Objeto del proyecto: Definición de la especificación del Código Seguro Para Interoperabilidad en el Transporte – TESC/DAT4m (Tarjeta Española Sin Contacto-Token Digital de Acceso para la movilidad).	**Fecha:** 08/03/2024
	Versión actual **2.0**

Especificación TESC/DAT4m para Operadores de Transporte

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 (1)	Miguel Cardo (Fidesmo) José Martín (Busmatick)	Primer borrador MIFARE
0.4 (2)	Francisco Sanchís Caurín (Pay-[In])	Actualización tras prueba Piloto Valencia
0.6 (3)	Miguel Cardo(Fidesmo)	Incorporación de DESFIRE y JAVA CARD
0.7 (4)	Jaime Huerta (ITS España)	Primera versión para aprobación
1 (5)	José Javier Jiménez (Diusframi) Martín Gruver (Palma Tools) Carlos Veciana (Almex) Jaime Huerta (ITS España)	
2(6)	Lidia Hipólito (Palma Tools) Gregorio Haro (ATMV) Javier Saralegui (NTT DATA)	Actualización para implementación en Valencia y Asturias

ÍNDICE

1. INTRODUCCIÓN 3

1.1. INTRODUCCIÓN A LA TESC/DAT4M 3
1.2. PROTOCOLO DE VALIDACIÓN 3

2. ESTRUCTURA DE INFORMACIÓN TESC/DAT4M 4

2.1. ELEMENTOS 4
2.2. INFORMACIÓN DEL TÍTULO 4
2.3. FIRMA (MAC) 5
2.4. UID DEL SOPORTE 7

3. APLICACIÓN A MIFARE CLASSIC 7

3.1. NOTA PRELIMINAR 7
3.2. SECTOR 0 7
3.3. SECTOR TESC/DAT4M 8
3.3.1. ESTRUCTURA DEL SECTOR TESC/DAT4M 8
3.3.2. DATOS TESC/DAT4M 9
3.3.3. MAC (FIRMA) 9
3.3.4. CLAVES MIFARE CLASSIC 9

4. INFORMACIÓN TESC/DAT4M / TARJETAS DESFIRE 11

4.1. IDENTIFICACIÓN TESC/DAT4M 11
4.2. DATOS TESC/DAT4M 12
4.3. CLAVES 12

5. INFORMACIÓN TESC/DAT4M / TARJETAS JAVACARD Y TELÉFONOS ANDROID 12

5.1. IDENTIFICACIÓN TESC/DAT4M 12
5.2. DATOS TESC/DAT4M 13
5.3. CLAVES 13

1. Introducción

1.1. Introducción a la TESC/DAT4m

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 entonces Ministerio de Fomento, se inició hace unos años el Proyecto Tarjeta Española Sin Contacto (TESC) llegando a formar parte del 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. Para el caso del QR se ha definido una propuesta de Token TESC en el documento *ITS_Interoperabilidad en el TP basada en QR - Modelos IO.*

Del mismo modo que los protocolos bancarios EMV en entornos de transporte, la filosofía de validación TESC es de sólo lectura y autenticación de datos, si bien se han apuntado 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 por Carretera del Ministerio de Transportes y Movilidad Sostenible 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/DAT4m

La clave de la tecnología TESC/DAT4m está en la sencillez y claridad de los elementos centrales del sistema de información que se describen seguidamente.

2.1. Elementos

Existen tres elementos fundamentales que componen el conjunto de información al que debe acceder un Operador de Transporte para poder proceder a la correcta validación de un título con estructura TESC/DAT4m

- Información del Título
- FIRMA o MAC (Message Authentication Code)
- UID del soporte

2.2. Información del Título

Se compone de 16 bytes que se distribuyen de la siguiente manera:

Campo	Bytes	Descripción
VERSIÓN	1	Versión de la norma
MAPA MEMORIA	1	Identificador del Mapa de memoria utilizado para distribuir la información en el TOKEN
INFORMACIÓN	14	Resto de Información que compone el Token

En la versión actual (Versión =1) se plantea un primer Mapa de Memoria (Mapa de Memoria=1), si bien en próximas versiones se añadirán diferentes mapas de memoria que añadan otros datos o los organicen de una manera diferente. Un ejemplo puede ser cuando se diseñe un título que requiera definir también la hora donde empieza o termina su validez. Los dos primeros campos siempre deberán mantenerse. Todas las versiones de datos futuras serán compatibles con esta primera versión

El Mapa de Memoria nº 1 estructura la información de la siguiente manera:

Campo	Bytes	Comentarios
VERSIÓN	1	Versión de la norma
MAPA MEMORIA	1	Identificador del Mapa de memoria utilizado para distribuir la información en el TOKEN
ENTIDAD	2	ID de la entidad coordinadora Codificado a nivel de bit: ppppppppppp – vvvvvvv – ssssssss Donde: • p= País: se corresponde con los 3 dígitos del prefijo telefónico internacional de cada país: para España, 034. En formato BCD. • v= Provincia: se corresponde con el código INE de 2 dígitos para cada provincia: para Valencia, 46. En formato BCD. • S= se corresponde con el número de secuencia asignado a la entidad dentro del país y la provincia, en formato BCD. Ejemplo 01.
EMISOR	2	ID del emisor de la tarjeta Se codifica de la misma forma que la ENTIDAD.

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

En versiones posteriores aparecerán más mapas de memoria según se detecten necesidades.

2.3. Firma (MAC)

La firma o 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 del soporte) y los datos TESC (16 bytes de Información del Título).

De esta manera, no sólo de verifica la integridad de la información, sino que además se impide que se copie la información en otro soporte con un UID diferente.

En las pruebas iniciales se utilizó el algoritmo propuesto por Global Platform, Card Specification[1]. Al tratarse de un algoritmo utilizado para proteger las comunicaciones con tarjetas inteligentes, se aseguraba que los fabricantes de lectores e integradores de sistemas dispondrían de una implementación de referencia. Para el desarrollo del sistema se ha optado por la utilización de pares de claves asimétricas. Dado que en posterior revisión se ha verificado que el algoritmo para firma basado en claves asimétricas recomendado en la citada referencia de Global Platform con RSA requiere un tamaño de firma que no es viable[2] para el caso de las Tarjetas sin contacto de transporte más comúnmente utilizadas (para esta versión del documento se incluye la propuesta para MIFARE Classic ®/ MIFARE PLUS ® y MIFARE DESFIRE ®), la propuesta se basa en dos algoritmos seleccionados para la firma:

- Algoritmo de firmado simétrico: AES-128 de acuerdo a "NIST Special Publication 800-38B – Recommendation for Block Cipher Modes of Operation – The CMAC Mode for Authentication", el firmado podrá ser completo (16 bytes) o aplicar un firmado reducido a 4 bytes (para optimizar el tamaño del QR). El firmado completo será necesario cuando se desee utilizar Módulos de Seguridad como Mifare SAM que permite que el SAM custodie las claves simétricas y que sólo puedan ser utilizadas para verificar y no se pueda usar para firmar, lo que requiere la firma completa.
- Algoritmo de firmado asimétrico: El firmado asimétrico se realizará obteniendo un hash de los datos TESC+UID (SHA1) aplicando sobre ese Hash mismo el algoritmo asimétrico basado en Curvas Elípticas ECC160-secp160r1. Se utiliza el algoritmo ECC160 porque es el algoritmo asimétrico que genera el menor tamaño de firma posible (40 bytes) cumpliendo con los niveles de seguridad mínimos aceptables en la actualidad.

  Así, el algoritmo de clave asimétrica utiliza pares de claves pública y privada de longitud en bits. La parte privada de la clave será conocida por la entidad coordinadora del Sistema para poder emitir la Firma correspondiente a cada token. En cambio, la parte pública de la clave será conocida por totos los agentes del Sistema con el fin de poder verificar la autenticidad de las firmas. Esta parte publica de la clave debe ser conocida por los integradores y también por los agentes que participen en el manejo de los tokens TESC/DAT4m, como los son los proveedores de soluciones tecnológicas

Se propone que para la firma del token para las tarjetas sin contacto de transporte:

- Se firme con algoritmo de clave simétrica (propiedad del propietario/ emisor de la tarjeta),
- Adicionalmente, siempre que haya espacio disponible, se firme con algoritmo de clave asimétrica y se almacene la firma de 40 bytes

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

[2] Existen claves asimétricas RSA menores de 512 bits pero se considera que su seguridad ya está comprometida.

Proceso de generación de firma:

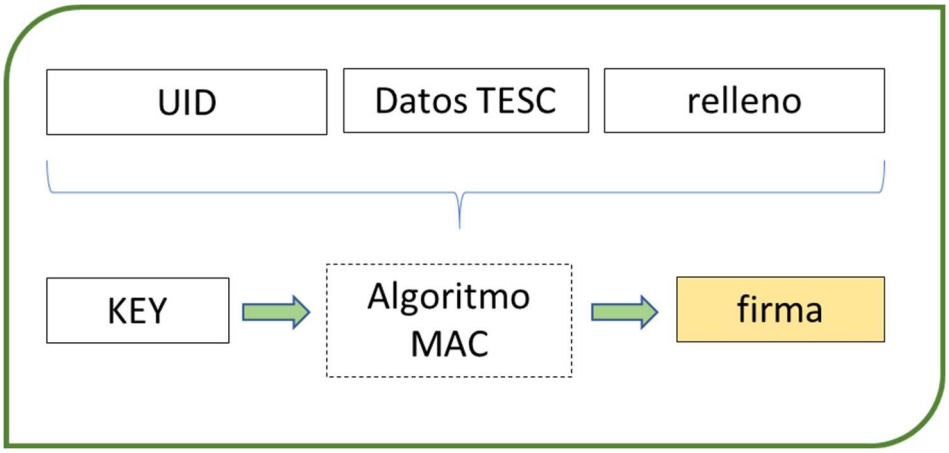

Figura 1 Algoritmo para el cálculo de MAC

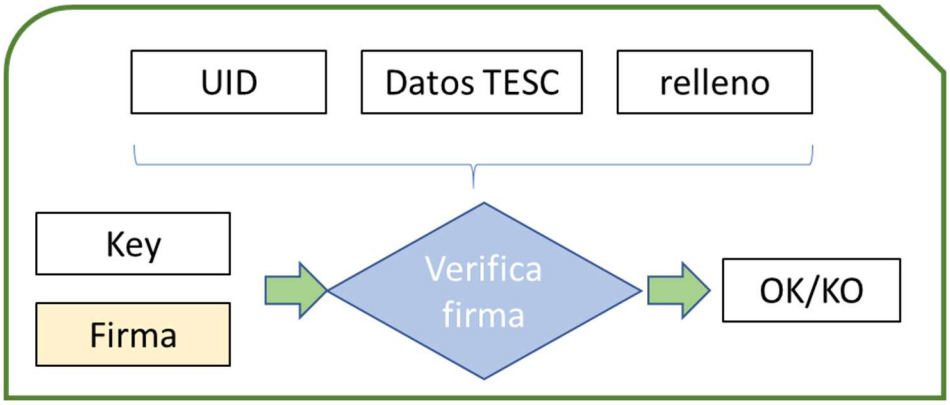

Figura 2 Algoritmo para el verificar la firma de MAC

El proceso de generación y verificación de firma es como sigue: el emisor genera un token con los datos y el UID,:

- Con la clave AES para la firma con algoritmo de claves simétricas
- Realiza un HASH de estos datos y cifra este Hash con la parte privada de la clave de emisor para la firma con algoritmo de claves asimétricas.

En el punto de verificación, con los datos del token y el UID; en paralelo:

- Con la clave AES para firma con algoritmo de claves simétricas
- Se realiza el hash y, con la parte publica de la clase de emisor verifica la firma;

Finalmente compara la firma en el token con la firma calculada en el punto de lectura para verificar la autenticidad del token, asegurándose que nadie ha modificado el contenido del token.

Para ello el equipo de lectura utilizará la clave que tenga disponible (clave pública asimétrica o clave simétrica) en el equipo, dando prioridad, en el caso de disponer de las dos, a la opción de usar la clave simétrica que tiene unos tiempos más cortos de procesamiento. La recomendación es que si es una TESC cuyo emisor se corresponde con el área de competencia en el punto de validación se usa la firma simétrica. Si es otro territorio, se usa la firma asimétrica.

2.4. UID del soporte

El UID (unique Identifier) se utiliza para la identificación del soporte individual (no confundir este UID del soporte con el ID de Usuario, este último lo gestiona la entidad coordinadora, mientras que el de soporte tiene su origen en el silicio del soporte).

En el Sistema TESC/DAT4m tiene dos aplicaciones importantes en lo que se refiere a la seguridad:

- En primer lugar se utiliza para elaborar y verificar la Firma (MAC). De esta manera un contenido "firmado" sólo es válido en el soporte para el que se preparó y si se copiara en otro, se detectaría en la verificación de la firma.
- En segundo lugar, es un método habitual utilizado en Transporte para elaborar listas negras y detectar soportes que deben ser rechazados.

En la versión actual, se admiten 4 soportes con las siguientes características de sus UID:

- Mifare Classic (4 Bytes)
- Mifare Desfire (7 Bytes)
- Java Card (8 Bytes)
- Teléfono Móvil (8 Bytes): Se trata de una función denominada "nº unico" compuesta por la App del móvil. Genera un número único (hash) en función de los siguientes elementos: imei, id del teléfono, id de la aplicación.
  Para un operador de Transporte es una función que es sólo de consulta por lo que lo importante es conocer la forma de acceder y tener la garantía de que es un número único.

3. Aplicación a Mifare Classic

3.1. 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".

3.2. Sector 0

El sector 0 contiene un byte con el número del sector TESC/DAT4M, precedido de una cadena fija de 2 bytes que podrá estar en cualquiera de los bloques 1 o 2.

- Cadena fija ("identificador TESC/DAT4M"): RM (0x524D en ASCII)
- Byte con el número del sector TESC/DAT4M
- Byte con el número de sector de la firma con algoritmo de claves asimétricas.
- Byte con versión de clave para firma con algoritmo de clave simétrica.
- Byte con versión de clave para firma con algoritmo de clave asimétrica.Clave de lectura: FFFFFFFFFFFF

Campo	Bytes	Descripción
CADENA FIJA TESC	1	RM (0x524D en ASCII)
Número sector TESC/DAT4M	1	Ej: 4. (dec) 0x04 (HEX)
Número sector firma algoritmo claves asimétricas	1	Ej: 15 (dec) 0x0F (HEX)
Versión de clave para firma con algoritmo clave simétrica	1	Almacenada en el sector indicado en "Número sector TESC/DAT4M" Ej: 1 (dec) 0x01 (HEX) para versión 1.

Campo	Bytes	Descripción
Versión de clave para firma con algoritmo clave asimétrica.	1	Almacenada en el sector indicado en "Número sector algoritmo claves asimétricas" Ej: 1 (dec) 0x01 (HEX) para versión 1.

Ejemplo: en el bloque 01 se indica que el sector TESC/DAT4M es el 4.

Bloque 00 | 24FE4EBB2F0804006263646566676869

Bloque 01 | 524D**04**0**101**00000000000000000000000

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"+"YY"+"ZZ" (Sector TESC/DAT4M y sector firma con algoritmo claves asimétricas), podrá estar en cualquier ubicación de los bloques 1 o 2 del sector 0 de la tarjeta. Esta posición será 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/DAT4M antes citadas y aplicando la búsqueda y análisis de la cadena TESC/DAT4M y sector donde se almacena la firma de clave asimétrica.

Los equipos dispondrán en su configuración de las claves de firma a utilizar según el emisor de la tarjeta pudiendo darse diferentes situaciones:

- Uso de firma con algoritmo de claves simétricas para el área de competencia del propietario/ emisor y uso de firma con algoritmo de claves asimétricas para interoperabilidad (para uso de TESC en otras regiones donde hay acuerdo de interoperabilidad).
- Uso de firma con algoritmo de claves asimétricas en todos los casos (en este caso debe tenerse en cuenta el uso del sector adicional donde se encuentra la firma con algoritmo de claves asimétricas y la mayor exigencia de capacidad de procesamiento para conseguir una transacción en los niveles de rapidez exigidos para transporte.
- Otras combinaciones.

Las claves simétricas y claves públicas serán distribuidas con los mecanismos definidos en el documento "*ITS_Interoperabilidad en el TP basada en QR - Modelos IO".*

3.3. Sector TESC/DAT4M

3.3.1. Estructura del sector TESC/DAT4M

El sector TESC/DAT4M contiene los datos que identifican al emisor y usuario de la tarjeta ("Datos TESC/DAT4M") y un MAC o firma que protege dichos datos.

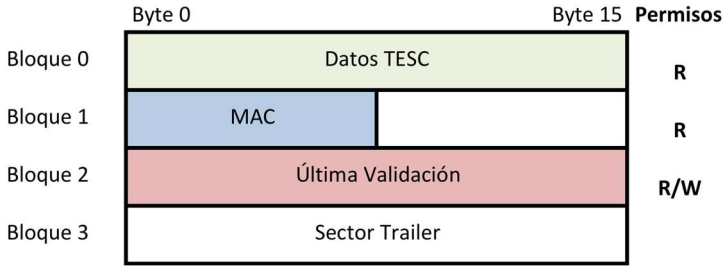

Figura 3 Estructura del sector TESC/DAT4M

En la versión actual se incluye como opcional la escritura, por lo que se indica la estructura de los datos a grabar sobre la última validación si se decidiera adoptar dicha funcionalidad.

3.3.2. Datos TESC/DAT4m

En el Bloque 0 del Sector TESC/DAT4m se situarán los 16 bytes de información del token.

Campo	Bytes	Descripción
VERSIÓN	1	Versión de la norma
MAPA MEMORIA	1	Identificador del Mapa de memoria utilizado para distribuir la información en el TOKEN
INFORMACIÓN	14	Resto de Información que compone el Token

3.3.3. MAC (firma)

Como se señala en el apartado anterior,

- Los 8 Bytes de la Firma(MAC) se ubicarán al principio del Bloque 1 del Sector TESC/DAT4m para firma con algoritmo de claves simétricas,
- En el sector que se indique para la firma con algoritmo de claves asimétricas (40 bytes, empezando por el principio del bloque 0 de dicho sector)

3.3.4. Claves MIFARE Classic

Se propone que la clave a modificar del sector TESC/DAT4M 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/DAT4M, ajustándose los bits de acceso a los bloques. De esta forma se permite la escritura en el bloque 2 del sector TESC/DAT4M para almacenar la última validación.

Por ello la propuesta será para el sector TESC/DAT4M:

- Bloque 0: Datos TESC/DAT4M
  - 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 16 bytes:

   a. Para UID de 4 bytes:

      “cs” + UID4B + “eT”+negado(”cs”+UID4B+ “eT”):

      Siendo:

      - “cs” valor hexadecimal ASCII para las letras cs=6373
      - UID4B: número de chip de 4 bytes: U1U2U3U4 (UX byte posición X)
      - “eT” valor hexadecimal ASCII para las letras eT=6554

      Ejemplo para UID 4 bytes F4673A54: **6373F4673A5465549C8C0B98C5AB9AAB**

   b. Para UID de 7 bytes:

      “c” + UID7B+negado(“c” + UID7B)

      Siendo:

      - “c” valor hexadecimal ASCII para la letra “c”=63
      - UID7B: número de chip de 7 bytes: U1U2U3U4U5U6U7 (UX byte posición X)

      Ejemplo para UID 7 bytes F4673A54F25B30: **63F4673A54F25B309C0B98C5AB0DA4CF**

b. Al resultado se le aplica cifrado AES128 en modo CBC. Se propone como clave maestra provisional: “TESC2024” = [5445534332303136ABBAACBCCDCFCEC9]

c. De los 16 bytes resultantes, la clave de lectura del sector TESC/DAT4M para MIFARE Classic serán el Byte10+Byte3+Byte16+Byte5+Byte1+Byte11 de los 16 bytes obtenidos. En el caso de MIFARE DESFIRE, los 16 bytes obtenidos.

Ejemplo UID 4 Bytes (ejemplo anterior):

- Cadena a encriptar: 6373F4673A5465549C8C0B98C5AB9AAB
- Clave encriptación: 5445534332303136ABBAACBCCDCFCEC9
- Resultado AES128 modo CBC= **8D**D3**7A**1F**AE**3FAA68ED**2CB6**D2CA01E9**31**
- Resultade clave TESC Classic: **2C7A31AE8DB6**

3.3.5. 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:

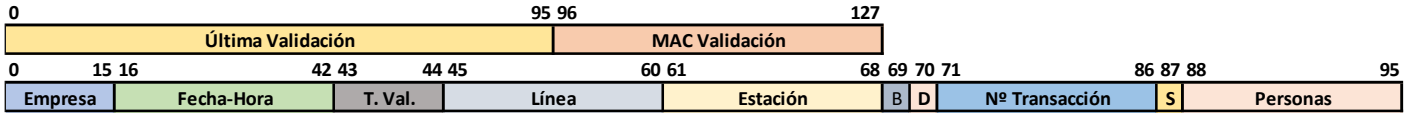

Figura 4 Estructura de los datos de validación TESC/DAT4M

De forma específica:

- 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.
- B (1 bit): Bit de bloqueo.
- D (1 bit): Bit de desbloqueo.
- S (1 bit): sentido.
- 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 cálculo de la MAC obtenida a partir de los datos TESC y ubicada en el bloque 1 para firma con algoritmo de clave simétrica.
- Con los 64 bits obtenidos se separa en dos bloques de 32 bits y se realiza un OR exclusive del siguiente modo: (Bit n) XOR (Bit n+32) obteniendo la MAC de 32 bits incluida al final del bloque 2.

4. Información TESC/DAT4M / TARJETAS **DESFIRE**

La información contenida en las tarjetas TESC/DAT4M sobre MIFARE DESFIRE será idéntica a la almacenada en las MIFARE CLASSIC/PLUS.

4.1. Identificación TESC/DAT4M

La forma de identificar que una tarjeta DESFIRE está asociada al esquema TESC/DAT4M es mediante la presencia de una *aplicación* (terminología DESFIRE) identificada por un AID (Application Identifier) de 3 bytes reservado para TESC/DAT4M a nivel nacional. Dicha aplicación es de tipo ISO, válida también para Java Card, por lo que no se solicitará una específica a NXP.

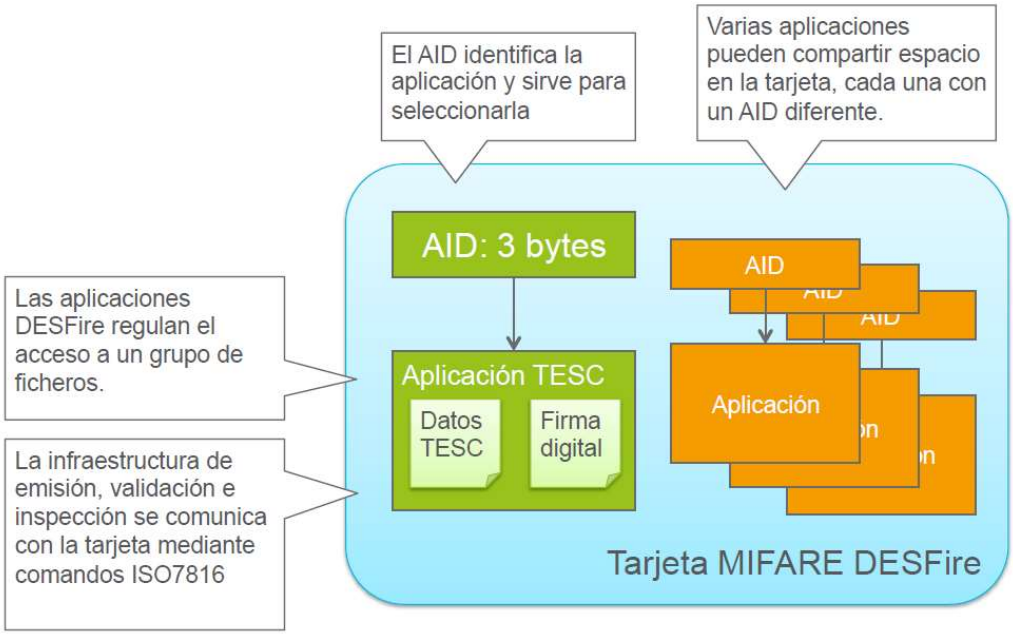

Figura 5 Estructura de aplicaciones DESFIRE.

4.2. Datos TESC/DAT4M

La aplicación TESC se compone de tres archivos:

Archivo 1 (STD-Standard Data File)-19 bytes:

Contiene Los mismos datos que en el mapa de memoria MIFARE Classic o en el applet JavaCard (datos TESC + datos de identificación de claves de firma) – TOTAL 19 Bytes.

- ID versión de la norma y mapa de memoria (2 bytes).
- ID entidad coordinadora (2 bytes)
- ID emisor (2 bytes)
- ID usuario (8 bytes)
- Fecha de caducidad de la tarjeta (2 bytes)
- Número sector firma algoritmo claves asimétricas (1 byte)
- Versión de clave para firma con algoritmo clave simétrica (1 byte)
- Versión de clave para firma con algoritmo clave asimétrica (1 byte)

Archivo 2 (STD-Standard Data File)-8+40bytes:

Firma digital de lo anterior (archivo 1).

- Firma con algoritmo de clave simétrica (primeros 8 bytes):
  - Firmada por la entidad emisora, utilizando su clave simétrica.
  - Verificación por cualquiera que disponga de la clave simétrica de la entidad emisora.
- Firma con algoritmo de clave asimétrica (64 bytes):
  - Firmada por la entidad coordinadora, utilizando su clave privada
  - Verificación por cualquiera que disponga de la clave pública de la entidad coordinadora

Archivo 3 (BD-Back up Data File)-16bytes:

Para la grabación de datos de validación en caso de que se elija esta opción (16 bytes), según se ha especificado para los datos de validación TESC para Classic/ PLUS.

4.3. Claves

- El proceso de lectura de la información podrá realizarse libremente sin necesidad de disponer de ninguna clave.
- Las claves públicas para verificar la firma (MAC) no dependerán del soporte utilizado.
- En el caso de las claves simétricas para firma, sí pueden ser propiedad del emisor.

5. Información TESC/DAT4M / TARJETAS **JAVACARD y Teléfonos Android**

El procedimiento para trabajar con tarjetas JavaCard y teléfonos Android se regula por los estándares de tarjetas ISO7816 y contactless/NFC ISO14443/4. El procedimiento es idéntico para ambos soportes.

5.1. Identificación TESC/DAT4M

Los datos TESC/DAT4M estarán almacenados en una aplicación específica, identificada con un AID reservado a nivel internacional. Una vez detectada la tarjeta/móvil por la antena NFC del dispositivo, se realizará la secuencia:

1. Selección de Aplicación con el AID
2. Lectura del UID de soporte (8bytes)
3. Lectura de los datos del token y su firma. (27bytes+8/40bytes)
4. Lectura de los datos de validación si se opta por escritura de datos de validación (16 bytes)

El Ministerio de Transportes y Movilidad Sostenible*, a través del Comité TESC/DAT4M, está en proceso de solicitud de reserva de una raíz o RID de uso exclusivo siguiendo el proceso definido en ISO 7816/5.*

5.2. Datos TESC/DAT4M

Los datos TESC/DAT4M estarán almacenados en el applet TESC/DAT4M JavaCard o en la APP Android. La forma de leer esta información es conforme al comando 'Read tag', usando los tags para **número de serie** y para **contenido token.**

5.3. Claves

- El proceso de lectura de la información podrá realizarse libremente sin necesidad de disponer de ninguna clave.
- Las claves públicas para verificar la firma (MAC) no dependerán del soporte utilizado y estarán distribuidas en los dispositivos de verificación.
- En el caso de las claves simétricas para firma, sí pueden ser propiedad del emisor.