Objeto del proyecto: Definición de la especificación del Código Seguro Para Interoperabilidad en el Transporte – TESC (Tarjeta Española Sin Contacto).	**Fecha:** 25/10/2017
	Versión actual **0.7**

Especificación TESC

Coordinador del proyecto: ITS España	
Dirección: Serrano 216, 1º Dcha.	**CP**: 28016
Teléfono: 91 353 13 43 **Mail**: itsspain@itsspain.com	

Versión	Autor	Comentarios
0.1	Miguel Cardo (Fidesmo)	Primer borrador MIFARE
0.2	Miguel Cardo (Fidesmo)	Especificación lugar de almacenamiento MAC
0.3	Miguel Cardo (Fidesmo)	Correcciones tras las pruebas con Almex
0.4	Francisco Sanchís Caurín (Pay-[In])	Actualización tras prueba Piloto Valencia
0.6	Miguel Cardo(Fidesmo)	Incorporación de DESFIRE y JAVA CARD
0.7	Jaime Huerta (ITS España)	Primera versión para aprobación

ÍNDICE

1. Introducción

1.1. Introducción a la TESC

Las Tarjetas sin Contacto se han constituido en un elemento imprescindible en cualquier sistema moderno de Pago en el Transporte Público. Ante esta perspectiva y bajo el amparo del Ministerio de Fomento, se inició hace unos años el Proyecto Tarjeta Española Sin Contacto (TESC) llegando a formar parte del vigente Plan de Infraestructuras, Transporte y Vivienda del Ministerio.

El Proyecto TESC se planteó inicialmente como una solución sencilla y estándar adaptable a cualquier Operador y Autoridad de transporte con el fin de limitar la heterogeneidad de soluciones que estaban apareciendo en cada entorno geográfico. Sin embargo, con el desarrollo de las reuniones se pasó a buscar una solución que permitiera la interoperabilidad de los diferentes Sistemas de Transporte.

Tras múltiples trabajos y pilotos desarrollados, el sistema finalmente definido se basa en una codificación segura que permite el registro de los usuarios al utilizar los servicios de diferentes operadores de manera que es posible una posterior gestión de la información donde se resuelvan las necesarias compensaciones económicas.

La base del Sistema es la Entidad o Entidades Coordinadoras que mantendrán relaciones contractuales y económicas tanto con los operadores adscritos al Sistema como con Entidades Emisoras TESC, que emitirán códigos para facilitar el acceso al Transporte a sus clientes.

Para el usuario, la TESC, es una funcionalidad agregada a cualquier tarjeta física o virtual (wearable, SIM-NFC, elemento seguro, etc) sin contacto, sea o no de transporte. TESC se basa en una codificación única, sencilla y segura, almacenada en el espacio libre de cualquier tarjeta sin contacto en funcionamiento, o de nueva creación. Como podrá verificarse, las estructuras de información definidas son susceptibles de ser utilizadas más adelante soportadas por otras tecnologías como códigos QR, Bluetooth, etc, con las que transmitir la identificación del usuario que accede al Sistema de Transporte.

Del mismo modo que los protocolos bancarios EMV, la filosofía de validación TESC es de sólo lectura, si bien se han incluido especificaciones para grabar en el soporte la última cancelación para aquellos casos en los que puede ser necesaria o de utilidad dicha funcionalidad compensando las complicaciones que ello añade.

Estas especificaciones técnicas son generadas y actualizadas desde el Comité Tarjeta Española Sin Contacto, presidido por la Dirección General de Transporte Terrestre del Ministerio de Fomento auxiliado en la secretaría por ITS España.

1.2. Protocolo de validación

La validación TESC se realiza mediante un software agregado a cualquier lector (validador) sin contacto que entra en funcionamiento únicamente cuando la validación por defecto devuelva un error (tarjeta o título no válido, etc...)

El validador (de un operador adscrito al sistema TESC) comprueba, del modo habitual la validez de una tarjeta. Solo si esta falla, ejecuta la "rutina" que busca la identificación TESC, y si esta no existe, rechaza la tarjeta.

En caso de existir información TESC, lee e interpreta los datos y en su caso acepta la tarjeta y registra su uso, con los datos TESC junto a la información del servicio utilizado.

Los datos de uso se almacenan en un fichero específico que se remite a la "entidad gestora" con los criterios y protocolos detallados en la documentación técnica y según los procedimientos contractuales acordados por las partes.

2. Estructura de Información TESC y aplicación a Mifare Classic

2.1. Nota preliminar

Es importante que los lectores acepten tarjetas con SAK = 0x38 para poder emplear tarjetas con emulación Mifare, como es el caso de las universitarias en España.

Otro factor a tener en cuenta para la lectura e interpretación del documento es que el criterio de escritura de bits es "BIG ENDIAN".

2.2. Sector 0

El sector 0 contiene un byte con el número del sector TESC, precedido de una cadena fija de 2 bytes que podrá estar en cualquiera de los bloques 1 o 2.

- Cadena fija ("identificador TESC"): RM (0x524D en ASCII)
- Byte con el número del sector TESC
- Clave de lectura: FFFFFFFFFFFF

Ejemplo: en el bloque 01 se indica que el sector TESC es el 4.

Bloque 00 | 24FE4EBB2F0804006263646566676869

Bloque 01 | 524D040000000000000000000000000000

Bloque 02 | 00000000000000000000000000000000

Bloque 03 | 000000000000FF078069FFFFFFFFFFFF

Debido a que las claves de lectura a emplear en este sector serán las claves "F", se especifica que en este caso, sea la clave A, con condición únicamente de lectura la que sea modificada.

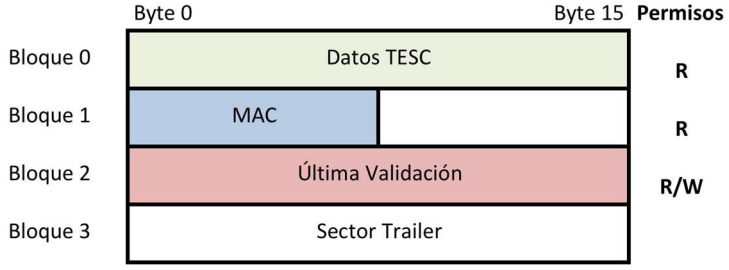
Como se indica, la cadena "524D" + "XX" (Sector TESC), podrá estar en cualquier ubicación de los bloques 1 o 2 del sector 0 de la tarjeta. Esta posición sera definida en cada caso por la Entidad Emisora (Propietaria) de la tarjeta que lo ajustará al uso que haga de su tarjeta.

Los integradores actualizarán sus equipos para añadir la posibilidad de autenticarse con las condiciones TESC antes citadas y aplicando la búsqueda y análisis de la cadena TESC.

2.3. Sector TESC

2.3.1. Estructura del sector TESC

El sector TESC contiene los datos que identifican al emisor y usuario de la tarjeta ("Datos TESC") y un MAC o firma que protege dichos datos.



2.3.2. Datos TESC

Campo	Bytes	Comentarios
Versión	2	Versión o tipo del mapa de memoria
Entidad	2	ID de la entidad coordinadora
Emisor	2	ID del emisor de la tarjeta
Usuario	8	ID del usuario, única para la combinación {Entidad, Emisor}
Validez	2	Último día de validez de la tarjeta como TESC Codificado a nivel de bit: aaaaaaa – mmmm – ddddd en el que el año 0 equivale al año 2000. Ejemplos: 25/1/2016 → 0x2039 27/10/2026 → 0x355B

2.3.3. MAC (firma)

El MAC (Message Authentication Code) protege los datos del sector TESC de la tarjeta frente a modificaciones no autorizadas y confirma su autenticidad. Se aplica sobre la concatenación del UID (número de serie de la tarjeta) y los datos TESC.

Se utilizará el algoritmo propuesto por Global Platform en el apéndice B.1.2.2 de la Card Specification[1]. Al tratarse de un algoritmo utilizado para proteger las comunicaciones con tarjetas inteligentes, aseguramos que los fabricantes de lectores e integradores de sistemas dispondrán de una implementación de referencia.

El algoritmo utiliza una clave secreta K_{MAC} de 16 bytes conocida por la entidad coordinadora de la tarjeta. Esta clave debe ser conocida por los integradores y también por los agentes que participen en el manejo de la tarjeta TESC, como los son los proveedores de soluciones tecnológicas.

Para las pruebas piloto se usará K_{MAC}: "*C3B2D1F40AA5839AA9385AA04F1D2B3C*"

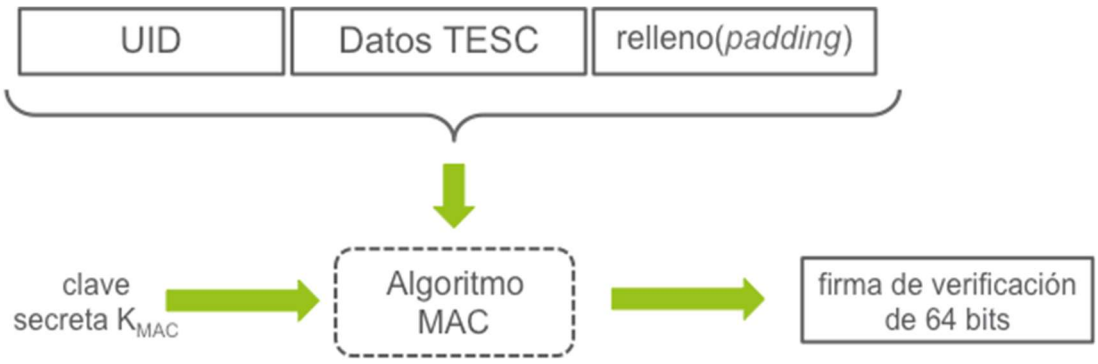


Figura 1 Algoritmo para el cálculo de MAC

Detalles

- Clave DES de doble longitud (16 bytes)
- Vector de inicialización (ICV): puesto a cero.

[1] *GlobalPlatform Card Specification version 2.*2.1. Document reference: GPC_SPE_034. Disponible en http://globalplatform.org/specificationscard.asp

- Algoritmo: especificado en ISO 9797-1 como *MAC Algorithm 3*. También se conoce como *Retail MAC*. En la librería de Java *BouncyCastle* el nombre de este algoritmo es "ISO9797ALG3Mac"[2]
- Relleno o *padding*: Para asegurar que la concatenación del UID y los datos TESC sea un múltiplo de 8 bytes, se propone rellenar como especifica Global Platform:
  a. Añadir '80' al final, sea cual sea la longitud de la concatenación UID+TESC.
  b. Si el resultado es múltiplo de 8 bytes, no hace falta añadir más.
  c. Si no, añadir ceros hasta que la longitud del bloque sea múltiplo de 8 bytes.

2.3.4. Claves MIFARE Classic

Se propone que la clave a modificar del sector TESC sea la clave A. A la vez como se detalla a continuación se propone que se configuren los bits de acceso para ajustar las condiciones de la forma más segura.

Clave de lectura / escritura

Conocida preferentemente por el emisor de la tarjeta. En este caso se deben configurar los permisos de la forma más segura posible para que el menor número de entidades puedan actuar sobre la tarjeta en modo escritura.

Según la operativa habitual, debería emplearse la clave A con permisos de lectura/escritura para el sector TESC, ajustándose los bits de acceso a los bloques. De esta forma se permite la escritura en el bloque 2 del sector TESC para almacenar la última validación.

Por ello la propuesta sera para el sector TESC:

- Bloque 0: Datos TESC
  - Clave A: Lectura
  - Clave B: Lectura / Escritura
- Bloque 1: MAC
  - Clave A: Lectura
  - Clave B: Lectura / Escritura
- Bloque 2: Datos última validación
  - Clave A: Lectura / Escritura
  - Clave B: Lectura / Escritura
- Bloque 3: Tráiler
  - Clave A: Lectura
  - Clave B: Lectura / Escritura

La configuración de los bits de acceso del bloque trailer seran: "F4 BF 00 69".

Cálculo de clave

Se deriva a partir del UID de la tarjeta aplicando el siguiente algoritmo:

a. Se forma una cadena de 8 bytes "cs" + UID + "eT": [6373U1U2U3U46554]

b. Al resultado se le aplica cifrado DES en modo ECB. Se propone como clave maestra provisional: "TESC2016" = [5445534332303136]

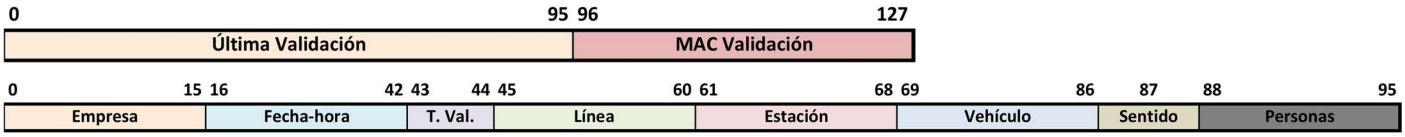
c. De los 8 bytes resultantes, la clave de lectura del sector TESC serán los 6 primeros bytes.

[2] http://www.cs.berkeley.edu/~jonah/bc/org/bouncycastle/crypto/macs/ISO9797Alg3Mac.html

2.3.5. Última validación

Para poder verificar correctamente la última validación del usuario, se define el bloque 2 del sector TESC para almacenar la información sobre la validación.

En el bloque 2 para un total de 128 bits se destinarán 96 bits para guardar la información de la validación y 32 bits para una MAC de seguridad. Quedando pues del siguiente modo la composición del bloque 2:



De forma especifica:

- Empresa (16 bits): Empresa operadora donde se realiza la validación.
- Fecha-Hora (27 bits): Fecha y hora de la validación. Fecha (16 bits en el formato anteriormente descrito) y Hora (11 bits). La hora se especifica como Hora(5 bits) y Minutos (6 bits): hhhhhmmmmmm
- Tipo de Validación (2 bits): Entrada, salida, transbordo.
- Línea (16 bits): Línea donde se realiza la validación.
- Estación (8 bits): Estación parada donde se realiza la validación.
- Vehículo (18 bits): Vehículo donde se accede si procede.
- Sentido (1 bit): Sentido de la marcha al realizar la validación.
- Personas (8 bits): Personas que han validado.

Los 32 bits de la "MAC Última Validación" se calculan siguiendo los siguientes pasos:

- Se siguen los mismos criterios que para el calculo de la MAC obtenida a partir de los datos TESC y ubicada en el bloque 1.
- Con los 64 bits obtenidos se separa en dos bloques de 32 bits y se realiza un OR Exclusivo del siguiente modo: (Bit n) XOR (Bit n+32), obteniendo la MAC de 32 bits incluida al final del bloque 2.

3. Ejemplos de cálculos

3.1. Cálculos de diversificación

En la siguiente tabla se muestran algunos valores de ejemplo que pueden servir para comprobar si los algoritmos implementados realizan correctamente el cálculo de la clave TESC diversificada de lectura/Escritura:

UID	Cadena detección sector 0	Versión	Entidad	Emisor	Usuario	Fecha de validez	Clave maestra para derivar clave Mifare	Clave lectura Mifare
4FE97D06	524D	0001	0001	0026	0000000000F10005	355B	5445534332303136	E0A3C5191F76
4F7D7D06	524D	0001	0001	0026	0000000000F10006	355B	5445534332303136	B7A714DB3DAC
84D94BBB	524D	0001	0001	0026	0000000000F10005	355B	5445534332303136	3848C46FBD90
A4C945BB	524D	0001	0001	0026	0000000000F10005	355B	5445534332303136	CC4258A50461

3.2. Cálculos de MAC

En la siguiente tabla se muestran algunos valores de ejemplo que pueden servir para comprobar si los algoritmos implementados realizan correctamente el cálculo de la MAC de seguridad:

UID	Cadena detección sector 0	Versión	Entidad	Emisor	Usuario	Fecha de validez	Kmac de 16 bytes	MAC
4FE97D06	524D	0001	0001	0026	0000000000F10005	355B	C3B2D1F40AA5839AA9385AA04F1D2B3C	817AD0EAB8D11F5E
4F7D7D06	524D	0001	0001	0026	0000000000F10006	355B	C3B2D1F40AA5839AA9385AA04F1D2B3C	1B1E687321C66232
84D94BBB	524D	0001	0001	0026	0000000000F10005	355B	C3B2D1F40AA5839AA9385AA04F1D2B3C	FD7B71ECCA9A145E
A4C945BB	524D	0001	0001	0026	0000000000F10005	355B	C3B2D1F40AA5839AA9385AA04F1D2B3C	72213769F3078491

4. Información TESC / TARJETAS **DESFIRE**

La información contenida en las tarjetas TESC sobre MIFARE DESFIRE será idéntica a la almacenada en las MIFARE CLASSIC/PLUS.

4.1. Identificación TESC

La forma de identificar que una tarjeta DESFIRE está asociada al esquema TESC es mediante la presencia de una *aplicación* (terminología DESFIRE) identificada por un AID (Application Identifier) de 3 bytes reservado para TESC a nivel nacional.

4.2. Datos TESC

Los datos TESC se almacenarán en dos registros de propósito general ("standard data files"), cada uno de 16 bytes:

- Registro almacenando los datos descritos en el apartado correspondiente de MIFARE Classic.
- Registro almacenando la firma MAC de protección de los datos anteriores
- Para los datos de validación, se propone un tercer registro.

4.3. Claves TESC

Los registros definidos en la sección anterior estarán protegidos por dos claves:

- Clave de lectura, derivada según un algoritmo similar al descrito en correspondiente de MIFARE Classic y compartida con los operadores de transporte participantes en el esquema TESC.
  Esta clave será también la clave de lectura/escritura para el registro que contiene los datos de validación.
- Clave de escritura, solamente conocida por la entidad emisora de la tarjeta.
- Clave MAC, con las mismas reglas que en el caso MIFARE Classic.

5. Información TESC / TARJETAS **JAVACARD**

El procedimiento de detección de TESC en este tipo de tarjetas es similar al propuesto para DESFIRE. La forma de recuperación de los datos se hará mediante comandos específicos.

El interfaz a usar será ISO 14443/4

5.1. Identificación TESC

Los datos TESC estarán almacenados en una aplicación específica, identificada con un AID reservado a nivel internacional. El Ministerio de Fomento, a través del Comité TESC, reservará una raíz o RID de uso exclusivo siguiendo el proceso definido en ISO 7816/5.

Bastará el comando SELECT para detectar si la aplicación con el AID TESC está presente en la tarjeta.

5.2. Datos TESC

Los datos TESC estarán almacenados en el applet TESC. La forma de almacenarlos queda a elección del implementador, pero se estandarizan los siguientes comandos:

- Lectura de los datos TESC
- Lectura de la firma digital de los datos TESC
- Escritura de los datos de validación.
- Lectura de los datos de validación

Ambos comandos se podrán ejecutar sin necesidad de autenticarse ante la tarjeta.

5.3. Claves TESC

- Las claves de escritura de los datos TESC serán conocidas únicamente por la entidad emisora de la tarjeta.
- No serán necesarias claves de lectura de los datos TESC: los comandos definidos en el apartado anterior se podrán ejecutar sin necesidad de autenticación mutua lector-tarjeta.
- Para la escritura de los datos de validación, se propone una clave simétrica derivada según el esquema propuesto en el apartado de Mifare Classic. La lectura no necesitará de clave.
- Se propone un sistema de clave asimétrica en la cual la clave privada sea únicamente conocida por la entidad coordinadora. Dicha clave privada se empleará para generar una firma digital, almacenada en la tarjeta y comprobable por cualquier operador de transporte, que tendrá acceso a la clave pública.

Para minimizar el espacio ocupado por la firma digital se define como algoritmo de firma el ECDSA (Elliptic Curve Digital Signature Algorithm) usando la curva P256 Brainpool y la función de hash SHA-2.