UNIVERSIDAD POLITÉCNICA DE MADRID

FACULTAD DE INFORMÁTICA

TRABAJO FIN DE CARRERA

PERSONALIZACIÓN Y AUTORIZACIÓN DE TARJETAS DE CRÉDITO: ADAPTACIÓN A EMV

AUTOR: SANTIAGO GARRÁN MARTÍN

TUTOR: JOSÉ CARRILLO VERDÚN

JULIO 2.009

DEDICATORIAS

Dedicado a mi mujer Luz María y a mi madre María Luisa, las dos personas sin cuyo estímulo seguramente no habría llevado a cabo este trabajo.

Y por supuesto a mis hijos, Claudia y Daniel, de quienes en ocasiones me he tenido que esconder para dedicar tiempo al proyecto, y a los que pienso compensar a partir de ahora...

RESUMEN

EMV es un nuevo estándar de medios de pago, que afecta a los dos elementos intervinientes en una transacción de pago con tarjeta: la propia tarjeta, a las que se dota de un nuevo chip, y el terminal en el que se realiza, que deberá interactuar fuertemente con ese chip.

Este estándar está suponiendo una revolución dentro del mundo de las tarjetas financieras, y como tal revolución, también está causando un gran impacto en las aplicaciones informáticas de las entidades financieras.

El presente trabajo fin de carrera tiene como tema central el análisis de ese impacto. Se han inventariado todas las tareas a realizar y los elementos afectados, haciendo foco en la personalización de tarjetas y la autorización de operaciones, las dos principales subaplicaciones informáticas presentes en cualquier entidad emisora de tarjetas.

Junto con el inventario de impactos, también se proponen las adaptaciones que sería necesario realizar en esas aplicaciones para resolverlos. Estas adaptaciones pueden consistir tanto en desarrollar nuevos programas como en modificar los ya existentes. También se especifican cuáles serían las principales modificaciones al esquema de Base de Datos.

Se ha hecho un énfasis especial en todo lo relacionado con la criptografía, ya que uno de los puntos fuertes del estándar EMV es dotar de mayor seguridad a las transacciones, seguridad que le viene dada por el uso intensivo que hace de métodos y procedimientos criptográficos no usados hasta ahora en el mundo de las tarjetas de crédito, como por ejemplo la criptografía asimétrica.

Otro aspecto muy importante es la gran cantidad de datos propios de la tarjeta y del usuario que se deben almacenar en un chip EMV. En el proyecto se han repasado muchos de ellos, indicando cuál es la mejor forma de generarlos y almacenarlos en la aplicación.

Por último, se aportan unas conclusiones sobre cómo ha funcionado hasta ahora el estándar y cuál podría ser el futuro del mismo de ahora en adelante.

SUMMARY

EMV is a new standard for methods of payment. It affects the two elements of card payment transaction: cards with a chip incorporated, and the terminal which must interact with this chip.

This standard is causing a revolution in the world of financial cards, and it is having a very big impact on the computing applications of financial organizations.

The analysis of that impact is the central matter of this graduate work. An inventory of tasks and affected elements was made, with focus on card personalization and authorization of operations, the two main computing applications present in any card issuing organization.

Together with the impact inventory, adaptations needed to solve them are proposed. This adaptations can consist both of developing new programs and to modifying existing ones. Also modifications to the database scheme are specified.

Criptography was specially emphasized, because it is a strong point of the EMV standard. EMV transactions are more secure, and this security is provided by an intensive use of criptographic methods and procedures, which have not been used until now in credit card world, (i.e. asymmetric criptography).

Another very important aspect is the large quantity of card and user data that have to be stored on a EMV chip. This project reviews most of them, and indicates the best way to generate and store in the application.

Finally, some conclusions about how the standard has worked until now and what its future could hold.

ÍNDICE

0. INTRODUCCIÓN

0.1. ANTECEDENTES

EMV es un estándar de medios de pago definido por los sistemas internacionales VISA y MasterCard, y adoptado por la Unión Europea en sus normativas SEPA.

Antes de profundizar en las características de este estándar, se repasará brevemente la historia de las tarjetas bancarias o de pago, desde sus comienzos hasta la aparición de EMV.

Las tarjetas bancarias, utilizadas como un medio de pago, tienen prácticamente un siglo de antigüedad, ya que las primeras aparecieron en Estados Unidos a principios del siglo XX, fruto de una idea surgida en las oficinas del Chase Manhattan Bank. Estas tarjetas primitivas sólo eran admitidas por la entidad que las emitía, y consistían en simples documentos de papel o cartón.

Las primeras tarjetas de plástico (el llamado "dinero de plástico") no aparecerá hasta 1950, con la creación del club Dinner's, también en Estados Unidos. Los miembros de este club recibían una tarjeta que les permitía consumir en más de 200 restaurantes de 27 ciudades simplemente presentándola y firmando el recibo. A fin de mes, el club les cobraba por los consumos realizadas y abonaba los importes correspondientes a los restaurantes.

El siguiente paso fue asignar una numeración estandarizada a las tarjetas, visible en relieve en el propio plástico. Este tipo de tarjeta fue ideada por American Express en 1959. Ese mismo año, Bank of America emitió la primera tarjeta de crédito "universal", es decir, con ella se podían pagar bienes o servicios en una gran gama de comercios de distintos tipos de todo Estados Unidos. Esta tarjeta, inicialmente denominada BankAmericard, pasó a denominarse **VISA** en 1976.

En 1966, un grupo de 14 bancos de Estados Unidos crearon un procedimiento estandarizado de intercambio y negociación de las transacciones realizadas en los comercios por tarjetas de distintos emisores, y formaron una asociación, denominada Interlink, que realizaba dicho intercambio mediante ese procedimiento. Posteriormente, otros grupos de bancos formaron otras sociedades similares, entre ellas una en California que con el tiempo (en 1979) pasaría a denominarse **MasterCard**.

Precisamente **VISA** y **MasterCard** son los promotores del actual estándar EMV, objetivo del presente proyecto.

Pero EMV no es el primer estándar relacionado con las tarjetas. Desde su aparición, se han ido estableciendo diversos estándares ISO que han ido fijando las características de las tarjetas a lo largo del tiempo.

Los primeros estándares relacionados con las tarjetas estaban orientados a las características físicas del plástico. Ejemplos de esos estándares son:

- ISO/IEC CR-80, CR-90 y CR-100

  Estas tres normas definen los tres formatos básicos de las tarjetas; en concreto, el CR-80 determina que el tamaño estándar de las tarjetas de crédito sea de 86 x 54 mm., con un grosor de 0,76 mm.

Con la aparición de las tarjetas, aparecieron también los defraudadores, que en un principio se limitaban a ser meros falsificadores, realizando copias falsas de los plásticos. Quedaba en manos del comerciante fiarse o no de las tarjetas con las que se le pretendía pagar.

Para dificultar la creación de copias falsas, surgió la idea de incorporar una banda magnética a las tarjetas de crédito. De esta forma se podían incluir muchos más datos en la propia tarjeta, aparte de los que se perciben a simple vista en el propio plástico; datos que sólo se podían recuperar de forma automática, mediante mecanismos lectores de bandas magnéticas.

Para garantizar la interoperatividad entre diferentes sistemas, se definieron más estándares ISO, que regulasen las características de las nuevas tarjetas de crédito con banda magnética. Los más destacados son:

- ISO 7810 y 7811

  Estándares internacionales que determinan algunas características de la banda magnética incorporada a las tarjetas, como pueden ser: posición de la banda magnética dentro de la tarjeta, técnica de grabación, codificación de los caracteres en las pistas, etcétera.

  Por ejemplo, determina que cada banda magnética constará de tres pistas de grabación independientes, que se codificarán de la siguiente forma:

  Pista 1:

  Admite hasta 79 caracteres alfanuméricos de este conjunto:

  ```
  !"#$&'()*+,./0123456789:;<=>@?ABCDEFGHIJKLMOPQRST
  UVWXYZ[\]^_
  ```

  Pista 2:

Admite hasta 40 caracteres numéricos de este conjunto:

0123456789:;<=>?

Pista 3:

Admite hasta 107 caracteres numéricos de este conjunto:

0123456789:;<=>?

En el ISO 7811 se definen otras características, como por ejemplo la coercitividad. La coercitividad de una banda magnética es la fuerza magnética necesaria para codificar y borrar esa banda, a mayor coercitividad, mayor resistencia contra campos magnéticos y vida más larga para las tarjetas (también, mayor coste económico).

Aunque la introducción de la banda magnética marcó un antes y un después en la historia de las tarjetas financieras, el progreso de las mismas no se detuvo ahí, y siguieron introduciéndose nuevos dispositivos, mecanismos y medidas de seguridad.

Los mecanismos de seguridad que se han ido incorporando a la banda magnética han consistido básicamente en introducir elementos cifrados como parte de los datos grabados en la tarjeta, bien sea en las pistas de las bandas magnéticas o en el propio plástico. Otros métodos se han basado en la grabación de números de secuencia.

Uno de los primeros fraudes que se produjo en el uso de las tarjetas fue la suplantación de identidad, es decir, la tarjeta podía ser utilizada por una persona no autorizada por el titular ni por la entidad para ello. Para combatir esta suplantación, se implantaron métodos para autenticar al titular (es decir, para asegurarse de que la persona que está utilizando la tarjeta es realmente el titular) fue el PIN o número secreto. Se le asignaba uno al titular, y se guardaba en la base de datos del Host, de forma que, siempre que se operase con la tarjeta, se debería introducir el PIN mediante un teclado al efecto, se enviaría el PIN tecleado al Host y allí se validaría.

Además, se asignaba un número máximo de reintentos consecutivos (generalmente 3) a partir de los cuales se consideraba que la tarjeta no estaba en poder del titular y se bloqueaba.

El problema de tener que enviar desde el terminal al Host el PIN tecleado, es que se ponía en riesgo la seguridad de ese PIN, ya que pinchando la línea cabía la posibilidad de hacerse con ese código. Para evitar esto, se pensó en cifrar el PIN tecleado antes de enviarlo por la línea, utilizando una clave común a ambos extremos de la comunicación.

Esto obligaba a que los terminales dispusieran de capacidad de hacer cifrados con el algoritmo DES, pero, si eran capaces de realizar esos cálculos, ¿por qué no hacer que el propio terminal valide el PIN tecleado? Para ello, se crearon dos datos cifrados, el NA y el PA, que se grabarían en la banda magnética de la tarjeta y permitirían al terminal validar el PIN. Así es como empezaron a grabarse los primeros datos en la banda magnética por motivos de seguridad de las transacciones.

El NA (Número Aleatorio) es un dato generado en Host, diferente para cada tarjeta. Este dato, concatenado con el PIN de la tarjeta, se cifra consigo mismo utilizando el algoritmo DES (al cifrarse consigo mismo se evita el uso de claves). El resultado de este cifrado, denominado PA (Parámetro de Autenticación), se graba también en la banda. La forma de validar el PIN en el terminal es así bastante sencilla: con el NA leído de la banda magnética y el PIN tecleado en el propio terminal, se aplica el DES y se compara el resultado con el PA de la banda, si son iguales, el PIN es correcto.

El problema de esta forma de validar el PIN es que el posible defraudador puede, conociendo el NA y el PA (que puede leer de la banda de la tarjeta), llegar a conocer el PIN, simplemente mediante ensayo/error. Otro problema de este método es la imposibilidad de cambiar el PIN por parte del titular.

Para evitar este problema del método NA/PA, se creó uno nuevo basado en el uso de claves de cifrado, comunes al cajero y al Host. Aplicando el DES al número de tarjeta, utilizando como clave esta clave común, se calcula un PIN que se comunica al cliente. Inclusive, el titular puede elegir su propio PIN, mediante la técnica del offset (dato que sumado al resultado del DES original da como resultado el PIN de la tarjeta). Cuando el offset utilizado es igual a cero, el PIN resultante se denomina PIN nativo, y es el que generalmente se asigna de forma inicial a la tarjeta. El dato que se graba en la banda magnética es el offset, nunca el PIN en claro.

El uso del offset supone un incremento en la seguridad de aquellos terminales que pueden almacenar las claves (como los cajeros), pero no se puede utilizar en aquellos otros que no disponen de las claves (la mayoría de los datáfonos de los comercios). En estos terminales de los comercios, sólo será posible validar el PIN en remoto, e inclusive ni eso, en caso de que no tengan siquiera posibilidad de cifrar datos, ya que entonces directamente no puede validarse el PIN, con el riesgo que conlleva.

Otro dato cifrado que se almacena en la banda y también en el plástico es el denominado código de verificación (CVV en la terminología VISA, CVC para MasterCard o CSS para Euro6000). Este dato se calcula a partir del número de tarjeta y la fecha de caducidad, y no puede ser cambiado por el titular. Se utiliza sobre todo en operaciones realizadas sin lectura de bandas magnéticas, como compras por Internet, por teléfono, o incluso en algunos terminales financieros de oficina sin lector de banda.

Este método sólo autentica la tarjeta, no al titular, que debe ser autenticado por otros medios (por ejemplo, petición de datos personales en el caso de banca telefónica, o autenticación mediante "*login*" en el caso de banca electrónica). Estos códigos, por tanto, por si mismos, proporcionan una seguridad muy débil, ya que no es necesario disponer físicamente de la tarjeta para intentar realizar operaciones fraudulentas.

Todos los códigos grabados en la banda magnética vistos hasta ahora no protegen de un posible duplicado fraudulento de la tarjeta, ya que basta con mantenerlos invariables en la copia falsa. Este método de fraude, denominado clonado o "*skimming*", permite utilizar la tarjeta fraudulentamente en todos aquellos entornos en los que no se solicite PIN, e inclusive en aquellos que lo soliciten si el defraudador ha conseguido obtener el PIN por otros medios.

Como método para autenticar la tarjeta (es decir, para poder dar por buena la tarjeta y descartar un posible fraude por duplicado o "*skimming*") se introdujo cómo medida de seguridad la secuenciación de las operaciones, que es un número que proporciona el Host en la respuesta a las peticiones de autorización realizadas por la tarjeta. Este número es diferente en cada transacción, y el cajero debe grabarlo en la banda magnética de la tarjeta que acaba de operar (cajeros). Esto hace que el duplicado fraudulento sólo pueda operar desde que se estampa hasta que la tarjeta auténtica opera en algún cajero con capacidad de regrabación (algún cajero de la propia entidad). Pero éste método no asegura una protección permanente contra la copia pirata.

Como se ve, las posibilidades de fraude en una banda magnética son grandes, sobre todo debido a la facilidad de realizar copias exactamente iguales de las tarjetas originales.

Para evitar este problema, surgieron otro tipo de tarjetas no basadas en la banda magnética, a la que sustituyeron (o complementaron) con un nuevo dispositivo más avanzado tecnológicamente: el "chip".

El chip es un microprocesador, pero lo suficientemente reducido de tamaño como para poder incorporarlo a una tarjeta.

Las tarjetas con chip (microprocesador) incorporado, también denominadas tarjetas inteligentes, son capaces de procesar datos y manejar programas, además de disponer de memoria sólo accesible desde el propio chip. Estas características hacen del chip un dispositivo más seguro que la banda magnética, sobre todo porque es más difícil de replicar.

Las características de las tarjetas inteligentes están reguladas también por un estándar ISO:

- ISO 7816

Este estándar está dividido en tres secciones, cada una de las cuales define las siguientes características:

- Características físicas de la tarjeta: no sólo del plástico, sino también de los "pines" o contactos del chip, además de características exigibles en cuanto a resistencia a distintas agresiones: rayos X, presiones, campos magnéticos, electricidad estática, etcétera.

- Dimensiones y posición de los contactos ("pines") respecto al plástico

- Señales eléctricas (valores de voltaje y corriente), procesos operacionales (conexión, activación, reset) y protocolos de transmisión (PTS, T=0).

En el entorno financiero, y antes de la llegada de EMV, las tarjetas chip se han utilizado principalmente para la implementación de las denominadas tarjetas monedero o monederos electrónicos.

En cambio, EMV utiliza el chip de una forma bastante diferente: aunque ambos, el monedero electrónico y el chip EMV, son medios de pago, existen diferencias básicas entre ellos: el antiguo monedero se concibió como un complemento a las tarjetas tradicionales, que podría ser utilizado en terminales off (sin conexión a ningún Host u ordenador remoto) y que debería ser recargado periódicamente. En cambio, el nuevo chip EMV nace con la vocación de sustituir a las propias tarjetas tradicionales de banda magnética, tanto de crédito como de débito (sustitución que no se producirá en un primer momento, pero sí a largo plazo).

Por tanto, y resumiendo, podemos decir que la tarjeta EMV recoge toda una historia de avances tecnológicos y soluciones de diseño aplicados en las tarjetas de banda magnética y en las tarjetas monedero, que han servido para la definición y el desarrollo del estándar EMV.

0.2. OBJETIVOS

Podemos dividir los objetivos en dos grupos: objetivos del presente proyecto y objetivos del estándar EMV, en general.

En cuanto a los primeros (**objetivos del proyecto**) básicamente son dos:

- Identificar el impacto causado en las aplicaciones bancarias de las entidades financieras por la migración al estándar EMV de las tarjetas emitidas por dichas entidades.

- Proponer una serie de cambios en el esquema de base de datos y de nuevos desarrollos y adaptaciones en los procesos de la entidad para adaptarlos al nuevo estándar.

Para cumplir estos dos objetivos de forma coherente, se irán presentando los desarrollos y adaptaciones propuestos de forma conjunta con los impactos que pretenden solucionar.

Y por lo que se refiere a los **objetivos generales del propio estándar EMV**, podemos destacar los siguientes:

- Aumento de la seguridad y reducción del fraude, respecto al incurrido con las tarjetas de banda magnética, apoyándose en el uso del chip y en algoritmos de cifrado más complejos y avanzados que los usados anteriormente.

- Posibilidad de controlar de forma más minuciosa el uso de la tarjeta sin conexión, en entornos "Off Line", consiguiéndose una mayor rapidez y flexibilidad a la hora de tomar decisiones sobre el riesgo de la tarjeta conforme a la situación y operatividad del titular.

- Obtención de otros beneficios adicionales, gracias a las posibilidades que permite el chip incorporado: por ejemplo, se pueden añadir en el mismo chip otras aplicaciones, como productos de prepago, aplicaciones de fidelización, control de acceso, firma digital...

La implantación de EMV exige una adaptación total de las plataformas actuales de medios de pago (renovación de terminales, emisión de nuevas tarjetas, modificaciones a las aplicaciones de back-office). El presente proyecto se centrará en las modificaciones del back-office relacionadas con la vertiente emisora de las entidades financieras (es decir, la personalización de tarjetas y la autorización de las operaciones por ellas realizadas), sin entrar en la vertiente adquirente (tratamiento y gestión de terminales propios, con capacidad para admitir operaciones de tarjetas tanto propias como ajenas).

0.3. ESTRUCTURACIÓN

La migración a EMV de cualquier entidad emisora de tarjetas incluye un gran número de tareas a realizar, de todo tipo: modificaciones a los programas, a las bases de datos, a los procedimientos, ...

Por seguir un orden a la hora de exponer estas tareas, en qué consisten y la forma de abordarlas, se han agrupado en tres capítulos:

- Capítulo 1: **Tareas de personalización de tarjetas**

  El conjunto de tareas más numeroso e importante lo componen todas aquellas tareas relacionadas directamente con la emisión de las tarjetas EMV de los clientes.

  Este capítulo está dividido en siete secciones:

  1.1 Tareas previas

  1.2 Seguridad Off Line (criptografía asimétrica)

  1.3 Seguridad On Line (criptografía simétrica)

  1.4 Parámetros y Perfiles EMV

  1.5 Circuito de personalización

- Capítulo 2: **Adaptación del Centro Autorizador**

  En cuanto a la adaptación del Centro Autorizador, éste deberá ser capaz de autorizar transacciones EMV en base a nuevos criterios. De esta forma, una transacción EMV quedará autorizada sólo en el caso de que se hayan validado satisfactoriamente, además de los parámetros actualmente utilizados, otros nuevos relativos a EMV: criptogramas de aplicación y parámetros de autorización EMV. Además, este centro deberá tener la capacidad de actuar, en el transcurso de una operación EMV, sobre el funcionamiento presente y futuro de la tarjeta: envío de scripts.

  Este capítulo está dividido en tres secciones:

  2.1 Autorización de transacciones EMV

  2.2 Criptogramas

2.3 Generación y gestión de scripts

- Capítulo 3: **Adaptación de interfases**

  Los emisores que deseen soportar transacciones financieras EMV se encontrarán en la necesidad de adaptar sus interfases Host-Host para incluir, tanto en los mensajes de autorización como en los de presentación, los datos de chip. En este capítulo se aborda la adaptación de estos interfases.

  Este capítulo está dividido en dos secciones:

  3.1 Adaptación interfases On Line

  3.2 Adaptación interfases batch

Como ya se indicó en el apartado de objetivos, la exposición de las tareas a realizar incluirá, para cada tarea, la explicación del impacto seguida de la descripción de los nuevos desarrollos, adaptaciones a procesos ya existentes y cambios en el esquema de base de datos de la entidad.

0.4. AUDIENCIA

Este proyecto puede interesar a diversos tipos de audiencia, y por diferentes motivos:

- Responsables de Departamentos de Medios de Pago de las entidades financieras: dispondrán de una guía con todos los temas a tener en cuenta en la migración de las tarjetas de sus entidades a EMV. También les servirá para tener una primera aproximación de tiempos y recursos que se deberán destinar a ese fin.

- Directores de Informática: les ayudará a hacerse una idea de los recursos necesarios y del tiempo estimado, de forma que puedan integrar la planificación de la migración a EMV dentro de la planificación general de todos los proyectos a acometer por las entidades cuya informática dirigen.

- Proveedores de soluciones para entidades financieras: pueden descubrir nuevos campos para los que concebir, diseñar, desarrollar y lanzar al mercado nuevos productos susceptibles de ser utilizados como apoyo por las entidades financieras en el proceso de migración.

- Y por último, técnicos informáticos especializados en medios de pago: pueden identificar temas en los que formarse de cara a la futura demanda de profesionales con conocimientos en este área.

1. TAREAS DE PERSONALIZACIÓN DE TARJETAS

Estas tareas son decisivas, porque el funcionamiento futuro de la tarjeta quedará seriamente condicionado por las decisiones que se tomen en el momento de personalizarla.

La emisión de tarjetas chip, requisito impuesto por el estándar EMV, impondrá la necesidad de amoldar los actuales procedimientos de personalización de tarjetas de banda a las nuevas tarjetas inteligentes. Así, se hará necesario introducir un nuevo mecanismo para la personalización del chip, además del mecanismo de personalización de las bandas.

Las entidades emisoras de tarjetas EMV deberán ser capaces de gestionar de forma eficaz todo un nuevo conjunto de datos (los datos EMV), además de incorporar las novedades que aparecerán en el circuito de personalización: software de personalización para las aplicaciones EMV, obtención de datos relativos a la criptografía asimétrica EMV,...

Además de los datos relativos al usuario, el emisor deberá gestionar, durante el proceso de personalización, datos relativos a la seguridad y al funcionamiento interno de la tarjeta.

A continuación se detallan una serie de puntos a tener en cuenta a la hora de adaptar los procesos implicados en la personalización de tarjetas a las nuevas necesidades del estándar EMV.

1.1. TAREAS PREVIAS

Estas tareas previas no implican modificaciones a la aplicación de la entidad, pero son muy importantes porque de su resultado dependerá cuál sea el comportamiento de las tarjetas que emita la entidad, y también el impacto en la aplicación en cuanto a desarrollos necesarios, y coste de los mismos.

1.1.1. Elección proveedor de tarjetas EMV

Este punto no implica modificaciones al software, pero es de gran importancia para cualquier entidad emisora de tarjetas. Se trata de elegir el proveedor de la entidad entre los distintos fabricantes de tarjetas EMV (Microelectrónica, FNMT, Gemalto, GyD, etcétera).

Hay que tener bien claro que estos fabricantes han de estar homologados tanto por MasterCard como por VISA Internacional, independientemente de bajo qué marca quiera la entidad emitir sus tarjetas.

Las tarjetas adquiridas a estos proveedores vienen con el plástico en blanco y el chip ya inserto en el mismo, y con el sistema operativo cargado en el chip.

Ahora bien, en este chip los parámetros EMV estarán sin personalizar, la tarjeta no incorporará en ningún caso datos específicos de los titulares.

Tampoco incorporará ninguna clave o certificado pre-cargado.

1.1.2. Elección / Desarrollo circuito de personalización

Este punto sí puede implicar modificaciones al software de la entidad, en función del circuito que se decida utilizar para obtener el Fichero de Personalización EMV.

Existen tres opciones diferentes a la hora de elegir este circuito, que dan lugar a diferentes cargas de trabajo para la entidad:

1. Asumir globalmente la personalización: es la más costosa en cuanto a desarrollos a realizar, ya que obliga no sólo a generar los datos del titular de la tarjeta y del perfil de la misma, sino también a hacer diferentes tratamientos de las claves: generación claves asimétricas (RSA), envío a MasterCard, importación de certificados, generación de firmas, generación claves simétricas (maestra, DAC, ...), proteger el fichero de personalización, simétricas y asimétricas), etcétera...

2. Utilizar los servicios de un centro de intercambio (CECA, Sermepa): puede hacerse de dos maneras, delegando cualquier tratamiento EMV en ese centro de intercambio (la opción que menos impacto tiene en el emisor, pero la más costosa

económicamente y la que provoca una mayor dependencia del exterior) o seguir generando el fichero de personalización con los datos del titular, como en las tarjetas de banda, y enviarlo a CECA o Sermepa para que éstos añadan los datos específicos EMV y devuelvan los ficheros así completados al emisor, que los enviará al personalizador que desee. Esta opción implica algunos desarrollos en el emisor pero le da un mayor control sobre sus tarjetas.

3. Optar por soluciones privadas: en este caso también hay dos opciones, como en el punto anterior, según la solución privada sea total o parcial.

El circuito elegido en el caso planteado en este proyecto se ajusta a esta última opción: utilización de una solución privada, en concreto una herramienta de personalización EMV (tipo H3P de Realsec).

En este caso, la entidad emisora definirá, tanto en la herramienta externa como en la aplicación Host, los perfiles EMV que desee para sus tarjetas.

Desde la aplicación se podrán enviar a la herramienta de personalización tanto la identificación del perfil al que va a pertenecer la tarjeta, como la asignación de valores específicos de ciertos datos para una tarjeta concreta.

A continuación, y con la periodicidad que desee, la entidad proporcionará a esta herramienta el mismo fichero que genera actualmente con los datos de las tarjetas de banda, más la identificación del perfil, más (opcionalmente) los valores de los datos EMV que se desee.

La herramienta generará entonces, a partir de este fichero y la definición de los perfiles, el fichero final con todos los datos necesarios para la fabricación de las tarjetas EMV definitivas: datos de banda y datos del chip.

1.1.3. Elección del estampador definitivo

La entidad deberá decidir a qué empresa estampadora envía el fichero generado en el punto anterior. No tiene por qué ser la misma que fabricó los plásticos originales, ni tampoco tiene por qué ser la misma que generó el fichero de personalización.

El envío puede realizarse directamente a los estampadores o realizarse a través de las entidades de intercambio (CECA y Sermepa).

1.2. SEGURIDAD OFFLINE (CRIPTOGRAFÍA ASIMÉTRICA)

El estándar EMV presenta, como una de las principales novedades, la posibilidad de garantizar la seguridad en transacciones llevadas a cabo en entorno Off Line. Dicha garantía se logra merced a la utilización de criptografía asimétrica o de clave pública.

En la criptografía simétrica, la usada habitualmente en el mundo de los medios de pago (por ejemplo en todo lo relacionado con el PIN de la tarjeta), la clave utilizada para cifrar es la misma que para descifrar, y es conocida tanto por el origen de los datos como por el destino. Por tanto, la seguridad del sistema se basa en la seguridad de la clave.

En cambio, en la criptografía asimétrica, no es necesario que el origen y el destino de los datos cifrados compartan la misma clave, sino que se trabaja con pares de claves (privada y pública), relacionadas matemáticamente. La clave privada sólo es conocida por una de las partes, mientras que la clave pública puede ser distribuida por el poseedor de la clave privada, con total libertad, a todas aquellas entidades con las que quiera intercambiar información.

En función de cuál de las dos claves se utilice para cifrar, se estarán garantizando objetivos de seguridad diferentes:

- *Autenticación*: el remitente distribuye su clave pública entre los posibles destinatarios de los datos a enviar. Como sólo el remitente conoce la clave privada necesaria para cifrarlos, el destinatario se asegura que los datos recibidos (y que él puede descifrar gracias a la clave pública) han sido efectivamente enviados por el remitente.

- *Confidencialidad* (o privacidad): el destinatario de los datos cifrados distribuye su clave pública entre los posibles remitentes para que estos cifren los datos a enviar. Sólo el destinatario, con su clave privada, podrá descifrarlos y conocerlos.

En el mundo EMV, la distribución de claves públicas y privadas no se realiza de forma libre entre las entidades, sino mediante certificados, distribuidos por los sistemas de pago (MasterCard y VISA), que se han establecido como autoridades de certificación.

Un certificado es un documento firmado digitalmente por una Autoridad de Confianza (o Autoridad de Certificación, por brevedad generalmente se la denominará “AC”, o en plural, “AACC”), que garantiza la relación entre una clave y su propietario. Un certificado contiene:

- Nombre del Titular a quien se le emite el certificado

- Nombre del emisor del certificado

- Número de serie del certificado

- Clave pública asociada al titular del certificado

- Período de validez

- Firma digital de la Autoridad de Confianza (generada con la clave privada de la autoridad, cualquiera puede descifrarla utilizando la clave pública; sirve para confirmar que el certificado lo generó realmente la Autoridad de Confianza).

Los emisores de tarjetas EMV (al igual que los adquirentes de operaciones, propietarios de los terminales EMV) deben enviar sus claves públicas a las AACC (autoridades de certificación: VISA Internacional y MasterCard), para que éstas las certifiquen y les devuelvan los certificados, junto con la claves públicas de las AACC. Esos certificados serán incluidos en las tarjetas EMV (o en los terminales EMV), junto con las claves privadas de las entidades emisoras (o adquirentes) y las claves públicas de las AACC.

Esto permite que la tarjeta y el terminal puedan autenticarse mutuamente, sin intervención de ningún Host. Para ello, ambos intervinientes (tarjeta y terminal) se intercambian los certificados, y al estar ambos en posesión de las claves públicas de las AACC, son capaces de comprobar que el certificado recibido del otro interviniente es correcto y ha sido generado por las AACC: básicamente, en esto consiste la autenticación, en comprobar que el otro interviniente es quien dice ser, y no se trata de una tarjeta o terminal duplicado o alterado.

Centrándonos de nuevo en las entidades emisoras de tarjetas, hay que resaltar que el uso de este tipo de criptografía les obligará a adaptarse a un escenario completamente nuevo. En este apartado se indicarán cuáles serán las adaptaciones a realizar en el Host Emisor para soportar todo aquello que el estándar EMV requiere en cuanto a este tipo de criptografía.

Como se ha visto, los datos necesarios para este tipo de autenticación Off Line (claves y certificados), son generados en parte por los Sistemas de Pago Internacionales (VISA y MasterCard) y en parte por el propio Emisor.

Los emisores EMV deben generar su par de claves RSA y solicitar a las AACC que, por un lado, le certifiquen la parte pública de la clave, y por otro le comuniquen las propias Claves Públicas de las AACC.

Existen varios tipos de autenticación Off Line: estática (SDA), dinámica (DDA) y combinada (CDA). Sea cual sea el tipo de autenticación elegida, el emisor necesitará generar un par de claves RSA únicas por tarjeta y además, certificarlas.

A continuación se describen las tareas a realizar por la entidad para cubrir el requerimiento EMV de autenticación Off Line.

1.2.1. Importación de las Claves Públicas RSA de los Sistemas de Pago Internacionales

1.2.1.1. Tareas a realizar

La primera tarea a realizar por el Emisor es importar las claves públicas recibidas de las autoridades de certificación (los Sistemas de Pago Internacionales, VISA y MasterCard).

Tanto en el caso de MasterCard como en el de VISA Internacional, el proceso de importación constará de los siguientes pasos:

1. Petición de las Claves Públicas: los Sistemas de Pago Internacionales comunicarán a sus miembros el valor de sus claves públicas, sólo tras recibir de éstos la petición correspondiente.

   En el caso de VISA, esta petición se encontrará implícita en la solicitud de certificación de una clave pública de Emisor.

2. Recepción de las Claves Públicas: los Sistemas de Pago Internacionales utilizan métodos diferentes para comunicar sus claves públicas (MasterCard envía sus claves públicas mediante un procedimiento independiente, VISA las comunica junto con los certificados que expide). A continuación se exponen ambos.

   a. MasterCard

      MasterCard envía por e-mail, a dos custodios de claves (o inspectores de seguridad) de la entidad, dos ficheros: uno conteniendo la propia clave pública de MasterCard autocertificada y otro con un HashCode de dicha clave. El HashCode consiste en un checksum de la clave.

      Los dos ficheros son enviados a ambos custodios, de forma que puedan cotejar que no han sido manipulados.

      Los custodios elegidos por la entidad deben previamente haberse registrado como inspectores de seguridad en MasterCard, de forma presencial. En ese

momento comunicarán además cuales son las direcciones de correo electrónico a las que MasterCard enviará los ficheros.

b. VISA Internacional

En el caso de VISA, no comunica su clave pública mediante un procedimiento específico, sino que lo hace cada vez que un Emisor le solicita la certificación de una de sus claves públicas. En ese caso, no sólo le envía el certificado correspondiente sino, además, la clave pública de VISA cuya parte privada se ha utilizado para calcular dicha certificación.

A diferencia de MasterCard, VISA solo registra a un custodio como representante de la entidad, el denominado Agente Autorizado. Este agente es el encargado de intercambiar la información (claves y certificados) con VISA, garantizando su seguridad.

Ambos sistemas de pago envían sus claves públicas en claro, pero autocertificadas, para proteger su integridad. Esto es, junto con la clave pública de la AC, los sistemas de pago adjuntan un certificado firmado digitalmente con la clave privada de la AC.

3. Verificación de las Claves Públicas: una vez recibidas las claves públicas de los sistemas internacionales, es necesario que la entidad verifique que no han sido manipuladas durante el envío. Para ello, se debe verificar el autocertificado que acompaña a las claves públicas tanto de MasterCard como de VISA.

4. Almacenamiento de las Claves Públicas y Datos Relacionados: sólo en el caso de que la fase de verificación haya resultado satisfactoria, el Emisor aceptará y en consecuencia almacenará, la clave recibida y los datos correspondientes.

El procedimiento a seguir en cada uno de estos pasos está descrito en los documentos:

- "*Registration Authority Document Set*", en el caso de MasterCard
- "*Visa Certificate Authority – User´s Guide*", en el caso de VISA

En cuanto a las características de estas claves, el estándar EMV establece cuáles son las longitudes con las que se debe trabajar y cuál su vigencia:

Longitud	**Exponente**	**Fecha de Caducidad**

896 bits	3	31 Diciembre 2004
1024 bits	3	31 Diciembre 2007
1152 bits	3	31 Diciembre 2010

Longitud y vigencia de claves RSA

1.2.1.2. Desarrollos y adaptaciones propuestos

* Procesos batch de *recepción de la Clave Pública de MasterCard*

Se deberán desarrollar dos procesos, uno para leer y almacenar la Clave Pública de MasterCard autocertificada, y otro para el HashCode. Los datos recibidos tienen la siguiente estructura:

Fichero con la Clave Pública autocertificada:

Nombre del dato	Longitud	Descripción
ID de MasterCard	5	RID de Europay
Índice de la Clave Pública de MC	1	Identificador de esta clave
Indicador del algoritmo de la Clave Pública de MC	1	Indica el algoritmo a utilizar con la Clave Pública de MC. Su valor está fijado a '01' (hex)
Longitud de la Clave Pública de MC	1	Longitud del módulo de la Clave Pública de MC en bytes (N_{CA})
Longitud del exponente de la Clave Pública de MC	1	Longitud del exponente de la Clave Pública de MC en bytes (igual a 1)
Dígitos más significativos de la Clave Pública de MC	N_{CA}-37	Este campo contiene los (N_{CA}-37) bytes más significativos del módulo de la Clave Pública de MC
Resto de la Clave Pública de MC	37	37 bytes menos significativos del módulo de la Clave Pública de MC

MC		módulo de la Clave Pública de MC
Exponente de la Clave Pública de MC	1	Su valor será 3 ó $2^{16}+1$
Certificado de la Clave Pública de MC	N_{CA}	Resultado de la Firma Digital

Tabla 1

Formato de Transferencia de Clave Pública de Mastercard autocertificada y Datos Asociados

Fichero con el Hashcode:

Nombre del dato	Longitud	Descripción
ID de MasterCard	5	RID de Europay
Índice de la Clave Pública de MC	1	Identificador de esta clave
Indicador del algoritmo de la Clave Pública de MC	1	Indica el algoritmo a utilizar con la Clave Pública de MC. Su valor está fijado a '01' (hex)
Check Sum de la Clave Pública de MC	20	Hash-Code

Tabla 2

Formato de Transferencia del Hash-Code de la Clave Pública de Mastercard autocertificada y Datos Asociados

* Proceso batch de *recepción de la Clave Pública de VISA*

Se desarrollará un único proceso, que lea y almacene la clave pública de VISA autocertificada. Los datos recibidos tienen la siguiente estructura:

Nombre del dato	Longitud	Descripción

Cabecera	1	Valor ‘20’ (hex)
Identificador Servicio	4	Identifica el servicio de VISA. Valores permitidos (hex): 1010 = Credit/Debit 2010 = Electron 3010 = Interlink 8010 = PLUS 999910 = Propietary ATM El valor elegido se rellena con ‘00’ hex por la izquierda hasta completar los 4 bytes de longitud del campo
Longitud de la Clave Pública de VISA Int.	2	Longitud del módulo de la Clave Pública de VISA en bytes (N_{CA})
Indicador del algoritmo de la Clave Pública de VISA Int.	1	Indica el algoritmo a utilizar con la Clave Pública de VISA. Su valor está fijado a ‘01’ (hex)
Longitud del exponente de la Clave Pública de VISA Int.	1	Longitud del exponente de la Clave Pública de VISA en bytes
ID de VISA	5	RID de VISA
Índice de la Clave Pública de VISA	1	Identificador de esta clave

Módulo de la Clave Pública de VISA	N_{CA}	Módulo de la Clave Pública en claro
Exponente de la Clave Pública de VISA	Var	Su valor será 3 ó $2^{16}+1$
Resultado Hash	20	Resultado de aplicar la función hash a datos relativos a la Clave Pública de VISA
Certificado de la Clave Pública de VISA	N_{CA}	Resultado de la Firma Digital

Tabla 3

Formato de Transferencia de Clave Pública de VISA Internacional autocertificada y Datos Asociados

* Proceso batch de *verificación de la Clave Pública de MasterCard*

Consta de los siguientes subprocesos:

- Verificación de la validez de algunos de los campos recibidos en la Clave Pública autocertificada de MasterCard (***tabla 1, "Formato de Transferencia de Clave Pública de Mastercard autocertificada y Datos Asociados"***):

  - El valor del campo "ID de MasterCard" debe coincidir con el esperado de MasterCard

  - El valor del campo "Índice de la Clave Pública de MC" debe ser diferente del recibido en ocasiones precedentes

  - El valor del campo "Indicador del algoritmo de la Clave Pública de MC" debe ser '01' hex

  - La "Longitud de la Clave Pública de MC" debe encontrarse dentro de las longitudes de clave pública aceptadas por MasterCard

  - La "Longitud del exponente de la Clave Pública de MC" debe ser '01' hex

- Recuperación de la Clave Pública de MasterCard. Se recuperan tanto el Módulo como el Exponente:

  - El Módulo es la concatenación de los campos "Dígitos más significativos de la Clave Pública de MC" y "Resto de la Clave Pública de MC" (***tabla 1***). Longitud total del Módulo: N_{CA} bytes

  - El exponente está contenido en el campo "Exponente de la Clave Pública de MC". Se verificará que se encuentra dentro de los exponentes de clave pública aceptados por MasterCard

- Verificación del Certificado Autofirmado de la Clave Pública de MasterCard. Se compone de varios pasos:

  - Aplicar el algoritmo indicado en el campo "Indicador del algoritmo de la Clave Pública de MC" al certificado recibido en el campo "Certificado de la Clave Pública de MC" (último campo de la ***tabla 1***), usando la clave pública recuperada en el punto anterior, para de esta forma recuperar a su vez los datos utilizados para la generación del certificado. Los datos recuperados son:

Nombre del dato	Longitud	Descripción
Cabecera de los Datos Recuperados	1	'6A' hex
Formato del Certificado	1	'10' hex
ID de MasterCard	5	RID de Europay
Fecha de expiración del Certificado	2	Mes/año, en formato MMAA a partir del cual el certificado se invalida
Número de Serie del Certificado	3	Valor de 3 bytes, establecido por MC. Comúnmente denominado "Tracking Number"
Indicador del algoritmo hash	1	Indica el algoritmo hash utilizado para calcular el certificado

		certificado
Indicador del algoritmo de la Clave Pública de MC	1	Indica el algoritmo a utilizar con la Clave Pública de MC. Su valor está fijado a '01' (hex)
Longitud de la Clave Pública de MC	1	Longitud del módulo de la Clave Pública de MC en bytes (N_{CA})
Longitud del exponente de la Clave Pública de MC	1	Longitud del exponente de la Clave Pública de MC en bytes (igual a 1)
Dígitos más significativos de la Clave Pública de MC	N_{CA}-37	Este campo contiene los (N_{CA}-37) bytes más significativos del módulo de la Clave Pública de MC
Resultado del hash	20	Hash de la Clave Pública de MC y sus datos asociados
Cola de los Datos Recuperados	1	'BC' hex

Tabla 4

Formato de los datos recuperados del certificado de la Clave Pública de MasterCard autocertificada

- Verificar que la "Cabecera de los Datos Recuperados" es igual a '6A' hex y el "Formato del Certificado" igual a '10' hex

- Verificar el campo "Resultado del hash".

  La manera de hacerlo es volver a calcular el hash (o huella digital):

  - Algoritmo utilizado para calcular el hash: según la normativa EMV contenida en "*Book2 – EMV2000 specifications*", (dirección de internet [EMVCO]), el

algoritmo hash utilizado será el SHA-1 cuyo identificador será '01' hex.

- Datos sobre los que aplicar el hash: se aplicará sobre los (N_{CA}+16) bytes resultado de concatenar todos los datos recuperados del certificado (***tabla 4, "Formato de los datos recuperados del certificado de la Clave Pública de MasterCard autocertificada"***) salvo la cabecera, la cola y el propio resultado del hash, más el Resto y el Exponente de la Clave Pública de MasterCard (***tabla 1, "Formato de Transferencia de Clave Pública de Mastercard autocertificada y Datos Asociados"***).

A continuación, se comprueba si el resultado así calculado coincide con el recuperado del certificado (campo "Resultado del hash" de la ***tabla 4, "Formato de los datos recuperados del certificado de la Clave Pública de MasterCard autocertificada"***).

- Verificación de la validez de algunos de los campos recuperados del certificado autofirmado de MasterCard (***tabla 4, "Formato de los datos recuperados del certificado de la Clave Pública de MasterCard autocertificada"***):

  - El "ID de MasterCard" recuperado del certificado debe coincidir con el recibido en la Clave Pública Autocertificada de MasterCard (***tabla 1***), en caso contrario, se debe rechazar la clave pública.

  - La "Fecha de expiración del Certificado" debe ser mayor que la actual. En caso contrario, el certificado autofirmado recibido está caducado y la clave pública debe ser rechazada.

  - El campo "Indicador del algoritmo de la Clave Pública de MasterCard" debe ser igual a '01' hex. En caso contrario, se debe rechazar la clave pública.

  - Los tres campos siguientes (8º, 9º y 10º de la ***tabla 4***, longitud del módulo, longitud del exponente y dígitos más significativos de la Clave Pública de MasterCard) deben coincidir con los campos recibidos junto con la Clave Pública autocertificada de MasterCard (campos 4º, 5º y 6º de la ***tabla 1***).

* Proceso batch de *verificación de la Clave Pública de VISA Internacional*

Consta de los siguientes subprocesos:

- Verificación de la validez de algunos de los campos recibidos en la Clave Pública autocertificada de VISA (***tabla 3, "Formato de Transferencia de Clave Pública de VISA Internacional autocertificada y Datos Asociados"***):

  - El valor del campo "ID de VISA" debe coincidir con el esperado de VISA Internacional

  - El valor del campo "Índice de la Clave Pública de VISA" debe ser diferente del recibido en ocasiones precedentes

  - El valor del campo "Indicador del algoritmo de la Clave Pública de VISA Int." debe ser '01' hex

  - La "Longitud de la Clave Pública de VISA Int." debe encontrarse dentro de las longitudes de clave pública aceptadas por VISA Internacional

  - La "Longitud del exponente de la Clave Pública de VISA Int." debe ser '01' hex

- Recuperación de la Clave Pública de VISA Internacional. Se recuperan tanto el Módulo como el Exponente:

  - El Módulo se encuentra en claro en el campo "Módulo de la Clave Público de VISA" (8º campo de la ***tabla 3***).

    Longitud del Módulo: N_{CA} bytes

  - El exponente está contenido en el campo "Exponente de la Clave Pública de VISA". Se verificará que se encuentra dentro de los exponentes de clave pública aceptados por VISA Internacional

- Verificación del Certificado Autofirmado de la Clave Pública de VISA Internacional. Se compone de varios pasos:

  - Aplicar el algoritmo indicado en el campo "Indicador del algoritmo de la Clave Pública de VISA Int." al certificado recibido en el campo "Certificado de la Clave Pública de VISA" (***tabla 3***), usando la clave pública recuperada en el punto anterior,

para de esta forma recuperar a su vez los datos utilizados para la generación del certificado. Los datos recuperados son:

Nombre del dato	Longitud	Descripción
Cabecera de los datos recuperados	1	'21' hex
Identificador del Servicio	4	Identifica el servicio de VISA. Valores permitidos (hex): 1010 = Credit/Debit 2010 = Electron 3010 = Interlink 8010 = PLUS 999910 = Propietary ATM El valor elegido se rellena con '00' hex por la izquierda hasta completar los 4 bytes de longitud del campo
ID de VISA Internacional	5	RID de VISA
Índice de la Clave Pública de VISA	1	Identifica de forma única la clave de VISA en cuestión

Fecha de expiración del Certificado	2	Mes/año, en formato MMAA a partir del cual el certificado se invalida
Indicador del algoritmo de la Clave Pública de VISA	1	Indica el algoritmo a utilizar con la Clave Pública de VISA. Su valor está fijado a '01' (hex)
Dígitos más significativos de la Clave Pública de VISA	Var	Este campo contiene los (N_{CA}-[36+e]) bytes más significativos del módulo de la Clave Pública de VISA, siendo 'e' la longitud del exponente de la Clave Pública de VISA
Indicador del algoritmo hash	1	Indica el algoritmo hash utilizado para calcular el certificado
Longitud del exponente de la Clave Pública de VISA	1	Longitud del exponente de la Clave Pública de VISA en bytes
Exponente de la Clave Pública de VISA	Var	Su valor será 3 ó 2^{16}+1
Resultado del hash	20	Hash de la Clave Pública de VISA y sus datos asociados

Tabla 5

Formato de los datos recuperados del certificado de la Clave Pública de VISA Internacional autocertificada

- Verificar el campo "Resultado del hash".

  La manera de hacerlo es volver a calcular el hash (o huella digital):

- Algoritmo utilizado para calcular el hash: según la normativa EMV contenida en "*Book2 – EMV2000 specifications*", (dirección de internet [EMVCO]), el algoritmo hash utilizado será el SHA-1 cuyo identificador será '01' hex.

- Datos sobre los que aplicar el hash: se aplicará sobre la cadena resultado de concatenar los datos 6º al 9º (ambos inclusive) recibidos en claro de VISA (***tabla 3, "Formato de Transferencia de Clave Pública de VISA Internacional autocertificada y Datos Asociados"***).

A continuación, se comprueba si el resultado así calculado coincide con el recuperado del certificado (campo "Resultado del hash" de la ***tabla 5, "Formato de los datos recuperados del certificado de la Clave Pública de VISA Internacional autocertificada"***)

* Proceso batch de *verificación del Hash-Code recibido de MasterCard*

Antes de dar por buena la clave recibida y proceder a almacenarla en nuestro sistema, hay que verificar el hash-code enviado por MasterCard junto con su clave pública autocertificada.

La manera de verificarlo es volverlo a calcular, teniendo en cuenta lo siguiente:

- El algoritmo utilizado para calcular el hash-code, según la normativa EMV contenida en "*Book2 – EMV2000 specifications*", (dirección de internet [EMVCO]), será el SHA-1 cuyo identificador será '01' hex.

- El dato sobre el que se aplicará el algoritmo es el resultado de concatenar algunos de los datos recibidos de MasterCard como parte del Formato de transferencia de su clave pública (***tabla 1***), en concreto los siguientes:

Nombre del dato	Longitud	Descripción
ID de MasterCard	5	RID de Europay
Índice de la Clave Pública de MasterCard	1	Identificador de esta clave

Pública de MasterCard		
Dígitos más significativos de la Clave Pública de MasterCard	N_{CA}-37	Este campo contiene los (N_{CA}-37) bytes más significativos del módulo de la Clave Pública de MasterCard
Resto de la Clave Pública de MasterCard	37	37 bytes menos significativos del módulo de la Clave Pública de MasterCard
Exponente de la Clave Pública de MasterCard	1	Su valor será 3

Tabla 6

Datos para el cálculo del Hash-Code de la Clave Pública de MasterCard

Este Hash Code así calculado debe coincidir con el recibido de MasterCard (campo "Check Sum de la Clave Pública de MasterCard" de la ***tabla 2***, ***"Formato de Transferencia del Hash-Code de la Clave Pública de Mastercard autocertificada y Datos Asociados"***).

* Proceso batch de *verificación del Hash-Code recibido de VISA Internacional*

Visa Internacional no envía un hash-Code de forma independiente a la clave pública autocertificada, como hace MasterCard. Lo que hace es publicarlo en su documentación o en su página web.

VISA envía a la un único hash-code, incluido dentro de los datos asociados al certificado (campo "Resultado Hash" de la ***tabla 3***, "***Formato de Transferencia de Clave Pública de VISA Internacional autocertificada y Datos Asociados***").

Este dato ya se verificó en uno de los subprocesos del proceso batch de *verificación de la Clave Pública de VISA Internacional*, por tanto el valor calculado allí se puede utilizar directamente, sin volverlo a calcular, para compararlo con el que VISA tiene publicado en su documentación y en su página web.

* Proceso batch de *Almacenamiento de las Claves Públicas y Datos Relacionados*

En el caso de que la verificación de los certificados recibidos haya resultado satisfactoria, el Emisor aceptará y en consecuencia almacenará, la clave recibida y los datos correspondientes.

El almacenamiento puede realizarse en el mismo proceso de verificación, o hacerse de forma independiente. En este caso hemos decidido hacerlo de forma independiente.

El almacenamiento tiene dos facetas:

- Importación de las claves y certificados desde el Módulo Criptográfico de la entidad (también denominado en ocasiones HSM, iniciales de "Host Security Module"), para que puedan ser utilizados posteriormente por los procesos que lo precisen,

- Almacenamiento de la clave pública en un fichero con la siguiente descripción:

Nombre del dato	Long.	Descripción
ID de MasterCard/VISA	5	RID de Europay/VISA
Índice de la Clave Pública de MasterCard/VISA	1	Identificador de esta clave
Fecha de caducidad del certificado	2	AAMM tras el cual el certificado no es válido
Número de serie del certificado	3	Valor de 3 bytes elegidos por MasterCard/VISA
Longitud de la Clave Pública de MasterCard/VISA	Var	Longitud del módulo de la Clave Pública de MasterCard/VISA en bytes (N_{CA})
Longitud del exponente de la Clave Pública de MasterCard/VISA	1	Longitud del exponente de la Clave Pública de MasterCard/VISA en bytes

Dígitos más significativos de la Clave Pública de MasterCard/VISA	Var	Este campo contiene los (N_{CA}-(36+*e*)) bytes más significativos del módulo de la Clave Pública de MasterCard/VISA, siendo '*e*' la longitud del exponente de la Clave Pública de MasterCard/VISA
Resto de la Clave Pública de MasterCard/VISA	Var	(36+*e*) bytes menos significativos del módulo de la Clave Pública de MasterCard/VISA
Exponente de la Clave Pública de MasterCard/VISA	Var	Su valor será 3 ó 2^{16}+1

Tabla 7

Clave Pública de Mastercard/VISA Internacional y Datos Asociados a almacenar

1.2.2. Generación de Claves RSA

1.2.2.1. Tareas a realizar

Los emisores deberán llevar a cabo el proceso de Generación de sus Claves RSA que, dependiendo de la complejidad de la autenticación Off Line elegida para sus tarjetas (SDA, DDA o CDA), les exigirá la generación de hasta tres tipos de claves RSA: de Emisor, de Tarjeta y para Cifrado de PIN.

1. Claves RSA de Emisor.

   Sea cual sea el tipo de autenticación Off Line elegida, los emisores siempre deberán generar al menos una pareja de claves RSA, las Claves RSA de Emisor.

   El número total de claves de este tipo utilizadas por el Emisor queda a su elección. Una misma entidad podrá contar con Claves RSA de Emisor de distinta longitud, o disponer de varias con el mismo tamaño.

   La longitud de las claves estará determinada por las vigencias indicadas en la tabla "*Longitud y vigencia de claves RSA*", mostrada en el anterior apartado, "*Importación de las Claves Públicas RSA de los Sistemas de Pago Internacionales*".

2. Claves RSA de Tarjeta

   Las entidades que emitan tarjetas cuya Autenticación Off Line sea dinámica (tarjetas DDA o CDA) deberán generar un par de claves RSA por tarjeta.

   Esto se puede hacer en la aplicación Host o, más comúnmente, existe la posibilidad de que sea la propia tarjeta la que las genere internamente (bien al ser personalizada, bien en tiempo de ejecución).

   La longitud y vigencia asociadas a este tipo de claves estarán condicionadas por las correspondientes a las de las Claves RSA de Emisor.

3. Claves RSA para Cifrado de PIN

   En una transacción EMV, existe la posibilidad de que el terminal presente el PIN Off Line cifrado a la tarjeta. Dicho cifrado, según normas EMV, debe obtenerse utilizando el algoritmo RSA. Debido a esto, para soportar esta funcionalidad y ser capaz de verificar este PIN, la tarjeta debe llevar almacenadas tanto la parte pública como la privada de la clave RSA a utilizar.

   A la hora de operar, el mecanismo sería el siguiente:

   1. La tarjeta envía al terminal la parte pública de su clave, convenientemente certificadas.

   2. El terminal, una vez comprobada la validez del certificado, extrae dicha clave.

   3. El terminal solicita el tecleo del PIN al titular de la tarjeta, lo cifra Clave Pública de Cifrado de PIN de la tarjeta, y se lo envía a la tarjeta

   4. La tarjeta recupera el PIN tecleado, descifrando con su Clave Privada el dato enviado por el terminal

   De esta forma, el PIN permanece en claro el mínimo tiempo posible, para evitar fraudes.

   El estándar EMV ofrece dos opciones a la hora de elegir con qué claves llevar a cabo el cifrado del PIN Off Line:

   - Utilizar para el cifrado del PIN Off Line las mismas Claves RSA de Tarjeta que se utilizan en el proceso de Autenticación Dinámica de la Tarjeta.

- Generar un par de Claves RSA Específicas para el Cifrado del PIN, únicas por tarjeta. Al igual que en el resto de claves RSA, su longitud y vigencia estarán condicionadas por las correspondientes a las de las Claves RSA de Emisor.

1.2.2.2. Desarrollos y adaptaciones propuestos

Se considerará que, aunque la entidad utilizará la autenticación dinámica, dejará que la generación de Claves RSA de Tarjeta se realice en la fase de personalización de las tarjetas. Además, se usarán las mismas claves para el cifrado del PIN Off Line.

Teniendo en cuenta ambas cosas, sólo será necesario generar las Claves RSA de Emisor.

* Proceso batch de *generación y almacenamiento de las Claves RSA de Emisor*

  Aunque el par de claves RSA (privada y pública) son generadas por el Módulo Criptográfico, será necesario almacenar algunos datos, asociados a la parte pública de la clave, en una tabla accesible desde la aplicación Host. El registro que se inserta en esta tabla en este momento (al generar la clave) se completará posteriormente con los datos que se extraigan del certificado de respuesta de MasterCard/VISA.

  La identificación de la clave pública será una etiqueta, única para cada clave, que incluirá:

  - Entorno de uso de la clave (en este caso será siempre "EMV", pero podría utilizarse para otros entornos como tarjetas monedero o cualquiera para el que la entidad necesite generar y almacenar claves públicas)
  - Producto (MasterCard o VISA Internacional)
  - Tipo de algoritmo (en éste caso, será siempre '01' hex, es decir, RSA, pero en otros entornos podrían utilizarse otros diferentes)
  - BIN de las tarjetas EMV (un mismo Emisor puede emitir tarjetas de varios BINES diferentes, y necesita una clave diferente para cada BIN)

- Índice de la Clave Pública de Emisor (este índice es el identificador único de la clave para todas las comunicaciones con MasterCard o VISA)

La definición (provisional) de la nueva tabla de Base de Datos es la siguiente:

CPEDASOC CLAVE PÚBLICA DE EMISOR - DATOS ASOCIADOS		
Clave Única**:** **Etiqueta de la Clave Pública de Emisor**		
Nombre del campo	**Longitud**	**Descripción**
Etiqueta de la Clave Pública de Emisor	3	Entorno de Uso
	Var	Producto
	3	BIN
	1	Tipo de algoritmo
	3	Índice de la Clave Publica de Emisor
Longitud del Módulo de la Clave Pública de Emisor	N_I	Longitud del Módulo de la Clave Pública de Emisor
Longitud del Exponente de la Clave Pública de Emisor	Var	Longitud del Exponente de la Clave Pública de Emisor
Exponente de la Clave Pública de Emisor	Var	Su valor será 3 ó $2^{16}+1$
Fecha de caducidad	2	Mes/año (en formato MMAA) a partir de los cuales la Clave Pública de Emisor se invalida

Esta definición provisional se hará definitiva en el apartado siguiente, "*Obtención de Certificados*", una vez se incorporen los datos asociados al certificado de la clave recibido de MasterCard o VISA Internacional.

1.2.3. Obtención de Certificados

1.2.3.1. Tareas a realizar

Una vez generados por el emisor los tres pares de claves RSA de la entidad (clave privada y clave pública de Emisor, de Tarjeta y de cifrado de PIN Off Line), el siguiente paso a realizar es certificar la parte pública de la claves (Claves Públicas RSA).

Cada tipo de clave tiene su propio procedimiento de certificación:

- Certificación de las Claves Públicas RSA de Emisor

  Las Claves Públicas RSA de Emisor deberán ser certificadas por los Sistemas Internacionales de Pago, en su calidad de AACC. Los certificados expedidos por MasterCard y Visa previa petición por parte del Emisor, deberán ser almacenados por este tras ser verificados.

  De hecho, ambos sistemas de pago establecen procedimientos pensados para asegurar que sus miembros sólo acepten aquellos certificados cuya validez haya sido comprobada. Estos procedimientos, diferentes para MasterCard y VISA Internacional, están definidos en los documentos:

  - "Registration Authority Document Set" (MasterCard)
  - "Visa Certificate Authority – User´s Guide" (VISA Internacional)

  Los procedimientos constan de los siguientes pasos (*entre paréntesis, quién debe realizarlo*):

  1) Petición del Certificado de la Clave Pública de Emisor mediante el envío de dicha clave autocertificada a las AACC (*Emisor*)

     La petición de certificados a los sistemas de pago internacionales necesitará tanto de la cumplimentación de los formularios requeridos, como del envío de la clave pública que el Emisor desea que se le certifique.

     La comunicación de la clave pública de Emisor, tanto en el caso de MasterCard como en el de Visa, deberá ser protegida en integridad.

Para ello, ambos sistemas de pago requieren que dicha clave les sea enviada autocertificada. Es decir, junto a la clave pública que se quiere certificar, la Entidad Emisora debe adjuntar la firma digital de dicha clave calculada utilizando la clave privada correspondiente.

2) Recepción y verificación del Autocertificado del Emisor (*Sistemas de Pago, en su calidad de AACC*)

   Una vez recibida tanto la petición de certificación como la clave pública a certificar, los sistemas de pago internacionales certificarán dicha clave sólo tras haber comprobado que su integridad no se ha visto comprometida durante el envío.

3) Generación y envío al Emisor del Certificado de la Clave Pública de Emisor (*Sistemas de Pago, en su calidad de AACC*)

   El certificado resultante del punto anterior será enviado a la Entidad Emisora en cuestión.

4) Recepción y verificación del Certificado de la Clave Pública de Emisor (*Emisor*)

   El certificado se recibe por diferente vía y de diferente forma, en función del Sistema de Pago que la envía:

   a. MasterCard envía un fichero de respuesta a cada uno de los Inspectores de Seguridad de la entidad que solicitaron previamente la certificación de la clave de emisor. Este fichero de respuesta, que les llega vía e-mail, deben procesarlo con una herramienta proporcionada previamente por MasterCard, obteniendo como resultado otro fichero que contiene el certificado y los datos asociados.

   b. VISA envía un diskette al Agente Autorizado VISA de la entidad, conteniendo el certificado junto con algunos datos asociados.

   Una vez recibido el certificado solicitado, el Emisor deberá comprobar la validez del mismo. Para ello, tanto VISA como MasterCard adjuntan a los certificados que expiden una firma digital.

   Esta firma, calculada por los sistemas internacionales utilizando su clave privada, tiene como objetivo el de proteger la integridad del certificado

enviado. Así, la integridad del certificado recibido será comprobada por parte del Emisor gracias a la verificación de dicha firma digital.

5) Almacenamiento del Certificado de la Clave Pública de Emisor y Datos relacionados (*Emisor*)

Sólo en el caso de que la fase anterior haya resultado satisfactoria, la Entidad Emisora aceptará el certificado recibido. Este certificado será almacenado junto con una serie de datos relacionados y necesarios para su futura gestión.

- Certificación de las Claves Públicas RSA de Tarjeta.

Las Claves Públicas RSA de Tarjeta serán certificadas por la propia Entidad Emisora. Para ello, es necesario que dicha entidad se convierta en Autoridad de Certificación, cumpliendo para ello todos los requisitos establecidos.

Los procedimientos a seguir para garantizar la validez de los certificados calculados, quedan a elección de la propia Entidad Emisora.

- Certificación de las Claves Públicas RSA para Cifrado del PIN.

Las Claves Públicas RSA para el Cifrado del PIN serán certificadas también por la Entidad Emisora. Para ello, dicha entidad deberá cumplir con todos los requisitos impuestos a una Autoridad de Certificación.

Los procedimientos a seguir para garantizar la validez de los certificados calculados, quedan a elección de la propia Entidad Emisora.

1.2.3.2. Desarrollos y adaptaciones propuestos

Partimos de la premisa, al igual que en el apartado anterior, de que la única clave a certificar será la Clave Pública RSA de Emisor.

Los procesos batch a desarrollar cubrirán dos grandes tareas:

- Exportación de la clave pública de emisor (*paso 1* del procedimiento de certificación descrito más arriba)

- Importación del certificado de clave pública de emisor (*pasos 4 y 5*)

A continuación se detallan los procesos incluidos en cada una de estas dos tareas.

En primer lugar, se repasarán los procesos que componen la tarea de **Exportación** de la Clave Pública de Emisor:

* Proceso batch de *construcción de la Clave Pública de Emisor AutoCertificada*

  Consta de los siguientes subprocesos:

  - Construcción del certificado autofirmado de la clave publica de emisor, consta de los siguientes pasos:

    1. En primer lugar se genera el número de serie del certificado (sólo para el caso de MasterCard), que debe ser un número de 3 bytes que identifique de forma única el certificado.

       En el caso de VISA Internacional, es la propia AC la que aporta el número, en el formulario "*Financial Institution Enrollment*", previa petición de la entidad emisora.

    2. A continuación se calcula el hash del certificado, de la siguiente forma:

       - Algoritmo utilizado para calcular el hash: según la normativa EMV contenida en "*Book2 – EMV2000 specifications*", (dirección de internet [EMVCO]), el algoritmo hash utilizado será el SHA-1 cuyo identificador será '01' hex.

       - El dato sobre el que se aplica el hash es el resultado de concatenar una serie de campos, distintos según el Sistema de Pago:

         Para MasterCard:

Nombre del dato	long.	Descripción
Formato del certificado	1	'11' hex
ID del certificado	4	Dependerá del tipo de certificado
Fecha de expiración del Certificado	2	Mes/año, en formato MMAA a partir del cual el certificado se invalida

		invalida
Número de serie del certificado	3	Dependerá del tipo de certificado
Indicador del algoritmo hash	1	'01' hex (algoritmo SHA-1)
Indicador del algoritmo de la Clave Pública de Emisor	1	Indica el algoritmo a utilizar con la Clave Pública de Emisor. Su valor está fijado a '01' (hex)
Longitud del módulo de la Clave Pública de Emisor	1	Longitud, en bytes, del módulo de la clave pública de emisor
Longitud del exponente de la Clave Pública de Emisor	1	Longitud, en bytes, del exponente de la clave pública de emisor
Clave Pública de Emisor o dígitos más significativos de la Clave Pública de Emisor	N_c-32 -K	Si N_S <= N_c-32-K entonces este campo contiene el módulo completo de la Clave Pública de Emisor, rellenado por la derecha con N_c-32-K-N_S bytes de valor 'BB' hex Si N_S > N_c-32-K entonces este campo contiene los N_c-32-K bytes más significativos del módulo de la Clave Pública de Emisor
Resto de la Clave Pública de Emisor	0 ó N_s-N_c +32+K	Este campo estará solo presente si N_S > N_c-32-K y, en el caso de estar presente, contendrá los N_S-N_c+32+K menos significativos del módulo de la Clave Pública de Emisor

Exponente de la Clave Pública de Emisor	1 ó 3	Su valor será 3 ó $2^{16}+1$

Tabla 9

Datos de la Clave Pública de Emisor a autofirmar para su envío a Mastercard

Para VISA Internacional:

Nombre del dato	long.	Descripción
Cabecera de los datos recuperados	1	'23' hex
Identificador del Servicio	4	Identifica el servicio de VISA. Valores permitidos (hex): 1010 = Credit/Debit 2010 = Electron 3010 = Interlink 8010 = PLUS 999910 = Propietary ATM El valor elegido se rellena con '00' hex por la izquierda hasta completar los 4 bytes de longitud del campo

Formato del certificado	1	'02' hex
Número de Identificación del Emisor	4	El BIN del Emisor, completado con 'FF' hex por la derecha
Fecha de expiración del Certificado	2	Mes/año, en formato MMAA a partir del cual el certificado se invalida
Número de serie del certificado	3	Aportado por VISA Internacional
Indicador del algoritmo hash	1	'01' hex (algoritmo SHA-1)
Indicador del algoritmo de la Clave Pública de Emisor	1	Indica el algoritmo a utilizar con la Clave Pública de Emisor. Su valor está fijado a '01' hex
Longitud del módulo de la Clave Pública de Emisor	1	Longitud, en bytes, del módulo de la Clave Pública de Emisor
Longitud del exponente de la Clave Pública de Emisor	1	Longitud, en bytes, del exponente de la Clave Pública de Emisor
Dígitos más significativos de la Clave Pública de Emisor	var	Este campo contiene los (N_I-[36+e]) bytes más significativos del módulo de la Clave Pública de Emisor (N_I), siendo 'e' la longitud del exponente de la Clave Pública de Emisor
Exponente de la Clave Pública de Emisor	var	Su valor será 3 ó 2^{16}+1

Tabla 10

Datos de la Clave Pública de Emisor a autofirmar para su envío a VISA Internacional

Los siguientes datos:

- Longitud del módulo de la Clave Pública de Emisor
- Longitud del exponente de la Clave Pública de Emisor
- Exponente de la Clave Pública de Emisor

se toman de la TABLA DE DATOS ASOCIADOS A LAS CLAVES PÚBLICAS DE EMISOR (**CPEDASOC**, ver apartado anterior: "Generación de claves RSA").

Y el dato:

- Módulo de la Clave Pública de Emisor

se recupera del Módulo Criptográfico, que es quien almacena el par de claves RSA de Emisor.

3. Una vez generado el número de certificado y calculado el hash, el último paso para calcular el certificado es calcular su Firma Digital.

   Esto se consigue mediante una llamada al Módulo Criptográfico, que es quien almacena el par de claves RSA de Emisor. En esta llamada se le pasarán al módulo los siguientes parámetros:

   - Comando a realizar: cálculo de Firma Digital
   - Algoritmo de cálculo: RSA, según indica el documento "Book2 – EMV2000 specifications" (dirección de internet [EMVCO])
   - Clave utilizada: Clave Privada de Emisor. En realidad sólo se le pasa una etiqueta, ya que la propia clave sólo la tiene el propio Módulo Criptográfico
   - Los datos a firmar son el resultado de la concatenación de una serie de campos, distintos según el Sistema de Pago:

     Para MasterCard:

- Dato fijo ‘6A’ hex

- Todos los datos enviados a MasterCard en la “Petición de Certificado” (ver ***tabla 9***, “***Datos de la Clave Pública de Emisor a autofirmar para su envío a Mastercard***”), salvo los dos últimos:

  - Resto de la Clave Pública de Emisor

  - Exponente de la Clave Pública de Emisor

- Resultado del hash, calculado en el paso 2

- Dato fijo ‘BC’ hex

Para VISA Internacional:

- Todos los datos enviados a VISA en la “Petición de Certificado” (ver ***tabla 10***, “***Datos de la Clave Pública de Emisor a autofirmar para su envío a VISA Internacional***”)

- Resultado del hash, calculado en el paso 2

- Formato de envío de la clave publica de emisor:

  Una vez que ya se tiene la clave autocertificada, sólo queda construir el formato en el que se va a enviar, que es distinto para los dos sistemas de pago.

  En cualquier caso, lo que se denomina “Clave Pública de Emisor Autocertificada” consta de:

  - Identificación del emisor

  - Datos característicos de la Clave Pública de Emisor

  - Clave Pública de Emisor en claro

  - Clave Pública de Emisor autofirmada (firma calculada en el paso 3 del subproceso anterior)

En concreto, estos datos están especificados en las siguientes tablas:

- Formato de Transferencia a MasterCard: Clave Pública de Emisor (Autocertificada) más Datos Asociados:

Nombre del dato	long.	Descripción
ID del Emisor del certificado	4	3-8 dígitos más significativos del PAN, rellenados por la derecha con 'FF' hex
Índice de la Clave Pública de Emisor	3	Número, elegido por el Emisor, con el que Identifica de forma única a la clave pública en cuestión
Indicador del algoritmo de la Clave Pública de Emisor	1	Indica el algoritmo a utilizar con la Clave Pública de Emisor. Su valor está fijado a '01' (hex)
Longitud del Módulo de la Clave Pública de Emisor	1	Longitud del Módulo de la Clave Pública de Emisor en bytes (N_I)
Longitud del Exponente de la Clave Pública de Emisor	1	Longitud del Exponente de la Clave Pública de Emisor en bytes (igual a 1 ó 3)
Dígitos más significativos de la Clave Pública de Emisor	N_I-36	Este campo contiene los (N_I-36) bytes más significativos del módulo de la Clave Pública de Emisor
Resto de la Clave Pública de Emisor	36	36 bytes menos significativos del módulo de la Clave Pública de Emisor
Exponente de la Clave Pública de Emisor	1	Su valor será 3 ó 2^{16}+1

Clave Pública de Emisor Autofirmada	N_{CA}	Resultado del algoritmo 'Firma Digital'

Tabla 11

Formato de Transferencia a MasterCard: Clave Pública de Emisor (autocertificada) y Datos asociados

- Formato de Transferencia a VISA Internacional: Clave Pública de Emisor (Autocertificada) más Datos Asociados:

Nombre del dato	Long.	Descripción
Cabecera	1	'22' hex
Longitud del Módulo de la Clave Pública de Emisor	1	Longitud del Módulo de la Clave Pública de Emisor en bytes (N_I)
Módulo de la Clave Pública de Emisor	Var	Módulo de la clave pública de emisor, en claro
Longitud del exponente de la Clave Pública de Emisor	1	Longitud del Exponente de la Clave Pública de Emisor en bytes (igual a 1 ó 3)
Exponente de la Clave Pública de Emisor	Var	Su valor será 3 ó $2^{16}+1$
Número de serie del certificado	3	Aportado por VISA Internacional
Clave Pública de Emisor Autofirmada	N_I	Resultado del algoritmo 'Firma Digital'

Tabla 12

Formato de Transferencia a VISA Internacional: Clave Pública de Emisor (autocertificada) y Datos asociados

Junto con la Clave Pública Autocertificada, las AACC exigen a los emisores el envío de un comprobante adicional, un hash-code. Este proceso es diferente para cada uno de los Sistemas de Pago.

A continuación se describen ambos:

* Proceso batch de *envío de Hash-Code a MasterCard*

  El proceso para generarlo se compone de dos subprocesos: cálculo del hash code y construcción del formato a enviar.

  - El cálculo del hash code se realiza de la siguiente forma:

    - Algoritmo utilizado para calcular el hash: según la normativa EMV contenida en "Book2 – EMV2000 specifications", (dirección de internet [EMVCO]), el algoritmo hash utilizado será el SHA-1 cuyo identificador será '01' hex.

    - El dato sobre el que se aplica el hash es el resultado de concatenar los siguientes campos:

Nombre del dato	Long.	Descripción
ID del emisor del certificado	4	3-8 dígitos más significativos del PAN, rellenados por la derecha con 'FF' hex
Índice de la Clave Pública de Emisor	3	Número, elegido por el Emisor, con el que Identifica de forma única a la clave pública en cuestión
Dígitos más significativos de la Clave Pública de Emisor	N_I-36	Este campo contiene los (N_I-36) bytes más significativos del módulo de la Clave Pública de Emisor
Resto de la Clave Pública de Emisor	36	36 bytes menos significativos del módulo de la Clave Pública de Emisor

Exponente de la Clave Pública de Emisor	1	Su valor será 3 ó $2^{16}+1$

Tabla 13

Datos para el cálculo del Hash-Code de la Clave Pública de Emisor para su envío a MasterCard

- Construcción del formato de transmisión del hash code:

  - Una vez calculado el Hash-Code, se concatena con otra serie de datos necesarios hasta completar el formato a enviar a MasterCard, que se describe en la siguiente tabla:

Nombre del dato	Long.	Descripción
ID del emisor del certificado	4	3-8 dígitos más significativos del PAN, rellenados por la derecha con 'FF' hex
Índice de la Clave Pública de Emisor	3	Número, elegido por el Emisor, con el que Identifica de forma única a la clave pública en cuestión
Indicador del algoritmo de la Clave Pública de Emisor	1	Indica el algoritmo a utilizar con la clave pública de emisor (valor fijo '01' hex)
Check Sum de la Clave Pública de Emisor	20	Hash-Code para la Clave Pública de Emisor

Tabla 14

Formato de transferencia: Hash-Code de la Clave Pública de Emisor y Datos Asociados para su envío a MasterCard

* Proceso batch de *envío de Hash-Code a VISA*

  En principio, sólo sería necesario automatizar el cálculo del hash-code, ya que el envío no se realiza de forma automática sino mediante un formulario denominado "Enrollment Form".

Pero además, resulta que el hash-code a enviar ya se calcula dentro del proceso *construcción de la Clave Pública de Emisor AutoCertificada para su envío a VISA Internacional*, por lo que el presente proceso podría ser copia de una parte del código de dicho proceso.

Una vez revisados los procesos de exportación de la Clave Pública de Emisor, se repasarán los procesos que componen la tarea de **Importación** del certificado de la clave pública de emisor recibido de las AACC.

Los certificados y sus datos asociados tienen formato diferente en función de la AC que lo haya generado:

- Certificado recibido de MasterCard:

  El fichero que contiene el certificado y los datos asociados, obtenido por una herramienta específica de MasterCard a partir del fichero recibido desde la propia AC por los Inspectores de Seguridad de la entidad, tiene el siguiente formato:

Nombre del dato	Longitud	Descripción
ID del Emisor del Certificado	4	3-8 dígitos más significativos del PAN, rellenado por la derecha con 'FF' hex
Índice de la Clave Pública de Emisor	3	Número, elegido por el Emisor, con el que identifica de forma única a la clave en cuestión
Índice de la Clave Pública de MasterCard	1	Índice que identifica a la clave pública utilizada por MasterCard para calcular el certificado
Resto de la Clave Pública de Emisor	37	37 bytes menos significativos del módulo de la Clave Pública de Emisor
Exponente de la Clave Pública de Emisor	1	Su valor será 3 ó $2^{16}+1$
Certificado de la Clave Pública de Emisor	N_{CA}	Resultado de la Firma Digital

de Emisor		

Tabla 15

Formato de Transferencia de Mastercard: Certificado de la Clave Pública de Emisor y Datos Asociados

- Certificado recibido de VISA Internacional:

  El fichero que contiene el certificado y los datos asociados, recibido en un diskette por el Agente Autorizado VISA de la entidad, tiene el siguiente formato:

Nombre del dato	Longitud	Descripción
Cabecera	1	Valor '24' (hex)
Identificador Servicio	4	Identifica el servicio de VISA. Valores permitidos (hex): 1010 = Credit/Debit 2010 = Electron 3010 = Interlink 8010 = PLUS 999910 = Propietary ATM El valor elegido se rellena con '00' hex por la izquierda hasta completar los 4 bytes de longitud del campo

ID del Emisor del certificado	4	BIN del Emisor, rellenado por la derecha con 'FF' hex
Número de serie del certificado	3	Número de serie del certificado, asignado por VISA
Fecha de caducidad del certificado	2	MMAA tras el cual el certificado no es válido
Longitud del Resto de la Clave Pública de Emisor	1	Longitud del resto del módulo de la clave pública de emisor
Resto de la Clave Pública de Emisor	Var	Este campo estará solo presente si $N_I > N_{cA}-36$ y, en el caso de estar presente, contendrá los $(N_I-N_{cA}+36)$ bytes menos significativos del módulo de la clave pública de Emisor (N_I)
Longitud del exponente de la Clave Pública de Emisor	1	Longitud del exponente de la clave pública de Emisor en bytes
Exponente de la Clave Pública de Emisor	Var	Su valor será 3 ó $2^{16}+1$
Índice de la Clave Pública de VISA Internacional	1	Índice de la clave pública de VISA utilizada para calcular este certificado
Certificado de la Clave Pública de Emisor	Var	Resultado de la Firma Digital
Firma Asociada	Var	Firma asociada al certificado de la Clave Pública de Emisor

Tabla 16

Formato de Transferencia de VISA Internacional: Certificado de la Clave Pública de Emisor y Datos Asociados

* Proceso batch de *verificación de datos asociados al certificado*

Este proceso deberá verificar algunos de los datos que acompañan al certificado son correctos, en concreto:

- ID del Emisor
- Índice de la Clave Pública de Emisor (sólo en el caso de MasterCard)
- Índice de la clave Pública de MC/VISA

* Proceso batch de *verificación del certificado de la clave publica de emisor*

Consta de los siguientes subprocesos:

- Recuperación de los datos utilizados para la generación del certificado:
  - Recuperación de los datos del certificado enviado por MasterCard:

    Algoritmo a utilizar: el indicado en el campo "Indicador del algoritmo de la Clave Pública de MC", recibido como uno de los datos asociados a la clave pública autocertificada de MasterCard (ver ***tabla 1, "Formato de Transferencia de Clave Pública de MasterCard autocertificada y Datos Asociados"***),

    Datos sobre los que aplicar el algoritmo: certificado recibido en el campo "Certificado de la Clave Pública de Emisor" (ver ***tabla 15***, "***Formato de Transferencia de Mastercard: Certificado de la Clave Pública de Emisor y Datos Asociados"),***

    Clave a utilizar: la clave pública de MasterCard que indique el Índice que acompaña al certificado (campo "Índice de la Clave Pública de MasterCard" de la ***tabla 15***). La asociación entre este índice y su Clave Pública de MasterCard se obtiene de la ***tabla 1***.

  - Recuperación de los datos del certificado enviado por VISA Internacional:

    Algoritmo a utilizar: el indicado en el campo "Indicador del algoritmo de la Clave Pública de VISA", recibido como uno de los datos asociados a la clave pública autocertificada de VISA

(ver ***tabla 3***, "***Formato de Transferencia de Clave Pública de VISA Internacional autocertificada y Datos Asociados***"),

Datos sobre los que aplicar el algoritmo: certificado recibido en el campo "Certificado de la Clave Pública de Emisor" (ver ***tabla 16***, "***Formato de Transferencia de VISA Internacional: Certificado de la Clave Pública de Emisor y Datos Asociados***"),

Clave a utilizar: la clave pública de VISA que indique el Índice que acompaña al certificado (campo "Índice de la Clave Pública de VISA" de la ***tabla 16***). La asociación entre este índice y su Clave Pública de VISA se obtiene de la ***tabla 3***.

- El formato de los datos recuperados del certificado será el mismo independientemente del sistema que haya emitido dicho certificado:

Nombre del dato	Longitud	Descripción
Cabecera de los Datos Recuperados	1	'6A' hex
Formato del Certificado	1	'02' hex
ID del Emisor del Certificado	4	3-8 dígitos más significativos del PAN, rellenados por la derecha con 'FF' hex
Fecha de expiración del Certificado	2	Mes/año, en formato MMAA a partir del cual el certificado se invalida
Número de Serie del Certificado	3	Valor de 3 bytes, establecido por VISA/MasterCard
Indicador del algoritmo hash	1	Indica el algoritmo hash utilizado para calcular el certificado
Indicador del algoritmo de la Clave Pública de Emisor	1	Indica el algoritmo a utilizar con la Clave Pública de Emisor. Su valor está fijado a

Emisor		'01' (hex)
Longitud de la Clave Pública de Emisor	1	Longitud del módulo de la Clave Pública de Emisor en bytes (N_I)
Longitud del exponente de la Clave Pública de Emisor	1	Longitud del exponente de la Clave Pública de Emisor en bytes
Clave Pública de Emisor o Dígitos más significativos de la Clave Pública de Emisor	Var	Si (N_I <= N_{CA}-36), entonces este campo contiene el módulo completo de la Clave Pública de Emisor, rellenado por la derecha con (N_{CA}-36 - N_I) bytes con valor 'BB' hex Si (N_I > N_{CA}-36), entonces este campo contiene los (N_{CA}-36) bytes más significativos del módulo de la Clave Pública de Emisor y sus datos asociados
Resultado del hash	20	Hash de la Clave Pública de Emisor y sus datos asociados
Cola de los Datos Recuperados	1	'BC' hex

Tabla 17

Formato de los datos recuperados del Certificado de la Clave Pública de Emisor

- Verificación bytes de cabecera y formato del certificado:

  - El valor del campo "Cabecera de los datos recuperados" debe ser '6A' hex

- El valor del campo “Formato del Certificado” debe ser ‘02' hex

▪ Cálculo y verificación del hash:

El cálculo se realiza de la siguiente forma:

- Algoritmo utilizado para calcular el hash: según la normativa EMV contenida en “Book2 – EMV2000 specifications”, (dirección de internet [EMVCO]), el algoritmo hash utilizado será el SHA-1 cuyo identificador será ‘01’ hex.

- El dato sobre el que se aplica el hash es el resultado de concatenar del 2º al 10º de los campos indicados en la ***tabla 17*** junto con el Resto y el Exponente de la Clave Pública de Emisor.

El hash así calculado debe coincidir con el hash recuperado del certificado (campo “Resultado del hash” de la ***tabla 17***).

▪ Verificación del resto de los datos incluidos en la ***tabla 17***, recuperados del certificado.

* Proceso batch de *validación de la firma asociada al certificado de VISA Internacional*

VISA Internacional siempre adjunta un dato más a los certificados de clave pública de emisor que expide. Esta dato es la “Firma Asociada” (ver ***tabla 16***, “***Formato de Transferencia de VISA Internacional: Certificado de la Clave Pública de Emisor y Datos Asociados***”), y es exclusivo de VISA. MasterCard no adjunta ningún dato adicional a los ya vistos en el apartado anterior.

Esta “Firma asociada” tiene como objetivo garantizar la integridad tanto de los datos en claro asociados al certificado como del propio certificado.

Aunque VISA siempre adjunta la Firma a los certificados, su uso es opcional por parte del Emisor; en el caso de querer utilizarlo, el proceso de verificación es el siguiente:

▪ Recuperación de los datos firmados:

Algoritmo a utilizar: el indicado en el campo “Indicador del algoritmo de la Clave Pública de VISA”, recibido como uno de los

datos asociados a la clave pública autocertificada de VISA (ver ***tabla 3***, "***Formato de Transferencia de Clave Pública de VISA Internacional autocertificada y Datos Asociados***"),

Datos sobre los que aplicar el algoritmo: firma recibida en el campo "Firma Asociada" (ver ***tabla 16***, "***Formato de Transferencia de VISA Internacional: Certificado de la Clave Pública de Emisor y Datos Asociados***"),

Clave a utilizar: la clave pública de VISA que indique el Índice que acompaña al certificado (campo "Índice de la Clave Pública de VISA" de la ***tabla 16***). La asociación entre este índice y su Clave Pública de VISA se obtiene de la ***tabla 3***.

Formato de los datos recuperados de la firma asociada al certificado:

Nombre del dato	Long.	Descripción
Cabecera de los Datos Recuperados	1	'00' hex
Código de formato de bloque	1	'01' hex
Caracteres de relleno	Var	'FF' hex, con una longitud de relleno igual a: (longitud del módulo de la clave usada para firmar – 38)
Separador	1	'00' hex
Indicador del algoritmo	15	Valor hexadecimal Indicando el algoritmo utilizado por VISA
Resultado del hash	20	Hash de la Clave Pública de Emisor y sus datos asociados

Tabla 18

Formato de los datos recuperados de la Firma Asociada al Certificado emitido por VISA Internacional

- Verificación del hash recuperado de la Firma Asociada:

La manera de hacerlo es volver a calcular el hash (o huella digital):

- Algoritmo utilizado para calcular el hash: según la normativa EMV contenida en "*Book2 – EMV2000 specifications*", (dirección de internet [EMVCO]), el algoritmo hash utilizado será el SHA-1 cuyo identificador será '01' hex.

- Datos sobre los que aplicar el hash: se aplicará sobre el resultado de concatenar los datos en claro incluidos en el certificado recibido de VISA (campos 1º al 10º de la ***tabla 16***, "***Formato de Transferencia de VISA Internacional: Certificado de la Clave Pública de Emisor y Datos Asociados***") con todos los datos recuperados de dicho certificado (***tabla 17***, "***Formato de los datos recuperados del Certificado de la Clave Pública de Emisor***")

Si el resultado de este cálculo coincide con el "Resultado del Hash" recuperado de la Firma Asociada (***tabla 18***, "***Formato de los datos recuperados de la Firma Asociada al Certificado emitido por VISA Internacional*** "), entonces el certificado recibido de VISA Internacional es correcto.

* Proceso batch de <u>*Almacenamiento del certificado*</u>

En el caso de que la verificación del certificado recibido haya resultado satisfactoria, el Emisor almacenará los datos recuperados del certificado en la tabla CPEDASOC (CLAVE PÚBLICA DE EMISOR - DATOS ASOCIADOS, ver el apartado "Generación de claves RSA"), completando de este modo el registro correspondiente a la clave certificada.

La definición definitiva de la tabla CPEDASOC, será la siguiente:

CPEDASOC <u>C</u>LAVE <u>P</u>ÚBLICA DE <u>E</u>MISOR - <u>D</u>ATOS <u>ASOC</u>IADOS		
Clave Única**:** **Etiqueta de la Clave Pública de Emisor**		
Nombre del campo	**Longitud**	**Descripción**
Etiqueta de la Clave Pública de Emisor	3	Entorno de Uso ('EMV')

Emisor	Var	Producto (‘MC’/’VISA’)
	3	BIN del Emisor
	1	Tipo de algoritmo (‘01’ hex, RSA)
	3	Índice de la Clave Publica de Emisor
Longitud del Módulo de la Clave Pública de Emisor	1	Longitud del Módulo de la clave pública de emisor en bytes (N_I)
Longitud del Exponente de la Clave Pública de Emisor	1	Longitud del Exponente de la Clave Pública de Emisor
Exponente de la Clave Pública de Emisor	Var	Su valor será 3 ó $2^{16}+1$
Fecha de caducidad de la Clave Pública de Emisor	2	Mes/año (en formato MMAA) a partir de los cuales la Clave Pública de Emisor se invalida
Tipo de algoritmo	1	Algoritmo utilizado para la generación de la clave RSA
Resto de la Clave Pública de Emisor	36	Bytes menos significativos del módulo de la Clave Pública de Emisor. Este campo sólo estará presente si ($N_I > N_{CA}$-36), siendo N_I y N_{CA} las longitudes en bytes del módulo de la clave pública del emisor y de la AC, respectivamente)
Certificado de la Clave Pública de Emisor	Var	Resultado del algoritmo “Firma Digital” calculado con la clave privada de la AC
Índice de la clave pública de MC/VISA	3	Identificador de la clave pública de la AC, correspondiente a la clave privada con la que se calculó el

		certificado

1.2.4. Cálculo de la Firma Digital de Datos Estáticos

1.2.4.1. Tareas a realizar

Una vez que el emisor ha cargado sus tarjetas con las claves públicas de emisor y de tarjeta, y los certificados correspondientes, éstas (las tarjetas) están ya preparadas para realizar de forma completa el proceso de autenticación dinámica mediante el pertinente diálogo con el terminal EMV.

Ahora bien, el proceso de autenticación Off Line estática (también denominado por sus siglas en inglés, SDA) obliga a la realización por parte del Host de una tarea más durante la fase de personalización de las tarjetas: se debe firmar cada una de ellas, calculando una firma digital estática y grabándola en el chip EMV de las tarjetas.

La Autenticación Estática SDA se basa en la validación por parte del terminal de ciertos datos almacenados en la tarjeta y que la caracterizan de forma unívoca. Estos datos (Datos Estáticos de Tarjeta) aparecen en la tarjeta firmados con la parte privada de la Clave RSA de Emisor, además de aparecer también en claro.

La Firma Digital de Datos Estáticos intenta evitar la duplicación de tarjetas.

Gracias a la utilización del método de firma digital, el emisor tiene la certeza de que sólo serán aceptadas aquellas tarjetas cuyos datos firmados no hayan sido manipulados.

1.2.4.2. Desarrollos y adaptaciones propuestos

En el caso de tarjetas EMV, el actual proceso de estampación de tarjetas de la entidad se convierte sólo en un primer paso de la estampación, en el que se establecen los valores necesarios para generar el plástico, la banda magnética y los datos para encarte y ensobrado.

Pero EMV hace necesario un segundo paso en el que se establezcan los valores que se grabarán en el chip EMV. Uno de esos valores es la Firma SDA.

Por tanto, el nuevo desarrollo consistirá en una rutina que realice el cálculo de dicha Firma:

* Rutina de *cálculo de la Firma SDA de una tarjeta y grabación del DAC*

  Esta rutina constará de los siguientes subprocesos:

- Generación del DAC:

  Para cada tarjeta, se deberá generar su Código de Autenticación de Datos o DAC, de la siguiente forma:

  - Se concatena el PAN de la tarjeta con su número de secuencia.

  - Se toman los 8 bytes menos significativos del resultado de la concatenación anterior, y se le aplica un Triple DES con la clave de DAC (MK_{DAC}).

  - El DAC son los dos bytes más significativos del resultado del paso anterior.

- Grabación del DAC:

  Para poder ser utilizado en la fase de autorización, el DAC se grabará en la tabla de Datos de tarjetas EMV (***TEMV***), concretamente en el campo TEMVDAC.

  La descripción completa de la tabla TEMV se muestra en el siguiente apartado, "*Parámetros y Perfiles EMV*".

- Cálculo de la Firma SDA:

  Los datos a firmar son los contenidos en la siguiente tabla:

Indicador del Algoritmo Hash
Código de Autenticación de Datos (DAC), calculado según el paso anterior
Fecha de Activación de la Aplicación, TAG ***5F25***
Fecha de Caducidad de la Aplicación, TAG ***5F24***
Control de Uso de la Aplicación, TAG ***9F07***
PAN, TAG ***5ª***

Número de Secuencia del PAN, TAG ***5F34***
IAC_ Default, TAG ***9F0D***
IAC_Denial, TAG ***9F0E***
IAC_Online, TAG ***9F0F***
CVM List, TAG ***8E***
Código del País Emisor (sólo para *VISA*)
Valor del campo correspondiente al TAG indicado por el 'SDA Tag List, TAG ***9F4A***'

Estos datos deberán ser firmados con la parte privada de la Clave RSA de Emisor.

1.3. SEGURIDAD ON LINE (CRIPTOGRAFÍA SIMÉTRICA)

No toda la seguridad del estándar EMV está basada en la criptografía asimétrica, también la simétrica juega su papel, no sólo para la autenticación On Line, sino también para todo lo relacionado con la autenticación On Line, mejorando significativamente el nivel de seguridad ya existente en este entorno.

Esta mejora en la seguridad de las transacciones On Line se basa en las nuevas capacidades que proporciona el chip EMV. Así, en el transcurso de una operación EMV On Line no sólo el Emisor debe autenticar a la tarjeta (cosa que ya ocurre con las operaciones de banda magnética) sino que la propia tarjeta ha de ser capaz de autenticar al Emisor, es decir, verificar que las respuestas que recibe proceden realmente del Host de su Emisor.

Además, existe otra clave simétrica que se utiliza en la autenticación estática, pero no por la tarjeta, sino en la fase de personalización: mediante esa clave, se calcula un dato llamado DAC (iniciales en inglés de "Código de Autenticación de Datos"), que se graba en la tarjeta para que sea posteriormente recuperado por el terminal si la autenticación estática de la tarjeta finaliza satisfactoriamente.

Para ambos casos (autenticación On Line y generación del DAC para autenticación Off Line), el estándar EMV utiliza criptografía simétrica, en concreto el algoritmo Triple DES. La seguridad de esta criptografía se basa en la utilización de claves comunes a la entidad Emisora y la tarjeta EMV.

1.3.1. Claves a grabar en la Tarjeta (para autenticación On Line)

Así como las claves asimétricas permiten la autenticación mutua entre terminal y tarjeta, en ambiente Off Line, las claves simétricas permiten la autenticación mutua entre tarjeta y Emisor, en ambiente On Line.

Para que esta autenticación en base a criptografía simétrica sea posible, es necesario que el Emisor y sus tarjetas compartan las mismas claves simétricas o, al menos, conozcan cómo se pueden obtener.

Para aumentar la seguridad del sistema, es obligatorio que las claves sean diferentes en cada tarjeta.

La manera más obvia de hacerlo parecería ser la de generar claves aleatorias diferentes para cada tarjeta. Esto claramente no es viable, ya que obligaría al Emisor a almacenar miles o incluso millones de claves en su Host.

Lo que realmente se hace es establecer procesos de diversificación. Estos procesos son métodos criptográficos mediante los cuales el Emisor, partiendo de las claves maestras y usando datos diferentes para cada tarjeta (pero conocidos), genera claves diferentes para cada tarjeta.

Tanto VISA como MasterCard definen métodos de diversificación en sus especificaciones, pero hay libertad para que los emisores utilicen métodos propietarios (al fin y al cabo, sólo el Emisor va a utilizarlos, bien en el Host, bien al incluirlos en las tarjetas por él emitidas).

Las claves simétricas que se deben generar y grabar en el chip de las tarjetas EMV son las siguientes (según el documento [EURO073]):

Clave	Descripción
Clave diversificada para cálculo de AC's (MK_{AC})	Clave, única por tarjeta, utilizada para el cálculo de los criptogramas de aplicación (AC's)
Clave diversificada para protección en integridad (MK_{SMI})	Clave, única por tarjeta, utilizada para la protección en integridad de los scripts
Clave diversificada para protección en confidencialidad (MK_{SMC})	Clave, única por tarjeta, utilizada para la protección en confidencialidad de los scripts
Clave diversificada para el cálculo del IDN o Número Dinámico de Tarjeta (MK_{IDN})	Clave, única por tarjeta, utilizada para el cálculo del Número Dinámico de Tarjeta. Esta clave sólo estará presente en aquellas tarjetas que soporten Autenticación Dinámica Off Line (DDA o CDA)

Tabla 19

Claves Simétricas por Tarjeta

Las claves deberán ser de longitud doble (16 bytes, ó 32 caracteres), de acuerdo al algoritmo utilizado (Triple DES).

1.3.2. Clave de cálculo del DAC (para autenticación Off Line)

Además de las claves almacenadas en las tarjetas, el Host Emisor debe generar otra clave simétrica que utilizará exclusivamente para el cálculo del DAC.

El DAC ó Código de Autenticación de Datos es uno de los datos que, según el estándar EMV, debe ser utilizado para el cálculo de la Firma Digital de Datos Estáticos de tarjeta. Este código será recuperado por el terminal en el transcurso de una operación Off Line y enviado al Emisor como prueba de que se ha efectuado satisfactoriamente el proceso de Autenticación Estática.

El Emisor será el responsable del cálculo del DAC, debiendo utilizar para ello una clave simétrica Triple DES: la Clave para el Cálculo del DAC (IMK_{DAC}). Esta clave, cuya función será únicamente la del cálculo de este código, deberá ser generada y almacenada por la entidad emisora siguiendo los requisitos de seguridad establecidos por los sistemas de pago internacionales.

1.3.3. Desarrollos y adaptaciones propuestos

Se parte del supuesto de que la entidad ya hacía uso de la criptografía simétrica y el Triple DES con sus tarjetas tradicionales, por lo que la introducción de nuevas claves no ha de suponer ningún desarrollo o adaptación en su aplicación informática.

Bastará con incrementar el número de claves que actualmente estén en uso por la entidad, incorporando las definidas más arriba.

Estas nuevas claves serán almacenadas para su uso posterior en la fase de autorización, y comunicadas a las entidades estampadoras para que las utilicen en la fase de personalización de las tarjetas EMV.

Por tanto, no es necesario ningún desarrollo específico.

1.4. PARÁMETROS Y PERFILES EMV

1.4.1. Definición de "parámetro EMV" y "perfil EMV"

El nuevo chip EMV permite al emisor almacenar en la propia tarjeta muchos más datos particulares (de la propia tarjeta y del usuario) de lo que le permitía la tarjeta de banda magnética.

Esta facilidad tiene la contrapartida de que obliga al emisor a gestionar todos estos nuevos datos, que denominaremos "parámetros EMV". Esta gestión comienza en la propia personalización de la tarjeta, fase durante la cual el emisor deberá decidir qué valores asignar a toda una serie de nuevos campos, muchos de ellos utilizados en la fase de autorización por la propia tarjeta, ya que EMV ha dotado de gran independencia a las tarjetas a la hora de autorizar transacciones financieras, pudiendo incluso actuar "en nombre" del emisor.

Los valores de los nuevos datos deberán ser determinado y gestionados por el Emisor, y comunicados al personalizador para su almacenamiento en el chip de la tarjeta. La lista completa se puede consultar en el Anexo A, "TABLA DE ETIQUETAS DE DATOS EMV".

Estos nuevos datos se denominan también "Parámetros EMV", y se almacenan en el chip en estructuras denominadas "TLV" (iniciales en inglés: Tag, Length, Value):

- **Etiqueta** ó 'TAG': campo identificativo, único para cada parámetro, puede ser de uno o dos bytes
- **Longitud**: longitud del dato en bytes
- **Valor**: contenido asignado al parámetro. Este contenido puede ser a su vez otra estructura TLV

Por otro lado, la proliferación de parámetros ha obligado a buscar soluciones que faciliten la asignación de valores a todos ellos. Una de estas soluciones ha sido la creación, por parte de los Sistemas de Pago Internacionales, Visa y MasterCard, del concepto de "perfil EMV".

Los Perfiles EMV fijan el valor de los parámetros de la tarjeta de forma que quede establecido el comportamiento de ésta. Estos Perfiles se han determinado en función de:

- Tipo de producto (crédito o débito) al que pertenece la tarjeta
- Gestión de Riesgo a llevar a cabo por parte de la tarjeta

- Métodos de Verificación de Usuario que soporte la tarjeta

- Autenticación de Emisor/Tarjeta soportada o no por la tarjeta

Por supuesto, los emisores tienen la opción de no utilizar los perfiles recomendados por los sistemas internacionales y, en su defecto, definir perfiles propios.

Sin embargo, los sistemas de intercambio españoles (EURO6000 y Sermepa) recomiendan, al menos durante los primeros estadios de la migración a EMV, elegir entre los perfiles ya establecidos aquellos que mejor se adapten a las necesidades del Emisor.

También las herramientas de personalización hacen uso del concepto de perfil, ya que la forma de trabajar es la siguiente:

- Se definen los perfiles en la propia herramienta, fijando los valores de los atributos enumerados más arriba (tipo de producto, gestión de riesgo, métodos de verificación de usuario, autenticación de emisor) y del resto que sean necesarios

- Se asigna un número de perfil a esa combinación de valores, también en la propia herramienta

- En el fichero de personalización que envíe el Host a la herramienta de personalización, deberá figurar para cada tarjeta el número de perfil que le corresponde, de forma que se tomen de ese perfil todos los parámetros EMV que no vengan fijados ya desde Host

Por último, existen otros parámetros utilizados en la gestión de las tarjetas EMV, que no van incluidos dentro del chip pero que condicionan la forma en que la aplicación Host realiza una serie de tareas relacionadas con EMV. Estos parámetros se denominan "parámetros EMV de entidad", y se hablará de ellos más adelante.

1.4.2. Relación entre Marca, Producto y Perfil EMV

La introducción del concepto de EMV obliga a aclarar cómo encajará este concepto con otros que puede parecer que cumplen funciones similares, como son la marca o el producto de una tarjeta.

Cualquier aplicación de Medios de Pago suele clasificar sus tarjetas según dos conceptos, la Marca y el Producto, que se podrían definir de la siguiente forma:

- La Marca de una tarjeta depende del sistema de pago bajo el que se ha emitido dicha tarjeta. Esta marca va impresa en el propio plástico, y permite que la tarjeta sea aceptada en comercios y cajeros de todo el mundo.

  Ejemplos de estas marcas son: VISA, MasterCard, American Express, Dinners Club...

- El Producto es un concepto que le permite a la entidad agrupar sus tarjetas en función de unas características comunes, que pueden ser de tipo comercial, de comportamiento, del colectivo al que van dirigidas, etcétera.

  Ejemplos típicos de productos podrían ser: tarjeta joven, tarjeta dorada, tarjeta para clientes VIP, tarjeta universitaria, y cualquier otro tipo de tarjeta que se le ocurra a la entidad. Como se puede apreciar, la creación de nuevos productos y su asignación a las tarjetas es algo que queda totalmente a discreción de la entidad, mientras que las marcas son entes externos y de asignación fija.

Estos dos conceptos, marca y producto, están relacionados con el concepto de perfil EMV de la siguiente forma:

- Un Perfil EMV sólo es válido para una marca de tarjeta determinada, que se fija al crear el perfil. Es decir, no podrá haber tarjetas VISA y MasterCard con el mismo perfil.

- Todo producto de tarjeta EMV tiene un perfil asociado (uno y sólo uno). Es decir, no se va a permitir que dos tarjetas del mismo producto tengan perfiles diferentes.

- Un único perfil puede estar asociado a varios productos de tarjeta diferentes (aunque todos pertenecientes a la misma marca). Es decir, podrá haber una tarjeta "VISA Electrón Joven" y otra "VISA Electrón VIP" que tengan el mismo perfil EMV.

En la fase de convivencia de tarjetas EMV y no EMV, habrá que tener contemplado el caso en que la entidad convierta uno de sus productos tradicionales en producto EMV, pero transitoriamente sigan existiendo tarjetas de ese producto que no sean EMV hasta que se reestampen (por renovación o por duplicado).

1.4.3. Descripción de los parámetros EMV

A continuación se describirá someramente algunos de los nuevos datos, agrupándolos en cinco categorías diferentes en función de su tipo:

1) Datos específicos de la tarjeta

2) Datos de la aplicación EMV

3) Parámetros para verificación de usuario

4) Parámetros para gestión de riesgo Off Line

    a. Datos definidos por el estándar EMV

    b. Datos definidos por MasterCard

    c. Datos definidos por VISA Internacional

5) Datos criptográficos

1.4.3.1. Datos específicos de la tarjeta

Estos datos son diferentes en cada tarjeta y el emisor puede asignarlos con total libertad.

A continuación se da una lista de los parámetros contenidos en esta categoría:

- Fecha de activación de la aplicación

  Indica el año/mes/día a partir del cual la aplicación EMV de la tarjeta pasará a estar operativa.

  Etiqueta del dato: TAG ***5F25***.

- Fecha de expiración de la aplicación

  Indica el año/mes/día a partir del cual la aplicación EMV de la tarjeta caduca.

  Esta fecha debe ser coherente con la fecha de caducidad grabada en la banda magnética y estampada en el plástico.

  Además, no se puede asignar a la tarjeta una fecha de caducidad mayor que la fecha de caducidad de los certificados incluidos en ella.

  Etiqueta del dato: TAG ***5F24***.

- PAN de la tarjeta

Es el número de la tarjeta, el mismo que aparece en el plástico y está grabado en la banda.

Etiqueta del dato: TAG ***5A***.

- Número de secuencia del PAN

  Sirve para diferenciar los sucesivos plásticos que se vayan estampando para un mismo PAN.

  En caso de no estar presente, el valor por defecto será cero.

  Etiqueta del dato: TAG ***5F34***.

- Nombre usuario

  Nombre del titular de la tarjeta, según el estándar ISO 7813.

  Este dato debe coincidir con el estampado en el plástico y el grabado en la banda magnética.

  Etiqueta del dato: TAG ***5F20***.

- Datos equivalentes de pista 2

  En este dato se graban los mismos datos que en la Pista 2 de la banda magnética, según el ISO 7813, excepto los centinelas de inicio y fin y el LRC.

  Etiqueta del dato: TAG ***57***.

- Datos discrecionales de pista 2

  MasterCard utiliza este dato para grabar parte de los datos de la pista 2, (ya grabados en el TAG ***57***). En concreto, en este dato graba los datos discrecionales, definidos en el ISO 7813.

  VISA no hace uso de este dato.

  Etiqueta del dato: TAG ***9F20***.

- Datos discrecionales de pista 1

VISA utiliza este dato para grabar los datos discrecionales de la pista 1 de la banda magnética de la tarjeta, que, según el ISO 7813, puede tener dos estructuras diferentes.

MasterCard no hace uso de este dato.

Etiqueta del dato: TAG ***9F1F***.

1.4.3.2. Datos de la aplicación EMV

Estos datos son propietarios de la aplicación, y están fijados por los sistemas de pago en base a las especificaciones de MasterCard y VISA Internacional.

El emisor debería ajustarse a los valores recomendados por las marcas.

- Código de moneda de la aplicación

  Moneda en la que se administra la tarjeta, de acuerdo a la norma ISO 4217.

  Etiqueta del dato: TAG ***9F42***.

  Su valor debe ser '0978' hex (euros).

- Exponente de la moneda de la aplicación

  Mediante este dato se indica cual es la posición de la coma de separación de los decimales dentro del importe (empezando por la derecha), según la norma ISO 4217.

  Etiqueta del dato: TAG ***9F44***.

  Su valor debe ser '02' hex (los euros tienen dos decimales).

- Localizador de ficheros de la aplicación (AFL)

  Mediante este dato se indica al terminal en que ficheros y registros están los datos que necesita leer durante una transacción EMV.

  La razón de ser de este dato está en que cada producto EMV (MasterCard, Maestro, VISA Oro, VISA Classic, VISA Electrón...) tiene ubicados en ficheros y registros diferentes los datos a utilizar en una transacción EMV.

Etiqueta del dato: TAG ***94***.

Valores posibles:

MasterCard: ’08 01 02 01 10 01 04 00’ hex.

Maestro: ’08 01 02 01 10 01 04 00’ hex.

VISA Classic: ’08 01 04 00 10 01 04 01’ hex.

VISA Electrón: ’08 01 04 00 10 01 04 01’ hex.

- Nombre del Fichero Dedicado

El Fichero Dedicado (DF) contiene información identificativa de la aplicación EMV. El nombre de ese fichero dedicado varía según el producto, ajustándose a la norma ISO 7816-4.

Etiqueta del dato: TAG ***84***.

Valores posibles:

MasterCard: ‘A0000000041010’ hex.

Maestro: ‘A0000000043060’ hex.

VISA Classic: ‘A0000000031010’ hex.

VISA Electrón: ‘A0000000032010’ hex.

- Identificador de la aplicación

Es similar al anterior, pero en este caso se hace referencia al nombre de la aplicación, no al del fichero dedicado DF (aunque pueden coincidir). El nombre de la aplicación se ajusta a la norma ISO 7816-5.

Etiqueta del dato: TAG ***4F***.

Valores posibles:

MasterCard: ‘A0000000041010’ hex.

Maestro: ‘A0000000043060’ hex.

VISA Classic: ‘A0000000031010’ hex.

VISA Electrón: ‘A0000000032010’ hex.

- Perfil de Intercambio de la Aplicación (AIP)

  Este dato se compone de una serie de indicadores de las capacidades de la tarjeta para soportar en su aplicación EMV determinadas funcionalidades específicas.

  En concreto, estas capacidades son:

  - Autenticación Off Line estática (SDA) soportada
  - Autenticación Off Line dinámica (DDA) soportada
  - Verificación de Usuario soportada
  - Gestión de riesgo ejecutada en el terminal
  - Autenticación de Emisor soportada

  Una de las ventajas del estándar EMV de las que ya se ha hablado a lo largo del documento es la posibilidad de autenticar la tarjeta (por parte del terminal y por parte del Host Emisor) y el propio Host Emisor (por parte de la tarjeta). Estas autenticaciones garantizan que todos los elementos que están interviniendo en una transacción EMV son legítimos.

  Existen varios tipos de autenticaciones, como se ha venido indicando anteriormente en el documento: DDA, SDA y CDA. Para soportar esta variedad de procesos de autenticación, las tarjetas EMV incorporan toda una serie de datos relacionados con las autenticaciones.

  A continuación se hacen algunas precisiones sobre cada uno de los tipos de autenticación:

  - Autenticación Off Line estática (SDA)

    Es la más simple, basta con calcular una Firma y grabar el dato en el chip EMV durante la personalización inicial.

La aplicación Host generará siempre la firma SDA, que se grabará en el chip de todas las tarjetas. De este modo se asegura que la tarjeta será autenticada por todos aquellos terminales EMV que tengan capacidad para ello.

- Autenticación Off Line dinámica (DDA)

  En caso de que las tarjetas vayan a utilizar autenticación DDA, se requiere que el chip correspondiente posea un procesador criptográfico, lo que encarece el coste de las tarjetas respecto a las DDA.

  Algunas entidades, como Euro6000, recomiendan iniciar la emisión de tarjetas sin la posibilidad de autenticación DDA, para abaratar costes, dejando para mas adelante la emisión de tarjetas que soporten DDA.

  La aplicación Host deberá tener contemplados ambos supuestos, teniendo en cuenta que los datos a grabar en el chip EMV varían en función de que posea o no capacidad de autenticación DDA.

- Autenticación de Emisor

  La autenticación de emisor es una característica de la tarjeta que le permite asegurarse de que las respuestas a sus peticiones de autorización han sido respondidas realmente por su Host Emisor.

  Según el estándar EMV, la autenticación del emisor por parte de la tarjeta es recomendable, pero no obligatoria. De esta forma, al personalizar las tarjetas, los datos a grabar en el chip EMV varían en función de que se desee o no que la tarjeta realice la autenticación de emisor. En terminología EMV, estas opciones de incluir o no autenticación de emisor se denominan “Partial Grade” (sin autenticación de emisor) o “Full Grade” (con autenticación de emisor).

  En las primeras fases de EMV, la posibilidad de que se realice o no la autenticación va a depender mucho del adquirente. Si el terminal adquirente y el Host adquirente son capaces de hacer llegar al Host Emisor datos EMV, el host Emisor deberá en ese caso calcular el ARPC correspondiente y devolverlo al Host adquirente. Si el terminal adquirente es “Partial Grade”, o no recibe el ARPC correspondiente del Emisor, no habrá autenticación de Emisor. En cualquier caso, las tarjetas EMV, aunque sean “Partial Grade”, deberán ser capaces de aceptar transacciones EMV con autenticación de Emisor o sin ella.

Etiqueta del dato: TAG ***82***.

- Nombre de la aplicación

  Se trata de un literal que contiene el nombre de la aplicación, codificado en hexadecimal (no confundir con el identificador de la aplicación, TAG ***4F***, que no es un literal sino un código).

  Etiqueta del dato: TAG ***50***.

  Ejemplos de valores posibles:

  '56495341' hex : "VISA"

  '4D617374657243617264' hex : "MasterCard"

  '4D61657374726F' hex : "Maestro"

- Indicador de la prioridad de la aplicación

  Indica la prioridad de la aplicación EMV dentro del directorio de aplicaciones presentes en el chip de la tarjeta.

  Etiqueta del dato: TAG ***87***.

  Valor recomendado: '01', por defecto para todas las tarjetas.

- Control de uso de la aplicación (AUC, Application Usage Control)

  Los datos a grabar en el chip EMV varían en función de que el emisor desee o no restringir el uso de la aplicación en cuanto al entorno geográfico y los servicios permitidos. Este control lo realiza el terminal.

  En concreto, se pueden realizar restricciones según los siguientes conceptos:

  - Permitir transacciones de efectivo nacionales

  - Permitir transacciones de efectivo no nacionales

  - Permitir compra de bienes nacionales

  - Permitir compra de bienes no nacionales

- Permitir compra de servicios nacionales
- Permitir compra de servicios no nacionales
- Permitir operar en ATMs (cajeros automáticos)
- Permitir operar en terminales distintos de ATMs
- Permitir Cash Back nacional
- Permitir Cash Back no nacional

Etiqueta del dato: TAG ***9F07***.

Valor recomendado: 'FF00' hex, por defecto para todas las tarjetas, es decir, permitir cualquier tipo de operatorias salvo Cash Back.

- Número de versión de la aplicación

Este número de versión es asignado a la aplicación por el correspondiente sistema de pago (VISA, MasterCard). Indica la prioridad de la aplicación EMV dentro del directorio de aplicaciones presentes en el chip de la tarjeta.

Etiqueta del dato: TAG ***9F08***.

Las versiones con las que se está trabajando actualmente son:

Aplicación *M/Chip 2.1* ó *4* de MasterCard: número de versión 00 02

Aplicación *VIS 1.3.2* de VISA: número de versión 00 84

Aplicación *VIS 1.4.0* de VISA: número de versión 00 8C

- Código del país emisor

En este dato se guarda el código del país al que pertenece el emisor de la tarjeta, de acuerdo a la norma ISO 3166.

Este dato lo utiliza el terminal cuando realiza restricciones geográficas sobre la operatividad de la tarjeta.

Etiqueta del dato: TAG ***5F28***.

Su valor debe ser '0724' hex (España).

- Código de servicio

  El código de servicio es un dato que ya se guardaba con anterioridad en la banda magnética, y que depende de las posibilidades que la tarjeta ofrezca a su titular.

  El valor grabado en este campo debe ser coherente con el grabado en la pista 2 de la banda magnética, y también con el contenido en el TAG ***57*** (Datos equivalentes de pista 2).

  Etiqueta del dato: TAG ***5F30***.

  Su valor debe ser '0201' hex para todas las tarjetas EMV.

- Lenguaje preferente de la aplicación

  Las tarjetas ya almacenan dentro de su banda magnética un código de lenguaje. En el caso del chip EMV cabe la posibilidad de tener hasta 4 lenguajes preferentes distintos, que se almacenan en el chip en orden de preferencia. Cada lenguaje se representa con dos caracteres alfabéticos que se corresponden a su código ISO 639.

  Etiqueta del dato: TAG ***5F2D***.

  Ejemplos de valores posibles:

  Tarjeta con un único lenguaje preferido (español): 5F2D 02 6573

  Tarjeta con un dos lenguajes (catalán y español): 5F2D 04 6361 6573

1.4.3.3. Parámetros para verificación de usuario

Se repasarán en este apartado todos aquellos datos relacionados con la verificación del usuario (no confundir con las autenticaciones, que se realizan entre tarjeta, terminal y/o Host Emisor sin intervención del usuario de la tarjeta).

- Lista CVM

  Un CVM es un método de verificación del usuario (CVM, Cardholder Verification Method). Estos métodos pueden ser:

- Presentación del PIN Off Line
- Firma del usuario
- Presentación del PIN On Line
- No realizar ningún método de verificación del usuario

El presente dato es una cadena de caracteres, que se corresponde con una lista de métodos de verificación del titular. Esta lista describe qué métodos de verificación usará el terminal para verificar al titular de la tarjeta, en qué orden y qué hacer si fallan.

Etiqueta del dato: TAG ***8E***.

Los valores recomendados dependen del producto:

- Valor recomendado por Sermepa (dirección de internet [SERM]) para cualquier tarjeta VISA:

  '0000 0000 0000 0000 1E03 0103 0203 1F00'

  (Firma, PIN Off Line, PIN On Line y CVM no soportado)

- Valores recomendados por CECA-Euro6000 (documento [EURO072]): recomienda dos listas de métodos diferentes, una que incluye PIN Off Line:

  '0000 0000 0000 0000 4103 5E03 4203 1F03'

  (PIN Off Line, Firma, PIN On Line y CVM no soportado)

  y otra que no:

  '0000 0000 0000 0000 0000 5E03 4203 1F03'

  (Firma, PIN On Line y CVM no soportado)

- PIN

Se trata del PIN del usuario, que se almacena en el chip en el mismo formato que en la banda magnética, es decir:

- Campo de control: ‘0’
- Longitud del PIN (formato BCD)
- Valor del PIN (BCD)
- ‘FF’ hex hasta completar 16 bytes

Este dato no tiene asignada ninguna etiqueta, ya que ni se almacena de la misma forma que el resto de los datos (está en una memoria protegida) ni se almacena en formato TLV.

- Número de presentaciones de PIN

  Límite máximo de intentos erróneos de PIN permitidas por la aplicación.

  Este dato, al igual que el PIN, tampoco tiene asignada ninguna etiqueta.

  Valor recomendado: 3, pero queda a elección del emisor.

1.4.3.4. Parámetros para Gestión de Riesgo Off Line

Las tarjetas EMV incorporan una serie de datos que permiten (a la propia tarjeta o al terminal donde está operando) realizar controles de riesgo sobre las operaciones realizadas en Off Line.

Estos controles se basan, sobre todo, en el uso de límites. Estos límites se pueden clasificar de diversas maneras:

* Según la magnitud sobre la que se aplican:
  - límites sobre el número total de operaciones
  - límites sobre el importe acumulado de las operaciones
* Según la acción a tomar cuando se rebasan:
  - límites inferiores, que provocan la obligatoriedad de conseguir la autorización mediante conexión On Line
  - límites superiores, que facultan al terminal a denegar la operación

* Según la moneda en la que se realiza la operación:
    - límites en moneda de la tarjeta
    - límites en otras monedas
* Según el país donde se realiza la operación:
    - límites en entorno nacional
    - límites en entorno no nacional

Dentro de los parámetros relativos a la gestión de riesgo Off Line, existen tres tipos diferentes:

a. Datos definidos por el estándar EMV
b. Datos definidos por MasterCard
c. Datos definidos por VISA Internacional

Cada una de los sistemas de pago (MasterCard y VISA), basándose en los parámetros propios y en los del estándar EMV, realizan el control del número de operaciones y de los importes de forma diferente.

A continuación se detallarán cuáles son los datos incluidos en cada uno de los tres grupos, para posteriormente explicar de qué forma realizan la gestión del riesgo a partir de esos datos tanto MasterCard como VISA Internacional.

a. Datos definidos en el estándar EMV

Estos parámetros forman parte del estándar EMV, por lo que cualquier tarjeta, sea VISA o MasterCard, debe contenerlos y utilizarlos apropiadamente.

- Gestión de Riesgo de la Tarjeta DOL1

  Este dato es una lista de etiquetas.

  Aunque está incluido en este grupo, en realidad ni la tarjeta ni el terminal utilizan este dato directamente para la gestión del riesgo Off Line; es utilizado por el terminal para saber qué datos debe proporcionar a la tarjeta para que ella calcule el criptograma de petición ARQC.

Etiqueta del dato: TAG ***8C***.

- Gestión de Riesgo de la Tarjeta DOL2

  Este dato también es una lista de etiquetas, en este caso se trata de los datos que el terminal debe proporcionar a la tarjeta una vez reciba respuesta a un ARQC desde el Host Emisor.

  Etiqueta del dato: TAG ***8D***.

- Códigos de Acción del Emisor (IACs)

  Estos códigos son mapas de bits que el emisor graba en la tarjeta, y que son recuperados de la misma por el terminal. Mediante estos códigos, el terminal conoce cuales son los condicionantes que provocarán que la operación se autorice o se deniegue en Off Line o que se deba pedir autorización On Line al Emisor.

  Existen tres mapas diferentes: uno para denegar Off Line (IAC-Default), otro para ir a On Line (IAC-On Line) y otro por defecto (IAC-Denial).

  Algunas de las condiciones que el terminal debe examinar son las siguientes:

    - No se ejecutó la autenticación Off Line
    - Fallo en la autenticación estática
    - Fallo en la autenticación dinámica
    - Faltan datos de la tarjeta
    - La tarjeta aparece en el fichero de excepciones del terminal
    - La tarjeta y el terminal tienen versiones de aplicación diferentes
    - La aplicación EMV de la tarjeta aún no está activa
    - La aplicación EMV de la tarjeta está caducada
    - El servicio solicitado no está permitido a la tarjeta
    - La tarjeta es nueva (aún no operó nunca)

- Verificación de usuario no satisfactoria
- CVM desconocido
- Límite de intentos de PIN excedidos
- PIN obligatorio y el terminal no tiene PIN PAD o no está operativo
- PIN obligatorio, el terminal tiene PIN PAD operativo pero no se introdujo PIN
- PIN On Line introducido
- Se ha excedido el "Floor Limit"
- Excedido el Límite Inferior de Operaciones Off Line consecutivas
- Excedido el Límite Superior de Operaciones Off Line consecutivas
- Operación seleccionada aleatoriamente para ser enviada On Line
- El comerciante está forzando el procesamiento On Line
- Autenticación de Emisor no satisfactoria
- Fallo al procesar scripts

El terminal evalúa las condiciones incluidas en los IACs recuperados de la tarjeta comparándolas con el Resultado de la Verificación del Terminal (TVR), y en función de esa evaluación realiza la acción pertinente (autorizar, denegar o pedir autorización en On Line).

A continuación se explican las diferencias de funcionamiento entre los tres IACs:

- *Códigos de acción del emisor por defecto (IAC-Default)*

  Cuando un terminal no tiene capacidad On Line, o ha pedido autorización On Line pero no ha recibido respuesta, utiliza el código de acción por defecto para saber qué condiciones deben cumplirse para poder solicitar a la tarjeta una autorización en Off Line (siempre y cuando se hayan superado las condiciones impuestas por el IAC-Denial).

Etiqueta del dato: TAG ***9F0D***.

- *Códigos de acción del emisor para denegar (IAC-Denial)*

  Mediante estos códigos se determina que condiciones se deben cumplir para que el terminal deniegue la operación en Off Line sin realizar ningún intento de ir a On Line.

  Etiqueta del dato: TAG ***9F0E***.

- *Códigos de acción del emisor para On Line (IAC-On Line)*

  Una vez superadas las condiciones impuestas por el IAC-Denial para no denegar en Off Line, el terminal, si tiene capacidad de ir a On Line, y se cumplen las condiciones del IAC-On Line, sólo puede autorizar la operación mediante solicitud en On Line al Emisor.

  Etiqueta del dato: TAG ***9F0F***.

- Límite Inferior Off Line

  Mediante este límite se fija el número máximo de transacciones consecutivas Off Line que puede autorizar la tarjeta antes de tener que pedir autorización al Emisor en On Line.

  Este límite sólo se utiliza en terminales On Line, no tiene sentido para terminales Off.

  Etiqueta del dato: TAG ***9F14***.

  Este dato tiene asociado por parte de MasterCard el nemotécnico ***LCOLL***.

- Límite Superior Off Line

  Mediante este límite se fija el número máximo de transacciones consecutivas Off Line que puede autorizar la tarjeta en un terminal Off. Sobrepasado este límite, se deniega la operación.

  Este límite sólo se utiliza en terminales Off, no tiene sentido para terminales On Line.

  Etiqueta del dato: TAG ***9F23***.

Este dato tiene asociado por parte de MasterCard el nemotécnico ***UCOLL***.

- Lista de objetos de datos del "Processing Options" (PDOL)

  Esta lista de etiquetas se la envía la tarjeta al terminal al inicio de la transacción para indicarle qué datos desea recibir la tarjeta (entre ellos, el código de moneda en el que se está realizando la transacción).

  MasterCard no utiliza este parámetro.

  Etiqueta del dato: TAG ***9F38***.

b. Datos definidos por MasterCard

El estándar EMV ha reservado un rango de TAGs para datos propietarios de los emisores (VISA y MasterCard). Los siguientes parámetros son propietarios de MasterCard, que los utiliza en la gestión de riesgo Off Line de sus tarjetas.

- Códigos de Acción del Emisor de la Tarjeta (CIACs)

  Estos CIACs (Card Issuer Action Codes) son similares a los IACs definidos en el estándar, ya que también se trata de listas de condiciones utilizadas para decidir si se puede autorizar o denegar una operación en Off Line o si se debe solicitar autorización al Emisor en On Line. Pero hay una diferencia fundamental: mientras que los IACs los utiliza el terminal para su gestión de riesgo y los compara con el TVR (también generado por el terminal), los CIACs los utiliza la tarjeta, comparándolos con el CVR. El CVR es el resultado de la verificación de la tarjeta, y es análogo al TVR del terminal.

  Sólo se utilizan en la personalización de tarjetas MasterCard; las tarjetas VISA, para realizar esta misma misión, utiliza las Acciones por Defecto de la Aplicación (ADA), en vez de los CIACs.

  Al igual que con los IACs, existen tres tipos de CIAC: para denegar (o Denial), para Off Line y para On Line.

  - *Códigos de acción del emisor de la Tarjeta - Denial (CIAC-Denial)*

    La tarjeta utiliza estos código para determinar en qué condiciones puede denegar una operación sin necesidad de solicitar autorización al Emisor en On Line.

Etiqueta del dato: TAG ***C3***.

- *Códigos de acción del emisor de la Tarjeta – Off Line (CIAC-Off Line)*

  Este código se utiliza en dos situaciones diferentes:

  - Si el terminal es Off Line, la tarjeta puede utilizar este código para denegar la transacción.

  - Si el terminal es On Line, y el CIAC On Line determinó que había que enviar una petición On Line al Emisor, y la petición ha sido respondida pero no se ha podido llevar a cabo la autenticación de Emisor, entonces es el CIAC Off Line el que permitirá a la tarjeta denegar la operación, en caso de cumplirse las condiciones correspondientes.

  Lógicamente, en cualquiera de los dos casos, se deben haber superado previamente las condiciones impuestas por el CIAC-Denial, ya que de lo contrario, la transacción se hubiese denegado directamente.

  Etiqueta del dato: TAG ***C4***.

- *Códigos de acción del emisor de la Tarjeta – On Line (CIAC-On Line)*

  Este código lo utiliza la tarjeta para determinar si debe pedir autorización On Line, en el caso en que se esté utilizando en un terminal On Line y se hayan superado las condiciones del CIAC Denial.

  Etiqueta del dato: TAG ***C5***.

- Máximo Importe Inferior Acumulado Off Line

  Este máximo se refiere a las operaciones Off Line realizadas de forma consecutiva. En el momento en que se pueda completar una operación On Line, los acumuladores se pondrán a cero.

  Si se excede este máximo, y el terminal tiene capacidad On Line, la transacción debe ser enviada On Line. Para terminales puramente Off Line, este límite no tiene validez.

  En principio, las operaciones que se tienen en cuenta son aquellas hechas en la misma moneda de la aplicación.

Si la moneda es distinta, este parámetro deja de tener validez, y el importe de la operación no se acumulará ni se realizará comparación alguna.

Etiqueta del dato: TAG ***CA***.

Este dato tiene asociado por parte de MasterCard el nemotécnico ***LMOLCA***.

- Máximo Importe Superior Acumulado Off Line

  Al igual que en el caso anterior, este máximo se refiere a las operaciones Off Line realizadas de forma consecutiva. En el momento en que se pueda completar una operación On Line, los acumuladores se pondrán a cero.

  Si se excede este máximo y el terminal no tiene capacidad On Line, la transacción se deniega. Para terminales On Line, este límite no tiene validez.

  En cuanto a operaciones en moneda diferente a la de la tarjeta, son aplicables a este límite las mismas consideraciones que en el límite anterior.

  Etiqueta del dato: TAG ***CB***.

  Este dato tiene asociado por parte de MasterCard el nemotécnico ***UMOLCA***.

- Control de la Aplicación

  Es un dato interno de la tarjeta, que se rellena durante la personalización y que fija el comportamiento de la tarjeta en determinadas circunstancias.

  De las características tratadas en este dato, la más relacionada con la gestión del riesgo es la que establece si la tarjeta debe o no inicializar los contadores Off Line cuando se ha realizado una autorización On Line pero no se ha realizado la Autenticación de Emisor.

  Etiqueta del dato: TAG ***D5***.

- Código de Acción de TVR de la Tarjeta

  Se trata de un código mediante el que el emisor establece las condiciones suficientes para que la tarjeta confirme la decisión, tomada por el terminal, de conectarse On Line.

Aunque se trata de un parámetro que aparentemente hace la misma función que el CIAC para On Line (establecer condiciones para conectarse On Line), hay una pequeña diferencia: el CIAC para On Line le permite a la tarjeta cuando recibe desde el terminal la solicitud de autorizar en Off, tanto permitir dicha autorización en Off como forzar ir a On Line. El código de TVR sólo se puede usar para ir a On Line, no para autorizar en Off Line.

Este parámetro sólo aparece en tarjetas EMV MasterCard con versión de aplicación MChip 2.1.

Etiqueta del dato: TAG ***C6***.

- Exponente del Factor de Control No Nacional

Mediante este exponente se calcula el valor del parámetro 'Factor de Control No Nacional' (siglas en inglés, NDCF). En concreto, NDCF = 2^n.

Este factor NDCF se utiliza como divisor de los Límites Inferior y Superior Off Line definidos por EMV (nemotécnicos ***LCOLL*** y ***UCOLL***, respectivamente), y los nuevos límites así calculados se utilizan en operaciones en las que el código de país del terminal difiere del código del país emisor o bien el código de moneda de la transacción no coincide con el código de moneda de la aplicación.

Ejemplo:

> Si el límite ***LCOLL*** es igual a 16 y el exponente n igual a 3, entonces el límite para operaciones en el extranjero o en monedas distintas de euro será igual a 2, ya que NDCF=2^3=8 y 16/8 = 2). Es decir, la tarjeta podrá realizar hasta 16 operaciones consecutivas en off, en entorno doméstico y en euros, antes de tener que pedir autorización On Line, pero sólo podrá realizar dos en el extranjero o en otra moneda.

Este parámetro sólo aparece en tarjetas EMV MasterCard con versión de aplicación MChip 2.1.

Etiqueta del dato: TAG ***CE***.

- Tabla de conversión de moneda

La inclusión de esta tabla de conversión permite el uso de hasta cinco monedas alternativas a la moneda de la aplicación.

La tabla contiene, para cada una de esas monedas, un ratio y un exponente de conversión que permiten convertir cualquier importe en una de esas cinco monedas en el importe equivalente en la moneda de la aplicación.

Este parámetro sólo aparece en tarjetas EMV MasterCard con versión de aplicación MChip 4.

Etiqueta del dato: TAG ***D1***.

- Tabla de chequeo adicional

  Esta tabla contiene valores que son comparados con los valores facilitados por el terminal durante la transacción; el resultado de esta comparación es una mapa de bits con ceros y unos (según coincidan o no los valores) que se graba en el CVR de la tarjeta.

  Este parámetro sólo aparece en tarjetas EMV MasterCard con versión de aplicación MChip 4.

  Etiqueta del dato: TAG ***D3***.

- Código de respuesta del ARPC

  Este dato es enviado por el Host Emisor junto con el ARPC de respuesta a una petición On Line realizada por la tarjeta. El Host Emisor puede mediante este dato indicarle a la tarjeta una serie de acciones que debe realizar a la recepción de la respuesta, o bien proporcionarle información útil que la tarjeta puede utilizar en futuras transacciones.

  Este parámetro sólo aparece en tarjetas EMV MasterCard con versión de aplicación MChip 4.

- Código de respuesta del ARPC por defecto

  Tiene el mismo formato que el código de respuesta de ARPC, y es utilizado por la tarjeta en aquellos casos en que no haya recibido ningún dato desde el Emisor durante una transacción On Line.

  Este parámetro sólo aparece en tarjetas EMV MasterCard con versión de aplicación MChip 4.

  Etiqueta del dato: TAG ***D6***.

- Longitud de datos de CDOL1

  Longitud de los datos que debe recibir la tarjeta del terminal. Estos datos los utiliza la tarjeta para generar los criptogramas.

  Este parámetro sólo aparece en tarjetas EMV MasterCard con versión de aplicación MChip 4.

  Etiqueta del dato: TAG ***C7***.

- Límites CFDC

  Las tarjetas EMV utilizan en cada transacción una clave diferente, denominada clave de sesión, que se deriva a partir de alguna de las claves de la tarjeta utilizando un número, que puede ser generado aleatoriamente, denominado número de sesión. Todo esto añade seguridad al sistema.

  Pero un terminal malintencionado puede intentar romper la clave mediante ataques de "fuerza bruta", uno de los cuales puede consistir en enviar diferentes combinaciones de datos pero manteniendo siempre el mismo número de sesión, de forma que la clave de sesión generada por la tarjeta sea siempre la misma.

  Para evitar esto, MasterCard establece un límite sobre el número de veces consecutivas que se puede utilizar la misma clave de sesión. Ese límite se denomina CFDC.

  En realidad se trata de tres límites, uno por cada clave de la tarjeta:

  - clave de integridad de scripts

  - clave de confidencialidad de scripts

  - clave de cálculo de criptogramas

  Este parámetro sólo aparece en tarjetas EMV MasterCard con versión de aplicación MChip 4.

- Límite del ATC

  Mediante este dato puede limitarse el número de transacciones que puede llegar a realizar una tarjeta. No se suele utilizar.

Este parámetro sólo aparece en tarjetas EMV MasterCard con versión de aplicación MChip 4.

- Límite del contador de script

  Mediante este dato puede limitarse el número de scripts que puede procesar una tarjeta en una misma transacción.

  Este parámetro sólo aparece en tarjetas EMV MasterCard con versión de aplicación MChip 4.

- Límite del contador global de script

  Mediante este dato puede limitarse el número de scripts que puede procesar una tarjeta a lo largo de toda su vida útil.

  Este parámetro sólo aparece en tarjetas EMV MasterCard con versión de aplicación MChip 4.

- Datos del ciclo de vida de la aplicación

  Los datos del ciclo de vida son 4:

  - Número de versión
  - ID Type Approval
  - ID Emisor de la Aplicación
  - ID Código de la Aplicación

  El "Número de versión", el "ID Type Approval" y el "ID Código de la Aplicación" son datos responsabilidad del personalizador, y transparentes para el Emisor.

  En cambio, el dato "ID Emisor de la Aplicación" le servirá al Emisor para identificar de forma inequívoca el personalizador y el lote de personalización.

  Este parámetro sólo aparece en tarjetas EMV MasterCard con versión de aplicación MChip 4.

  Etiqueta del dato: TAG ***9F7E***.

c. Datos definidos por VISA Internacional

- Acción por Defecto de la Aplicación

  Las Acciones por Defecto de la Aplicación (ADA, Application Default Action) cumplen en las tarjetas VISA una función parecida a la que realizan los CIACs en las tarjetas MasterCard: el emisor indica las acciones a tomar por la tarjeta ante ciertas condiciones excepcionales.

  Es un dato obligatorio si se realiza autenticación de emisor, si no está presente se considerará a cero por defecto.

  Etiqueta del dato: TAG ***9F52***.

- Indicador de Autenticación de Emisor

  Las tarjetas VISA utilizan este indicador cuando se deniega una operación: si el indicador marca como obligatoria la autenticación de emisor, y ésta no se llevó a cabo o tuvo resultado erróneo, se denegará la transacción (siempre que las acciones por defecto de la aplicación, ADA, así lo indiquen).

  Las tarjetas MasterCard no necesitan de este indicador para la denegación: les basta con que falle la autenticación o, si lo que sucede es que no se ha recibido, también pueden denegar, basándose en los CIACs de Denegación o de On Line.

  Etiqueta del dato: TAG ***9F56***.

- Código de moneda de la aplicación

  Moneda en la que se administra la tarjeta, de acuerdo a la norma ISO 4217.

  Este dato es usado internamente por las tarjetas VISA, y debe tener el mismo valor que el código de moneda del estándar EMV identificado con el TAG ***9F42***.

  Su valor debe ser ‘0978’ hex (euros).

  Etiqueta del dato: TAG ***9F51***.

- Código de país del emisor

  En este dato se guarda el código del país al que pertenece el emisor de la tarjeta, de acuerdo a la norma ISO 3166.

Este dato lo utilizan las tarjetas VISA cuando analizan las posibles restricciones geográficas sobre las transacciones. Debe tener el mismo valor que el código de país almacenado en el TAG ***5F28***.

Su valor debe ser '0724' hex (España).

Etiqueta del dato: TAG ***9F57***.

- Indicador geográfico

  Este dato lo utilizan las tarjetas VISA para determinar si la aplicación EMV es válida para efectuar transacciones nacionales o internacionales. Es obligatorio en las tarjetas que soportan restricciones geográficas.

  Posibles valores:

  "40" hex: aplicación sólo válida para transacciones internacionales

  "80" hex: aplicación sólo válida para transacciones nacionales

  "C0" hex: aplicación válida para transacciones nacionales e internacionales

  Este dato es propietario VISA. Las tarjetas MasterCard restringen el ámbito geográfico en el que pueden ser utilizadas mediante el Control de Uso de la Aplicación (AUC, TAG ***9F07***), un parámetro definido en el estándar.

  Etiqueta del dato: TAG ***9F55***.

- Código de moneda secundaria de la aplicación

  Este dato propietario VISA indica la moneda cuyos importes serán convertidos al importe equivalente en la moneda de la tarjeta. Este código cumple la norma ISO 4217.

  Es un dato obligatorio para tarjetas con capacidad de doble moneda.

  Etiqueta del dato: TAG ***9F76***.

- Factor de Conversión de Moneda

Este dato propietario VISA es un valor decimal usado para convertir el importe de las transacciones realizadas en moneda secundaria (TAG ***9F76***) en el equivalente en la moneda de la tarjeta (TAG ***9F51***).

Es un dato obligatorio para tarjetas con capacidad de doble moneda.

Etiqueta del dato: TAG ***9F73***.

- Límite total de importe acumulado Off Line

  Se utiliza en la gestión de riesgo realizada con el 1er Generate AC. Si el 'Importe total acumulado en operaciones Off Line consecutivas' supera este limite y el terminal tiene capacidad On Line, la transacción debe ser enviada On Line.

  Sólo se tienen en cuenta las operaciones Off Line consecutivas realizadas en la misma divisa de la aplicación (euros). Si la operación se realiza en la moneda secundaria, se utiliza el Límite total de importe acumulado Off Line – Doble moneda (TAG ***9F75***).

  Etiqueta del dato: TAG ***9F54***.

- Límite total de importe acumulado Off Line – doble moneda

  Se utiliza en la gestión de riesgo realizada con el 1er Generate AC. Si el 'Importe total acumulado en operaciones Off Line consecutivas con doble moneda' supera este límite y el terminal tiene capacidad On Line, la transacción debe ser enviada On Line.

  Se tienen en cuenta las operaciones Off Line consecutivas realizadas tanto en la divisa primaria como en la divisa secundaria de la aplicación (en este caso se convierte el importe al equivalente en la moneda primaria).

  Etiqueta del dato: TAG ***9F75***.

- Límite superior total de importe acumulado Off Line

  Se utiliza en la gestión de riesgo realizada con el 2º Generate AC, siempre que en el 1er Generate AC se solicitase la autorización On Line y no hubiese sido posible realizar la conexión. En este caso, se compara este límite con los dos contadores internos de la tarjeta, tanto con el de 'Importe total acumulado en operaciones Off Line consecutivas' como con el de 'Importe total acumulado en operaciones Off

Line consecutivas con doble moneda'. Si alguno de los dos supera el límite, la transacción se deniega.

Por tanto, este límite tiene en cuenta tanto las operaciones realizadas en la moneda primaria de la aplicación (euro) como las realizadas en la moneda secundaria.

Etiqueta del dato: TAG ***9F5C***.

- Límite total inferior de operaciones Off Line consecutivas

  Si este valor es excedido y el terminal tiene capacidad On Line, la transacción debe ser enviada On Line.

  Se tienen en cuenta todas las operaciones Off Line, independientemente de la moneda de la transacción y del país del terminal.

  Etiqueta del dato: TAG ***9F58***.

- Límite total superior de operaciones Off Line consecutivas

  Si este valor es excedido y el terminal no tiene capacidad On Line, la transacción se deniega.

  Se tienen en cuenta todas las operaciones Off Line, independientemente de la moneda de la transacción y del país del terminal.

  Etiqueta del dato: TAG ***9F59***.

- Límite total de operaciones Off Line consecutivas (Internacional – Moneda)

  En este caso se consideran operaciones internacionales aquellas en las que el código de moneda de la transacción es distinto del código designado por el emisor de la tarjeta.

  Si este valor es excedido y el terminal tiene capacidad On Line, la transacción debe ser enviada On Line.

  Etiqueta del dato: TAG ***9F53***.

- Límite total de operaciones Off Line consecutivas (Internacional – País)

En este caso se consideran operaciones internacionales aquellas en las que el código de país del emisor de la tarjeta es diferente del código de país del terminal.

Si este valor es excedido y el terminal tiene capacidad On Line, la transacción debe ser enviada On Line.

Etiqueta del dato: TAG ***9F72***.

- Límite de operaciones Off Line consecutivas internacionales

  En este caso se consideran operaciones internacionales tanto aquellas en las que el código de moneda de la transacción es distinto del código designado por el emisor de la tarjeta como aquellas en las que el código de país del emisor de la tarjeta es diferente del código de país del terminal.

  Si este valor es excedido y el terminal no tiene capacidad On Line, la transacción se deniega.

  Este dato es opcional, ya que sólo es soportado por tarjetas EMV cuyo chip tenga implementadas determinadas versiones del sistema operativo.

  Etiqueta del dato: TAG ***9F5E***.

- Disponible Importe Off Line Restante

  Este dato indica si se permite la recuperación del importe disponible para ser consumido Off Line.

  Este dato es opcional, ya que sólo es soportado por tarjetas EMV cuyo chip tenga implementadas determinadas versiones del sistema operativo.

  Etiqueta del dato: TAG ***9F5D***.

- Datos de la gestión de riesgo en transacciones VLP

  Las transacciones VLP ("VISA Low-Value Payment") son transacciones que pueden ser autorizadas por la tarjeta en Off Line y sin necesidad de ningún tipo de verificación del usuario. Es suficiente con que el importe de la transacción sea inferior a un importe máximo fijado por el Emisor y que queden fondos disponibles (existe un fondo inicial que se va disminuyendo con cada transacción VLP, y que sólo se "recarga" cuando se realiza una transacción On Line).

Las transacciones VLP sólo están soportadas por tarjetas VISA con versión 1.4.0 de su aplicación.

Las tarjetas que soportan transacciones VLP incluyen en su personalización los siguientes datos:

- Código de autorización VLP del Emisor (etiqueta: TAG **9F74**)
- Límite de fondos VLP (etiqueta: TAG **9F77**)
- Límite por transacción única VLP (etiqueta: TAG **9F78**)
- Fondos VLP disponibles (etiqueta: TAG **9F79**)

- Indicador de bloqueo mediante script

Con este indicador se marca si la tarjeta puede o no ser bloqueada permanentemente mediante un script.

Este indicador es exclusivo de VISA.

Las tarjetas MasterCard no admiten el uso de este indicador, por lo que el host emisor tendrá en exclusiva la capacidad de bloquear la tarjeta, no dando opción a la propia tarjeta de tomar dicha decisión.

Etiqueta del dato: TAG ***C5***.

Este TAG lo utiliza MasterCard para un uso totalmente diferente, en concreto para almacenar el "*CIAC On Line*", el código de acción del emisor de la tarjeta para ir a On Line. Esto es posible porque el estándar EMV reserva un rango de TAGs para datos propietarios de los emisores (VISA y MasterCard).

Datos definidos por los dos sistemas (MasterCard y VISA)

- Datos del emisor de la aplicación (IAD)

Se trata de datos propietarios de la aplicación, que deben ser transmitidos al Emisor en las transacciones On Line.

Algunos de los datos son comunes a tarjetas VISA y MasterCard:

- Índice de derivación de la clave

- Número de versión del criptograma

- CVR (Resultado de la verificación de la tarjeta)

Las tarjetas VISA añaden a estos unos "datos discrecionales", y las MasterCard el DAC/IDN.

Etiqueta del dato: TAG ***9F10***.

1.4.3.5. Datos criptográficos

Los datos criptográficos grabados en el chip EMV se usan para garantizar la seguridad en las transacciones EMV.

A continuación se especifican cuáles son esos datos, aportando en algunos casos información adicional respecto a lo ya expuesto en los apartados de "*Seguridad Off Line (criptografía asimétrica)*" y "*Seguridad On Line (criptografía simétrica)*".

Datos de criptografía asimétrica

- SDA Tag List

  Este dato es una lista con las etiquetas de los datos primitivos incluidos en la firma digital de datos estáticos de la aplicación (firma SDA).

  Su valor por defecto es 82 (es decir, en la lista sólo se incluiría el "Perfil de Intercambio de la Aplicación" o AIP).

  Etiqueta del dato: TAG ***9F4A***.

- Índice de Derivación de la Clave Pública de CA

  Este dato es enviado por la tarjeta al terminal para que éste sepa cual de las claves públicas de CA (VISA o MasterCard) tiene que utilizar para comprobar el certificado de la clave pública de emisor residente en la tarjeta.

  Etiqueta del dato: TAG ***8F***.

- Exponente y Resto de la Clave Pública del Emisor

  El Exponente y el Resto son los dos datos característicos de la clave pública de emisor residente en la tarjeta.

Etiquetas de los datos: TAGs ***9F32*** (Exponente) y ***92*** (Resto).

- Certificado de la Clave Pública del Emisor

  Este dato lo genera la autoridad certificadora, aplicando su clave de CA sobre la clave pública de emisor. Con este certificado se garantiza la validez de la clave pública del emisor de la tarjeta.

  Etiqueta del dato: TAG ***90***.

- Firma de datos estáticos de la Aplicación

  Este dato es una firma digital, generada por el emisor en la fase de personalización, a partir de ciertos datos característicos de la tarjeta.

  Esta firma se utiliza en el proceso de autenticación estática de datos, asegurando la integridad de los datos firmados.

  Etiqueta del dato: TAG ***93***.

- Certificado de la Clave Pública de la Tarjeta

  Este dato lo genera la entidad emisora, aplicando su clave de emisor sobre la clave pública de la tarjeta. Con este certificado se garantiza la validez de la clave pública de la tarjeta.

  Es obligatorio incluir este dato si se desea que la tarjeta soporte autenticación dinámica de datos.

  Etiqueta del dato: TAG ***9F46***.

- Exponente y Resto de la Clave Pública de la Tarjeta

  El Exponente y el Resto son los dos datos característicos de la clave pública de la tarjeta.

  Es obligatorio incluir estos dos datos si se desea que la tarjeta soporte autenticación dinámica de datos.

  Etiquetas de los datos: TAGs ***9F47*** (Exponente) y ***9F48*** (Resto).

- Clave Privada de la Tarjeta

Es obligatorio incluir este dato si se desea que la tarjeta soporte autenticación dinámica de datos.

Las claves privadas no se almacenan en la tarjeta de la misma forma que el resto de datos; se guardan en memorias especiales, que se borran al intentar leerlas desde el exterior de la tarjeta, y sólo son accesibles por el módulo criptográfico del propio chip, que es el único que necesita usarla.

Por tanto, no se almacenan como estructuras TLV ni tienen asociado ningún TAG.

- Certificado de la Clave Pública para el Cifrado de PIN

  Este dato lo genera la entidad emisora, aplicando su clave de emisor sobre la clave pública de cifrado de PIN. Con este certificado se garantiza la validez de la clave pública de cifrado de PIN.

  Es obligatorio incluir este dato si se desea que la tarjeta soporte verificación del PIN cifrado Off Line.

  Etiqueta del dato: TAG ***9F2D***.

- Exponente y Resto de la Clave Pública para el Cifrado de PIN

  El Exponente y el Resto son los dos datos característicos de la clave pública para el Cifrado de PIN.

  Es obligatorio incluir este dato si se desea que la tarjeta soporte verificación del PIN cifrado Off Line.

  Etiquetas de los datos: TAGs ***9F2E*** (Exponente) y ***9F2F*** (Resto).

- Clave Privada para el Cifrado de PIN

  Es obligatorio incluir este dato si se desea que la tarjeta soporte verificación del PIN cifrado Off Line.

  Las claves privadas no se almacenan en la tarjeta de la misma forma que el resto de datos; se guardan en memorias especiales, que se borran al intentar leerlas desde el exterior de la tarjeta, y sólo son accesibles por el módulo criptográfico del propio chip, que es el único que necesita usarla.

  Por tanto, no se almacenan como estructuras TLV ni tienen asociado ningún TAG.

Datos de criptografía simétrica

- Número de Versión del Criptograma

  El número de versión del criptograma es un dato utilizado por el emisor para calcular las claves de la tarjeta a partir de una clave maestra, mediante un proceso denominado "derivación".

  La tarjeta deberá por tanto transmitir este dato al Emisor en las transacciones On Line.

  Este dato forma parte de los "Datos del Emisor de la Aplicación" (TAG ***9F10***), ya mencionados en el apartado "*Parámetros para Gestión de Riesgo Off Line*".

- Índice de derivación de la clave

  Este índice identifica dos cosas:

  - versión de las claves simétricas a utilizar
  - método de diversificación se utilizó para generar las claves de la tarjeta

  En el estándar EMV hay definido un método de diversificación que genera las claves de la tarjeta (K_{AC}, K_{SMI} y K_{SMC}) por derivación de 3 claves maestras de emisor:

  - Clave para cálculo de AC's (MK_{AC})
  - Clave para protección en integridad (MK_{SMI})
  - Clave para protección en confidencialidad (MK_{SMC})

  Este método es sólo una propuesta de EMVco, pero no es obligatorio utilizarlo. De hecho, Euro6000 tiene definido un método propietario que utiliza con las tarjetas MasterCard, en el que sólo define una clave maestra inicial, diferente para cada BIN, denominada clave única por BIN (MK_{BIN}).

  A partir de esta clave única, mediante derivación, se generan las tres claves de la tarjeta (K_{AC}, K_{SMI} y K_{SMC}).

  Para VISA, este índice de derivación forma parte de los "Datos del Emisor de la Aplicación" (TAG ***9F10***), ya mencionados en el apartado "*Parámetros para Gestión*

de Riesgo Off Line". En cambio, MasterCard lo identifica mediante una etiqueta específica, el TAG ***C8***.

- Clave diversificada para el cálculo de ACs (MK_{AC})

  Clave única por tarjeta, utilizada para el cálculo de los criptogramas de aplicación (ACs).

  Al igual que en el caso de la parte privada de las claves asimétricas, las claves simétricas tampoco se almacenan en la tarjeta de la misma forma que el resto de datos; se guardan en memorias especiales, que se borran al intentar leerlas desde el exterior de la tarjeta, y sólo son accesibles por el módulo criptográfico del propio chip, que es el único que necesita usarlas.

  Por tanto, no se almacenan como estructuras TLV ni tienen asociado ningún TAG.

- Clave diversificada para protección en integridad (MK_{SMI})

  Clave única por tarjeta, utilizada para protección en integridad de los scripts.

  Al igual que en el caso de la parte privada de las claves asimétricas, las claves simétricas tampoco se almacenan en la tarjeta de la misma forma que el resto de datos; se guardan en memorias especiales, que se borran al intentar leerlas desde el exterior de la tarjeta, y sólo son accesibles por el módulo criptográfico del propio chip, que es el único que necesita usarlas.

  Por tanto, no se almacenan como estructuras TLV ni tienen asociado ningún TAG.

- Clave diversificada para protección en confidencialidad (MK_{SMC})

  Clave única por tarjeta, utilizada para protección de datos confidenciales en los scripts.

  Al igual que en el caso de la parte privada de las claves asimétricas, las claves simétricas tampoco se almacenan en la tarjeta de la misma forma que el resto de datos; se guardan en memorias especiales, que se borran al intentar leerlas desde el exterior de la tarjeta, y sólo son accesibles por el módulo criptográfico del propio chip, que es el único que necesita usarlas.

  Por tanto, no se almacenan como estructuras TLV ni tienen asociado ningún TAG.

- Clave diversificada del IDN (MK_{IDN})

Clave única por tarjeta, utilizada para el cálculo del número dinámico de tarjeta (IDN).

Es obligatorio incluir este dato si se desea que la tarjeta soporte autenticación dinámica.

Al igual que en el caso de la parte privada de las claves asimétricas, las claves simétricas tampoco se almacenan en la tarjeta de la misma forma que el resto de datos; se guardan en memorias especiales, que se borran al intentar leerlas desde el exterior de la tarjeta, y sólo son accesibles por el módulo criptográfico del propio chip, que es el único que necesita usarlas.

Por tanto, no se almacenan como estructuras TLV ni tienen asociado ningún TAG.

1.4.4. Clasificación y almacenamiento de los Parámetros EMV

Para poder decidir cuántas y cuáles van a ser las estructuras de datos en las que se van a almacenar los parámetros en la aplicación, es necesario clasificarlos, tomando como criterio la forma de almacenarlos.

Una posible agrupación sería la siguiente:

1. Datos propios de la tarjeta
2. Datos propios de la tarjeta exclusivos de EMV
3. Datos asignables por perfiles
4. Datos asignables por marca
5. Datos de criptografía
6. Datos específicos del personalizador
7. Otros datos no almacenados en BDD

A continuación se repasa cuáles son los datos contenidos en cada grupo, y cómo se almacenarán.

1.4.4.1. Datos propios de la tarjeta

En este grupo se incluirán los siguientes:

TAG	Descripción
57	Datos equivalentes de Pista 2
5A	PAN
5F20	Nombre de usuario
5F24	Fecha de expiración de la aplicación
5F25	Fecha de activación de la aplicación
5F2D	Lenguaje preferente de la aplicación
5F30	Código de servicio
5F34	Número de secuencia de PAN
9F1F	Datos Discrecionales de Pista 1
9F20	Datos Discrecionales de Pista 2

Todos estos datos ya existían en la tabla de Tarjetas de la BDD de la aplicación con anterioridad a EMV, por lo que no será necesario habilitar nuevos campos para almacenarlos.

1.4.4.2. Datos propios de la tarjeta exclusivos de EMV

En este grupo se incluirán los siguientes:

TAG	Descripción
9F14	Límite Inferior Off Line
9F23	Límite Superior Off Line
9F53	Límite total de operaciones Off Line consecutivas (Internacional-Moneda) (VISA)
9F54	Límite total de importe acumulado Off Line (VISA)

9F58	Límite total inferior de operaciones Off Line consecutivas (VISA)
9F59	Límite total superior de operaciones Off Line consecutivas (VISA)
9F5C	Límite superior total de importe acumulado Off Line (VISA)
9F72	Límite total de operaciones Off Line consecutivas (Internacional-País) (VISA)
9F75	Límite total de importe acumulado Off Line – Doble moneda (VISA)
CA	Máximo Importe Inferior Acumulado Off Line (MasterCard)
CB	Máximo Importe Superior Acumulado Off Line (MasterCard)

Todos estos datos son límites utilizados por la tarjeta en Off Line, que pueden asignarse libremente, por lo que se deberían habilitar campos en la tabla de Tarjetas para almacenarlos. En realidad no se añadirán campos a las tablas de Tarjetas ya existentes en la aplicación, sino que se crearán tablas nuevas, exclusivas para almacenar los datos EMV particulares de cada tarjeta.

1.4.4.3. Datos asignables por perfiles

En este grupo se incluirán los siguientes:

TAG	**Descripción**
82	Perfil de intercambio de la aplicación (AIP)
8E	Lista CVM (métodos de verificación de usuario)
9F07	Control de Uso de la Aplicación
9F0D	Código de Acción del Emisor Default (IAC-Default)
9F0E	Código de Acción del Emisor Denial (IAC- Denial)
9F0F	Código de Acción del Emisor On Line (IAC-On Line)
9F52	Acción por Defecto de la Aplicación (ADA) (VISA)

9F55 Indicador geográfico (VISA)

9F56 Indicador de la autenticación de emisor (VISA)

9F73 Factor de conversión de moneda (VISA)

9F76 Código de moneda secundaria de la aplicación (VISA)

C3 Código de acción del emisor de la tarjeta Denial (CIAC-Denial) (MasterCard)

C4 Código de acción del emisor de la tarjeta Off Line (CIAC-Off Line) (MasterCard)

C5 Código de Acción del Emisor de la tarjeta On Line (CIAC-On Line) (MasterCard)

Indicador de bloqueo mediante script (VISA)

C6 Código de Acción de TVR de la Tarjeta (MasterCard)

C7 Longitud de datos de CDOL1 (MasterCard)

CE Exponente del Factor de Control No Nacional (MasterCard)

D1 Tabla de conversión de moneda

D3 Tabla de chequeo adicional

D5 Control de la Aplicación (MasterCard)

D6 Código de respuesta del ARPC por defecto

Todos estos datos no se van a asignar individualmente a cada tarjeta, sino de forma conjunta a perfiles.

1.4.4.4. Datos asignables por marca

En este grupo se incluirán los siguientes:

TAG	Descripción
4F	Identificador de la aplicación
50	Nombre de la aplicación
5F28	Código de país de emisor
84	Nombre del Fichero Dedicado (DF)
87	Indicador de prioridad de la aplicación
8C	Gestión de riesgo de la tarjeta DOL1 (CDOL1)
8D	Gestión de riesgo de la tarjeta DOL2 (CDOL2)
94	Localizador de ficheros de la aplicación (AFL)
9F08	Número de Versión de la Aplicación
9F38	Lista de objeto de datos del "processing options" (PDOL)
9F42	Código de la moneda de la aplicación
9F44	Exponente de la moneda de la aplicación
9F51	Código de moneda del Emisor (VISA)
9F57	Código de país del Emisor (VISA)

En este caso, la asignación de valores va a depender exclusivamente de la marca de la tarjeta (MasterCard o VISA). Estos datos se definirán en la herramienta de personalización, no es necesario definir ningún almacenamiento específico en la BDD.

1.4.4.5. Datos de criptografía

En este grupo se incluirán los siguientes:

TAG	Descripción
8F	Índice de derivación de la clave pública de CA

90	Certificado de la clave pública del Emisor
92	Resto de la clave pública del Emisor
93	Firma de los datos estáticos
9F10	Datos del Emisor de la Aplicación
9F2D	Certificado de la clave pública para el cifrado del PIN
9F2E	Exponente de la clave pública para el cifrado del PIN
9F2F	Resto de la clave pública para el cifrado del PIN
9F32	Exponente de la clave pública del Emisor
9F46	Certificado de la clave pública de la Tarjeta
9F47	Exponente de la clave pública de la Tarjeta
9F48	Resto de la clave pública de la Tarjeta
9F4A	SDA Tag List
C8	Índice de derivación de la clave (MasterCard)

Estos datos criptográficos están almacenados en el módulo criptográfico de la entidad, y de allí serán tomados directamente por la herramienta de personalización. Por tanto, no es necesario definir ningún almacenamiento específico para ellos en la BDD.

1.4.4.6. Datos específicos del personalizador

En este grupo se incluirán los siguientes:

TAG	**Descripción**
9F7E	Datos del Ciclo de Vida de la Aplicación (MasterCard)

Este dato es generado por el propio personalizador, y no se va a almacenar en la BDD.

1.4.4.7. Otros datos no almacenados en BDD

En este grupo se incluirán los siguientes:

TAG	Descripción
9F5D	Disponible Importe Off Line Restante (VISA)
9F5E	Límite de operaciones Off Line consecutivas internacionales (VISA)
9F74	Código de autorización VLP del Emisor (VISA)
9F77	Límite de fondos VLP (VISA)
9F78	Límite por transacción única VLP (VISA)
9F79	Fondos VLP Disponibles (VISA)

Estos datos no se almacenarán en la BDD de la entidad porque no se van a incluir en la personalización de las tarjetas, al corresponder a datos demasiado ligados a versiones específicas de los chips.

1.4.5. Parámetros EMV de Entidad

Además de los parámetros EMV mencionados en el apartado anterior, y que van grabados en la tarjeta en forma de estructuras TLV, existen otros no incluidos en el chip, que deben ser establecidos por la entidad y que marcarán su comportamiento general en algunos aspectos. Todas las tarjetas de la entidad, sean de la marca que sean, funcionarán según ese patrón de comportamiento.

Estos parámetros, cuyo valor debe establecer la entidad, son los siguientes:

- Control sobre la primera transacción de una tarjeta.

  Este parámetro (y el siguiente) tienen como función evitar el mal uso de las tarjetas nuevas controlando la ejecución de la primera transacción.

  Existen dos formas de controlar si una tarjeta opera por primera vez:

  1. Indicador de tarjeta nueva: este indicador se desactiva cuando se produce la primera autorización On Line correcta del Emisor.

     Este control es realizado tanto por la tarjeta como por el terminal.

  2. Fecha de activación: la tarjeta no se activa hasta que no se alcanza la fecha indicada por este parámetro.

Este control sólo lo realiza el terminal.

El uso de la primera opción es más seguro, pero obliga a forzar que la primera transacción se realice On Line, y en un entorno adaptado a EMV, ya que la tarjeta debe ser regrabada para marcarla como ya usada (no nueva).

La segunda opción no necesita de ninguna regrabación, por lo que la primera transacción puede realizarse también en un entorno no adaptado a EMV.

Además, esta segunda opción permite optar entre:

- forzar que la ejecución de la primera transacción se realice On Line o,

- simplemente intentar realizar la primera transacción en On Line, pero permitir que se pueda realizar en Off Line siempre que no se pueda intentar en On Line (ojo, sólo en el caso en que no se pueda intentar; si se deniega en On Line, ya no se intenta en Off Line).

VISA recomienda el uso del indicador, aunque en una primera fase (hasta que la infraestructura de oficinas y cajeros estuvo adaptada a EMV), recomendó el uso de la fecha de activación.

MasterCard usa la fecha de activación como único método para identificar las tarjetas nuevas.

Además, el uso de la fecha de activación obliga a informar otro nuevo parámetro de entidad para fijar el número de días a añadir a la fecha de alta para calcular la fecha de activación de una tarjeta EMV.

La fecha de activación es un dato perteneciente al estándar, identificado por el TAG ***5F25***.

- Uso de Scripts de Emisor.

Este parámetro se utilizará para indicar si la aplicación va a utilizar Scripts de Emisor.

Independientemente de que este parámetro permita el uso de scripts, se podrá prohibir dicho uso para determinadas tarjetas, mediante el establecimiento de excepciones.

Los scripts sólo se utilizan en la fase de autorización. Pese a ello, es necesario conocer, durante la fase de personalización, si se va a hacer uso o no de dichos scripts, para decidir si se graban o no determinados datos en el chip.

1.4.6. Desarrollos y adaptaciones propuestos

* Nueva tabla de BDD *Datos de Tarjetas EMV*

Sólo los datos relacionados con los límites para gestión de riesgo Off Line van a almacenarse en la tabla de datos de tarjetas EMV, cuya definición será la siguiente:

TEMV DATOS DE TARJETAS EMV		
Clave Única**:** **TEMVPAN (PAN de la tarjeta)**		
Nombre del campo	**Longitud**	**Descripción**
TEMVPAN	DEC (16,0)	PAN de la Tarjeta
TEMV9F14	DEC (3,0)	Límite Inferior Off Line
TEMV9F23	DEC (3,0)	Límite Superior Off Line
TEMV9F53	DEC (3,0)	Límite total de operaciones Off Line consecutivas (Internacional-Moneda) (VISA)
TEMV9F54	DEC (8,2)	Límite total de importe acumulado Off Line (VISA)
TEMV9F58	DEC (3,0)	Límite total inferior de operaciones Off Line consecutivas (VISA)
TEMV9F59	DEC (3,0)	Límite total superior de operaciones Off Line consecutivas (VISA)
TEMV9F5C	DEC (8,2)	Límite superior total de importe acumulado Off Line (VISA)

TEMV9F72	DEC (3,0)	Límite total de operaciones Off Line consecutivas (Internacional-País) (VISA)
TEMV9F75	DEC (8,2)	Límite total de importe acumulado Off Line – Doble moneda (VISA)
TEMVCA	DEC (8,2)	Máximo Importe Inferior Acumulado Off Line (MasterCard)
TEMVCB	DEC (8,2)	Máximo Importe Superior Acumulado Off Line (MasterCard)

* Nueva tabla de BDD *Perfiles EMV*

La clave de esta tabla será un número, de libre designación por el Emisor.

Este número deberá posteriormente asignado a todas las tarjetas para las que se desee que sus datos EMV se ajusten a los establecidos en ese número de perfil.

Dentro de los datos del perfil se incluirá la marca de la tarjeta para la que es válido el perfil.

La tabla de Perfiles EMV incluirá de nuevo todos los límites incluidos en la tabla TEMV, pero sólo a efectos de asignación a las tarjetas por defecto, en caso de que no se les asignen valores individuales.

Por supuesto, esta tabla también incluirá todos aquellos datos que se han definido más arriba como específicos del perfil.

PEMV DATOS DE PERFILES EMV		
Clave Única**:** **PEMVNPER (Número de Perfil)**		
Nombre del campo	**Longitud**	**Descripción**

PEMVNPER	DEC (3,0)	Número de Perfil
PEMVMARCA	CHAR (2)	Marca (VISA o MasterCard) de las tarjetas a las que puede ser asignado este perfil
PEMV9F14	DEC (3,0)	Límite Inferior Off Line
PEMV9F23	DEC (3,0)	Límite Superior Off Line
PEMV9F53	DEC (3,0)	Límite total de operaciones Off Line consecutivas (Internacional-Moneda) (VISA)
PEMV9F54	DEC (8,2)	Límite total de importe acumulado Off Line (VISA)
PEMV9F58	DEC (3,0)	Límite total inferior de operaciones Off Line consecutivas (VISA)
PEMV9F59	DEC (3,0)	Límite total superior de operaciones Off Line consecutivas (VISA)
PEMV9F5C	DEC (8,2)	Límite superior total de importe acumulado Off Line (VISA)
PEMV9F72	DEC (3,0)	Límite total de operaciones Off Line consecutivas (Internacional-País) (VISA)
PEMV9F75	DEC (8,2)	Límite total de importe acumulado Off Line – Doble moneda (VISA)
PEMVCA	DEC (8,2)	Máximo Importe Inferior Acumulado Off Line (MasterCard)
PEMVCB	DEC (8,2)	Máximo Importe Superior Acumulado Off Line (MasterCard)
PEMV82	2 bytes HEX	Perfil de intercambio de la aplicación (AIP)
PEMV8E	8 bytes HEX	Lista CVM (métodos de verificación de usuario)
PEMV9F07	2 bytes HEX	Control de Uso de la Aplicación

PEMV9F0D	5 bytes HEX	Código de Acción del Emisor Default (IAC-Default)
PEMV9F0E	5 bytes HEX	Código de Acción del Emisor Denial (IAC- Denial)
PEMV9F0F	5 bytes HEX	Código de Acción del Emisor On Line (IAC-On Line)
PEMV9F52	2 bytes HEX	Acción por Defecto de la Aplicación (ADA) (VISA)
PEMV9F55	1 byte HEX	Indicador geográfico (VISA)
PEMV9F56	1 byte HEX	Indicador de la autenticación de emisor (VISA)
PEMV9F73	4 bytes HEX	Factor de conversión de moneda (VISA)
PEMV9F76	2 bytes HEX	Código de moneda secundaria de la aplicación (VISA)
PEMVC3	3 bytes HEX	Código de acción del emisor de la tarjeta Denial (CIAC-Denial) (MasterCard)
PEMVC4	3 bytes HEX	Código de acción del emisor de la tarjeta Off Line (CIAC-Off Line) (MasterCard)
PEMVC5	3 bytes HEX	Código de Acción del Emisor de la tarjeta On Line (CIAC-On Line) (MasterCard) ó Indicador de bloqueo mediante script (VISA)
PEMVC6	5 bytes HEX	Código de Acción de TVR de la Tarjeta (MasterCard)
PEMVC7	1 byte HEX	Longitud de datos de CDOL1 (MasterCard)
PEMVCE	1 byte HEX	Exponente del Factor de Control No Nacional (MasterCard)

PEMVD1	19 bytes HEX	Tabla de conversión de moneda
PEMVD3	12 bytes HEX	Tabla de chequeo adicional
PEMVD5	2 bytes HEX	Control de la Aplicación (MasterCard): 1 byte para MChip 2.1 2 bytes para MChip 4
PEMVD6	2 bytes HEX	Código de respuesta del ARPC por defecto

* Nueva tabla de BDD *Límites máximos por Perfil EMV*

Esta tabla, cuya clave será el número de perfil, contendrá los límites máximos que el terminalista podrá asignar a una tarjeta perteneciente a ese perfil.

Sólo se hace referencia a los topes máximos; para los límites inferiores no habrá limitación (podrán variar desde cero hasta el valor que tenga el correspondiente límite superior).

LMPE LÍMITES MÁXIMOS POR PERFIL EMV		
Clave Única**:** **LMPENPER (Número de perfil)**		
Nombre del campo	**Longitud**	**Descripción**
LMPENPER	DEC (3,0)	Número de Perfil
LMPE9F23	DEC (3,0)	Máximo valor del campo TEMV9F23
LMPE9F53	DEC (3,0)	Máximo valor del campo TEMV9F53
LMPE9F54	DEC (8,2)	Máximo valor del campo TEMV9F54

LMPE9F59	DEC (3,0)	Máximo valor del campo TEMV9F59
LMPE9F5C	DEC (8,2)	Máximo valor del campo TEMV9F5c
LMPE9F72	DEC (3,0)	Máximo valor del campo TEMV9F72
LMPE9F75	DEC (8,2)	Máximo valor del campo TEMV9F75
LMPECB	DEC (8,2)	Máximo valor del campo TEMVCB

* Nueva tabla de BDD *Parámetros EMV a nivel de Entidad*

Además de los parámetros EMV con estructura TLV, que se graban en la tarjeta, existen otros parámetros de comportamiento general que deben ser definidos y fijados por la entidad. Todas las tarjetas de la entidad, sean de la marca que sean, funcionarán según ese patrón de comportamiento.

Estos parámetros se guardarán en una nueva tabla de BDD, que contendrá un único elemento para cada entidad (precisamente la entidad es la clave del registro):

EMVE PARÁMETROS EMV A NIVEL DE ENTIDAD		
Clave Única**:** **EMVECSB (Código de entidad -CSB-)**		
Nombre del campo	**Longitud**	**Descripción**
EMVECSB	DEC (4,0)	CSB de la entidad
EMVEC1TX	CHAR (1)	Tipo de parámetro EMV utilizado para el control de la primera transacción de una tarjeta nueva. Posibles valores: - 'F' Fecha de activación

		- 'N' Indicador de tarjeta nueva
EMVEDIAS	DEC (3,0)	Número de días desde la fecha de alta hasta la fecha de activación. Sólo se utiliza si CTRLPRITX = 'F'
EMVEUSCR	CHAR (1)	Indicador de uso de scripts de Emisor. Posibles valores: - 'S' Sí se usan - 'N' No se usan

* Modificar tabla de BDD *Productos de Tarjeta*:

  En la actual tabla de BDD de Productos de Tarjeta de la Entidad deberá incluirse un nuevo campo para almacenar el perfil EMV que se asignará (por defecto) a las tarjetas de ese producto.

  La identificación de este perfil es un número, el mismo que es clave a su vez de la tabla de perfiles EMV ***PEMV*** (campo PEMVNPER).

  Además, habrá que asegurarse de que la marca del Producto (VISA o MasterCard) sea coherente con la marca del perfil (campo PEMVMARCA de la tabla ***PEMV***)

* Nueva operatoria de terminal para *Mantenimiento de Límites EMV de Tarjetas*

  Mediante esta operatoria se permite a un terminalista asignar a una tarjeta los parámetros para control de Riesgo Off Line contenidos en la tabla ***TEMV***.

  Se capturarán por pantalla los nuevos límites, y se comprobará que no superan los topes máximos almacenados en la tabla ***LMPE***.

* Nueva operatoria de terminal para *Mantenimiento de Perfiles EMV*

  Mediante esta operatoria se permitirá las operaciones típicas de alta, baja, consulta y modificación de perfiles (es decir, de los datos contenidos en ***PEMV***).

Se validará que los Límites de Control de Riesgo Off asignables por defecto a las tarjetas no excederán de los topes máximos almacenados en la tabla ***LMPE***.

Una modificación en las características de un perfil hará que todas las tarjetas a las que a partir de ese momento se les asigne ese perfil, se estampen con esa modificación en sus características particulares.

1.5. CIRCUITO DE PERSONALIZACIÓN

La naturaleza de los nuevos datos EMV obliga al Emisor a proteger la integridad y confidencialidad de esos datos, asegurando la comunicación con el personalizador mediante un método seguro.

La forma de comunicarse entre el Emisor y el Personalizador es mediante el envío del denominado Fichero de Personalización.

Sobre este Fichero de Personalización se concentran todos los procesos necesarios para la generación y gestión de datos EMV:

- Generación y Gestión de Datos de usuario
- Definición y Gestión de Perfiles
- Generación y Gestión de Claves EMV

A continuación se describirá la forma en que se protegerá el fichero de personalización y de forma especial, el PIN de la tarjeta.

1.5.1. Protección del Fichero de Personalización

La protección del fichero de personalización tiene dos objetivos: protección en integridad y protección en confidencialidad. A continuación se repasa cómo conseguir ambas.

1.5.1.1. Protección en Integridad.

La protección en integridad significa que los datos enviados por el Emisor deben llegar de manera íntegra y sin manipular al personalizador. Existen múltiples métodos criptográficos para hacer esto, por ello, la forma más rápida de poner en marcha esta protección es utilizar el método que ya utilice el personalizador en sus comunicaciones con otras entidades emisoras.

1.5.1.2. Protección en Confidencialidad.

Varios datos de los que se envían en el fichero de personalización, son de naturaleza confidencial, como por ejemplo el PAN de la tarjeta y el PIN.

Para evitar que accesos malintencionados puedan hacerse con estos datos confidenciales, se hace necesario proteger criptográficamente estos datos, es decir, deberán viajar cifrados en el Fichero de Personalización.

Al igual que en el caso de la protección en integridad, lo más rápido para el Emisor es adoptar el proceso que a tal efecto esté utilizando ya el Personalizador en sus comunicaciones con otras entidades emisoras.

1.5.2. Tratamiento del PIN EMV

El PIN EMV (denominado también PIN Off Line) permite a la tarjeta verificar la identidad del usuario de forma Off Line. Este dato es, por tanto, especialmente importante, y sólo el usuario debería conocerlo.

El Emisor puede optar o no porque sus tarjetas soporten este método de verificación. En caso afirmativo, deberá comunicar al Personalizador el valor del PIN, convenientemente cifrado, ya que nunca se debe tener acceso en claro a este dato durante el proceso de personalización.

Además, el Emisor ha de asegurarse de que el personalizador es capaz de grabar el PIN (en claro) en la tarjeta sin tener acceso a su valor en ningún momento.

Al igual que en el caso de la protección del resto de datos, lo más rápido para el Emisor es adoptar el método de protección del PIN que esté utilizando ya el Personalizador en sus comunicaciones con otras entidades emisoras.

1.5.3. Fichero de Respuesta

Una vez finalizada la personalización de las tarjetas, el Personalizador deberá enviar al Emisor un fichero de respuesta para comunicarle qué tarjetas han sido personalizadas correctamente y cuáles no.

1.5.4. Desarrollos y adaptaciones propuestos

* Nuevos procesos batch de *Protección en Integridad y Confidencialidad del Fichero de Personalización (incluido el PIN Off Line)*

  Como se ha comentado en todos los casos, la definición de estos procesos queda a expensas de la elección del Personalizador por parte del Emisor y de los procesos que dicho Personalizador aporte.

* Nuevo proceso batch de *Tratamiento del Fichero de Respuesta del Personalizador*

  Este batch procesará el fichero recibido del personalizador en respuesta al Fichero de Personalización, y para aquellas tarjetas que no hayan podido ser personalizadas, generará un registro en un fichero de rechazos, que deberá ser

examinado por el departamento de Medios de Pago de la Entidad, corregido en aquello que sea necesario, y marcado como pendiente de reenvío.

* Nuevo proceso batch de *Reenvío de Tarjetas rechazadas por el Personalizador.*

  Este proceso recogerá del fichero de rechazos aquellos que hayan sido corregidos y que estén pendientes de reenvío, y los añadirá al proceso usual de generación del Fichero de Personalización.

2. ADAPTACIÓN CENTRO AUTORIZADOR

La autorización On Line de transacciones EMV obliga a realizar unas validaciones más complejas que las que se realizan actualmente.

A las comprobaciones que se llevan a cabo en la actualidad, se añadirán otras nuevas tales como verificación de criptogramas de aplicación y de parámetros de autorización EMV.

Por otro lado, el centro autorizador tendrá la capacidad no sólo de autorizar transacciones EMV sino de enviar, en el transcurso de una autorización, comandos con los que actuar sobre el comportamiento de la tarjeta: estos son los llamados scripts.

2.1. AUTORIZACIÓN TRANSACCIONES EMV

La autorización de operaciones EMV implica varias tareas nuevas:

1. Identificar la operación como EMV
2. Validar los nuevos parámetros EMV
3. Generar los nuevos datos de respuesta EMV

A continuación se detalla cada uno de ellos.

2.1.1. Identificar la operación como EMV

Para considerar una operación como EMV necesariamente debe haberse realizado con una tarjeta EMV.

Pero sólo con eso no basta, las tarjetas EMV pueden realizar hasta tres tipos de operaciones diferentes: EMV, no EMV y operaciones en "fallback".

2.1.1.1. Operación EMV pura

Es aquella para la que se diseñó el estándar, y en la que se aprovecha toda la seguridad de su diseño: es una operación realizada por una tarjeta EMV en un terminal EMV.

El emisor recibirá, en la petición de autorización, todos los datos EMV que el terminal haya leído del chip de la tarjeta, más datos propios del terminal.

Con toda esta colección de datos, más los datos tradicionales (número de tarjeta, importe, etcétera) el emisor podrá autorizar o denegar con más conocimiento de causa, y aplicar reglas más complejas en cuanto a la gestión del riesgo, además de poder actualizar la tarjeta enviando instrucciones al respecto en la respuesta (los denominados "scripts" de emisor).

2.1.1.2. Operación no EMV

Es aquella realizada en un terminal no EMV, o con sus capacidades EMV inutilizadas. En este caso, para el terminal la tarjeta es como cualquier otra tarjeta de banda magnética.

2.1.1.3. Operación en "Fallback"

Aquella realizada por la tarjeta EMV en un terminal EMV pero utilizando la banda magnética.

Esto puede suceder por diversas causas (problemas en el chip de la tarjeta, problemas en el lector del terminal, problemas de interoperatividad, ...).

En este caso, la operación se realiza con la banda magnética pero el adquirente enviará una indicación al emisor para que este actúe en consecuencia (por ejemplo, puede darse el caso de que las entidades emisoras decidan no autorizar operaciones de este tipo).

Es importante determinar con seguridad si una operación es EMV o no de cara a posibles reclamaciones. Por tanto, deberá almacenarse el tipo de operación en el histórico de operaciones con tarjeta de la entidad.

2.1.2. Validar los nuevos parámetros EMV

Estos nuevos parámetros son:

- Contador de Transacciones ATC
- Código de Autenticación DAC
- Número dinámico IDN
- Criptograma de petición de autorización ARQC: generado por la tarjeta y enviado al emisor en cada petición de autorización

En este apartado se revisará cómo realizar la validación de los tres primeros parámetros. Todo lo relacionado con criptogramas se revisará en un apartado específico.

Por supuesto, todas estas validaciones no sustituyen, sino que complementan, las ya realizadas tradicionalmente con las tarjetas de banda magnética.

2.1.2.1. Validación del contador de transacciones ATC

El contador de transacciones (Application Transaction Counter, ATC) es un dato almacenado en el chip de la tarjeta (TAG ***9F36***), que la propia tarjeta va actualizando a medida que se realizan transacciones, tanto On Line como Off Line. Por tanto, el valor del ATC identifica de forma única cada una de las transacciones realizadas por la tarjeta EMV.

Su validación es opcional, no obligatoria, aunque sí recomendada.

Si se almacena este dato también en el Host, se puede comparar el ATC recibido con el almacenado, de forma que se deniegue toda operación On Line cuyo ATC no sea mayor que el ATC almacenado.

Una excepción serían las tarjetas en renovación, en cuyo caso si el plástico que está operando es el antiguo, no se valida el ATC.

2.1.2.2. Validación del código de autenticación DAC

El código de autenticación de datos (Data Authentication Code, DAC) es un dato almacenado en el chip de la tarjeta (TAG ***9F45***), que se calcula y graba en la personalización y ya no varía durante la vida de la tarjeta.

El terminal le solicita este dato a la tarjeta después de comprobar que la Autenticación Estática de la Tarjeta Off Line (SDA) se ha realizado satisfactoriamente, y lo envía al Emisor como prueba de esa autenticación.

El Emisor puede comparar el DAC recibido con el almacenado, de forma que se deniegue la operación cuando no coincidan.

Su validación es opcional, no obligatoria, aunque sí recomendada.

2.1.2.3. Validación del número dinámico de tarjeta IDN

El Número Dinámico de Tarjeta (IDN) es generado por la tarjeta durante el proceso de Autenticación Dinámica de Datos. Su valor se obtiene a partir de una clave simétrica específica para su cálculo que se encuentra almacenada en la propia tarjeta: clave diversificada para el cálculo del IDN, $\underline{MK_{IDN}}$ (ver ***tabla 19***, "*claves simétricas de tarjeta*", y el apartado "datos criptográficos" del punto ***1.4***).

Uno de los datos a partir de los que se calcula el IDN (el ATC) varía en cada transacción, por lo que el IDN también es distinto. Por tanto no se puede almacenar en BDD y deberá calcularse en cada transacción (tanto por la tarjeta, como por el Host).

Su validación es opcional, no obligatoria, aunque sí recomendada, y sólo la pueden realizar las tarjetas que soporten autenticación dinámica de datos Off Line.

2.1.3. Generar los nuevos datos de respuesta EMV

Los nuevos datos de respuesta son:

- Criptograma de respuesta ARPC
- Scripts de actualización de datos del chip

Todo lo relacionado con criptogramas y scripts se revisará en apartados específicos.

2.1.4. Desarrollos y adaptaciones propuestos

* Nueva tabla de BDD *Datos de Tarjetas EMV*

La tabla TEMV ya se definió en el apartado "Parámetros EMV de Entidad", pero ahora hay que añadir más campos, utilizados durante las validaciones de la operación, como el ATC (el contador de transacciones) y el DAC (código de autenticación de datos).

Por tanto, la nueva definición de la tabla queda como sigue:

TEMV DATOS DE TARJETAS EMV		
Clave Única**:** **TEMVPAN (PAN de la tarjeta)**		
Nombre del campo	**Longitud**	**Descripción**
TEMVPAN	DEC (16,0)	PAN de la Tarjeta
TEMV9F14	DEC (3,0)	Límite Inferior Off Line
TEMV9F23	DEC (3,0)	Límite Superior Off Line
TEMV9F53	DEC (3,0)	Límite total de operaciones Off Line consecutivas (Internacional-Moneda) (VISA)
TEMV9F54	DEC (8,2)	Límite total de importe acumulado Off Line (VISA)
TEMV9F58	DEC (3,0)	Límite total inferior de operaciones Off Line consecutivas (VISA)
TEMV9F59	DEC (3,0)	Límite total superior de operaciones Off Line consecutivas (VISA)
TEMV9F5C	DEC (8,2)	Límite superior total de importe acumulado Off Line (VISA)
TEMV9F72	DEC (3,0)	Límite total de operaciones Off Line consecutivas (Internacional-País) (VISA)

		(Internacional-País) (VISA)
TEMV9F75	DEC (8,2)	Límite total de importe acumulado Off Line – Doble moneda (VISA)
TEMVCA	DEC (8,2)	Máximo Importe Inferior Acumulado Off Line (MasterCard)
TEMVCB	DEC (8,2)	Máximo Importe Superior Acumulado Off Line (MasterCard)
TEMVATC	DEC (6,0)	Último valor recibido de la tarjeta del contador de transacciones ATC
TEMVDAC	2 bytes HEX	Código de autenticación de datos, se almacena durante la personalización, en el momento de generar la Firma SDA

* Nueva tabla de BDD *Histórico de operaciones con Tarjetas EMV*

Es conveniente almacenar en BDD todos los nuevos datos relacionados con una transacción EMV, de cara a posibles reclamaciones de clientes o incidencias con las operatorias, o simplemente para poder consultarlos.

Para ello se creará un nuevo histórico, denominado HEMV, complementario al que ya tenga la entidad, y que se grabará sólo cuando la operación sea EMV pura, es decir si existen datos específicos de EMV. No se insertará registro para operaciones en Fallback o aquellas que, aun siendo efectuadas con tarjetas EMV, se han llevado a cabo terminales no EMV, por lo que no existen datos EMV para ellas.

Los registros aquí grabados tendrán siempre un registro afín en el histórico actual de la aplicación, de forma que puede incluso compartir la clave de inserción de ese histórico.

Este nuevo histórico tendrá la siguiente descripción:

HEMV HISTÓRICO DE OPERACIONES EMV		
Clave Única**:** **(clave del histórico actual)**		
Nombre del campo	**Longitud**	**Descripción**
Clave del histórico actual	---	Podrán ser uno o más campos, y corresponderán a la clave única del Histórico actual de la aplicación
HEMV9F26	8 bytes HEX	Criptograma de petición de autorización enviado por la tarjeta (ARQC), TAG ***9F26***
HEMV9F27	CHAR (1)	Tipo de criptograma ARQC, TAG ***9F27***
HEMVARPC	8 bytes HEX	Criptograma de respuesta enviado por el Host Emisor (ARPC)
HEMVATC	DEC (6,0)	Contador de transacciones (ATC) (enviado por la tarjeta)

* Modificación de la actual tabla de BDD *Histórico de operaciones con Tarjetas*

Se añadirá un indicador de si la operación es EMV. Mediante este indicador quedarán marcadas las operaciones en BDD de tres formas diferentes:

- Operación EMV: hecha por una tarjeta EMV a través de su chip en un terminal EMV
- Operación no EMV: o bien la tarjeta no es EMV o bien no lo es el terminal
- Operación no EMV por "fallback": tanto la tarjeta como el terminal son EMV pero la operación se debió realizar a través de la banda debido a un fallo en el chip.

Sólo las "Operaciones EMV" llevarán asociado un registro en la tabla HEMV.

* Nueva rutina On Line de *Validaciones EMV sobre la operación*

Esta rutina validará todos los nuevos parámetros EMV asociados a la tarjeta y a la operación. Deberá ser invocada desde los procesos actuales de validación de datos de las tarjetas, cuando se detecte que la tarjeta (y la operación) son EMV.

La rutina leerá en primer lugar el registro correspondiente de la nueva tabla de datos complementarios EMV (***TEMV***), para pasar a continuación a realizar las siguientes validaciones:

- Validación del ATC

  Si el ATC viene informado, se comparará con el valor almacenado en BDD (campo TEMVATC de la tabla ***TEMV***).

  Si el contador almacenado es superior al recibido, y la transacción es On Line se devuelve incidencia.

  Sólo se autorizarán aquellas transacciones en las que el ATC recibido sea mayor que el almacenado (salvo el caso especial en que la tarjeta esté en proceso de renovación y el mensaje de petición provenga de la tarjeta antigua).

  Por supuesto, el ATC almacenado se deberá actualizar con el valor recibido de la tarjeta, cuando la transacción sea autorizada.

- Validación del DAC

  Si el DAC viene informado, se comparará con el valor almacenado en BDD (campo TEMVDAC de la tabla ***TEMV***).

  Si son iguales, significa que el DAC recibido es correcto, y se podrá seguir con la autorización de la operación.

- Validación del criptograma ARQC

  Si el criptograma de petición ARQC viene informado, se invocará al proceso de *Generación de Criptogramas* (que se detallará en el apartado correspondiente) para que calcule el ARQC, pasándole los datos recibidos de la operación, enviados por el adquirente.

Se compara el criptograma devuelto por este proceso con el recibido en la petición de autorización, y si son iguales, significa que el ARQC recibido es correcto.

- Validación del IDN

Si el Número Dinámico de Tarjeta (IDN) viene informado, habrá que calcularlo para ver si coinciden ambos (el recibido y el calculado).

El método de cálculo es el siguiente:

- Obtención de la clave de IDN de la tarjeta MK_{IDN} (por diversificación de la clave K_{IDN}):

  Hay que recordar que esta clave se graba ya diversificada en cada tarjeta, pero en el HSM del Host sólo se guarda la Clave Maestra para cálculo de IDN (K_{IDN}).

  Los pasos a seguir para calcular la MK_{IDN} de la tarjeta a partir de la K_{IDN} maestra son los siguientes:

  1. concatenar el PAN de la tarjeta con el número de secuencia de la tarjeta
  2. cifrar mediante Triple DES el resultado del paso 1, utilizando la clave K_{IDN}
  3. calcular el XOR del PAN con una cadena de 'FF' hex
  4. concatenar el resultado del paso 3 con el número de secuencia de la tarjeta
  5. cifrar mediante Triple DES el resultado del paso 4, utilizando la clave K_{IDN}
  6. concatenar el resultado del paso 2 con el resultado del paso 5

  El resultado del paso 6 es la clave de IDN de la tarjeta (MK_{IDN}).

- Cálculo del IDN:

  Los pasos a seguir para calcular el IDN son:

1. concatenar el ATC de la operación con una cadena de ‘00’ hex

2. cifrar mediante Triple DES el resultado del paso 1, utilizando la clave MK_{IDN}, calculada en el primer punto de este método

3. el IDN serán los dos bytes más significativos del resultado del paso 2

Si el IDN generado según el método que se acaba de describir es igual al IDN recibido, se continúa con la autorización.

- Validación del contador de scripts

  En este punto se invocará al proceso de *Validación de contador de scripts*, que se detallará en el apartado correspondiente.

* Modificación de la actual rutina On Line de *Autorización de operaciones*

Esta rutina es el actual Centro Autorizador de la entidad, utilizado para autorizar o denegar las operaciones de las actuales tarjetas de la entidad (no EMV).

Deberán introducirse modificaciones en ciertas partes del código de la rutina, donde se realizan determinadas tareas:

- Actualización de los datos de tarjetas en la BDD propia

  En la parte del código donde la rutina de autorización actualiza los datos de las tarjetas en las tablas de BDD que correspondan, se deberá añadir la actualización de la nueva tabla ***TEMV***.

  Esta actualización debe hacerse sobre los siguientes campos:

  - Actualizar TEMVATC con el ATC recibido de la tarjeta (sólo si la operación se autoriza)

  - Actualizar campos de scripts: se verá con más detalle en el apartado correspondiente

  Por supuesto, estas actualizaciones sólo se realizarán si la tarjeta es EMV (y la operación también lo es).

- Generación de datos de respuesta

En la parte del código donde la rutina de autorización genera los datos de respuesta (por ejemplo, el código de autorización, o el texto descriptivo de las denegaciones, según corresponda), se deberá añadir una llamada a la rutina de *Generación de Criptogramas*, para generar el ARPC de respuesta (ya sea de autorización o de denegación), siempre que se haya recibido (y validado como OK) un criptograma de petición ARQC.

También se deberá llamar a la rutina de *Tratamiento de scripts*, que se detallará en el apartado correspondiente.

- Almacenamiento de la operación en Histórico

  En la parte del código donde la rutina de autorización deja constancia de la operación en el histórico de la entidad, se deberá añadir la grabación del nuevo histórico ***HEMV***.

  Esta grabación sólo se realizará si la tarjeta es EMV (y la operación también lo es), y se rellenarán los campos de ***HEMV*** de la siguiente forma:

  - Clave: igual a la clave que se haya utilizado para grabar el Histórico actual

  - HEMV9F26: ARQC recibido

  - HEMV9F27: tipo de criptograma recibido

  - HEMVARPC: ARPC generado

  - HEMVATC: ATC recibido de la tarjeta

  Además, se deberá rellenar el nuevo campo en el histórico de la entidad, en el que se marca el tipo de la operación respecto a EMV: operación EMV, no EMV o en “fallback”.

2.2. CRIPTOGRAMAS

Una de las aportaciones del estándar EMV a la seguridad de las transacciones On Line es el manejo de criptogramas.

Los criptogramas son unas códigos de redundancia, resultado de cifrar ciertos datos de los mensajes de petición de autorización y de respuesta, intercambiados entre la tarjeta y su emisor. Estos códigos se añaden a dichos mensajes, y deben ser generados y verificados por la tarjeta y/o el emisor.

En el caso de la aplicación Host, se deberán realizar dos tareas nuevas:

1. Verificar el criptograma de petición generado por la tarjeta (ARQC) y recibido en la petición de autorización

2. Construir el criptograma de respuesta (ARPC) que se enviará en la respuesta al terminal (que a su vez se lo pasará a la tarjeta).

A continuación se revisarán ambas tareas en detalle.

Además del ARQC y el ARPC, existe otro criptograma denominado TC o segundo criptograma, que es generado por la tarjeta tras el procesamiento del ARPC devuelto por el Host Emisor. Por el momento no se va a realizar ningún tratamiento con este criptograma en las aplicaciones Host.

2.2.1. Validación del criptograma ARQC

El mensaje de petición de autorización enviado por una tarjeta EMV que haya operado en entorno EMV incluye un criptograma de petición de autorización, denominado ARQC.

Este criptograma ha sido calculado por la tarjeta y enviado al Host Emisor por el terminal adquirente.

La verificación consta de los siguientes pasos:

1. Derivación de la Clave por Tarjeta MK_{AC}.

2. Derivación de la Clave de Sesión SK_{AC}.

3. Cálculo del Criptograma ARQC.

4. Comprobación del Criptograma ARQC.

A continuación se repasan en detalle cada uno de los pasos.

2.2.1.1. Derivación de la Clave por Tarjeta MK_{AC}

Se toma la clave única para cálculo de ACs (IMK_{AC}) y se diversifica.

Esta diversificación se realiza a partir del PAN de la tarjeta y ciertos datos, distintos según el método de diversificación elegido por la entidad. Estos datos se toman del mensaje de petición de autorización.

2.2.1.2. Derivación de la Clave de Sesión SK_{AC}

Se toma la clave diversificada por tarjeta calculada en el punto anterior (MK_{AC}) y se diversifica de nuevo.

Esta segunda diversificación es el resultado de aplicar un cifrado Triple DES sobre ciertos datos de la transacción, recibidos en el mensaje de petición de autorización.

El método de diversificación varía según la marca (VISA o MasterCard).

2.2.1.3. Cálculo del Criptograma ARQC

El ARQC es el resultado de aplicar un algoritmo de MAC a un conjunto de datos, tanto de la tarjeta como de la propia transacción, que el Emisor recibe dentro del mensaje de petición de autorización.

Dichos datos son una combinación de datos de tarjeta y de datos propios de la transacción. Estos últimos, son aportados por el terminal durante el transcurso de la transacción EMV. En cualquier caso, todos los datos necesarios para el cálculo del ARQC serán enviados al Centro Autorizador en el mensaje de petición de autorización.

2.2.1.4. Comprobación del Criptograma ARQC

Una vez calculado el ARQC, se compara con el generado por la tarjeta, recibido en el mensaje de petición de autorización. Sólo en caso de que coincidan, se dará por buena la validación.

2.2.2. Generación del criptograma ARPC

El criptograma de respuesta ARPC es generado por el Emisor para ser enviado en la respuesta a la tarjeta.

Este criptograma, calculado a partir de una clave sólo conocida por el Emisor y su tarjeta, tiene como función el de servir a la tarjeta para autenticar al Emisor.

La generación del ARPC consta de los siguientes pasos:

1. Derivación de la Clave por Tarjeta MK_{AC}.

2. Cálculo del Criptograma ARQC.

3. Comprobación del Criptograma ARQC.

2.2.2.1. Derivación de la Clave por Tarjeta MK_{AC} .

La clave calculada en este apartado coincide con la calculada en el primer paso de la '*Validación del criptograma ARQC*'.

2.2.2.2. Cálculo del criptograma ARPC

El criptograma de respuesta ARPC se calcula aplicando el triple DES, con la clave calculada en el punto anterior (MK_{AC}), a una serie de datos, bien sean recibidos en el mensaje de petición de autorización o bien generados por el emisor durante la propia autorización.

El criptograma de respuesta ARPC junto con los datos necesarios para su cálculo deben ser enviados en el mensaje de respuesta.

2.2.3. Desarrollos y adaptaciones propuestos

* Nueva tabla de BDD *Histórico de operaciones con Tarjetas EMV*

  Como ya se vio en el apartado anterior, el nuevo histórico de operaciones EMV, ***HEMV***, incluye tres nuevos campos relacionados con los criptogramas: dos relacionados con el criptograma de petición ARQC (campos HEMV9F26 y HEMV9F27) y uno con el de respuesta ARPC (HEMVARPC).

* Nueva rutina On Line de *Generación de criptogramas*

  Esta nueva rutina generará los dos criptogramas, el ARQC y el ARPC, en función del comando con el que se la invoque.

  - Generación del ARQC

    Incluye tres pasos:

    1. ***Derivación de la Clave por Tarjeta MK_{AC}***

       Los pasos a seguir para calcular la MK_{AC} de la tarjeta a partir de la K_{AC} maestra, según el método de derivación estándar de EMV, son los siguientes:

1. concatenar el PAN de la tarjeta (TAG ***5A***) con el número de secuencia de la tarjeta (TAG ***9F34***)

2. cifrar mediante Triple DES el resultado del paso 1, utilizando la clave K_{AC}

3. calcular el XOR del resultado del paso 1 con una cadena de 'FF' hex

4. cifrar mediante Triple DES el resultado del paso 3, utilizando la clave K_{AC}

5. concatenar el resultado del paso 2 con el resultado del paso 4

6. se tomará el resultado del paso 5 y, para el bit menos significativo de cada byte, se fijará de forma que se asegure que cada uno de los 16 bytes tiene un número impar de bits distintos de cero (para cumplir con los requerimientos de paridad impar de las claves DES)

7. el resultado del paso 6 será la clave MK_{AC}

2. Derivación de la Clave de Sesión SK_{AC}

- Para MasterCard:

    1. concatenar los siguientes datos:

        - el ATC (TAG ***9F36***) recibido de la tarjeta

        - 2 bytes 'F0' '00' hex.

        - un número aleatorio generado por la tarjeta y enviado al Emisor en el mensaje de petición (TAG ***9F37***)

    2. cifrar mediante Triple DES el resultado del paso 1, utilizando la clave MK_{AC}

    3. concatenar los siguientes datos:

        - el ATC (TAG ***9F36***) recibido de la tarjeta

- 2 bytes ‘0F’ ‘00’ hex. *(nótese que el primer byte es ‘0F’, diferente del utilizado en el paso 1, ‘F0’)*

- un número aleatorio generado por la tarjeta y enviado al Emisor en el mensaje de petición (TAG ***9F37***)

4. cifrar mediante Triple DES el resultado del paso 3, utilizando la clave MK_{AC}

5. concatenar el resultado del paso 2 con el del paso 4

6. el resultado del paso 5 será la clave SK_{AC}

- Para VISA: no es necesario calcular una clave de sesión, ya que se utiliza directamente MK_{AC} para calcular el criptograma. Es decir, $SK_{AC} = MK_{AC}$

3. Cálculo del Criptograma ARQC

El ARQC será el resultado de aplicar un algoritmo de MAC sobre unos determinados datos, utilizando la clave de sesión calculada en el punto anterior:

- Algoritmo: MAC según la norma ANSI X9.19-1

- Clave: SK_{AC} calculada en el punto anterior

- Datos: concatenación de los datos correspondientes a las siguientes etiquetas:

TAG ***9F02***	Cantidad Autorizada
TAG ***9F03***	Otra Cantidad
TAG ***9F1A***	Código de País del Terminal
TAG ***95***	Resultado de la Verificación del Terminal (TVR)
TAG ***5F2A***	Código de Moneda de la Transacción
TAG ***9A***	Fecha de la Transacción

TAG ***9C*** Tipo de Transacción

TAG ***9F37*** Número Aleatorio

TAG ***82*** Perfil de Intercambio de la Aplicación (AIP)

TAG ***9F36*** Contador de Transacciones de la Aplicación (ATC)

TAG ***9F10*** Datos de Aplicación del Emisor, se toman bytes distintos según el tipo de tarjeta:

- VISA: bytes 4º al 7º
- MasterCard MChip 2.1: 3º al 6º
- MasterCard MChip 4: 3º al 8º

- Generación del ARPC

  Incluye dos pasos:

  1. ***Derivación de la Clave por Tarjeta MK_{AC}***

     Igual al punto 1 de la generación del ARQC (la clave es la misma). No es necesario diversificarla por sesión.

  2. ***Cálculo del Criptograma ARPC***

     Los pasos a seguir para calcular el ARPC son:

     1. concatenar el ARC (código de respuesta de 2 bytes, enviado por el Emisor a la tarjeta, como parte del TAG ***91***) con 6 bytes '00' hex

     2. calcular el XOR del ARQC recibido de la tarjeta y del resultado del paso 1

     3. cifrar mediante Triple DES el resultado del paso 2, utilizando la clave MK_{AC} calculada en el paso anterior

2.3. GENERACIÓN Y GESTIÓN DE SCRIPTS

El estándar EMV proporciona al Emisor la posibilidad de enviar comandos a la tarjeta durante el transcurso de una transacción financiera llevada a cabo On Line.

Con estos comandos, denominados también comandos transparentes de Emisor o scripts, el Emisor puede actuar sobre la tarjeta, modificando algunos de los parámetros que determinan su funcionamiento.

2.3.1. Tipos de scripts

Mediante scripts se pueden llevar a cabo las siguientes funciones:

- Bloqueo de la tarjeta:

  El Emisor puede, mediante este script, deshabilitar la tarjeta. Este bloqueo es irreversible, una vez bloqueada, la tarjeta no podrá desbloquearse.

  La transacción durante la que se envía este script, será completada tanto por la tarjeta como por el terminal. La tarjeta quedará bloqueada una vez completada dicha transacción.

- Bloqueo de la Aplicación EMV:

  Con este script se pretende bloquear la aplicación EMV seleccionada.

  La transacción durante la que se envía este script, será completada tanto por la tarjeta como por el terminal.

  Este comando será procesado en modo de mensaje securizado para integridad.

- Desbloqueo de la Aplicación EMV:

  El desbloqueo de una aplicación EMV sólo podrá llevarse a cabo en un terminal controlado por el emisor (terminal atendido), mediante el script correspondiente.

  Este script será procesado en modo de mensaje securizado para integridad.

- Cambio/Desbloqueo de PIN:

Mediante este script se permite la posibilidad de desbloquear el PIN de una tarjeta, más concretamente de una aplicación EMV. Además, también será posible cambiar el PIN al mismo tiempo que se desbloquea.

El mensaje utilizado para la opción de Cambio de PIN irá securizado para confidencialidad e integridad. En cuanto a la opción de Desbloqueo de PIN, el mensaje necesario irá tan sólo protegido para integridad.

El cambio de PIN de tarjetas EMV sólo se permitirá en cajeros EMV propios, de forma que siempre se cambie simultáneamente el PIN de la banda y el PIN del chip. Este cambio de PIN será comunicado al Host de la misma forma que actualmente, y en la respuesta, el Host enviará un script de cambio de PIN al cajero para que éste se lo haga llegar a la tarjeta.

Este script es de envío único, es decir, se envía como respuesta a la operatoria de cajero de cambio de PIN y no se vuelve a reenviar nunca, independientemente de que se reciba el OK o no. Sólo se volverá a reenviar un script de cambio de PIN cuando se reciba una nueva operatoria de cambio de PIN desde el cajero.

- Actualización de Datos:

  Gracias a este script se podrán modificar algunos de los datos almacenados en la tarjeta, en concreto los relacionados con la gestión de riesgo Off Line llevada a cabo por la tarjeta.

Para el caso planteado en este proyecto, se utilizarán sólo aquellos scripts que los Sistemas Internacionales han considerado más necesarios: el bloqueo de tarjeta y el desbloqueo/cambio de PIN.

2.3.2. Restricciones de uso

Por supuesto, la utilización de scripts es totalmente opcional, quedando a libre elección del emisor no utilizarlos o utilizar sólo alguno de los tipos.

VISA permite inhabilitar el bloqueo de tarjeta. Basta con grabar en el chip de la tarjeta, en el momento de la personalización, el valor adecuado en el TAG C5. De esta forma, el chip ignorará cualquier script de bloqueo que le llegue desde el Emisor.

2.3.3. Creación de scripts y sus desencadenantes

El centro autorizador no genera los scripts hasta el momento en que se van a enviar a la tarjeta, pero la manera en que este centro autorizador detecta que debe generar y enviar un determinado script puede variar.

En el caso de los tipos de scripts que se van a utilizar (bloqueo de tarjeta y desbloqueo/cambio de PIN), los desencadenantes son los siguientes:

- Si el titular denuncia la tarjeta por pérdida o robo, el centro autorizador deberá enviar un script de bloqueo de tarjeta en la siguiente petición de autorización On Line que envíe la tarjeta

- Si el PIN Off Line de la tarjeta quedó bloqueado por tres errores consecutivos por parte del titular en la introducción del PIN, cabe la posibilidad de que el titular, por vía telefónica o presencialmente, solicite su desbloqueo (pero manteniendo el PIN). En ese caso, el centro autorizador deberá enviar un script de desbloqueo de PIN Off Line en la siguiente petición de autorización (que el titular deberá realizar en un terminal que disponga de PIN On Line como primer método de autenticación)

- El mismo caso que el anterior, pero el titular ha olvidado el PIN: el titular, por vía telefónica o presencialmente, solicite un nuevo PIN, que se le envía mediante algún medio seguro. El centro autorizador deberá enviar un script de desbloqueo más cambio de PIN Off Line en la siguiente petición de autorización (que el titular deberá realizar en un terminal que disponga de PIN On Line como primer método de autenticación)

- Un cambio de PIN realizado en un cajero propio también debe desencadenar el envío del script de cambio de PIN a la tarjeta, para que no quede incoherente con el grabado en la banda magnética

2.3.4. Confirmaciones de ejecución y scripts pendientes

Cuando ocurre alguna de las circunstancias desencadenantes descritas en el apartado anterior, el script correspondiente pasa a estar en la situación de pendiente de envío.

Una vez el centro autorizador ha logrado enviar el script a la tarjeta, como parte de una respuesta a una petición On Line, dicho script pasa a situación de pendiente de confirmar.

Si todo es correcto y la tarjeta ejecuta de forma satisfactoria el script recibido del Emisor, deberá informarle de dicha circunstancia en la petición de autorización inmediatamente posterior. La manera de informar es mediante un contador de scripts ejecutados correctamente, que se almacena en el chip, y que inicialmente tiene valor cero.

Cuando el Emisor recibe la confirmación de la correcta ejecución de un script, lo borra de la lista de los scripts pendientes de confirmar.

En caso de que en peticiones posteriores al envío de un script, no se recibiese la confirmación de su correcta ejecución por parte de la tarjeta, deberá reenviarse dicho script. La excepción es el script de cambio de PIN, que sólo se envía una vez, sin importar si llega el OK o no.

2.3.5. Desarrollos y adaptaciones propuestos

* Uso de Scripts: parámetro de entidad incluido en la nueva tabla ***Parámetros EMV de Entidad***

  Como ya se explicó en el apartado de "Parámetros y Perfiles EMV", uno de los parámetros incluidos en la nueva tabla de Parámetros EMV de Entidad (***EMVE***) es el Indicador de Uso de Scripts (campo EMVEUSCR).

  Este indicador general afecta a todas las tarjetas de la entidad. Cuando esté desactivado, el centro autorizador no generará ni enviará a las tarjetas ningún script.

* Indicador de Bloqueo: parámetro por perfil incluido en la nueva tabla ***Perfiles EMV***

  Como ya se explicó en el apartado de "Parámetros y Perfiles EMV", uno de los parámetros incluidos en la nueva tabla de Parámetros EMV por Perfil (***PEMV***) es el Indicador de Bloqueo mediante Script (campo PEMVC5).

  Este campo permite prohibir la ejecución del script de bloqueo en las tarjetas que lo tengan activado (sólo válido para tarjetas VISA), que serán todas aquellas que pertenezcan a perfiles con ese indicador activado.

* Nueva tabla de BDD ***Datos de Tarjetas EMV***

  La tabla ***TEMV*** ya se definió en el apartado "Parámetros EMV de Entidad", añadiéndose más campos en el apartado "Autorización Transacciones EMV".

  Ahora, y por último, se añadirán los campos para el tratamiento de scripts:

  - 3 contadores de número de scripts: pendientes de envío, pendientes de confirmación y confirmados por la tarjeta
  - una tabla con 4 pares de campos del tipo: nemotécnico + indicador de estado

  La definición definitiva de la tabla ***TEMV*** quedará como sigue:

TEMV DATOS DE TARJETAS EMV		
Clave Única**:** **TEMVPAN (PAN de la tarjeta)**		
Nombre del campo	**Longitud**	**Descripción**
TEMVPAN	DEC (16,0)	PAN de la Tarjeta
TEMV9F14	DEC (3,0)	Límite Inferior Off Line
TEMV9F23	DEC (3,0)	Límite Superior Off Line
TEMV9F53	DEC (3,0)	Límite total de operaciones Off Line consecutivas (Internacional-Moneda) (VISA)
TEMV9F54	DEC (8,2)	Límite total de importe acumulado Off Line (VISA)
TEMV9F58	DEC (3,0)	Límite total inferior de operaciones Off Line consecutivas (VISA)
TEMV9F59	DEC (3,0)	Límite total superior de operaciones Off Line consecutivas (VISA)
TEMV9F5C	DEC (8,2)	Límite superior total de importe acumulado Off Line (VISA)
TEMV9F72	DEC (3,0)	Límite total de operaciones Off Line consecutivas (Internacional-País) (VISA)
TEMV9F75	DEC (8,2)	Límite total de importe acumulado Off Line – Doble moneda (VISA)
TEMVCA	DEC (8,2)	Máximo Importe Inferior Acumulado Off Line (MasterCard)
TEMVCB	DEC (8,2)	Máximo Importe Superior Acumulado Off Line (MasterCard)

<table>
<tr><td>TEMVATC</td><td>DEC (6,0)</td><td>Último valor recibido de la tarjeta del contador de transacciones ATC</td></tr>
<tr><td>TEMVDAC</td><td>2 bytes HEX</td><td>Código de autenticación de datos, se almacena durante la personalización, en el momento de generar la Firma SDA</td></tr>
<tr><td>TEMVSCOK</td><td>DEC (2,0)</td><td>Contador del número de scripts procesados OK por la tarjeta</td></tr>
<tr><td>TEMVNSPC</td><td>DEC (2,0)</td><td>Contador del número de scripts pendientes de confirmación de ejecución OK por la tarjeta</td></tr>
<tr><td>TEMVNSPE</td><td>DEC (2,0)</td><td>Contador del número de scripts pendientes de enviar a la tarjeta</td></tr>
<tr><td>TEMVSCPE</td><td>CHAR (20)</td><td>Tabla con 4 ocurrencias de los siguientes dos elementos: TEMVNEMO y TEMVINDI

<table>
<tr><td>TEMVNEMO (i)</td><td>CHAR (2)</td><td>Nemotécnico del i-ésimo script pendiente de procesar por la tarjeta (los scripts están ordenados de más reciente a más antiguo):

‘DP’: desbloqueo de PIN

‘CP’: cambio de PIN

‘BT’: bloqueo de tarjeta</td></tr>
<tr><td>TEMVINDI (i)</td><td>CHAR (1)</td><td>Indicador de estado del envío del i-ésimo script:

‘0’: script pendiente de envío

‘1’: script enviado pero no confirmado</td></tr>
</table>
i:1..4</td></tr>
</table>

* Nueva tabla de BDD *Histórico de operaciones con Tarjetas EMV*

La tabla ***HEMV*** ya se definió en el apartado "Autorización Transacciones EMV", pero ahora se añadirán dos campos más para almacenar la siguiente información:

- Contador del número de scripts procesados correctamente por la tarjeta
- Script enviado a la tarjeta en la respuesta de la transacción

La definición definitiva de la tabla ***HEMV*** es la siguiente:

HEMV HISTÓRICO DE OPERACIONES EMV		
Clave Única**:** **(clave del histórico actual)**		
Nombre del campo	**Longitud**	**Descripción**
Clave del histórico actual	---	Podrán ser uno o más campos, y corresponderán a la clave única del Histórico actual de la aplicación
HEMV9F26	8 bytes HEX	Criptograma de petición de autorización enviado por la tarjeta (ARQC), TAG ***9F26***
HEMV9F27	CHAR (1)	Tipo de criptograma ARQC, TAG ***9F27***
HEMVARPC	8 bytes HEX	Criptograma de respuesta enviado por el Host Emisor (ARPC)
HEMVATC	DEC (6,0)	Contador de transacciones (ATC) (enviado por la tarjeta)
HEMVSCOK	DEC (2,0)	Contador de número de scripts ejecutados OK (enviado por la tarjeta)
HEMVSCRI	CHAR (N)	Scripts enviados en la respuesta a la petición de autorización

		autorización

* Nueva rutina On Line de *Validación de contador de scripts*

Esta nueva rutina será invocada desde la rutina, también nueva, de "Validaciones EMV sobre la operación", descrita en el apartado de "Autorización Transacciones EMV".

Esta validación sólo se realiza si la entidad soporta scripts (campo EMVEUSCR de la tabla ***EMVE***) y la operación es EMV y On Line.

La misión de esta rutina es comprobar que el contador de scripts ejecutados OK, recibido de la tarjeta, es coherente con los contadores almacenados en TEMV:

- El contador recibido deberá ser mayor o igual a TEMVSCOK (número de scripts ejecutados correctamente por la tarjeta), ya que la tarjeta no puede enviar un valor del contador inferior a otro valor enviado anteriormente.

- El contador recibido tampoco podrá ser mayor a la suma de TEMVSCOK y TEMVNSPC (número de scripts pendientes de confirmación de proceso OK por parte de la tarjeta)

Validación del contador de scripts en tarjetas en renovación:

- Cuando una tarjeta EMV está en renovación, se da la circunstancia de que pueden coexistir dos plásticos con sus respectivos chips, pudiendo recibir operaciones de ambos. Aquí el problema reside en cuando validar y/o actualizar los contadores de scripts y cuando enviar scripts pendientes.

- Como norma general, cuando se esté autorizando una petición realizada con el plástico antiguo, no se validará el contador de scripts ni se actualizarán los contadores residentes en TEMV; únicamente se enviarán los scripts pendientes.

- Cuando se esté autorizando una petición realizada con el plástico nuevo, el proceso a realizar será el mismo que con una tarjeta normal (es decir, una tarjeta que no esté en renovación).

* Modificación de la actual rutina On Line de *Autorización de operaciones*

Esta rutina es el actual Centro Autorizador de la entidad, utilizado para autorizar o denegar las operaciones de las actuales tarjetas de la entidad (no EMV).

Además de las modificaciones vistas en el apartado "Autorización Transacciones EMV", deberán introducirse modificaciones adicionales, derivadas de la necesidad de tratar los scripts, en ciertas partes del código de la rutina, donde se realizan determinadas tareas:

- Actualización de los datos de tarjetas en la BDD propia

  En la parte del código donde la rutina de autorización actualiza los datos de las tarjetas en las tablas de BDD que correspondan, se deberá añadir la actualización de la nueva tabla ***TEMV***.

  Esta actualización afecta a los siguientes campos:

  TEMVSCOK, TEMVNSPC, TEMVNEMO, TEMVINDI

  y se realiza de la siguiente forma:

  Se comprueba si el valor del Contador de Scripts ejecutados OK, enviado por la tarjeta, es distinto del almacenado en BDD (TEMVSCOK).

  Si son distintos, significa que la tarjeta ha ejecutado alguno de los scripts que para la aplicación estaban pendientes de confirmar, por lo que se han de actualizar los campos de la siguiente forma:

  TEMVNSPC = TEMVNSPC + TEMVSCOK - Contador de scripts + TEMVNSPE

  TEMVSCOK = Contador de scripts

  Además se deben borrar los scripts enviados:

  TEMVNEMO (i) = espacios

  TEMVINDI (i) = espacios

  En ambos casos, para todo i > (TEMVNSPC + TEMVNSPE)

Los campos TEMVNSPC y TEMVINDI pueden sufrir nuevas modificaciones, ya que en el caso de que se deban enviar nuevos scripts, se deberán guardar.

Por supuesto, estas actualizaciones sólo se realizarán si la tarjeta es EMV (y la operación también lo es).

- Generación de datos de respuesta

  Una vez actualizados los datos de control de número de scripts confirmados o pendientes de confirmación, en la parte del código donde la rutina de autorización genera los datos de respuesta (por ejemplo, el código de autorización, o el texto descriptivo de las denegaciones, según corresponda), se deberá añadir una llamada a la rutina de *Tratamiento de scripts*, para que ésta devuelva los scripts a añadir a la respuesta a la transacción en curso que se va a enviar a la tarjeta.

  Esta llamada se realizará cuando la tarjeta tenga scripts pendientes de envío (TEMVNSPE > cero) o pendientes de confirmación de proceso OK (TEMVNSPC > cero). Y por supuesto, sólo si la entidad soporta scripts (campo EMVEUSCR de la tabla ***EMVE***) y la operación es EMV y On Line.

- Almacenamiento de la operación en Histórico

  Cuando se grabe la tabla ***HEMV*** (ver condiciones de grabación en el apartado "Autorización Transacciones EMV"), los campos correspondientes a scripts se grabarán de la siguiente forma:

  - HEMVSCOK: Contador de scripts ejecutados OK por la tarjeta, recibido en la petición

  - HEMVSCRI: scripts generadas y enviadas por el Host en la actual ejecución

* Nueva rutina On Line de *Tratamiento de scripts*

La rutina será invocada por el centro autorizador sólo si la tarjeta tiene scripts pendientes de envío o de confirmación, ya que en ambos casos se deberá enviar el correspondiente script en la respuesta (por primera vez o como reenvío, en el caso de que sean scripts pendientes de confirmar).

La rutina recorrerá la tabla de scripts pendientes (TEMVSCPE) contenida en la tabla de BDD ***TEMV***. Por cada nemotécnico que encuentre relleno (TEMVNEMO distinto de espacios), deberá generar el script correspondiente (DP: desbloqueo de PIN, CP: cambio de PIN, BT: bloqueo de tarjeta).

El script consiste en una cadena de caracteres, diferente para cada tipo, que, de forma resumida, contiene:

- Un byte identificador del tipo de script

- Una serie de bytes fijos, iguales para todos los scripts

- Un conjunto de datos, diferente según el tipo de script: en la actualización de datos, los nuevos valores a asignar; en el cambio de PIN, el nuevo PIN; y en los scripts de bloqueos/desbloqueos, no se informa (no hay datos específicos).

- Un MAC, calculado sobre los datos anteriores, que sirve para proteger la integridad del script (es decir, que el receptor pueda asegurarse de que el script que le ha llegado está completo). Para calcular este MAC se utiliza la clave MK_{SMI}.

- En el caso del cambio de PIN, el nuevo PIN se envía dentro de un bloque de PIN, securizado mediante una clave para proteger la confidencialidad (MK_{SMC}).

La rutina devolverá al Centro Autorizador la siguiente información:

- scripts a enviar, ya en el formato en el que se envían a la tarjeta

- número de scripts que se han formateado para envío

- número indicando cuántos de los que estaban pendientes de envío se envían posprimera vez

La rutina, además, regrabará TEMV de la siguiente forma:

TEMVNSPC = TEMVNSPC + núm. de scripts enviados por 1ª vez

TEMVNSPE = TEMVNSPE – núm. de scripts enviados por 1ª vez

TEMVINDI (i) = ‘1’ de todos aquellos scripts enviados por 1ª vez

* Nueva operatoria de terminal para *Alta de orden de envío de script de Desbloqueo de PIN*

  Mediante esta transacción se añadirá una orden de envío de script de desbloqueo del PIN Off Line de una determinada tarjeta. Este script quedará pendiente de envío hasta que sea transmitido a la tarjeta por el Centro Autorizador en posteriores respuestas a peticiones On Line.

  Se capturará por pantalla el PAN de la tarjeta cuyo PIN se quiere desbloquear.

  - Validaciones

    - Verificar si la entidad soporta scripts (campo EMVEUSCR de la tabla ***EMVE***)

    - Validar que la tarjeta existe en la BDD de la entidad, y es EMV

    - Validar que la tarjeta no haya alcanzado ya el máximo número de scripts pendientes (TEMVNSPC + TEMVNSPE = 4)

    - Validar que la tarjeta no tenga ya pendiente de envío otro script de desbloqueo de PIN (TEMVNEMO = 'DP') o de cambio de PIN (TEMVNEMO = 'CP'), que también desbloquea el PIN

    - Validar que la tarjeta no tenga ya pendiente un script de bloqueo de tarjeta (TEMVNEMO = 'BT'). No tiene lógica desbloquear el PIN de una tarjeta que se va a bloquear de forma irreversible

  - Actualización de la tabla TEMV:

    - Avanzar una posición en la tabla TEMVSCPE los scripts (TEMVNEMO + TEMVINDI) que ya estuvieran en ella (es decir, el de la posición 3 a la 4, el de la 2 a la 3, y el de la 1 a la 2)

    - Añadir el script de desbloqueo a la primera posición de la tabla TEMVSCPE:

      TEMVNEMO (1) = 'DP' (desbloqueo de PIN)

      TEMVINDI (1) = '0' (pendiente de envío)

    - Sumar 1 al contador TEMVNSPE

* Nueva operatoria de terminal para *Baja de orden de envío de script de Desbloqueo de PIN*

  Es contraria a la anterior. Mediante esta transacción se eliminará la orden de envío del script de desbloqueo de PIN Off Line que estuviese pendiente de enviar para una determinada tarjeta.

  Se capturará por pantalla el PAN de la tarjeta cuyo PIN se quiere desbloquear.

  - Validaciones

    - Buscar en la tabla TEMVSCPE un script 'DP' pendiente de envío. Si no existe, o ya está enviado, no se puede anular.

  - Actualización de la tabla TEMV:

    - Retroceder una posición en la tabla TEMVSCPE los scripts (TEMVNEMO + TEMVINDI) que ya estuvieran en ella (es decir, el de la posición 2 a la 1, el de la 3 a la 2, y el de la 4 a la 3)

    - Rellenar a espacios los campos del último script:

      TEMVNEMO (4) = espacios

      TEMVINDI (4) = espacios

    - Restar 1 al contador TEMVNSPE

* Modificación de la actual operatoria de cajero automático de *Cambio de PIN de tarjeta*

  Hay que añadir algunas validaciones nuevas:

  - Si el cambio de PIN lo está solicitando una tarjeta EMV pero la operación no es EMV entonces no se permitirá dicho cambio de PIN. Esto puede suceder por dos causas: que el cajero no sea EMV, o que, siéndolo, no haya podido leer el chip de la tarjeta ("fallback")

  - Verificar si la entidad soporta scripts (campo EMVEUSCR de la tabla ***EMVE***)

  - Validar que la tarjeta existe en la BDD de la entidad, y es EMV

- Validar que la tarjeta no haya alcanzado ya el máximo número de scripts pendientes (TEMVNSPC + TEMVNSPE = 4)

- Validar que la tarjeta no tenga ya pendiente un script de bloqueo de tarjeta (TEMVNEMO = 'BT'). No tiene lógica desbloquear el PIN de una tarjeta que se va a bloquear de forma irreversible

Además del proceso de cambio de PIN de la banda magnética, realizado actualmente, y sólo si la tarjeta es EMV, la transacción deberá realizar las siguientes tareas:

- Actualización de la tabla TEMV con los datos relativos a "scripts ejecutados OK" que le han llegado desde la tarjeta en el mensaje de petición. Esto lo hará de forma similar a como lo hace la rutina de centro autorizador

- Inserción del script 'CP' como script pendiente de envío en la tabla TEMVSCPE, de forma similar a como se hace con el desbloqueo de PIN en las operatoria de "*Alta de orden de envío de script de Desbloqueo de PIN*"

- Envío al cajero del script de cambio de PIN. Para ello, deberá invocar a la nueva rutina de "*Tratamiento de scripts*" para que construya los scripts pendientes (incluido el de cambio de PIN que se acaba de insertar)

* Nueva operatoria de terminal de *Alta de orden de envío de script de bloqueo de tarjeta*

Mediante esta transacción se añadirá una orden de envío de script de bloqueo de una determinada tarjeta. Este script quedará pendiente de envío hasta que sea transmitido a la tarjeta por el Centro Autorizador en posteriores respuestas a peticiones On Line.

Se capturará por pantalla el PAN de la tarjeta que se quiere bloquear.

- Validaciones

  - Verificar si la entidad soporta scripts (campo EMVEUSCR de la tabla ***EMVE***)

  - Verificar que el perfil de la tarjeta admite el bloqueo (campo PEMVC5 de la tabla ***TEMV***)

  - Validar que la tarjeta existe en la BDD de la entidad, y es EMV

- Validar que la tarjeta no haya alcanzado ya el máximo número de scripts pendientes (TEMVNSPC + TEMVNSPE = 4)

- Validar que la tarjeta no tenga ya pendiente de envío otro script de bloqueo de tarjeta (TEMVNEMO = 'BT')

▪ Actualización de la tabla TEMV:

- Avanzar una posición en la tabla TEMVSCPE los scripts (TEMVNEMO + TEMVINDI) que ya estuvieran en ella (es decir, el de la posición 3 a la 4, el de la 2 a la 3, y el de la 1 a la 2)

- Añadir el script de bloqueo a la primera posición de la tabla TEMVSCPE:

  TEMVNEMO (1) = 'BT' (bloqueo de tarjeta)

  TEMVINDI (1) = '0' (pendiente de envío)

- Sumar 1 al contador TEMVNSPE

* Nueva operatoria de terminal de *Baja de orden de envío de script de bloqueo de tarjeta*

  Es contraria a la anterior, de forma similar a como la "*Baja de orden de envío de script de Desbloqueo de PIN*" es contraria al "*Alta de orden de envío de script de Desbloqueo de PIN*".

* Modificación de la actual operatoria de terminal de *Denuncia de tarjeta*

  Si la tarjeta que se está bloqueando es EMV, y el bloqueo que se quiere introducir no es reversible, se deberá dar de alta una orden de envío de script de bloqueo de tarjeta. Se realizarán, por tanto, las mismas validaciones y tareas que se realizan en la nueva operatoria de terminal "*Alta de orden de envío de script de bloqueo de tarjeta*".

  A las tarjetas a las que se denuncia con un bloqueo reversible, no se les puede enviar el script de bloqueo de tarjeta.

3. ADAPTACIÓN DE INTERFASES

Como consecuencia de la introducción del estándar, se hace necesario intercambiar entre los emisores de las tarjetas y los adquirentes de las operaciones muchos más datos que anteriormente.

Además, muchos de estos datos corresponden a mapas de bits, criptogramas, scripts, y en general cadenas hexadecimales no imprimibles.

Ambas circunstancias son la causa de que haya surgido la necesidad de modificar los interfases de comunicación entre entidades adquirentes y emisoras. En realidad, los interfases no son directos entre ellas, sino que se centralizan en los centros de intercambio (Euro6000, Servired y Sistemas 4B, en el caso de España).

Los interfases afectados son tanto los utilizados en la conexión On Line como en el intercambio batch.

A continuación se detalla algo más el alcance de estos cambios.

3.1. ADAPTACIÓN INTERFASES ON LINE

3.1.1. Formato del interfase: ISO 8583

Los interfaces On Line de los tres centros de intercambio españoles se basan en el mismo estándar: el ISO 8583. Por tanto, el impacto al que hace referencia este apartado será siempre desde el punto de vista de ese estándar.

El ISO 8583 se basa en el envío de uno (o dos) mapas de bits en los que cada posición representa un dato distinto, y el cero y el uno la ausencia o presencia del dato en el mensaje.

La otra característica fundamental es que muchos de los datos contenidos en un mensaje ISO 8583 lo hacen en forma de estructura LV (longitud y valor), muy similar a las estructuras TLV en que se basa la representación de datos de EMV.

3.1.2. Datos EMV a intercambiar propios de los terminales

El dato más característico de un terminal dentro del ISO 8583 es el bit 22 o datos del punto de servicio (DPS), en el que se hace una descripción completa de las características del terminal relacionadas con la tarjeta o la operación.

Estos datos, aparte de identificar la transacción como EMV (modo de captura de datos, capacidades del terminal...) suministran información en el caso de verificación de usuario mediante PIN Off Line. Esta información es relevante para el emisor en el caso de gestionar la autorización.

Consta de 12 posiciones, cada una de las cuales describe una característica concreta.

Las posiciones afectadas por EMV son las siguientes:

- Posición 1: Capacidad de captura de datos del terminal

    1: No utilizado terminal

    2: Lectura de banda magnética

    5: Lectura de chip (EMV)

    6: Tecleo de los datos en el terminal

- Posición 7: Modo de captura de los datos en el terminal

1: No utilizado terminal

2: Lectura de banda magnética

5: Lectura de chip (EMV)

6: Tecleo de los datos en el terminal

8: Lectura de otros tipos de chip

S: Lectura de banda magnética

T: Tecleo del relieve por "fallback" del chip

U: Información no obtenida de la tarjeta (operatoria con móvil)

- Posición 8: Método de identificación del cliente

  0: No identificado

  1: PIN (On Line u Off Line EMV)

  5: Lectura de chip (EMV)

  S: Verificación de firma manuscrita o documentación

  T: PIN de telefonía móvil (PIN 5)

  U: 3D Secure

  X: UCAF

- Posición 9: Entidad que identifica al cliente

  0 No identificado

  1 Tarjeta chip (PIN Off Line EMV)

  3 Centro autorizador

  4 Aceptador (comercio)

- Posición 10: Capacidad del terminal para modificar los datos de la tarjeta

    0 Desconocida

    1 No utilizado terminal o terminal sin capacidad

    3 Capacidad del terminal para dar mensajes

3.1.3. Resto de datos EMV a intercambiar

El resto de datos a intercambiar, relativos a la tarjeta, al terminal, o a la propia operación, están agrupados dentro de un único bit, el 55. Como son bastante numerosos, el estándar ISO 8583 decidió no asignar un bit a cada uno, sino agruparlos dentro del bit 55, pero manteniendo su estructura TLV. Incluso el propio bit 55 tiene estructura TLV.

Los datos que el terminal puede enviar al emisor (vía centro de intercambio) son los siguientes:

Datos de la tarjeta

5F34 Número secuencial de la tarjeta

9F26 Criptograma de aplicación

9F27 Información del criptograma de aplicación

9F10 Datos de aplicación del emisor (IAD)

9F36 Contador de transacciones de aplicación

82 Perfil de intercambio de la aplicación (AIP)

Datos del terminal

9F34 Resultados de los métodos de verificación de usuario (CVMR)

95 Resultados de verificación del terminal (TVR)

9A Fecha de la transacción

9F37 Número aleatorio

9C Tipo de transacción

9F1A Código de país del terminal (TCC)

9F33 Capacidades del terminal

9F1E Número de serie del terminal

Datos de la operación

9F02 Importe de la transacción

9F03 Otro importe (cashback)

5F2A Código de divisa

Datos opcionales

9F35 Tipo de terminal

9F53 Código de categoría de la transacción (MasterCard)

9F09 Número de versión de la aplicación

9F41 Contador de secuencia de la aplicación

En la repuesta del Emisor a la tarjeta, pueden aparecer datos adicionales:

Datos adicionales

91 Datos de autenticación del emisor

8A Código de respuesta de autorización

71 Plantilla 1 de Scripts de emisor

72 Plantilla 2 de Scripts de emisor

3.2. ADAPTACIÓN INTERFASES BATCH

Los interfases batch utilizados por los centros de intercambio son bastante diferentes, e incluso un mismo centro tiene interfases diferentes dependiendo de la entidad con la que intercambie datos.

La mayoría de estos interfases son ficheros planos con una estructura fija, que se acomodan poco a la estructura de los nuevos datos EMV. Únicamente Sermepa tiene un interfase batch que cumple el ISO 8583, aunque la tendencia lógica será que todos los demás centros seguirán ese mismo camino.

Por tanto, la lista dada para el interfase On Line es válida para el interfase batch, en cuanto a impacto del estándar EMV, así como los desarrollos y adaptaciones propuestos.

3.3. DESARROLLOS Y ADAPTACIONES PROPUESTOS

* Modificación proceso de *Interpretación Mensajería ISO 8583*

  La entidad ya debería disponer de procesos de interpretación de la mensajería ISO 8583, tanto la recibida, como de la que debe de enviar.

  Estos procesos deberán adaptarse para tratar los dos bits afectados, 22 y 55, y en este último caso tratar todos los TAGs de los que consta ese bit 55. Deberá identificarlos y pasarlos al centro autorizador.

  Del bit 22 tomará el indicador de operación en "fallback", ya que el Emsiro lo necesita de cara a las decisiones de autorización.

  Así mismo, deberá el formar el bit 55 de respuesta con los nuevos datos, que le serán proporcionados por el centro autorizador.

  Este indicador general afecta a todas las tarjetas de la entidad. Cuando esté desactivado, el centro autorizador no generará ni enviará a las tarjetas ningún script.

4. CONCLUSIONES

4.1. SITUACIÓN ACTUAL

La migración a EMV, en cuanto a cifras, está en la siguiente situación:

- La migración de los terminales está en la recta final, con un 82% de los TPVs ya migrados y un 97% de los cajeros.

- En cambio, sólo un 9,5% de las tarjetas han sido migradas, lo que representa un volumen muy bajo

Las cifras son del primer trimestre de 2.009 (Fuente: Comisión de Seguimiento de la Migración a la SEPA, presidida por el Banco de España, dirección de Internet [SEPA]).

De estos datos se puede deducir que hay riesgo de incumplir la fecha del 31 de diciembre de 2.010, en la cual SEPA estableció el límite para la migración de todas las tarjetas a EMV.

La mayoría de las entidades financieras tienen casi a punto sus aplicaciones para comenzar a emitir de forma masiva tarjetas EMV, pero la realidad es que las cifras dicen que la migración acaba de comenzar. Muchas de las entidades aún no han emitido ni una tarjeta EMV, y otras lo han hecho pero en forma de "pilotos".

En una emisión "piloto", la entidad fabrica sólo unos pocos plásticos, que distribuye entre los propios empleados de la entidad. Estos empleados se encargan de operar con las nuevas tarjetas, detectar posibles anomalías en el funcionamiento y comunicar esas anomalías a los técnicos. Los técnicos a su vez, tras investigar y descubrir el origen del problema, corrigen lo que sea necesario consiguiendo de esta forma la depuración progresiva de los nuevos desarrollos.

En resumen, aunque la migración a EMV está bastante avanzada en el aspecto técnico, aún está en las primeras fases en cuanto al grado de penetración.

Se trata, además, de un proceso ya irreversible: a medio plazo, todas las tarjetas españolas, y la mayor parte de los terminales serán EMV, provocando que la mayoría de las operaciones también lo sean.

La introducción del estándar está empezando ya a reducir el fraude, aunque mínimamente. Esta rebaja será más significativa a medida que el porcentaje de tarjetas EMV vaya aumentando.

Ahora bien, también existen algunos problemas que se deberán ir solucionando en el futuro, como por ejemplo:

- el estándar no es global (Estados Unidos, África, Asia no lo han adoptado todavía), y está lejos el momento en que lo llegue a ser. Esto provoca que las tarjetas EMV funcionen como tarjetas de banda magnética tradicionales cuando salen de la "zona EMV", perdiéndose todas las ventajas en la seguridad aportadas por el estándar.

- sería deseable que se extendiese el uso del PIN a todas las operaciones, independientemente del tipo de terminal en el que se realicen. En España se debería ir sustituyendo la firma por el PIN, como método de autentificación del titular en los comercios. En este caso, el problema es de procedimiento, de acostumbrar a comerciantes y clientes, más que un problema técnico, ya que es muy sencillo personalizar las tarjetas EMV para que sólo admitan la firma como método de autentificación cuando sea imposible teclear el PIN. Ahora mismo, en España aún es válido el llamado "bypass" de PIN, es decir, cuando el terminal del comercio comprueba que la tarjeta es EMV y solicita el PIN, el comerciante puede omitir esta introducción y seguir normalmente con la operación. Esto debería ser evitado.

Como conclusión final, podría decirse que el estándar, aunque ya ha empezado a aportar beneficios en cuanto a la seguridad de las operaciones, aún no ha alcanzado el grado de madurez necesario como para que se empiecen a notar sus efectos a nivel global.

Es más, en esta primera fase, y en países como España, el fraude ha aumentado, ya que los defraudadores se han ido desplazando hacia el sur, desde los países en los que el EMV está más avanzado (Alemania, Francia, Reino Unido), hacia España. En nuestro país, las tarjetas de banda magnética siguen siendo mayoría, y son presa fácil del "skimming" (clonado de tarjetas válidas), que sigue siendo la primera causa de fraude.

4.2. EVOLUCIÓN FUTURA

A la hora de hablar de cuál puede ser el futuro de EMV, hay tres aspectos a considerar:

- Posibles mejoras técnicas
- Posibles mejoras operativas
- Nuevos productos y estándares

4.2.1. Posibles mejoras técnicas

La seguridad es uno de los aspectos en los que más se está investigando, ya que también es uno de los rasgos más destacados del estándar EMV.

En este sentido, los avances en cuanto a criptografía son los que más aportaran a esa seguridad. Para hacer más robusta la seguridad de las claves utilizadas, la solución más inmediata es ampliar el tamaño de las claves. Eso es algo que EMV hace periódicamente, ya que es algo que dificulta mucho los posibles ataques de "fuerza bruta" contra la seguridad del estándar.

Otra solución para mejorar la protección criptográfica es la de utilizar algoritmos más seguros. En este sentido, hay una línea de investigación abierta para sustituir el RSA como algoritmo estándar para criptografía asimétrica, por otro algoritmo más potente.

Uno de los que se están investigando es el denominado algoritmo de Curva Elíptica, (o por sus siglas CCE, Criptografía de Curva Elíptica). Permite mantener una seguridad similar a la de RSA pero utilizando claves bastante más cortas.

Ya en otro sentido totalmente distinto, hay también evolución en cuanto a la tecnología empleada: las tarjetas sin contacto, o de proximidad, que incorporan una antena para transmisión de datos por radiofrecuencia, están ganando terreno ya que permiten prescindir de los lectores de tarjetas típicos, que podían ser manipulados con objetivos fraudulentos, al ser accesibles al público. En cambio, con los chips sin contacto, el lector de la tarjeta (en este caso, más bien receptor que lector) puede estar escondido de la vista e inaccesible a posibles manipuladores.

4.2.2. Posibles mejoras operativas

Las mejoras en la seguridad, en cuanto a la operativa, pasan por insistir en la obligatoriedad del PIN, en todos los ámbitos, incluido el comercio típico.

La resistencia de los comerciantes a pedir el PIN ha de ser vencida, de forma que los titulares de las tarjetas se acostumbren a teclear el PIN en todos los lugares en los que quieran utilizar su tarjeta.

Una manera de conseguir esto progresivamente es el establecimiento de unos límites en cuanto al número y el importe de las operaciones permitidas con by-pass de PIN. Esto implica modificaciones en la aplicación de la entidad, pero permite cierta flexibilidad en cuanto a la obligatoriedad de introducir el PIN.

4.2.3. Nuevos productos y estándares

Los productos EMV pueden ser introducidos comercialmente simplemente apelando a su condición de tarjetas más seguras.

Ahora bien, existe la posibilidad de conseguir una penetración más rápida en el mercado si al chip EMV se le añaden otras funcionalidades que le den más potencia, como por ejemplo la firma electrónica. Las capacidades criptográficas que obligatoriamente debe reunir el chip EMV pueden ser aprovechadas para realizar los cifrados que se utilizan en el calculo de las firmas digitales.

Esta unión de EMV y firma digital está siendo explorada por diversas entidades, que están a punto de emitir tarjetas EMV con este valor añadido incorporado.

Otra de las posibilidades del chip podría ser la de almacenar diferentes certificados en la memoria que incorpora, de forma similar a como hace con los certificados EMV.

Por último, simplemente mencionar el estándar PCI DSS, un nuevo estándar que define el conjunto de requerimientos para gestionar la seguridad, definir políticas y procedimientos de seguridad, arquitectura de red, diseño de software y todo tipo de medidas de protección que intervienen en el tratamiento, procesado o almacenamiento de información de tarjetas de crédito.

Su finalidad, al igual que en el caso de EMV, es la reducción del fraude. Pero en este caso, además de VISA y MasterCard, también han intervenido American Express, JCB y Discover, todas ellas grandes compañías emisoras de tarjetas de crédito.

5. GLOSARIO

ATM:

Cajero automático. ATM son sus iniciales en inglés (Automatic Teller Machine)

Autenticar:

Asegurarse, mediante algún procedimiento, de que el interlocutor es quien dice ser. En EMV, la tarjeta y el terminal pueden autenticarse mutuamente, y también la tarjeta y el Emisor.

Autoridad de certificación (o AC):

Entidad de confianza, emisora de certificados, a los que aporta su firma, utilizando su clave pública, de forma que el poseedor del certificado puede ser autenticado. En el caso de EMV, las AACC son VISA Internacional y MasterCard.

BIN:

Prefijo del número de tarjeta (6 primeras cifras del PAN). Es un identificador único, asignado por MasterCard y VISA, que permite conocer el tipo de tarjeta, el emisor, etcétera.

Cash back:

Operación mediante la cual un titular de tarjeta percibe comisión sobre una operación realizada por otro titular debido a su intermediación.

CDA:

Método combinado de autenticación: estática y dinámica.

Centro de intercambio:

Entidad por la que pasa el flujo de operaciones con tarjeta, y que facilita el encaminamiento de las mismas entre los adquirentes y los emisores. En España hay tres: Sermepa/Servired, CECA/Euro6000 y Sistema 4B.

Certificado digital:

También denominado simplemente certificado: documento digital, firmado por una autoridad de certificación con su clave privada. El elemento firmado es la clave pública de otra entidad.

Clave:

Información secreta utilizada por los algoritmos criptográficos y que les permite cifrar y/o descifrar mensajes.

Clave de sesión:

Clave, única por sesión, utilizada durante una transacción. Suele generarse a partir de una clave maestra o de una clave de la tarjeta, y para la diversificación utiliza algún elemento que varíe en cada transacción.

Clave de tarjeta:

Clave, única por tarjeta, utilizada por la misma para diversos usos. Suele generarse por diversificación de una clave maestra.

Clave privada:

Del par de claves RSA, aquella que sólo es conocida por la entidad propietaria.

Clave pública:

Del par de claves RSA, aquella que el propietario entrega al resto de entidades.

Clave asimétrica:

Cualquiera de las dos claves (pública y privada) utilizadas en los algoritmos de criptografía asimétrica (como el RSA).

Clave simétrica:

Aquella que sirve para cifrar y descifrar, y que es conocida y compartida por las dos entidades que se intercambian el mensaje cifrado.

Confidencialidad:

Característica de un cifrado que asegura que el mensaje sólo podrá ser visto en claro por quien debe leerlo.

Criptografía asimétrica:

Criptografía basada en el uso de pares de claves, distintas para el cifrado y descifrado, denominadas clave pública y clave privada.

Criptografía simétrica:

Criptografía basada en el uso de la misma clave para cifrar y descifrar. La clave debe ser conocida y compartida por ambos interlocutores.

Criptograma:

Mensaje cifrado que sirve para la autenticación mutua de la tarjeta y el Emisor.

Custodio:

Persona encargada dentro de una entidad de mantener el secreto de las claves criptográficas.

CVC:

Código de 3 cifras grabado en el plástico de las tarjetas MasterCard y que permite su autenticación.

CVV:

Código de 3 cifras grabado en el plástico de las tarjetas VISA y que permite su autenticación.

DDA:

Método de autenticación dinámica de la tarjeta, que consiste en generar un código, diferente en cada transacción, y firmarlo con su clave privada.

Derivación:

Método criptográfico mediante el cual, partiendo de una única clave maestra, y usando elementos variables, permite generar claves diferentes para cada uno de esos elementos. Estos métodos también se denominan de diversificación.

DES:

Método simétrico de cifrado, que utiliza claves de 8 bytes.

EMV:

Estándar de seguridad para transacciones con tarjeta. Iniciales de Europay, MasterCard y VISA.

Entidad adquirente:

Aquella que facilita los terminales en los que se realizan operaciones con tarjetas de otras entidades.

Entidad emisora:

Por contraposición a entidad adquirente: aquella cuyas tarjetas operan en los terminales del adquirente.

Fallback:

Circunstancia que se produce cuando una tarjeta EMV intenta operar en un terminal EMV pero falla la lectura del chip, debiéndose intentar realizar la operación mediante la banda magnética.

Firma digital:

Código que se añade a un mensaje, generado mediante el cifrado de ciertos datos del mensaje por parte del firmante, con su clave privada, y que garantiza el no repudio del mismo.

Hash Code:

Código de redundancia que se añade a un mensaje para garantizar la integridad del mismo.

HSM:

Módulo Criptográfico, también denominado por sus siglas en inglés, “Host Security Module”, que permite realizar con seguridad procesos criptográficos, y también almacenar las claves de la entidad de forma segura.

Integridad:

Característica de un cifrado que asegura que el mensaje no ha sido manipulado.

Monedero electrónico:

Tarjeta que incluye un chip que permite realizar pagos de poco importe a gran velocidad, debido a que puede realizarlos Off Line. El saldo disponible debe haber sido cargado previamente.

NA:

También llamado Número Aleatorio, es un dato grabado en la tarjeta por el Emisor, diferente para cada tarjeta. Permite la validación del PIN en Off Line.

Offset:

Dato grabado en la tarjeta, que varía en función del PIN, y que permite calcularlo y validarlo (si se conoce la clave maestra de PIN).

PA:

Resultado de concatenar el NA con el PIN y cifrarlo consigo mismo, usando el algoritmo DES. Este dato es grabado en la tarjeta por el Emisor, y permite la validación del PIN en Off Line.

PAN:

Iniciales en inglés de "Personal Account Number". Es el número de la tarjeta, los dígitos que aparecen en el relieve del plástico y que la identifican.

PIN:

Iniciales en inglés de "Personal Identification Number". Es el número secreto asignado al titular, que usa para autenticarse en los terminales que lo requieran.

RSA:

Algoritmo de cifrado simétrico, basado en un par de claves, la privada y la pública, que realizan acciones contrarias: con una se cifra y con otra se descifra.

Script:

También llamados comandos transparentes de Emisor: comandos, porque con ellos el Emisor ordena a la tarjeta que realice determinadas acciones; transparentes, porque el Emisor los añade a la respuesta a una petición On Line de la tarjeta, sin afectar para nada a la transacción en curso; y de Emisor, porque es el Emisor quien los genera.

SDA:

Método de autenticación estática de la tarjeta, que consiste en generar un código, en la fase de personalización, que se graba en el chip de la tarjeta y ya no cambia en toda la vida de ésta. Puede ser validado por el terminal.

SEPA:

Siglas en inglés de "Single Euro Payment Area": Área Única de Pagos en Euros. Entre otras normativas, ha establecido una que obliga las entidades emisoras de tarjetas a que todas las tarjetas en circulación en los países pertenecientes al área SEPA sean EMV antes del 31 de Diciembre de 2010.

Skimming:

Fraude consistente en duplicar una tarjeta de banda magnética auténtica, copiando de manera exacta todos los datos contenidos en las pistas de esa banda. Esta técnica también se denomina "clonado" de tarjetas.

Triple DES:

Algoritmo de cifrado simétrico, basado en el DES, pero que utiliza claves el doble de largas que éste.

6. BIBLIOGRAFÍA

- [EURO071] Guía de Personalización de Tarjetas EURO6000 EMV. Parámetros de la Tarjeta.

  Versión 4.00, Enero de 2.007

  Documentación EURO6000-CECA

- [EURO072] Guía de Personalización de Tarjetas EURO6000 EMV. Perfiles de personalización.

  Versión 4.01, Enero de 2.007

  Documentación EURO6000-CECA

- [EURO073] Guía de Seguridad EMV. Criptografía Simétrica en Transacciones EMV.

  Versión 2.01, Septiembre de 2.007

  Documentación EURO6000-CECA

- [EURO074] Guía de Seguridad EMV. Servicios de Certificación EMV.

  Versión 2.00, Septiembre de 2.007

  Documentación EURO6000-CECA

- [EURO075] Autorización de Transacciones EMV.

  Versión 2.00, Enero de 2.007

  Documentación EURO6000-CECA

Direcciones de Internet

- [EMVCO] EMVCo
  http://www.emvco.com/

- [EURO] EURO6000
  http://www.euro6000.com/
  (opción → "Tecnología" → "– Tarjeta CHIP–EMV")

- [SERM] Sermepa
  http://www.sermepa.es/

- [SI4B] Sistema 4B
  http://www.4b.es/

- [SEPA] SEPA (Indicadores migración a EMV)
  http://www.sepaesp.es/docs/Indicadores_SEPA.pdf

7. ANEXOS

7.1. ANEXO A

TABLA DE ETIQUETAS DE DATOS EMV

ETIQUETA	LONGITUD	DESCRIPCIÓN DEL DATO
4F	07	Identificador de la aplicación
50	*xx*	Nombre de la aplicación
57	13	Datos equivalentes de Pista 2
5A	08	PAN
5F20	1A	Nombre de usuario
5F24	03	Fecha de expiración de la aplicación
5F25	03	Fecha de activación de la aplicación
5F28	02	Código de país de emisor
5F2D	02-08	Lenguaje preferente de la aplicación
5F30	02	Código de país emisor
5F34	01	Número de secuencia de PAN
82	02	Perfil de intercambio de la aplicación (AIP)
84	07	Nombre del Fichero Dedicado (DF)
87	01	Indicador de prioridad de la aplicación
8C	*xx*	Gestión de riesgo de la tarjeta DOL1 (CDOL1)
8D	*xx*	Gestión de riesgo de la tarjeta DOL2 (CDOL2)
8E	*xx*	Lista CVM (métodos de verificación de usuario)

8F	01	Índice de derivación de la clave pública de CA
90	*xx*	Certificado de la clave pública del Emisor
92	*xx*	Resto de la clave pública del Emisor
93	*xx*	Firma de los datos estáticos
94	08	Localizador de ficheros de la aplicación (AFL)
9F07	02	Control de Uso de la Aplicación
9F08	02	Número de Versión de la Aplicación
9F0D	05	Código de Acción del Emisor Default (IAC-Default)
9F0E	05	Código de Acción del Emisor Denial (IAC-Denial)
9F0F	05	Código de Acción del Emisor On Line (IAC-On Line)
9F10	var.	Datos del Emisor de la Aplicación
9F14	01	Límite Inferior Off Line
9F1F	0A	Datos Discrecionales de Pista 1
9F20	03	Datos Discrecionales de Pista 2
9F23	01	Límite Superior Off Line
9F2D	*xx*	Certificado de la clave pública para el cifrado del PIN
9F2E	*xx*	Exponente de la clave pública para el cifrado del PIN
9F2F	*xx*	Resto de la clave pública para el cifrado del PIN

9F32	01	Exponente de la clave pública del Emisor
9F38	*xx*	Lista de objeto de datos del "processing options" (PDOL)
9F42	02	Código de la moneda de la aplicación
9F44	01	Exponente de la moneda de la aplicación
9F46	*xx*	Certificado de la clave pública de la Tarjeta
9F47	*xx*	Exponente de la clave pública de la Tarjeta
9F48	*xx*	Resto de la clave pública de la Tarjeta
9F4A	01	SDA Tag List
9F51	02	Código de moneda del Emisor (*VISA*)
9F52	02	Acción por Defecto de la Aplicación (ADA) (*VISA*)
9F53	01	Límite total de operaciones Off Line consecutivas (Internacional-Moneda) (*VISA*)
9F54	06	Límite total de importe acumulado Off Line (*VISA*)
9F55	01	Indicador geográfico (*VISA*)
9F56	01	Indicador de la autenticación de emisor (*VISA*)
9F57	02	Código de país del Emisor (*VISA*)
9F58	01	Límite total inferior de operaciones Off Line consecutivas (*VISA*)
9F59	01	Límite total superior de operaciones Off Line consecutivas (*VISA*)

9F5C	06	Límite superior total de importe acumulado Off Line (*VISA*)
9F5D	01	Disponible Importe Off Line Restante (*VISA*)
9F5E	01	Límite de operaciones Off Line consecutivas internacionales (*VISA*)
9F72	01	Límite total de operaciones Off Line consecutivas (Internacional-País) (*VISA*)
9F73	04	Factor de conversión de moneda (*VISA*)
9F74	06	Código de autorización VLP del Emisor (*VISA*)
9F75	06	Límite total de importe acumulado Off Line – Doble moneda (*VISA*)
9F76	02	Código de moneda secundaria de la aplicación (*VISA*)
9F77	06	Límite de fondos VLP (*VISA*)
9F78	06	Límite por transacción única VLP (*VISA*)
9F79	06	Fondos VLP Disponibles (*VISA*)
9F7E	30	Datos del Ciclo de Vida de la Aplicación (*MasterCard*)
C3	03	Código de acción del emisor de la tarjeta Denial (CIAC-Denial) (*MasterCard*)
C4	03	Código de acción del emisor de la tarjeta Off Line (CIAC-Off Line) (*MasterCard*)
C5	03 ó	Código de Acción del Emisor de la tarjeta On Line (CIAC-On Line) (*MasterCard*) Indicador de bloqueo mediante script (*VISA*)

	01	
C6	05	Código de Acción de TVR de la Tarjeta (*MasterCard*)
C7	01	Longitud de datos de CDOL1 (*MasterCard*)
C8	01	Índice de derivación de la clave (*MasterCard*)
CA	06	Máximo Importe Inferior Acumulado Off Line (*MasterCard*)
CB	06	Máximo Importe Superior Acumulado Off Line (*MasterCard*)
CE	01	Exponente del Factor de Control No Nacional (*MasterCard*)
D1	19	Tabla de conversión de moneda (*MasterCard*)
D3	12	Tabla de chequeo adicional (*MasterCard*)
D5	*xx*	Control de la aplicación (*MasterCard*)
D6	02	Código de respuesta del ARPC por defecto (*MasterCard*)

(Información extraída del documento [EURO071])