sin contactos que se puede utilizar para acceder a determinados servicios e instalaciones y realizar el pago en los transportes públicos.

La tarjeta nació como una forma de unificar las distintas tarjetas que hasta ahora se necesitaban para el acceso a los diferentes servicios, y su presentación se realizó en octubre del año 2009. A mediados del año 2010, más de 10.000 ciudadanos habían solicitado ya la Tarjeta Ciudadana. La tecnología elegida por este Ayuntamiento permitirá la incorporación de nuevos servicios de una manera sencilla.

La empresa seleccionada por el Ayuntamiento para la implantación fue la encargada del desarrollo de los sistemas de gestión y control necesarios para el funcionamiento del sistema, del diseño y suministro de las tarjetas inteligentes que se utilizan, de la instalación de dos cajeros ciudadanos donde puede recargarse la tarjeta y acceder a la información, así como de la puesta en marcha de la oficina de gestión.

La implantación del sistema partía con una inversión inicial de 212.000 €, debido a que se reutilizaban ciertas partes de los sistemas que ya estaban funcionando, como el servicio de autobuses municipales y el préstamo de bicicletas, por lo que el coste se redujo al ser posible la reutilización de algunos dispositivos y equipamiento. Por otro lado, fue necesaria su adaptación, puesto que pertenecían a distintos fabricantes.

Para facilitar los trámites de emisión, se creó una oficina de gestión, donde, entre otras funciones, se encarga de realizar la emisión de la Tarjeta.

La oficina de gestión se ha ampliado con cinco nuevos puntos de emisión repartidos por todo el municipio a lo largo del año 2010. El próximo paso que se está estudiando es llegar a los núcleos más alejados de Ponferrada, para que estos puedan realizar la solicitud sin tener que desplazarse.

Además de la oficina de gestión, se crearon dos cajeros ciudadanos, donde se pueden realizar la compra de los billetes para el autobús urbano, consultar el saldo de la tarjeta, modificar la clave de acceso de la tarjeta (PIN),... El uso de la tarjeta en estos cajeros es muy sencillo, siendo únicamente necesario acercar la tarjeta al cajero hasta que este responda, momento en el que será necesario introducir el PIN de la tarjeta.

Los servicios que se prestan actualmente con la tarjeta son los siguientes:

- Servicio de acceso con vehículos a zonas peatonales para residentes.
- Servicio de autobuses urbanos: la tarjeta permite el pago de los viajes en el transporte urbano de Ponferrada. Los ciudadanos pueden realizar la recarga en las oficinas de gestión o en los cajeros ciudadanos.
- Servicio de préstamo de bicicletas: la tarjeta facilita el servicio de préstamo de bicicletas. Este sistema es completamente nuevo, puesto que el sistema anterior era incompatible con las nuevas tarjetas, por lo que se tuvieron que cambiar todos los dispositivos de lectura.
- Beneficios sociales: acceso gratuito a los museos de la ciudad y otras instalaciones (por ejemplo, el castillo de los templarios) o acceso gratis en un periodo de tiempo concreto a exposiciones.
- Futuros servicios: acceso a instalaciones deportivas, monedero electrónico, pago de la zonas de estacionamiento regulado (O.R.A.), pago de tasas e impuestos municipales, acceso a internet en los centros culturales,..

El Ayuntamiento ha previsto que, debido a que la Tarjeta Ciudadana está dirigida a los ciudadanos empadronados en el municipio, en el caso de actividades en las que no sea necesario estar empadronado se podrá solicitar otra tarjeta que ofrece estos servicios, la Tarjeta Evoluciona. La emisión de la Tarjeta Ciudadana será gratis para sus ciudadanos empadronados, y la Tarjeta Evoluciona tendrá un coste de tres euros. En ambos casos, la sustitución por pérdida o deterioro llevará un coste asociado que se establecerá cada año en las ordenanzas fiscales.

La solicitud de la tarjeta se lleva a cabo de forma presencial en la oficina de gestión, pues exige la identificación del titular y su emisión es inmediata, en el mismo momento de la solicitud. El Ayuntamiento requiere de la siguiente documentación (independientemente de si es la Tarjeta Ciudadana o la Tarjeta Evoluciona):

- Documento Nacional de Identidad vigente o cualquier documento acreditativo de la identidad (pasaporte o tarjeta de residencia).
- Formulario de solicitud, que se puede descargar de la página web del Ayuntamiento, donde se solicitan los siguientes datos:
  - Datos del solicitante: nombre, apellidos, NIF, fecha de nacimiento.
  - Datos del representante (en su caso): nombre, apellidos, NIF, relación con el solicitante.
  - Datos a efectos de notificación: dirección, código postal, correo electrónico y teléfono.
  - Servicios reconocidos: se deberá marcar qué tipo de servicios solicita.
  - Observaciones: se indicará si se solicitan nuevos servicios (en caso de querer ampliar los servicios que incluyó en la tarjeta en el momento de la solicitud) o si solicita la renovación por deterioro o extravío.
- Otra documentación: en caso de ser menor de 25 años, se deberá presentar certificado o matrícula acreditativos de cursar estudios en un centro oficial; en caso de ser jubilado, se debe adjuntar documento acreditativo de esta condición; fotocopia de escrituras o arrendamiento para las personas que solicitan el servicio de acceso a zonas peatonales;...

La personalización de la tarjeta respecto al usuario únicamente incluye el nombre y apellidos y número de identificación del mismo.

Figura 5 Tarjeta Ciudadana del Ayuntamiento de Ponferrada

A la hora de recargar la tarjeta para los transportes públicos, el Ayuntamiento ha previsto dos formas para mayor comodidad de los ciudadanos:

- En la oficina de gestión de la Tarjeta Ciudadana.
- En la red de cajeros ciudadanos.

El funcionamiento de la tarjeta en los transportes públicos es muy sencillo, una vez recargada la tarjeta en alguno de los puntos mencionados, ésta se debe acercar a una suficiente distancia a los lectores de proximidad instalados en el interior del autobús, al lado del conductor.

Una de las situaciones a tener en cuenta al poner en marcha un proyecto de este tipo, es el periodo de coexistencia de dos soportes, en el caso del Ayuntamiento de Ponferrada optó por dejar un periodo de tiempo donde se permitían utilizar ambos soportes (el que se venía utilizando hasta ese momento y la nueva Tarjeta Ciudadana), retirando paulatinamente las tarjetas antiguas para que no supusiese un grave perjuicio para el ciudadano.

6.2 TARJETA DEL AYUNTAMIENTO DE ALCOBENDAS

El Ayuntamiento de Alcobendas es uno de los pioneros en la implantación de una Tarjeta Ciudadana. En el año 1999 se empezó a gestionar su implantación dentro del proyecto ITACA (Información, Tramitación y Atención Ciudadana en Alcobendas). Este proyecto tenía como objetivo mejorar y facilitar la relación entre el Ayuntamiento de Alcobendas y sus ciudadanos, mediante una atención integrada (canales presencial, telefónico y por medios electrónicos).

En esta primera fase, la tarjeta permitía acceder a información, gestión, pago y reserva de instalaciones deportivas, para lo que fue necesario un acuerdo con Caja Madrid que permitía los pagos on-line mediante las cuentas privadas de los usuarios en las entidades financieras. La tarjeta estaba fabricada por la FNMT-RCM, disponía de chip y banda magnética, permitiendo servicios de monedero electrónico. Las principales utilidades eran las siguientes:

- Información personal: padrón e impuestos.
- Gestión: justificante del padrón, solicitud de certificado de padrón, domiciliación de tributos, pago de recibos (IBI, vehículos, quioscos, IAE, tasa de basuras y actividades económicas).
- Reserva de instalaciones deportivas: tenis, paddle, squash, frontón, billar, tenis de mesa, fisioterapia, rayos UVA y masajes.

Según ha evolucionado la tecnología, el proyecto ITACA se ha ido adaptando. En 2004, dentro de la segunda fase, se realiza la adaptación de la tarjeta para poder ofrecer nuevos servicios. La nueva tarjeta ofrecía una identificación personalizada y servicios de información y gestión. En el año 2010 se habían emitido más de 16.000 tarjetas.

La implantación de esta tarjeta permitió unificar los servicios en los que era necesario un carné municipal, sustituyendo estos carnés por la nueva Tarjeta Ciudadana. Como se ha explicado anteriormente, en el proceso de implantación de una Tarjeta Ciudadana es importante reutilizar las infraestructuras y los servicios ya existentes, en los que es necesario la identificación, permitiendo un despliegue más rápido de la misma.

Además, permite integrar toda la información en un único sistema, siendo más sencillo la interoperabilidad y la comunicación.

Los principales servicios que ofrece esta tarjeta son los siguientes:

- Identificación de los ciudadanos que residen en Alcobendas. La tarjeta identifica al usuario mediante su nombre y su foto, y al Ayuntamiento mediante el fondo, su logo y el nombre de la tarjeta (Tarjeta de ALCOBENDAS). Esta identificación se utilizará tanto para el control de accesos a ciertas instalaciones como para la identificación mediante medios electrónicos para realizar trámites a través de las páginas web que pone a disposición el Ayuntamiento.

- Servicios municipales: entre los más importantes destaca el acceso a la carpeta ciudadana, desde donde se podrán consultar los expedientes de licencias, solicitudes y actos comunicados, realizar trámites, acceder a la bolsa de empleo (dar de alta, modificar el currículum o renovar la inscripción), acceso al padrón municipal, realizar consultas de los escritos, solicitudes y comunicaciones presentadas en el Registro y consultas sobre reservas deportivas sin disfrutar.

- Tarjeta de fidelización: la tarjeta permite obtener descuentos en comercios adheridos al programa (Centro Comercial Abierto “Las Tiendas del Centro). Cuanto mayor es el despliegue y el número de usuarios que la utilicen, mayor será el potencial beneficio para las tiendas y para los usuarios, pues un número mayor de comercios querrán adherirse al programa. Los descuentos se conseguirán con el mero hecho de presentar la tarjeta en el momento de la compra.

- Instalaciones deportivas: gestión de las reservas en los polideportivos municipales.

- Puestos de autoservicio de información y gestión: los puestos, mediante el uso de la tarjeta, permiten realizar trámites y solicitar información de forma segura. Además, estos puestos permiten realizar la solicitud de la tarjeta, mensajes SMS, acceso a internet, web municipal, ofertas de empleo, formación y correo electrónico.

La emisión de la tarjeta es gratuita, y está dirigida a los ciudadanos empadronados en el Ayuntamiento de Alcobendas.

Para realizar su solicitud, el Ayuntamiento ha instalado puestos de información y gestión y a través de la web, mediante un formulario telemático.

Los datos que solicita el Ayuntamiento a los ciudadanos en los puestos de información y gestión son los siguientes:

- Nombre.
- Apellidos.
- N.I.F.
- Dirección.
- Teléfono.
- Correo electrónico.

En la tarjeta se incluyen como datos impresos el número de tarjeta y el nombre del ciudadano a la que estará asociado.

Figura 6 Tarjeta Ciudadana del Ayuntamiento de Alcobendas

Los trámites que puede realizar un ciudadano, asociados a la tarjeta de Alcobendas, son:

- Solicitud de la tarjeta.
- Duplicado de la clave de acceso: en caso de extravío, olvido, que se haya bloqueado por no introducir la clave correctamente varias veces,... Este procedimiento se puede realizar a través del envío de un correo electrónico (webtarjetas@aytoalcobendas.com) o en los puestos autoservicio de información y gestión.
- Duplicado de la tarjeta: debido a extravío, deterioro, robo,... Para solicitar el duplicado, se requiere cumplimentar la solicitud de duplicado, que se entregará en los puestos autoservicio de información y gestión o mediante correo electrónico.
- Cancelación de la tarjeta: se deberá cumplimentar un impreso de solicitud de cancelación donde se indicará el motivo de la cancelación.
- Cambio de claves: debido a que su seguridad se haya visto amenazada o por motivos de bloqueo o duplicados de claves. Se puede realizar a través de la dirección web del Ayuntamiento, indicando la antigua clave y la nueva (en el caso de bloqueo de la tarjeta o de extravío, este trámite no se puede realizar).

La tarjeta de Alcobendas está bastante extendida entre sus ciudadanos, debido a que lleva varios años en circulación. Las últimas estadísticas muestran que casi la mitad de sus ciudadanos posee una tarjeta, unos 50.000 usuarios de los aproximadamente 110.000 habitantes empadronados en el municipio.

6.3 TARJETA CIUDADANA DEL AYUNTAMIENTO DE GIJÓN

La Tarjeta Ciudadana de Gijón permite realizar de forma rápida y sencilla numerosos trámites y hacer uso de los servicios locales. No es necesario estar empadronado en Gijón para poder acceder a sus servicios, sino que cualquier persona puede solicitar. La Tarjeta Ciudadana que se suministra es una tarjeta inteligente, dotada de un chip de proximidad, es decir, se trata de una tarjeta sin contactos, y una banda magnética.

Entre los servicios que se ofrecen destacan los siguientes:

- Transporte municipal de autobuses.
- Acceso gratuito a las bicicletas instaladas dentro del sistema GijónBici.
- Acceso a instalaciones deportivas, piscinas y campos de golf (necesario abono).
- Acceso a bibliotecas, mediatecas y préstamo de libros.
- Pago del estacionamiento regulado (O.R.A.), mediante la banda magnética.
- Trámites con el Ayuntamiento: acreditación de la identidad en la Oficina Virtual.
- Acceso a aseos públicos.
- Descuentos en la entrada al Acuario.
- Acceso a Cimadevilla en horario nocturno con vehículo propio.
- Acceso a los centros de trabajos y control horario para los empleados municipales.

Esta tarjeta se creó para sustituir a los anteriores y numerosos carnets necesarios en la ciudad, como el carnet de bibliotecas o la credencial de abonado a las piscinas municipales, y los unifica en una única tarjeta, con la que se puede acceder a estos servicios.

La solicitud de emisión de la tarjeta se puede realizar presencialmente o a través de internet, en la Oficina Virtual, adjuntando a la solicitud el DNI escaneado en formato PDF y una fotografía tamaño carnet en formato JPG, posteriormente el ciudadano recibe un correo electrónico con el número de la Tarjeta Ciudadana y el PIN temporal, que le permita acceder a la Oficina Virtual mientras se emite la Tarjeta definitiva. La tarjeta se enviará a la dirección postal indicada o se podrá recoger en una de las Oficinas de Atención al Ciudadano que se indique en la solicitud.

Figura 7 Modelos de Tarjetas Ciudadanas del Ayuntamiento de Gijón

El Ayuntamiento ha previsto que para su uso en servicios que requieran pagos (por ejemplo, el transporte municipal o la O.R.A.), sea necesario primero cargarla con dinero debido a que la tarjeta no está asociada a ninguna entidad financiera; esta carga de dinero se realiza de forma diferente, dependiendo del servicio requerido, puesto que esta tarjeta incluye dos monederos diferenciados:

- Transporte público: se recarga en los cajeros que existen en las Oficinas de Atención al Ciudadano, en las instalaciones deportivas y en otros lugares como hospitales a los que acudan un número importante de ciudadanos. El Ayuntamiento ha impuesto un importe máximo a cargar de 150 €.

- Ordenamiento Regulado de Aparcamiento (O.R.A.): su recarga se realiza en cualquiera de los parquímetros que se encuentran en la calle, mediante la banda magnética de la tarjeta, con un máximo de 6 €.

La Tarjeta Ciudadana de Gijón, como en todos los casos estudiados, es gratuita, así como su renovación. Pero en caso de extravío o deterioro, se deberá abonar una cantidad por gastos de emisión, según se establezca en las ordenanzas fiscales del Ayuntamiento (en 2010, esta tasa era de 5 €).

Si el problema es el olvido del PIN, se podrá solicitar mediante un formulario web a través de la Oficina Virtual, o presencialmente en cualquiera de las Oficinas de Atención al Ciudadano. Si se desea cambiar el PIN, se podrá realizar en cualquiera de los Cajeros Ciudadanos que están repartidos por la ciudad.

La tarjeta ha tenido muy buena acogida en la ciudadanía, sobre todo en los servicios de transporte de autobús (debido a que el billete es más barato) y la reserva y bonos de instalaciones deportivas y piscinas públicas. Según un estudio realizado por el Ayuntamiento, en 2009 el 67% de los ciudadanos de Gijón ya tenía la tarjeta (se habían emitido más de 160.000 tarjetas entre personas físicas y personas jurídicas), y el 92% de los ciudadanos conocían de su existencia.

6.4 TARJETA CIUDADANA DEL AYUNTAMIENTO DE ZARAGOZA

El Ayuntamiento de Zaragoza empezó en abril de 2010 la implantación de una Tarjeta Ciudadana que, como en la mayoría de los casos, unifica los servicios que ya se ofrecían mediante otras tarjetas, con la colaboración de Ibercaja (entidad financiera que permitirá el sistema de pago) y Transportes Urbanos de Zaragoza (TUZSA).

En este caso, el Ayuntamiento ha optado por una tarjeta con tres modalidades (adultos, menores y tarjeta oro), que prestan los mismos servicios, salvo en el caso de la tarjeta oro, dirigida a los mayores de 65 años, que permite el acceso a un mayor número de servicios relacionados con los centros de mayores.

El sistema que se ha implementado permite el uso de tarjeta tanto como monedero electrónico (siendo necesario realizar la recarga antes de poder utilizar la tarjeta para el pago de servicios) o asociando la tarjeta a una cuenta corriente.

Los servicios que ofrece el municipio mediante el uso de la tarjeta son:

- Transporte urbano: billete del autobús.
- Acceso a piscinas y centros deportivos.
- Parkings: permitirá el pago de los aparcamientos públicos.
- Servicio de bicicletas BiZi.
- Centros de mayores: está previsto que esta tarjeta sustituya paulatinamente la tarjeta del mayor, con nuevos servicios, como el pago de comedor, identificación para el acceso a distintos recintos,...
- Bibliotecas y museos municipales.

- Acceso a servicios sociales: acceso a internet en las salas de Inclusión digital.
- WiFi municipal.
- Servicios y tramitación, como certificados de empadronamiento, información, y servicios de Administración Electrónica.
- Otros futuros servicios previstos por el Ayuntamiento son: tranvía, pago de tasas de los aparcamientos en superficie, centros de ocio, centros culturales, etc.

Como en la mayoría de las implantaciones que hemos visto, la emisión de la tarjeta es gratis, pero su renovación puede suponer costes adicionales derivados de los gastos de emisión.

El Ayuntamiento tiene como objetivo de despliegue de la tarjeta ciudadana una emisión de unas 100.000 tarjetas a finales del año 2010, y que al final de la legislatura la mitad de los ciudadanos de Zaragoza utilicen esta tarjeta.

Figura 8 Tarjeta Ciudadana del Ayuntamiento de Zaragoza

6.5 OTRAS TARJETAS

En el presente apartado se presentan otras iniciativas de Tarjetas Ciudadanas que han implementado en algunas Administraciones Públicas.

6.5.1 Tarjeta sanitaria del País Vasco

En el País Vasco se ha realizado la implantación de la tarjeta electrónica sanitaria ONA. Esta tarjeta ha ido añadiendo servicios a los contemplados como tarjeta sanitaria, por lo que su despliegue e implantación empezó siendo rápido. Algunos de los servicios que ofrecía esta tarjeta eran:

- Servicios sanitarios: reservas de citas médicas, solicitud cambio de médico,…
- Trámites administrativos: tramitación del IRPF, tramitación de tasas y pagos electrónicos, consulta de datos fiscales, consulta de la vida laboral, consulta de datos catastrales, obtención del certificado de empadronamiento,…
- Acceso a polideportivos municipales.
- Consulta de catálogos y préstamo de libros de las bibliotecas municipales.
- Firma electrónica reconocida.

Esta tarjeta es dual, es decir, con y sin contactos, y además incluye una banda magnética. La personalización de la misma incluye el nombre de usuario, el número de la seguridad social, el número de la tarjeta sanitaria y la fecha de caducidad de la tarjeta. A continuación se muestra una imagen de la tarjeta:

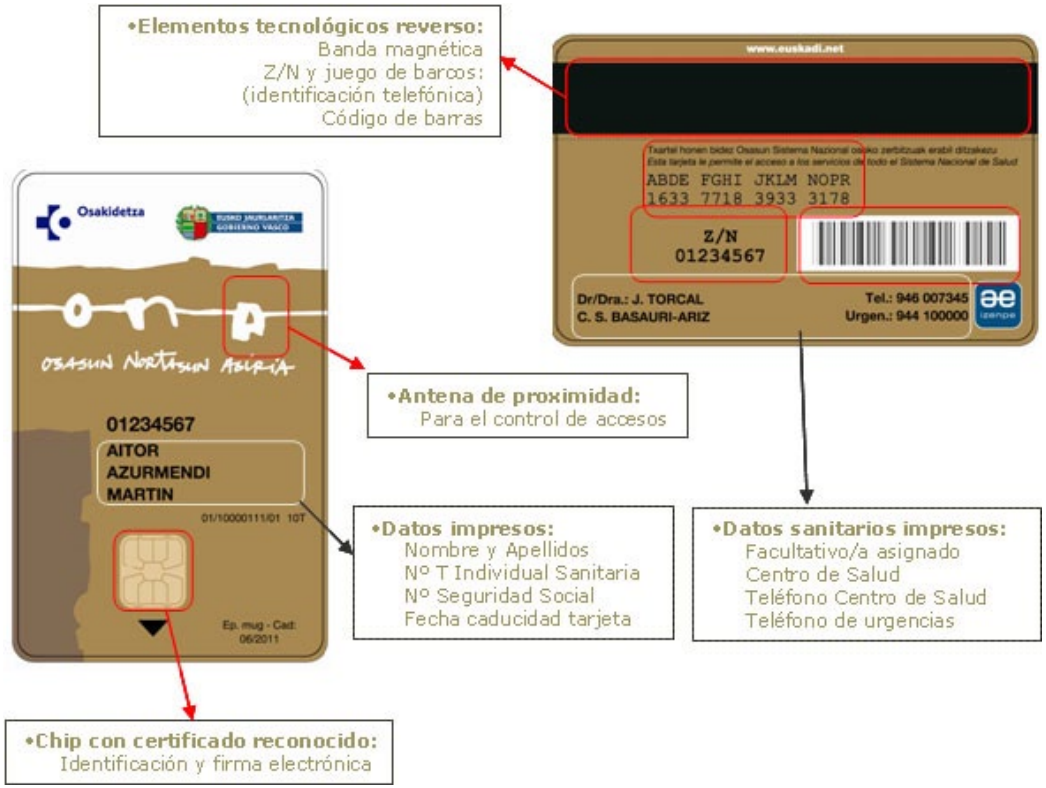


Figura 9 Tarjeta Sanitaria del País Vasco - ONA

La tarjeta es gratuita y pueden solicitarla las personas mayores de 16 años en cualquiera de los puntos de solicitud de la red que se ha desplegado para su implementación, Ayuntamientos, bibliotecas, polideportivos municipales,... El Gobierno ha optado por facilitar su solicitud de manera que se realice un despliegue rápido y sin complicaciones para los ciudadanos, y de manera progresiva, aumentando los puntos de solicitud en los distintos pueblos a medida que se vayan implementando los servicios.

El problema de esta tarjeta es su complejidad a la hora de que los usuarios obtengan beneficios, puesto que aunque la brecha digital cada vez es menor, es necesario un lector de tarjetas, requiere unos conocimientos informáticos avanzados, el software no es compatible con todos los sistemas operativos (sólo aceptaba Windows), la mayoría de los servicios que ofrece se pueden realizar con el DNIe (la Ley 11/2007 exige que el DNI electrónico se pueda utilizar en cualquier trámite con la administración),...., por lo que el uso de la misma ha sido muy limitado (en el año 2009 se decidió ralentizar su distribución aunque el despliegue llega casi al 10% de la población del País Vasco).

6.5.2 Tarjeta Ciudadana y Tarjeta de Acreditación en el Gobierno de Navarra

Es interesante mostrar en este estudio la experiencia de la Diputación de Navarra. Esta administración ha creado un Registro Central de Tarjetas, que está posibilitando el despliegue de las Tarjetas Ciudadanas en los Ayuntamientos. En su inicio, varias Entidades Locales estaban estudiando la viabilidad de realizar un proyecto de Tarjeta Ciudadana, y fue el Servicio de Calidad y Modernización del Departamento de Administración Local del Gobierno de Navarra quien propuso el desarrollo de este novedoso sistema de manera que se pueda aglutinar en una única tarjeta todos los servicios disponibles para los ciudadanos, con independencia de su residencia o domicilio social.

Estas Tarjetas Ciudadanas, desplegadas por numerosos Ayuntamientos de Navarra, permiten el acceso a multitud de servicios:

- Transporte urbano en la comarca de Pamplona (previa carga del monedero electrónico).
- Acceso y préstamo de libros en las bibliotecas públicas.
- Acceso a instalaciones deportivas: polideportivos, piscinas municipales,...

- Servicio de préstamo de bicicletas (Pamplona).
- Servicios de administración electrónica, mediante la identificación en la Oficina Virtual.
- Descuentos en comercios adheridos.
- Futuros servicios: transporte interurbano, acceso a museos y centros sociales,...

La idea que subyace es que todas las tarjetas que emitan los Ayuntamientos puedan ser utilizadas en otros municipios y así acceder a un mayor número de servicios, unificando las tarjetas municipales en una única tarjeta. El proyecto permite que cada Entidad Local pueda elegir el diseño de la misma, los proveedores que la suministran, los servicios que ofrece en su localidad, etc.

Además, se ha diseñado de forma que no es necesario emitir una nueva tarjeta cada vez que un ciudadano quiera acceder a servicios de otro Ayuntamiento, sino que se activan estos servicios municipales en la tarjeta personal para que pueda utilizarlos sin necesidad de cambiar de tarjeta. En el momento de su emisión, se debe comprobar si el usuario dispone de una Tarjeta activa en el Registro Central de Tarjetas, puesto que si ya tiene una operativa, solamente es necesario validar los nuevos servicios.

Adicionalmente a la tarjeta ciudadana, existe otro tipo de tarjetas que promueve el Gobierno de Navarra, son las tarjetas de acreditación, destinada a los trabajadores de los Ayuntamientos y del Gobierno de Navarra, y que presenta las mismas características que las tarjetas ciudadanas y ofrece los mismos servicios, con una pequeña excepción, esta tarjeta incorpora firma electrónica, que permite realizar los trámites con la administración, mediante un certificado de Empleado Público.

Las ventajas que ha conseguido el Gobierno Navarro con este sistema de tarjeta ciudadana son claras:

- Acceso a servicios de otros Ayuntamientos.
- Modelo uniforme de gestión de las tarjetas, de los sistemas y de los usuarios.

- Abaratamiento de costes.
- Mejora de la calidad de los servicios y del uso de las tarjetas en las Entidades Locales, independientemente de los recursos.
- Identificación del ciudadano y controles de acceso análogos.

Es importante remarcar el modelo organizativo utilizado para poder llevar a cabo la implantación y despliegue de las tarjetas:

- Se ha centralizado el diseño de la tarjeta y de los sistemas, así como la captación para la financiación de las mismas. Además, el Registro Central de Tarjetas se ocupa de gestionar y coordinar los diferentes servicios que ofrece cada Administración adherida.
- Por su parte, los Ayuntamientos se encargan de la emisión de las tarjetas, utilización en sus servicios y renovación de las mismas.

Los datos del usuario necesarios que aparecerán en la tarjeta son:

- Nombre y apellidos.
- Fotografía tamaño carnet.
- D.N.I. o documento de identificación.

Figura 10 Tarjeta Ciudadana y Tarjeta de Acreditación en el Gobierno de Navarra

En el mes de abril del año 2010, se habían emitido más de 232.000 tarjetas ciudadanas. Para ello, han contado con la colaboración de Caja Navarra, que suministra el 50% de las tarjetas, y Caja Rural y Caja Laboral, las cuales suministran cada una el 25% restante de las tarjetas.


7 CONCLUSIONES
Junta de Castilla y León
red de municipios digitales de Castilla y León

7. CONCLUSIONES

La legislación vigente en materia de Administración Electrónica reconoce el derecho de los ciudadanos a relacionarse con las Administraciones Públicas a través de medios electrónicos y el deber de las Administraciones de utilizar las tecnologías TIC, de manera que se aseguren los principios de disponibilidad, accesibilidad, integridad, autenticidad, confidencialidad y conservación de los datos.

Las tarjetas inteligentes pueden ser la llave de acceso a estos servicios si se utilizan de manera correcta, proporcionando un mayor nivel de seguridad, tanto físico como lógico, y, adicionalmente, su uso para autenticación con certificados y firma electrónica en el caso de elegir tarjetas criptográficas en su implementación.

La tecnología asociada a los diversos tipos de tarjeta (con contactos, sin contactos, híbridas, criptográficas,...) está madura y en los últimos años se ha realizado un gran esfuerzo en desarrollar unos estándares internacionales que permiten la integración de nuevos servicios y aplicaciones, independientemente del fabricante de tarjetas y de dispositivos lectores y del sistema operativo con el que operen.

En los últimos tiempos, el uso de tarjetas inteligentes en España se está generalizando, gracias en parte a la nueva normativa europea que obliga a que las tarjetas financieras cumplan el estándar EMV, parte debido a la gran distribución y difusión del DNI electrónico, bandera del impulso que se le está dando a la Administración Electrónica. Aunque no son los únicos proyectos; actualmente existen un gran número de servicios y aplicaciones que permiten el uso de tarjetas: controles de acceso, pago en autopistas y párquines, servicios sanitarios, servicios universitarios, máquinas expendedoras, etc.

Si la legislación favorece el uso de estos sistemas y la tecnología está suficientemente asentada para asegurar su estabilidad, se puede considerar un buen momento para la implantación de sistemas basados en las Tarjetas Ciudadanas, que faciliten a los ciudadanos el acceso a los servicios.

Sin embargo, aunque las condiciones sean las idóneas según el análisis exhaustivo de la viabilidad del proyecto y los servicios que se quieren prestar, no implica el éxito del mismo. El principal componente de un sistema de tarjetas es el usuario: si el ciudadano no percibe su utilidad, no es obligatorio su uso (como podría ocurrir para el acceso al transporte público), no encuentra mejoras sustanciales respecto al antiguo sis-

tema o no conoce ni siquiera la posibilidad de utilizar tarjetas inteligentes para el acceso a ciertos servicios, el proyecto se atascará. Por esta razón, es muy importante que un proyecto de implantación de la Tarjeta Ciudadana en cualquier municipio se vea impulsado por el acceso a servicios realmente útiles para el ciudadano (acceso a zonas peatonales, tarjeta transporte, reserva y acceso a instalaciones municipales, etc). Además, deberá realizarse una buena campaña de difusión y comunicación, y con una gestión del cambio ágil y fácil, de manera que el ciudadano se familiarice rápidamente con el uso de las tarjetas y se sienta identificado con el proyecto.

Este libro ha pretendido arrojar cierta luz sobre conceptos de tarjetas chip y tarjetas inteligente, tecnologías actuales y principales funcionalidades y aplicaciones que nos podemos encontrar, y recoge algunas de los proyectos que se han realizado o se están llevando a cabo actualmente. La implantación de sistemas basados en Tarjetas Ciudadanas es una solución que empieza a extenderse paso a paso por toda la geografía española, pues presenta grandes ventajas para la prestación de servicios (en general, el transporte público es un servicio muy proclive al uso de estas tecnologías, pues ya exige un control de accesos con billetes o tarjetas con banda magnética).

La Red de Municipios Digitales de Castilla y León pretende con este libro plantear las nociones básicas para la implantación de un sistema de Tarjeta Ciudadana, y presentar los elementos a estudiar cuando se realice el análisis de situación y viabilidad que deben acompañar el proyecto. Los elementos están al alcance de cualquier Ayuntamiento, la tecnología y la legislación favorecen su despliegue, y existen experiencias con éxito. En este contexto, sólo cabe una pregunta, ¿cuál será el próximo Ayuntamiento en realizar un proyecto de estas características?


0411 0914 0
9972
T

TABLA DE FIGURAS

REFERENCIAS

Para la elaboración del presente libro, se han tenido en consideración los documentos, presentaciones e información de las siguientes fuentes:

Fabricantes, distribuidores y desarrolladores de soluciones de tarjetas

Akrocard	http://www.akrocard.com/
Barcitronic	http://www.barcitronic.com/
Bit4ID Ibérica	http://www.bit4id.com/espanol/
C3PO	http://www.c3po.es
CardLogix	http://www.cardlogix.com/
Datacard	http://www.datacard.com/
Dz Card	http://www.dzcard.com/
FNMT	http://www.fnmt.es/
Gemalto	http://www.gemalto.com/
GyD Ibérica	http://www.gi-de.com
HID Global	http://www.hidglobal.com/espanol
Idensis	http://www.idensis.com/
Kalysis	http://www.kalysis.com
Oberthur	http://www.oberthurcs.com/
SanDisk (Microelectrónica)	http://www.sandisk.com/

Organismos y grupos internacionales de estandarización

ISO - International Organization for Standardization	http://www.iso.org/
CEN - European Committee for Standardization	https://www.cen.eu/
EMVCo	http://www.emvco.com/
JavaCard	http://www.oracle.com/technetwork/java/javacard/overview/overview-jsp-135353.html
Multos Consorcium	http://www.multos.com/
NIST - National Institute of Standards and Technology	http://www.nist.gov/
PC/SC Workgroup	http://www.pcscworkgroup.com/
SCANet – Sistema de Codificación Académica Normalizado en Red	http://scanet.udl.es/spa/

Administraciones y organismos públicos españoles

Ajuntament de Barcelona http://www.bicing.cat/home/
Ayuntamiento de Ponferrada http://www.ponferrada.org/ponferrada/cm/temas/tarjetaciudadana
Ayuntamiento de Alcobendas http://www.alcobendas.org/
Ayuntamiento de Gijón http://www.gijon.es/tc
Ayuntamiento de Zaragoza http://www.zaragoza.es/ciudad/sectores/tarjetaciudadana/
DNIe (Ministerio del Interior) http://www.dnielectronico.es/
Gobierno del País Vasco – Tarjeta ONA http://www.euskadi.net/r33-ona2/es/
Gobierno de Navarra – Proyecto ITACA http://www.navarra.es/
Universidad Autónoma de Madrid – UAM http://www.uam.es/carne/
Universidad Nacional de Educación a Distancia – UNED http://portal.uned.es/portal/page?_pageid=93,1015053,93_20544334&_dad=portal&_schema=PORTAL
Universidad de Oviedo http://ti.innova.uniovi.es/Home_2/index.jsp
Universidad Politécnica de Madrid – UPM http://www.upm.es/institucional/PAS/PAS+Laboral/CarneUniversitario
Universidad Pontificia de Salamanca – UPSAM http://www.upsam.es
Universidad de Valladolid – UVA http://www.uva.es/
“DNI electrónico. Guía de Referencia Básica” v1.2 – Comisión Técnica de Apoyo a la Implantación del DNI electrónico. Grupo de Trabajo de Comunicación y Divulgación
“Guía metodológica para la implantación de sistemas de bicicletas públicas en España” IDAE (Instituto para la Diversificación y Ahorro de la Energía), Ministerio de Industria, Turismo y Comercio. Noviembre de 2007.


ANEXO I ESTÁNDARES
DE LAS TARJETAS CHIP
Junta de
Castilla y León
red de municipios digitales
de Castilla y León

AI. ESTÁNDARES DE LAS TARJETAS CHIP

En este apartado se pretenden describir someramente los estándares y especificaciones en el ámbito de las tarjetas inteligentes que se utilizan actualmente. Primero, se describen los estándares que definen la configuración física de las tarjetas.

Posteriormente, se explican aquellas normas que definen los sistemas operativos que se utilizan en los circuitos integrados de las tarjetas. Seguidamente, se especifican y detallan los estándares internacionales ISO a los que se debe ajustar en la fabricación de la tarjeta según las distintas tecnologías existentes.

A continuación se muestran los criterios de evaluación de la seguridad más utilizados para la certificación de productos y elementos, tanto hardware, como software o firmware.

AI.1 TAMAÑOS Y CONTACTOS DE LA TARJETA INTELIGENTE

La norma ISO/IEC 7816-1 define los posibles tamaños para una tarjeta inteligente y del circuito integrado, así como la posición de los contactos en el chip, tal y como se muestra en las siguientes figuras:

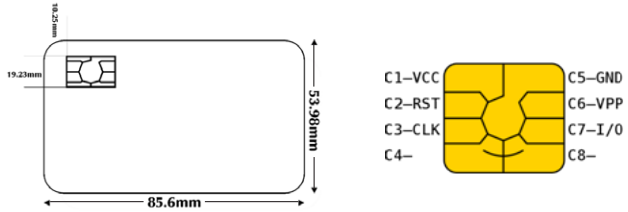
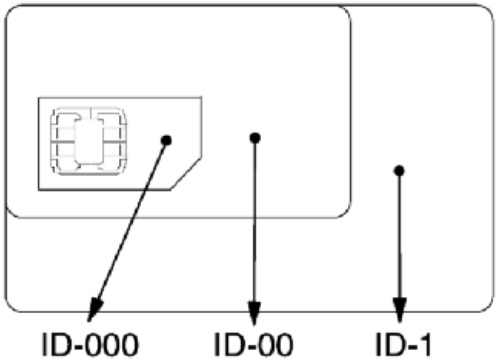


Figura 11 Dimensiones de la tarjeta y contactos del chip

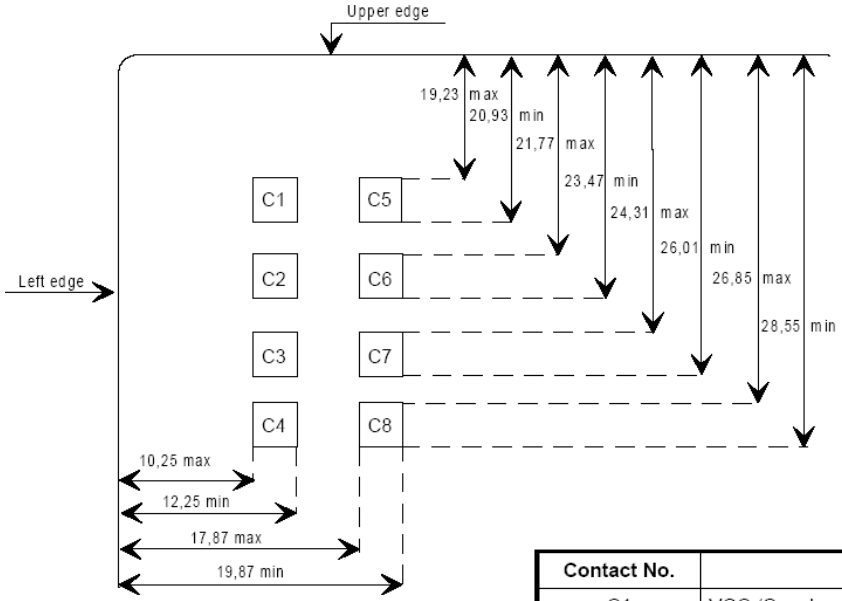


Formato	Dimensiones
ID-1	85,60 mm x 53,98 mm
ID-000	25 mm x 15 mm
ID-00	66 mm x 33 mm

Figura 12 Tamaños de tarjetas según ISO/IEC-7816

La disposición de los contactos que se muestra en la Figura 1 se define en la especificación ISO/IEC 7816-2 y es la más común, pero existe otra disposición diferente, actualmente en desuso, definida por AFNOR, Association Française de Normalisation, debido al intento de compatibilizarla con las tarjetas de banda magnética.

En la siguiente figura se muestran la disposición de los contactos en el chip y las funciones predeterminadas de cada contacto, que se definen en la especificación:



Contact No.	Assignment	Contact No.	Assignment
C1	VCC (Supply voltage)	C5	GND (Ground)
C2	RST (Reset signal)	C6	VPP Variable supply voltage (e.g. programming voltage)
C3	CLK (Clock signal)	C7	I/O (Data input/output)
C4	Reserved for future use in other parts of ISO/IEC 7816	C8	Reserved for future use in other parts of ISO/IEC 7816

Figura 13 Distancia de los contactos del chip de la tarjeta y funciones de los contactos *Fuente: ISO/IEC 7816-2*

AI.2 ESTÁNDARES DE SISTEMAS OPERATIVOS

Existen múltiples sistemas operativos, comúnmente denominados máscara, y se desarrollan a medida de los elementos físicos y de los requisitos de las aplicaciones. Hace unos años, cada fabricante de tarjeta diseñaba su sistema operativo, de manera que existían cantidad de sistemas operativos, que impedía el desarrollo de aplicaciones generales para cualquier tipo de tarjeta.

Actualmente, esta tendencia está cambiando gracias a la implementación de sistemas operativos desarrollados por consorcios o grupos de empresas, que permiten el desarrollo de aplicaciones sin tener que diseñarlas según el tipo de sistema operativo que utilice la tarjeta.

Los sistemas operativos pueden ser de dos tipos: privados / propietarios, si están desarrollados por un determinado fabricante, o sistemas abiertos, que puede modificar cualquier usuario. Es muy importante definir bien desde el inicio el tipo de plataforma o sistema operativo que se selecciona para la implantación de servicios basados en tarjetas inteligentes, puesto que de ello dependerán los costos, la capacidad de desarrollo y la interoperabilidad entre aplicaciones.

AI.2.1 Sistemas Operativos Privados / Propietarios

Los sistemas propietarios o privados suelen estar diseñados por compañías de servicios o empresas del sector financiero, para un circuito integrado específico, y no funcionarán en chips distintos de para los que están desarrollados, a no ser que se realicen modificaciones. Tampoco son interoperables, es decir, las aplicaciones que se desarrollen no funcionarán sobre otros modelos de tarjetas. Además, al residir en la memoria ROM de la tarjeta, no pueden modificarse y no existe posibilidad de evolución, a no ser que la incluya el fabricante en sus desarrollos.

Las dos tecnologías que soportan estos sistemas operativos se presentan a continuación.

WG10

Es un sistema operativo que está basado en la norma ISO/IEC 7816. En 1999, el European Committee for Standardization (CEN), en el Comité Técnico 224, desarrolla el estándar europeo EN 1546, mayormente conocido por CEN/TC224/WG10, ratificada por AENOR en el año 2000, "*Sistemas de tarjetas de identificación. Monedero electrónico intersectorial*", y consta de cuatro partes.

Las tarjetas que tienen instalado este sistema operativo ofrecen un nivel de seguridad e integración alto para aplicaciones de monedero electrónico, basadas en soluciones prepago. Otras aplicaciones para las que se suele utilizar este sistema operativo son: tarjetas sanitarias, almacenamiento de datos confidenciales, tarjetas de transportes y universitarias,..

TIBC

TIBC (Tarjeta Inteligente para Bancos y Cajas de Ahorro) es un sistema operativo que desarrolló SERMEPA, empresa dedicada a soluciones TIC en medios de pago, para las primeras tarjetas inteligentes, como base para el monedero electrónico Visa Cash (TIBC 1.0). El sistema operativo integra criptografía simétrica (DES) y es multiaplicación.

La segunda generación de este sistema operativo, denominado Advantis, combina en un mismo circuito aplicaciones de débito y crédito bajo el estándar EMV y el monedero electrónico bajo estándar CEPS, permitiendo la generación de firmas electrónicas y autenticación off-line, y asegurando la interoperabilidad mundial como medio de pago y monedero. TIBC 3.0, la tercera generación de este sistema operativo, se ha implementado como solución para las tarjetas VISA de España y Latinoamérica con aplicaciones EMV de crédito y débito.

Este sistema se utiliza en aplicaciones de monedero electrónico, control de accesos, autenticación por huella dactilar y reconocimiento facial, fidelización,... La Tesorería de la Seguridad Social eligió este sistema para su proyecto TASS (Tarjeta de la Seguridad Social).

AI.2.2 Sistemas Operativos Abiertos

Los sistemas operativos abiertos se empezaron a utilizar en el desarrollo de aplicaciones para tarjetas inteligentes en el año 1997. El uso de este tipo de sistemas facilita el desarrollo de aplicaciones, puesto que se programa en lenguajes de más alto nivel, por ejemplo, C++ o Java, y no es el fabricante el que impone el sistema operativo, abriéndose el mercado a terceros.

Existen varios sistemas operativos abiertos que a continuación se detallan.

MULTOS

Es un sistema operativo abierto de tarjetas inteligentes desarrollado por Maosco Ltd., grupo inglés en el sector financiero y de tarjetas. Este sistema fue impulsado por MasterCard, aunque el control de la especificación está en el Consorcio MultOS, es decir, Maosco Ltd. Este consorcio es un grupo de organizaciones internacionales que tienen por objetivo promover su uso como estándar por la industria de tarjetas inteligentes.

MultOS tiene un nivel de seguridad muy alto, debido a que se desarrolló para su aplicación en el sector financiero. Es un sistema multiaplicación (monedero electrónico, tarjetas universitarias, tarjetas sanitarias, etc.), permitiendo la instalación y eliminación de aplicaciones en la tarjeta. Para el desarrollo de aplicaciones se utiliza un lenguaje propietario, MEL (Multos Executable Language), aunque existen conversores para otros lenguajes, como por ejemplo C.

Java Card

Java Card es un sistema operativo desarrollado por Sun Microsystems, proporcionando un entorno seguro para aplicaciones de tarjetas inteligentes. Es un sistema multiaplicación, que contiene una *máquina virtual de Java* (JVM), y como el sistema MultOS permite añadir aplicaciones aún cuando la tarjeta haya sido emitida al usuario final.

Este sistema se puede utilizar para gran número de aplicaciones: tarjetas SIM (proporciona servicios adicionales como venta de entradas,

banca online,...), tarjetas financieras (tanto para transacciones online y offline), tarjetas de identidad, tarjetas sanitarias, control de accesos lógico y físico, transportes, autopistas,...

AI.3 ESTÁNDARES INTERNACIONALES DE TARJETAS INTELIGENTES

La compatibilidad de las tarjetas en cualquier lugar del mundo es imprescindible para que su utilización se haya generalizado, sobre todo como medio de pago y mecanismos de identificación y autenticación, razón por la cual las entidades responsables de la estandarización a nivel mundial, ISO (International Standards Organization) e IEC (International Electrotechnical Commission, han tenido que desarrollar diferentes estándares para evitar las incompatibilidades dependiendo de la tecnología utilizada.

En el siguiente apartado se pretende explicar brevemente los estándares de las tarjetas que describen las funcionalidades y especificaciones de cada tipo de tarjetas.

AI.3.1 ISO/IEC 7810 – Identification cards – Physical characteristics

La última versión de este estándar es del año 2003 (ISO/IEC 7810:2003), y define las características físicas para las tarjetas utilizadas para identificación: materiales de las tarjetas (tipos de plásticos utilizados), fabricación (flexibilidad, tolerancia a la temperatura), características (posición y cableado de los elementos electrónicos en el chip, posición de los contactos,...) y dimensiones para cuatro tamaños de tarjetas distintos. La norma ISO/IEC 10373-1 estandariza y define las pruebas que se deben realizar para comprobar que los parámetros especificados de una tarjeta se corresponden con los definidos en el estándar ISO/IEC 7810. Este estándar no contempla las tarjetas delgadas flexibles, que son objeto de una norma específica.

Los cuatro tipos de tarjetas que define este estándar son denominados ID-1, ID-2, ID-3 e ID-000.

Formato de tarjeta	Dimensiones	Utilización
ID-1	85,60 mm x 53,98 mm	Tarjetas bancarias y de identificación
ID-2	105 mm x 74 mm	Antiguas tarjetas alemanas (anteriores a noviembre de 2010)
ID-3	125 mm x 88 mm	Pasaportes y Visas
ID-000	25 mm x 15 mm	Tarjetas SIM (teléfonos móviles)

ID-1

Este formato se utiliza para los siguientes usos: tarjetas bancarias (tarjetas de crédito, tarjetas de débito, tarjetas ATM,…), carnets de conducir (Estados Unidos, Brasil, Canadá, Australia, Noruega,…), documento nacional de identidad de ciertos países (Bélgica, Bulgaria, Croacia, Brasil, Chile,…), tarjetas de fidelización, tarjetas de visitas, pasaporte de los Estados Unidos, etc.

ID-2

Las dimensiones de estas tarjetas se corresponden con el formato A7. Este formato se ha utilizado principalmente para los carnets de identidad alemanes, aunque desde noviembre de 2010, estas tarjetas se sustituirán por el formato ID-1.

ID-3

En este caso se corresponde con el formato B7. Es un formato comúnmente utilizado para pasaportes y visas.

ID-000

Este formato se definió primero en la norma ENV 1375-1, *Identification card systems — Intersector integrated circuit(s) card additional formats — Part 1: ID-000 card size and physical characteristics.* Adicionalmente, en el anexo B del estándar se explica cómo se puede integrar una tarjeta de este tamaño en una tarjeta con formato ID-1. Estas tarjetas se conocen como un nuevo tipo ID-1/000.

AI.3.2 ISO/IEC 7811 – Identification cards – Recording technique

El estándar *ISO/IEC 7811 Identification cards — Recording technique* describe las técnicas de grabación para las tarjetas de identificación. Consta de nueve partes, cada una de las cuales se ha ido actualizando según los avances que se produzcan respecto a la tecnología y las técnicas utilizadas.

Las partes de las que consta este estándar son (el año que aparece entre paréntesis es el año en el que aparece la última versión de cada parte del estándar):

Part 1 (2002): Embossing

Esta parte trata sobre la manera de realizar la estampación/repujado de la tarjeta.

Part 2 (2001): Magnetic Stripe - Low Coercitivity

Define las técnicas sobre la banda magnética de la tarjeta para las tarjetas de baja coercitividad, LO-CO, que utiliza los denominados ferromagnetos “blandos”, materiales de resistencia baja.

Parte 3 (1995): Location of embossed characters on ID-1 cards

Definía la localización de los caracteres estampados en las tarjetas ID-1. Esta parte se ha retirado y se encuentra incluida en la Parte 1.

Parte 4 (1995): Location of read-only magnetic tracks – Tracks 1 and 2

Definía la localización de los tracks 1 y 2 en tarjetas de banda magnética. Esta parte también está obsoleta y se incluye en la Parte 2.

Parte 5 (1995): Location of read-write magnetic track – Track 3

Igual que la anterior, pero para el track 3. Está retirada y se incluye en la Parte 2.

Parte 6 (2008): Magnetic stripe – High coercivity

En esta parte detalla las características de la banda magnética en tarjetas de alta coercitividad, HI-CO, que utiliza ferromagnetos “duros” con mayor resistencia, como la ferrita de bario. Es una de las partes que se han actualizado más recientemente.

Parte 7 (2004): Magnetic stripe – High coercivity, high density

Esta parte define la banda magnética de alta coercitividad y alta densidad, que permite una capacidad diez veces mayor que las detalladas en la Parte 6.

Parte 8 (2008): Magnetic stripe -- Coercivity of 51,7 kA/m (650 Oe)

Detalla las características de la banda magnética para una coercitividad de 51,7 kA/m, incluyendo cualquier capa superpuesta de protección.

Parte 9 (2008): Tactile identifier mark

Especifica las características físicas para las marcas identificadoras táctiles de las tarjetas, que permiten a los discapacitados visuales distinguir unas tarjetas de otras. Define el lugar de la tarjeta donde se debe poner la TIM (Tactile Identifier Mark) y el diseño de los puntos del lenguaje Braille para un reconocimiento rápido y sencillo.

AI.3.3 ISO/IEC 7813 – Information technology – Identification cards – Financial transaction cards

Este estándar define las propiedades y parámetros de las tarjetas de identificación utilizadas en transacciones financieras. La última versión es del año 2006, y define las características físicas (tamaño, forma, localización de la banda magnética,...) y las características magnéticas y estructura de datos y contenido de las pistas de las tarjetas, tanto en circuitos integrados con contactos como los de sin contactos.

Este estándar se complementa y debe cumplir los requerimientos de los estándares ISO/IEC 7811, para la estampación de caracteres y las características de la banda magnética, ISO/IEC 7816-1 para las tarjetas sin contactos, e ISO/IEC 10536-1, ISO/IEC 14443-1 o ISO/IEC 15693-1, para las tarjetas con contactos, según corresponda.

AI.3.4 ISO/IEC 7816 – Identification cards – Integrated circuit cards

Este estándar define las especificaciones para las tarjetas inteligentes con contactos. Es una extensión del estándar ISO/IEC 7810, y como esta norma, está dividido en varias partes, dependiendo de las características que defina (los años entre paréntesis son los años de la última actualización de cada parte).

Parte 1 (1998): Physical characteristics

Define las características físicas de las tarjetas, según las especificaciones detalladas en los estándares ISO/IECD 7810 e ISO/IEC 7813, como por ejemplo: dimensiones, resistencia, tensión mecánica, radiación electromagnética, protección frente a luz ultravioleta y rayos X, grado de torsión, etc. Dependiendo de las dimensiones, se especifican los siguientes formatos:

Formato de tarjeta	Dimensiones	Utilización
ID-1	85,60 mm x 53,98 mm	Tarjetas bancarias (tarjetas de crédito)
ID-000	25 mm x 15 mm	Tarjetas SIM (teléfonos móviles)
ID-00	66 mm x 33 mm	Mini-tarjetas o Tarjetas SIM (teléfonos móviles con tecnología GSM)

En 2003 se hizo una enmienda para la altura máxima de la superficie de contacto para los circuitos integrados.

Parte 2 (2007): Cards with contacts – Dimensions and location of the contacts

Define las dimensiones, localización y función de los contactos del circuito integrado (chip) de las tarjetas para el tipo ID-1. Se debe utilizar en conjunción con el estándar ISO/IEC 7816-1.

Parte 3 (2006): Cards with contacts – Electrical interface and transmission protocols

Esta parte detalla el interfaz eléctrico de la tarjeta (alimentación, estructura de las señales, voltaje, procedimiento operativo) y los protocolos de transmisión de la información para tarjetas asíncronas entre el circuito integrado y un dispositivo (terminales de tarjetas).

Parte 4 (2005): Organization, security and commands for interchange

Esta parte detalla la organización, seguridad y comandos para el intercambio de información entre cualquier tipo de tarjeta (con contactos, de proximidad, de radiofrecuencia,...).

Parte 5 (2004): Registration of application providers

Define la manera de registrar las aplicaciones y asignar los identificadores en el procedimiento de registro, comprobando la disponibilidad de asignar los identificadores a los proveedores de aplicaciones relevantes.

Parte 6 (2004): Interindustry data elements for interchange

Especifica los datos (DEs, Data Elements) utilizados para el intercambio basado en circuitos integrados tanto para las tarjetas con contacto como las tarjetas sin contactos.

Parte 7 (1999): Interindustry commands for Structured Card Query Language (SCQL)

Esta parte define el concepto de una base de datos SCQL y los comandos utilizados para ello.

Parte 8 (2004): Commands for security operations

Especifica los comandos que pueden utilizarse para operaciones criptográficas, adicionalmente a los comandos que se detallaban en la ISO/IEC 7816-4. En los anexos se muestran ejemplos de operaciones relacionadas con firmas electrónicas, certificados e importación y exportación de claves asimétricas. No se incluye en esta parte de la norma la evaluación de los algoritmos y protocolos que se deben utilizar.

Parte 9 (2004): Commands for card management

Especifica los comandos para la gestión de la tarjeta y los ficheros almacenados en la misma, como pueden ser los de creación y eliminación de ficheros, cubriendo el ciclo de vida completo de la tarjeta (desde la fabricación hasta que la tarjeta haya expirado).

Parte 10 (1999): Electronic signals and answer to reset for synchronous cards

Esta parte detalla la respuesta al reset, la alimentación, la estructura de las señales, las condiciones de operación,... para el intercambio de datos entre el circuito integrado de la tarjeta y un dispositivo que se comunican mediante transmisión síncrona. Esta parte amplía la especificación ISO/IEC 7816-3, y define dos tipos de tarjetas síncrona: tipo 1 y tipo 2.

Parte 11 (2004): Personal verification through biometric methods

Especifica los comandos utilizados para la verificación mediante métodos biométricos que ya se habían enumerado en la especificación ISO/IEC 7816-4. Algunos de los objetos que se utilizarán se definen en esta parte, pero otros pueden estar definidos en la norma ISO/IEC 19785-1.

Parte 12 (2005): Cards with contacts – USB electrical interface and operating procedures

En esta parte del estándar se especifican las condiciones de operación de las tarjetas mediante un interfaz USB (a este tipo de tarjetas, se las denomina USB-IC).

Parte 13 (2007): Commands for application management in a multi-application environment

Esta parte especifica los comandos para la gestión de aplicaciones en un entorno multiaplicación. Cubre todo el ciclo de vida de la tarjeta.

Parte 14 (2006): Full-Duplex Single Wire Protocol for Smart Cards

Esta parte no ha sido aprobada por los comités técnicos de ISO y finalmente se ha retirado.

Parte 15 (2004): Cryptographic information application

Especifica las funcionalidades criptográficas de la tarjeta para las aplicaciones, y define una sintaxis común, en formato ASN.1, y el formato de la información criptográfica y los mecanismos para compartir esta información.

En 2007, se realizó una primera enmienda a este documento, para incluir ejemplos de uso de aplicaciones criptográficas. En 2008, se realizó una segunda enmienda que corrige errores y definen extensiones para entornos multiaplicación.

AI.3.5 ISO/IEC 10536 – Identification cards – Contactless integrated circuit(s) cards – Close-coupled cards

Este estándar define las características de las tarjetas sin contactos de cercanía, que se detallan en el apartado 2.4.3 (distancia para poder operar de menos de dos milímetros, es decir, la tarjeta debe estar casi en contacto con el lector para poder iniciara la comunicación). El estándar se compone de tres partes.

Parte 1 (2000): Physical characteristics

Define las características físicas de las tarjetas si contactos de cercanía, conocidas como Close-coupled cards (CICC). Sólo aplica a tarjetas de identificación del tipo ID-1, bien sea introduciendo la tarjeta en el lector o situándola sobre la superficie del terminal.

Parte 2 (1995): Dimensions and location of coupling areas

Especifica las dimensiones, localización, naturaleza y asignación de las áreas de acople que proporcionan el interfaz necesario para la comunicación entre los CCDs (Card Coupling Devices) con las CICC para los tipos de tarjetas ID-1, y se muestran algunos ejemplos de estos elementos.

Parte 3 (1996): Electronic signals and reset procedures

Especifica la naturaleza y las características de los campos electromagnéticos necesarios para la alimentación y la comunicación bidireccional entre los dispositivos lectores y las tarjetas chip para los tipos de tarjeta ID-1.

Existe una parte 4, ISO/ IEC 10536-4 – Answer to reset and transmission protocols, que finalmente no ha sido aprobada.

AI.3.6 ISO/IEC 14443 – Identification cards – Contactless integrated circuit cards

Este estándar define las tarjetas chip sin contactos, es decir, las denominadas tarjetas de proximidad utilizadas para identificación, y los protocolos de transmisión para comunicarse. El estándar consta de cuatro partes.

Parte 1 (2008): Physical characteristics

En esta parte se definen las características físicas de este tipo de tarjetas, denominadas PICC (Proximity Integrated Circuit Card). Existen dos tipos de tarjetas, Tipo A y Tipo B, que se comunican mediante radiofrecuencia a 13,56 MHz. La diferencia entre los dos tipos estriba en los métodos de modulación, los esquemas de codificación y los procedimientos de inicialización y protocolos, que se describen en las siguientes partes de esta especificación.

Parte 2 (2010): Radio frequency power and signal interface

Especifica las características de los campos electromagnéticos para la alimentación y la comunicación bidireccional entre las tarjetas de proximidad y los dispositivos, denominados PCDs (Proximity Coupling Device). Las características más importantes son: frecuencia de operación de 13,56 MHz. y velocidad de transmisión de datos de 106 kbits/s.

Parte 3 (2001): Initialization and anticollision

En esta parte se detallan los protocolos de inicialización de los procedimientos para los dos tipos de tarjetas y los procedimientos de anticolisión.

En 2005 se realizó una enmienda, la cual se volvió a modificar en 2006 para definir las tasas de bits (bitrates). En 2006, se realizó una nueva enmienda, SO/IEC 14443-3:2001/Amd 3:2006, para el manejo de los campos reservados y sus valores.

Parte 4 (2008): Transmission protocol

En esta parte se especifica los protocolos de transmisión (semi-dúplex) necesarios para estos entornos y se definen las secuencias de activación y desactivación de los protocolos, siendo aplicable tanto a las tarjetas Tipo A como a las tarjetas Tipo B.

Por último, cabe destacar que este estándar se utiliza en varias tecnologías, entre las que cabe destacar:

- MiFare – implementa las partes 1, 2 y 3 del estándar para tarjetas de *Tipo A*.
- Calypso (RFID) – implementa las partes 1, 2, 3 y 4 del estándar para tarjetas de *Tipo B*.
- Las tarjetas de crédito RFID cumplen con los requerimientos del *Tipo B* especificados en el estándar.
- Los pasaportes biométricos implementan el estándar completo.

AI.3.7 ISO/IEC 15497 – Identification cards – Thin flexible cards

Las tarjetas flexibles se utilizan para automatizar los controles de accesos a bienes y servicios, como pueden ser las tarjetas utilizadas en los peajes de las autopistas, los aparcamientos, los transportes públicos, cupones de descuento,... Las aplicaciones pueden utilizar varios métodos de grabación, como pueden ser bandas magnéticas, código de barras, sin contactos, reconocimiento del iris,...

Este estándar define las características de este tipo de tarjetas y se compone de tres partes.

Parte 1 (2008): Physical characteristics

Especifica las características físicas para este tipo de tarjetas: tamaño de tarjetas, dimensiones, almacenamiento y uso de las tarjetas bajo ciertas condiciones ambientales,...

Parte 2 (2007): Magnetic recording technique

Especifica las características de la banda magnética y de la codificación de las tarjetas.

Parte 3 (2008): Test methods

Detalla los métodos de prueba y procedimientos para llevar a cabo medidas respecto de la banda magnética y características de codificación, aunque no entra en los criterios de aceptación.

AI.3.8 ISO/IEC 15693 – Identification cards – Contactless integrated circuit(s) cards – Vicinity cards

Este estándar especifica las características de las tarjetas lejanas, denominadas *Vicinity Cards*, tarjetas sin contactos cuya distancia de la tarjeta al dispositivo puede llegar a unos pocos metros. La desventaja de este tipo de tarjetas es la concurrencia que se puede producir en la comunicación entre las tarjetas y el dispositivo lector. La frecuencia de operación de estas tarjetas es 13,56 MHz. Al tener que operar a mayor distancia, el campo magnético debe ser menor (desde 0.15 A/m a 5 A/m) que para las tarjetas de proximidad (1,5 A/m a 7,5 A/m).

Parte 1 (2010): Physical characteristics

En esta parte se definen las características físicas de las Vicinity Cards (VICCs).

Parte 2 (2006): Air interface and initialization

Define los interfaces para la alimentación y las comunicaciones (radiofrecuencia o comunicación radio) entre las tarjetas y el dispositivo lector. Dependiendo de la alimentación, se generarán una o dos portadoras de la señal, lo cual permite a los sistemas adaptarse a distintos requerimientos operacionales, dependiendo del tipo de ruido a alta y baja frecuencia.

Parte 3 (2009): Anticollision and transmission protocol

Esta parte desarrolla los protocolos de transmisión y anticolisión.


ANEXO II TECNOLOGÍAS
DE IMPRESIÓN SEGURA
Junta de
Castilla y León
red de municipios digitales
de Castilla y León

AII. TECNOLOGÍAS DE IMPRESIÓN SEGURA

A continuación se exponen algunos de los métodos más utilizados en la impresión de tarjetas, que intentan dificultar en la medida de lo posible el fraude por falsas duplicaciones (la mayoría de estas técnicas ya se utilizaban hace bastantes años en la impresión de billetes, por lo que están muy extendidas y probadas):

- Marca de agua digital: este método inserta una imagen en la tarjeta que es difícil apreciar por los seres humanos. Esta imagen puede contener información acerca del usuario de la tarjeta, del fabricante, el terminal, el emisor de las mismas,... La marca de agua se inserta en el momento de la impresión, es decir, implica un proceso de marcado, y otro de detección cuando se quiera comprobar la misma.

- Técnicas de impresión segura: estas técnicas permiten incluir imágenes, logos, ... como fondo de las tarjetas en el momento de la impresión, dificultando la copia de la misma:

  - Técnicas sobre la fotografía y el fondo

    – Guilloches: es la impresión de figuras formadas por líneas asimétricas entrelazadas que forman bandas de seguridad. Su diseño requiere de técnicas CAD, y es una de las técnicas más antiguas puesto que se utiliza en la fabricación de papel moneda por la dificultad de la falsificación.

    – Efecto Iris: se trata de producir imágenes con mezclas de colores, de manera que dependiendo del ángulo de visión, se observa una diferencia de color. Esta técnica ofrece gran seguridad dada la complejidad para reproducir el efecto.

  - Técnicas sobre el cuerpo de la tarjeta

    – Overlay: consisten en incluir una lamina de poliéster, revestimiento y tinta en la tarjeta, transparentes, de alta resistencia y durabilidad, que añaden unos cuatro micras de espesor, posteriormente a la impresión personalizada de la tarjeta, protegiendo esta información

frente a manipulaciones o frente al uso cotidiano de la misma. El barniz overlay es aplicado con tecnología de transferencia térmica, y se debe recortar en la parte del chip para poder conectar los contactos. Existe un overlay holográfico, que consiste en una película fotosensible expuesta a un rayo láser, creando un grabado microscópico que proyecto una imagen similar a un objeto en 3D.

- Dispositivo de imagen difractiva ópticamente variable (DOVID): en este caso, a diferencia del caso del efecto Iris, se utilizan las propiedades de refracción de la luz. Los más conocidos son los hologramas (cuando se iluminan adecuadamente, se obtiene una figura tridimensional, que varía al cambiar el ángulo de iluminación), pero también existen otros tipos como los kinegramas o los OVDs. Son imágenes que cambian de color según la inclinación y el ángulo de la luz, de manera que no se pueden copiar y dificultan enormemente su falsificación.

• Tintas especiales

- Tintas ultravioletas y fluorescentes: son tintas que permanecen invisibles ante la luz normal, pero visibles a la luz ultravioleta con un efecto fluorescente y profundidad.
- Tintas OVI (Optically Variable Ink): son tintas de diferentes pigmentos de color, por lo que cambian de color según el ángulo de inclinación de la tarjeta. Los colores que se suelen mezclar son: rojo y verde, oro y verde, o marrón y verde.
- Tintas perlescentes (tintas metálicas especiales): muestran diferentes colores según la luz que reciba (por el efecto de interferencia), y pueden producir efectos policromados, mostrando diferentes colores. Estas tintas se suelen utilizar en la impresión de tarjetas de crédito (plata, oro,...).
- Tintas iridiscentes: cambian la tonalidad de la figura impresa dependiendo del ángulo de iluminación y observación, sin apreciarse un cambio de color significativo.
- Tintas TIR: son tintas especiales transparentes a la iluminación infrarroja, que cambian de color expuestas a una luz especial, garantizando la correcta lectura de las líneas OCR. Se utilizan para enmascarar elementos de seguridad de la tarjeta.

- Técnicas de grabación e impresión

  – Impresoras láser: las imágenes grabadas con estas impresoras no se pueden sustituir pero pueden ser alteradas mediante ciertas técnicas.

  – Termoimpresión: son más económicas que las impresoras láser y no se pueden alterar las imágenes grabadas. Utilizan para ello distintos tipos de tinta, como las tintas OVI.

  – Embosado: es la impresión en relieve mediante una rueda que contiene el molde de todos los caracteres. La superficie que sobresale del plástico se entinta, de manera que se resalten los caracteres.

  – Indent: es similar a la técnica de embosado, pero en este caso el carácter impreso no sobresale (sería similar a una máquina de escribir).

  – Microimpresión: es la impresión de caracteres en un tamaño muy pequeño, de 200 micras de altura, con lo cual las impresoras ordinarias no pueden reproducir estos textos a la misma resolución.

  – Impresión codificada: el texto impreso sólo puede interpretarse mediante una lente especial, viéndose como una imagen borrosa si no utilizamos la lente.

- Técnicas anti-copia: existen soluciones software que permiten insertar ciertos elementos que dificultan la copia de las tarjetas, como textos ocultos que aparecen cuando se realizan copias, o Fingerprint, software que modifica el grosor de las líneas de forma irregular, de manera que los métodos de copia no obtienen el mismo resultado.

- Técnicas de codificación de las imágenes: existen dispositivos que permiten codificar una imagen dentro de otra, de manera que se dificulta la percepción de las imágenes, puesto que son invisibles a simple vista para el ojo humano, y la falsificación. Entre estos dispositivos destaca Scrambled Indicia®, de la empresa Graphic Security Systems Corporation, implementado por varios países en sus billetes y en documentos de identidad. Para la decodificación de las imágenes o información que se haya ocultado es necesario un decodificador óptico.


ANEXO III CRITERIOS DE EVALUACIÓN DE LA SEGURIDAD
Junta de Castilla y León
red de municipios digitales de Castilla y León

AIII. CRITERIOS DE EVALUACIÓN DE LA SEGURIDAD

En la actualidad, cualquier elemento de cualquier sistema TIC (Tecnologías de la Información y las Comunicaciones) desempeña un papel crítico que puede provocar que el funcionamiento y/o el uso, si no se realiza de una manera apropiada y segura, no sea correcto y comprometa la seguridad del sistema, creciendo el daño potencial que podría provocar un fallo del mismo.

Al existir vulnerabilidades en cualquier sistema, es necesario proteger la información. Por esta razón, la evaluación de la seguridad de un producto, en el caso que nos concierne, el de tarjetas inteligentes, no puede depender de criterios ambiguos o parciales, sino que deben ser concretos, precisos e independientes. La evaluación de esta seguridad permitirá proporcionar un nivel de confianza concreto.

La unificación de estos criterios ha permitido crear una serie de normas y recomendaciones que permiten medir, en función de la adaptación de las características de tarjetas y lectores a estos criterios, la funcionalidad de seguridad que ofrecen. En este apartado se pretende mostrar las normas y criterios de seguridad más utilizados a la hora de definir las características de las tarjetas inteligentes, bien sean desarrollados por entes públicos (Common Criteria) o privados (FLIPS, EMV).

AIII.1 COMMON CRITERIA (ISO/IEC 15408)

Estas normas y criterios se desarrollaron a mediados de los noventa, y pretendían aunar en un único desarrollo las normas necesarias para la evaluación de los productos de seguridad en sistemas TIC.

Finalmente, ISO lo convirtió en estándar en 1999, *ISO/IEC 15408 – Information technology – Security techniques – Evaluation criteria for IT security*, agrupando en un único estándar un conjunto de criterios de evaluación de la seguridad que hasta ahora aplicaba cada organización o gobierno, especificando los requerimientos funcionales de seguridad, permitiendo que los fabricantes puedan implementar estos criterios en sus productos, y los laboratorios puedan evaluarlos y determinar si se cumplen los requisitos de seguridad. La certificación Common Criteria (CC) de un producto IT permitirá medir el nivel de seguridad y confianza que ofrece.

De esta manera, se aunaron los criterios europeos (definidos por ITSEC, *Information Technology Security Evaluation Criteria*), los criterios americanos (definidos por TCSEC, *Trusted Computer System Evaluation Criteria*) y los criterios canadienses (CTCPEC, *Canadian Trusted Computer Product Evaluation Criteria*), permitiendo la comparación de los resultados de evaluaciones de seguridad realizados a diferentes productos. El desarrollo se llevó a cabo con la participación de los gobiernos de Canadá, Francia, Alemania, Holanda, Reino Unido y Estados Unidos.

En el estándar se describen diferentes áreas de aplicación: soporte criptográfico, protección de los datos del titular,..., y consta de tres partes. CC permite determinar las funciones de seguridad del producto y el entorno de aplicación, los diferentes niveles de confianza del producto (EAL, Evaluation Assurance Levels) que determinan el nivel de exigencia en sus desarrollos, y la confianza de que sólo un laboratorio acreditado por un esquema de certificación nacional (el Centro Criptológico Nacional, en el caso de España) puede realizar las evaluaciones CC.

El proceso de evaluación conlleva verificar los siguientes aspectos:

- Definición de los requisitos de seguridad del producto.
- Implementación de los requisitos de seguridad del producto.
- Desarrollo y documentación del producto.

La seguridad quedará conformada según unos perfiles de protección estándares (conjunto de requisitos para una categoría de productos específica) para cualquier producto, de forma independiente, que permitirán selección un nivel de confianza, desde el *EAL1 al EAL7*.

Los perfiles de protección están compuestos por requisitos funcionales (SFR, Security Funcional Requirement) y requisitos de confianza o aseguramiento (SAR, Security Assurance Requirement).

Part 1 (2009): Introduction and general model

Establece los conceptos generales (términos y abreviaciones) y principios para la evaluación de la seguridad de productos IT, y especifica el modelo general de evaluación.

Part 2 (2008): Security functional components

Define el contenido y presentación de los requerimientos funcionales (SFR) que deben ser evaluados según CC. Contiene un catálogo de componentes de seguridad predefinidos que se corresponden con la mayor parte de las necesidades de seguridad que se encuentran en el mercado. Este catálogo se organiza en una estructura jerárquica de clases, familias y componentes.

También proporciona una guía para especificar requerimientos de seguridad personalizados cuando no es posible utilizar los componentes predefinidos.

Part 3 (2008): Security assurance components

Define el contenido y presentación de los requisitos de confianza o aseguramiento (SAR) y los niveles de seguridad (EAL). Esta presentación de las clases, familias y componentes se realiza según una estructura jerárquica.

AIII.2 FIPS 140

FIPS, Federal Information Processing Standards, son una serie de estándares desarrollados por el gobierno de Estados Unidos, para las agencias del gobierno no militares y sus contratistas.

La serie FIPS 140, publicada por el NIST, National Institute of Standards and Technologies, especifica los requisitos de seguridad para el hardware y los módulos de software criptográfico. Existen dos versiones publicadas y una en desarrollo:

- FIPS 140-1 se publicó en enero del año 1994, y definía cuatro niveles de seguridad y once áreas de seguridad.
- FIPS 140-2 se publicó en mayo del año 2001, tiene en cuenta la evolución de la tecnología y comentarios que se han ido realizando sobre la primera versión por los fabricantes, proveedores, probadores y comunidades de usuarios.
- FIPS 140-3 es una nueva versión del estándar que está actualmente en desarrollo. En el primer borrador del estándar, introduce una nueva sección de seguridad del software, define un nivel de seguridad adicional y nuevos requerimientos. En el último borrador se vuelve a los cuatro niveles de seguridad y limita el nivel de seguridad del software a los niveles 1 y 2.

Los requerimientos de seguridad que se definen cubren once áreas relacionadas con el diseño e implementación de módulos criptográficos:

- Especificaciones de los módulos criptográficos.
- Puertos e interfaces de los módulos criptográficos.
- Reglas, servicios y autenticación, especificando quién puede acceder a los módulos y qué operaciones puede realizar, así como la manera de verificar estos requisitos.
- Modelo finito de estados de los módulos, y las transiciones entre los mismos.
- Seguridad física.
- Entorno de operación.
- Gestión de las claves criptográficas.

- EMI/EMC, interferencias y compatibilidad electromagnéticas.
- Auto-test, pruebas de los módulos, especificando los elementos sobre los que realizar las pruebas, cuándo realizarlas y las acciones a tomar si el test presenta algún error.
- Garantía del diseño, incluyendo la documentación que debe acompañar al módulo para demostrar que ha sido diseñado e implementado correctamente.
- Mitigación de otros ataques.

El estándar define cuatros niveles de seguridad, pero no especifica en detalle el nivel de seguridad requerido según la aplicación:

- *Level 1*: es el nivel más bajo de seguridad e impone requerimientos básicos a los módulos criptográficos. En este nivel no se especifica mecanismos físicos de seguridad. Un ejemplo de un modulo criptográfico de este nivel sería la tarjeta encriptadora de un ordenador personal, que permite la codificación de los datos.
- *Level 2:* mejora los mecanismos de seguridad añadiendo ciertos requerimientos para evitar la adulteración de los elementos, por ejemplo, mediante sellos o recubrimientos que deban ser rotos para acceder físicamente a las claves criptográficas y parámetros de seguridad críticos dentro del módulo. Requiere que exista una autenticación basada en perfiles.
- *Level 3:* añade requerimientos que prevengan el acceso a los CSPs del módulo criptográfico. Físicamente, debe impedir el acceso al módulo mediante el borrado de la información si se “abre” el módulo.
- *Level 4:* proporciona el nivel de seguridad más alto que se define en el estándar. Proporciona mecanismos para detectar y responder a cualquier intento no autorizado de acceso al módulo criptográfico. También proporciona protección frente a condiciones medioambientales o fluctuaciones en el voltaje y temperatura dentro de los rangos normales de operación, si éstas comprometen la seguridad del módulo.

AIII.3 EMV

Las instituciones financieras pronto se dieron cuenta que era necesario una estandarización de las tarjetas electrónicas, que permitiese su uso como medios de pago y garantizase mayor seguridad. Después de largas deliberaciones, tres de las principales marcas de tarjetas de crédito / débito, MasterCard, Visa y Europay publicaron en 1996 la primera versión de EMV, estándar de interoperabilidad para tarjetas inteligentes que define una serie de características de seguridad que deben cumplir estas tarjetas. En el año 2000, se publicó una revisión del estándar. Este estándar está basado en las especificaciones ISO/IEC 7816 y se trabaja coordinado con ISO para asegurar futuras compatibilidades según se actualizan los estándares.

El despliegue de tarjetas que cumplieran el estándar EMV ha sido gradual, puesto que es costoso de implementar y certificar, convirtiéndose en la actualidad en el estándar de facto para tarjetas inteligentes utilizadas como medios de pago. En estos momentos, la mayoría de entidades financieras a nivel mundial están migrando las antiguas tarjetas de banda magnética a tarjetas inteligentes con chip. En Europa, esta migración debía realizarse antes de final del año 2010 (590 millones de tarjetas aproximadamente), y se las podrá dotar de una capacidad de autenticación fuerte y firma electrónica reconocida.

El procedimiento para llevar a cabo una transacción EMV difiere de los empleados para tarjetas de banda magnética:

- Lectura de la tarjeta: se conecta la tarjeta al dispositivo lector y se activan los contactos del chip de la tarjeta.
- Se selecciona la aplicación que se debe utilizar (en entornos multiaplicación) y se leen los datos de la misma.
- Autenticación de la tarjeta y verificación del titular, mediante una clave o código PIN.
- Verificación de parámetros: análisis de la posibilidad de la transacción según los parámetros definidos.
- Procesamiento de la transacción, actualización de los datos de la tarjeta y fin de la operación.

Actualmente hay más de mil millones de tarjetas EMV en circulación, según las estadísticas que muestra el organismo EMVCo, formado por las empresas American Express, JCB, MasterCard y Visa según sus números, en septiembre de 2010 había aproximadamente 1.082 millones de tarjetas en circulación, y más de quince millones de terminales y dispositivos lectores según el estándar EMV, que equivale respectivamente al 36% de todas las tarjetas en circulación y el 65% de terminales implantados. EMVCo gestiona, mantiene y mejora las especificaciones EMV, donde se incluyen además directrices para los TPVs y los cajeros automáticos, además de establecer los requerimientos de los procesos de testing y aceptación que evalúan el cumplimento de los productos con el estándar.

La primera revisión del estándar, EMV 3.0, se publicó en 1996, modificándose en 1998, EMV 3.1.1. La versión EMV 4.0 se publicó en diciembre de 2000. La última versión del estándar, EMV 4.2, publicada en el año 2008, consta de cuatro libros, cada uno dedicado a temas específicos sobre las tarjetas y el funcionamiento de las aplicaciones que deben aceptar:

- *Book 1 – Application Independent ICC to Terminal Interface Requirements*: describe los requisitos mínimos para las tarjetas inteligentes y terminales, que aseguren el correcto funcionamiento e interoperabilidad, independientemente de la aplicación utilizada.
- *Book 2 – Security and Key Management*: describe los mínimos requisitos de seguridad que aseguren la interoperabilidad y el correcto funcionamiento de tarjetas y terminales.
- *Book 3 – Application Specification*: define los procedimientos necesarios para realizar las transacciones de pagos en un entorno internacional de intercambio.
- *Book 4 – Cardholder, Attendant, and Acquirer Interface Requirements*: define los requerimientos obligatorios, recomendados y opcionales de los terminales que son necesarios para que acepten las tarjetas que cumplen el estándar.

Adicionalmente, existen otros dos estándares:

- *EMV CPA 1.0 (Common Payment Application)*: descripción funcional de una aplicación que cumple los requerimientos del estándar EMV.
- *EMV CPS 1.1 (Card Personalisation Specification)*: describe los comandos para la personalización de las aplicaciones que se encuentran en la tarjeta.

AIII.4 PC/SC (PERSONAL COMPUTER/SMART CARD)

El PC/SC Workgroup se ocupa de establecer el estándar para la integración de tarjetas inteligentes y lectores de tarjetas en el entorno informático, para que puedan funcionar correctamente. Además, facilita el desarrollo de aplicaciones de tarjetas inteligentes para ordenadores personales y otras plataformas. Concretamente, se define un API para que los desarrolladores puedan integrar sus aplicaciones independientemente del tipo de lector, del fabricante de la tarjeta, del tipo de plataforma donde se encuentra,...

El grupo está formado por cuatro miembros principales: Gemalto, Microsoft, Oracle y Toshiba; y varios miembros asociados.

Las siglas que se utilizan tienen el siguiente significado:

- ICC – Integrated Circuit Card: tarjeta de circuito integrado (tarjeta chip).
- IFD – Interface Device: lector de tarjetas.

La versión 2.0 se publicó por primera vez en agosto de 2004. La última versión de la especificación, PC/SC v2.01.9 se publicó en abril de 2010, y está formada por diez partes y una adenda:

- Parte 1: proporciona una introducción a la especificación y visión general de la arquitectura y de los componentes definidos en el grupo de trabajo.
- Parte 2: detalla los requisitos y características de interoperabilidad para las tarjetas y los lectores
- Parte 3: define los interfaces y los requisitos de funcionalidad para los lectores. Además, proporciona información sobre los números RID.
- Parte 4: proporciona consideraciones de diseño de los lectores, en particular, la implementación recomendada para lectores integrados en teclados PS/2.

- Parte 5: describe el interfaz y la funcionalidad del Resource Manager, componente obligatorio del sistema.
- Parte 6: describe el modelo de proveedor de servicio (Service Provider), define la interfaz e indica la forma de extender este modelo para poder cumplir los requerimientos específicos de ciertas aplicaciones.
- Parte 7: realiza consideraciones de diseño para el desarrollo de aplicaciones, y la forma de utilizar otros componentes.
- Parte 8: detalla recomendaciones para la implementación de servicios de seguridad y privacidad según los estándares, orientado a ordenadores personales e internet, y requerimientos criptográficos y de almacenamiento.
- Parte 9: describe la gestión de lectores con extensión de capacidades, como el interfaz del usuario o funcionalidades de seguridad.
- Parte 10: describe la gestión de lectores con capacidad para la utilización del PIN de seguridad.
- Adenda: lista las referencias ISO.

Junta de Castilla y León

red de municipios digitales de Castilla y León