I

(Actos cuya publicación es una condición para su aplicabilidad)

REGLAMENTO (CE) Nº 1360/2002 DE LA COMISIÓN

de 13 de junio de 2002

por el que se adapta por séptima vez al progreso técnico el Reglamento (CEE) nº 3821/85 del Consejo relativo al aparato de control en el sector de los transportes por carretera

(Texto pertinente a efectos del EEE)

LA COMISIÓN DE LAS COMUNIDADES EUROPEAS,

Visto el Tratado constitutivo de la Comunidad Europea,

Visto el Reglamento (CEE) nº 3821/85 del Consejo, de 20 de diciembre de 1985, relativo al aparato de control en el sector de los transportes por carretera ([1]), cuya última modificación la constituye el Reglamento (CE) nº 2135/98 ([2]), y, en particular, sus artículos 17 y 18,

Considerando lo siguiente:

(1) Deben adaptarse al progreso técnico las disposiciones técnicas definidas en el anexo I B del Reglamento (CEE) nº 3821/85, prestando especial atención a la seguridad general del sistema y a la interoperabilidad entre el aparato de control y las tarjetas de conductor.

(2) La adaptación del aparato exige además una adaptación del anexo II del Reglamento (CEE) nº 3821/85 que define las marcas y los certificados de homologación.

(3) El Comité establecido por el artículo 18 del Reglamento (CE) nº 3821/85 no emitió dictamen sobre las medidas previstas en la propuesta y, por tanto, la Comisión presentó al Consejo una propuesta sobre dichas medidas.

(4) Dado que el plazo establecido en la letra b) del apartado 5 del artículo 18 del Reglamento (CEE) nº 3821/85 ha expirado sin que el Consejo se haya pronunciado, incumbe a la Comisión adoptar tales medidas.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

El anexo del Reglamento (CE) nº 2135/98 será sustituido por el anexo del presente Reglamento.

Artículo 2

El anexo II del Reglamento (CEE) nº 3821/85 quedará modificado como sigue:

1) El primer párrafo del punto 1 del capítulo I quedará modificado como sigue:
   — Las letras «GR» distintivas de Grecia se sustituirán por el número «23»;
   — Las letras «IRL» distintivas de Irlanda se sustituirán por el número «24»;
   — Se añadirá el número «12» como distintivo de Austria;
   — Se añadirá el número «17» como distintivo de Finlandia;
   — Se añadirá el número «5» como distintivo de Suecia.

2) El segundo párrafo del punto 1 del capítulo I quedará modificado como sigue:
   — Después de las palabras «de la hoja» se incluirá el texto «o de una tarjeta de tacógrafo».

3) El punto 2 del capítulo I quedará modificado como sigue:
   — Después de las palabras «en cada hoja de registro» se incluirá el texto «y en cada tarjeta de tacógrafo».

4) En el capítulo II, después del título se añadirá el texto «PARA PRODUCTOS CONFORMES AL ANEXO I»

([1]) DO L 370 de 31.12.1985, p. 8.
([2]) DO L 274 de 9.10.1998, p. 1.

5) Se añadirá el siguiente capítulo III:

«III. FICHA DE HOMOLOGACIÓN PARA PRODUCTOS CONFORMES AL ANEXO I B

El Estado que haya procedido a una homologación expedirá al solicitante un certificado de homologación, extendido de acuerdo con el siguiente modelo. Para la comunicación a los demás Estados miembros de las homologaciones concedidas o de las posibles retiradas, cada Estado miembro utilizará copias de dicho documento.

FICHA DE HOMOLOGACIÓN PARA PRODUCTOS CONFORMES AL ANEXO I B

Administración competente .....

Notificación relativa a (*):

☐ La homologación de

☐ La retirada de la homologación de

☐ un modelo de aparato de control

☐ un componente del aparato de control (**) .....

☐ una tarjeta de conductor

☐ una tarjeta del centro de ensayo

☐ una tarjeta de la empresa

☐ una tarjeta de control

Nº de homologación .....

1. Marca de fábrica o registrada .....
2. Denominación del modelo .....
3. Nombre y apellidos del fabricante .....
4. Dirección del fabricante .....
5. Presentado para su homologación el .....
6. Laboratorio(s) .....
7. Fecha y número del(de los) ensayo(s) .....
8. Fecha de homologación .....
9. Fecha de la retirada de la homologación .....
10. Modelo o modelos de componentes del aparato de control con los que se va a utilizar el componente .....
11. Lugar .....
12. Fecha .....
13. Documentos descriptivos adjuntos .....

---

14. Observaciones (incluida la posición de precintos, en su caso)

.....

(firma)

(*) Marque las casillas que proceda.
(**) Indique el componente al que se refiere la notificación.»

Artículo 3

El presente Reglamento entrará en vigor el vigésimo día siguiente al de su publicación en el *Diario Oficial de las Comunidades Europeas*.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el 13 de junio de 2002.

Por la Comisión
Loyola DE PALACIO
Vicepresidente

ANEXO

«ANEXO I B

CONDICIONES DE FABRICACIÓN, ENSAYO, INSTALACIÓN Y CONTROL

A fin de preservar la interoperabilidad del software de los equipos definidos en el presente anexo, se han mantenido en la lengua original de redacción del texto, es decir, en inglés, algunas siglas, términos o expresiones de programación informática. En ocasiones se han añadido traducciones literales, entre paréntesis y a título informativo, detrás de algunas de estas expresiones, con el fin de facilitar su comprensión.

ÍNDICE

I. DEFINICIONES

A los efectos del presente anexo, se entenderá por:

a) **Activación**:

La fase en que el aparato de control pasa a ser totalmente operativo y realiza todas sus funciones, incluidas las de seguridad.

La activación de un aparato de control exige el uso de una tarjeta del centro de ensayo y la introducción del código PIN correspondiente.

b) **Autentificación**:

Una función con la que se establece y verifica una identidad.

c) **Autenticidad**:

La propiedad de que una información proceda de alguien cuya identidad pueda verificarse.

d) **Autodiagnóstico (BIT)**:

Prueba que se lleva a cabo a petición del operario o por orden de un equipo externo.

e) **Día civil**:

Un día comprendido entre las 00.00 y las 24.00 horas. Todos los días se referirán al tiempo universal coordinado.

f) **Calibrado**:

La actualización o confirmación de parámetros del vehículo que van a guardarse en la memoria. Dichos parámetros incluyen la identificación del vehículo (VIN, VRN y Estado miembro donde se matriculó) y sus características [w, k, l, tamaño de los neumáticos, valor de ajuste del dispositivo limitador de la velocidad (en su caso), hora real correspondiente al tiempo universal coordinado, lectura actual del cuentakilómetros].

Para calibrar un aparato de control se precisa una tarjeta del centro de ensayo.

g) **Número de tarjeta**:

Una secuencia de 16 caracteres alfanuméricos que identifican una tarjeta de tacógrafo en un Estado miembro. El número de tarjeta incluye un índice consecutivo (en su caso), un índice de sustitución y un índice de renovación.

Por consiguiente, cada tarjeta se identifica con el código del Estado miembro que la asigna y con el número de la propia tarjeta.

h) **Índice consecutivo de la tarjeta**:

El 14º carácter alfanumérico del número de la tarjeta. Este carácter sirve para diferenciar las distintas tarjetas asignadas a una empresa o a un organismo con derecho a utilizar varias tarjetas de tacógrafo. La empresa o el organismo se identifica con los 13 primeros caracteres del número de la tarjeta.

i) **Índice de renovación de la tarjeta**:

El 16º carácter alfanumérico del número de la tarjeta. Este carácter se incrementa en una unidad cada vez que se renueva la tarjeta de tacógrafo.

j) **Índice de sustitución de la tarjeta**:

El 15º carácter alfanumérico del número de la tarjeta. Este carácter se incrementa en una unidad cada vez que se sustituye la tarjeta de tacógrafo.

k) **Coeficiente característico del vehículo**:

La característica numérica que da el valor de la señal de salida emitida por la pieza prevista en el vehículo para su conexión con el aparato de control (toma de salida de la caja de cambio en algunos casos, rueda del vehículo en otros casos), cuando el vehículo recorre la distancia de 1 km, medida en condiciones normales de ensayo (véase el capítulo VI.5). El coeficiente característico se expresa en impulsos por kilómetro (w = … imp/km).

l) **Tarjeta de la empresa**:

Una tarjeta de tacógrafo asignada por las autoridades de los Estados miembros al propietario de vehículos provistos del aparato de control.

Esta tarjeta identifica a la empresa y permite visualizar, transferir e imprimir la información que se encuentre almacenada en el aparato o aparatos de control instalado(s) por esa empresa.

m) **Constante del aparato de control**:

La característica numérica que da el valor de la señal de entrada necesaria para obtener la indicación y el registro de una distancia recorrida en 1 km; dicha constante deberá expresarse en impulsos por kilómetro (k = … imp/km).

n) **Período de conducción continuo (contabilizado por el aparato de control)** ([1]):

Los tiempos de conducción acumulados de un conductor en particular, contados desde el momento en que terminara su último período de DISPONIBILIDAD o PAUSA/DESCANSO o período INDETERMINADO ([2]) de 45 minutos o más (este período puede haberse dividido en varias pausas de 15 minutos o más). Para calcular este tiempo se tienen en cuenta las actividades anteriores que han quedado registradas en la tarjeta del conductor. Si el conductor no ha introducido su tarjeta, los cálculos se basan en los registros de la memoria correspondientes al período en que no estuvo introducida la tarjeta, y en los registros de la ranura que corresponda.

o) **Tarjeta de control**:

Una tarjeta de tacógrafo asignada por las autoridades de los Estados miembros a las autoridades de control competentes en cada país.

La tarjeta de control identifica al organismo de control y posiblemente al agente encargado del control y permite acceder a la información almacenada en la memoria o en las tarjetas de conductor a efectos de su lectura, impresión o transferencia.

p) **Tiempo de descanso acumulado (contabilizado por el aparato de control)** ([1]):

El tiempo de descanso acumulado, referido a un conductor en particular, se calcula a partir de los períodos de DISPONIBILIDAD actual acumulados o los tiempos de PAUSA/DESCANSO o los períodos INDETERMINADOS ([2]) de 15 minutos o más, contados desde el momento en que terminara su último período de DISPONIBILIDAD o PAUSA/DESCANSO o período INDETERMINADO ([2]) de 45 minutos o más (este período puede haberse dividido en varias pausas de 15 minutos o más).

Para calcular este tiempo se tienen en cuenta las actividades anteriores que han quedado registradas en la tarjeta del conductor. Los cálculos no incluyen los períodos indeterminados que tengan una duración negativa (comienzo del período indeterminado > final del período indeterminado) a consecuencia de un solapamiento temporal entre dos aparatos de control distintos.

Si el conductor no ha introducido su tarjeta, los cálculos se basan en los registros de la memoria correspondientes al período en que no estuvo introducida la tarjeta, y en los registros de la ranura que corresponda.

q) **Memoria de datos**:

Un dispositivo de almacenamiento electrónico incorporado en el aparato de control.

r) **Firma digital**:

Datos adjuntos o una transformación criptográfica de un bloque de datos que permite al destinatario comprobar la autenticidad e integridad de dicho bloque.

s) **Transferencia**:

La copia, junto con la firma digital, de una parte o de la totalidad de un conjunto de datos almacenados en la memoria del vehículo o en la memoria de una tarjeta de tacógrafo.

La transferencia no podrá modificar ni borrar ninguno de los datos almacenados.

([1]) Este modo de calcular el período de conducción continuo y el tiempo de descanso acumulado permite al aparato de control calcular el momento de activación del aviso de conducción continua, y no prejuzga la interpretación legal que deba hacerse de dichos tiempos.

([2]) Los períodos INDETERMINADOS son aquellos en que la tarjeta del conductor no está insertada en el aparato de control y tampoco se introducen manualmente las actividades de dicho conductor

t) **Tarjeta de conductor**:

Una tarjeta de tacógrafo asignada por las autoridades de los Estados miembros a conductores individuales.

Esta tarjeta identifica al conductor y permite almacenar datos sobre su actividad.

u) **Circunferencia efectiva de los neumáticos de las ruedas**:

La media de las distancias recorridas por cada una de las ruedas que arrastran el vehículo (ruedas motrices) al realizar una rotación completa. La medida de dichas distancias deberá hacerse en condiciones normales de ensayo (capítulo VI.5) y se expresará en la forma "l = … mm". Los fabricantes de los vehículos podrán sustituir la medición de estas distancias por un cálculo teórico que tenga en cuenta el reparto del peso sobre los ejes, con el vehículo descargado y en condiciones normales de marcha ([1]). Los métodos de dicho cálculo teórico se someterán a la aprobación de una autoridad competente del Estado miembro que corresponda.

v) **Incidente**:

Operación anormal detectada por el aparato de control y que puede deberse a un intento de fraude.

w) **Fallo**:

Operación anormal detectada por el aparato de control y que puede deberse a un fallo de funcionamiento.

x) **Instalación**:

Montaje del aparato de control en un vehículo.

y) **Sensor de movimiento**:

Parte del aparato de control que ofrece una señal representativa de la velocidad del vehículo o la distancia recorrida.

z) **Tarjeta no válida**:

Una tarjeta que está defectuosa, no ha superado la autentificación inicial, no ha alcanzado todavía la fecha de comienzo de validez, o ha sobrepasado la fecha de caducidad.

aa) **Fuera de ámbito**:

Cuando el uso del aparato de control no es obligatorio, de conformidad con lo dispuesto en el Reglamento (CEE) nº 3820/85 del Consejo.

bb) **Exceso de velocidad**:

Rebasamiento de la velocidad autorizada para el vehículo. Se define como un período de más de 60 segundos durante el cual la velocidad del vehículo, medida por el aparato de control, sobrepasa el valor de ajuste del dispositivo limitador de la velocidad, regulado con arreglo a la Directiva 92/6/CEE del Consejo, de 10 de febrero de 1992, relativa a la instalación y a la utilización de dispositivos de limitación de velocidad en determinadas categorías de vehículos de motor en la Comunidad ([2]).

cc) **Control periódico**:

Conjunto de operaciones con las que se comprueba que el aparato de control funciona correctamente y que sus valores de ajuste corresponden a los parámetros del vehículo.

dd) **Impresora**:

Componente del aparato de control que permite imprimir los datos almacenados.

ee) **Aparato de control**:

La totalidad del aparato destinado a ser instalado en vehículos de carretera, para indicar, registrar y almacenar automática o semiautomáticamente datos acerca de la marcha de dichos vehículos y de determinados tiempos de trabajo de sus conductores.

([1]) Directiva 97/27/CE del Parlamento Europeo y del Consejo, de 22 de julio de 1997, relativa a las masas y dimensiones de determinadas categorías de vehículos de motor y de sus remolques y por la que se modifica la Directiva 70/156/CEE (DO L 233 de 25.8.1997, p. 1).

([2]) DO L 57 de 2.3.1992, p. 27.

ff) **Renovación**:

Asignación de una nueva tarjeta de tacógrafo cuando la tarjeta existente alcanza su fecha de caducidad o se ha devuelto a la autoridad emisora por un fallo de funcionamiento. La renovación implica siempre la certeza de que no coexistirán dos tarjetas válidas.

gg) **Reparación**:

Reparación de un sensor de movimiento o de una unidad intravehicular que precisa ser abierta, desconectada de su fuente de alimentación o desconectada de otros componentes del aparato de control.

hh) **Sustitución**:

Emisión de una tarjeta de tacógrafo en sustitución de una tarjeta existente que se haya declarado perdida, robada o defectuosa y que no se haya devuelto a la autoridad emisora. La sustitución implica siempre el riesgo de que coexistan dos tarjetas válidas.

ii) **Certificación de seguridad**:

Procedimiento por el que un organismo de certificación ITSEC ([1]) garantiza que el aparato de control (o componente) o la tarjeta de tacógrafo que se investiga cumple los requisitos de seguridad definidos en el apéndice 10 Objetivos genéricos de seguridad.

jj) **Comprobación automática**:

Comprobación que realiza de manera cíclica y automática el aparato de control para detectar posibles fallos.

kk) **Tarjeta de tacógrafo**:

Tarjeta inteligente que se utiliza con el aparato de control. Las tarjetas de tacógrafo comunican al aparato de control la identidad (o el grupo de identidad) del titular y además permiten la transferencia y el almacenamiento de datos. Las tarjetas de tacógrafo pueden ser de varios tipos:

— tarjeta de conductor,

— tarjeta de control,

— tarjeta del centro de ensayo,

— tarjeta de la empresa.

ll) **Homologación**:

Procedimiento por el que un Estado miembro certifica que el aparato de control (o componente) o la tarjeta de tacógrafo que se investiga cumple los requisitos del presente Reglamento.

mm) **Tamaño de los neumáticos**:

Designación de las dimensiones de los neumáticos (ruedas motrices externas) con arreglo a la Directiva 92/23/CEE del Consejo ([2]).

nn) **Identificación del vehículo**:

Números que identifican el vehículo: número de matrícula (VRN), Estado miembro donde está matriculado, y número de bastidor (VIN) ([3]).

oo) **Unidad intravehicular (VU)**:

El aparato de control, excepto el sensor de movimiento y los cables que conectan dicho sensor. Puede tratarse de una sola unidad o de varias unidades repartidas por el vehículo, siempre que cumplan los requisitos de seguridad del presente Reglamento.

([1]) Recomendación 95/144/CE, de 7 de abril de 1995, relativa a los criterios comunes de evaluación de la seguridad en las tecnologías de la información (DO L 93 de 26.4.1995, p. 27).
([2]) DO L 129 de 14.5.1992, p. 95.
([3]) Directiva 76/114/CEE del Consejo (DO L 24 de 30.1.1976, p. 1).

pp) **Semana (a efectos de cálculo en el aparato de control)**:

El período que va de las 00.00 horas de un lunes a las 24.00 horas de un domingo, referido al tiempo universal coordinado.

qq) **Tarjeta del centro de ensayo**:

Una tarjeta de tacógrafo asignada por las autoridades de un Estado miembro a un fabricante de aparatos de control, a un instalador, a un fabricante de vehículos o a un centro de ensayo, y aprobada por ese Estado miembro.

La tarjeta del centro de ensayo identifica al titular y permite probar, calibrar o transferir el aparato de control.

II. CARACTERÍSTICAS GENERALES Y FUNCIONES DEL APARATO DE CONTROL

000 Todo vehículo que lleve instalado un aparato de control conforme a lo dispuesto en el presente anexo debe incorporar además un indicador de velocidad y un cuentakilómetros. Estas funciones pueden estar incluidas en el aparato de control.

1. **Características generales**

El aparato de control sirve para registrar, almacenar, visualizar, imprimir y enviar datos relacionados con las actividades del conductor.

001 El aparato de control incluye cables, un sensor de movimiento y una unidad intravehicular.

002 La unidad intravehicular incluye una unidad de proceso, una memoria de datos, un reloj en tiempo real, dos dispositivos de interfaz para tarjeta inteligente (conductor y segundo conductor), una impresora, una pantalla, un avisador luminoso, un conector de calibrado/transferencia y accesorios para la entrada de datos por parte del usuario.

El aparato de control puede estar conectado a otros dispositivos mediante conectores adicionales.

003 Ninguna función o dispositivo, homologado o no, que se incluya o se conecte al aparato de control deberá interferir ni ser capaz de interferir con el funcionamiento correcto y seguro del aparato de control ni con lo dispuesto en el presente Reglamento.

Los usuarios del aparato de control se identifican a sí mismos con las tarjetas de tacógrafo.

004 El aparato de control proporciona derechos de acceso selectivo a los datos y funciones según el tipo o la identidad del usuario.

El aparato de control registra y almacena datos en su memoria y en las tarjetas de tacógrafo.

El registro y almacenamiento de datos se ajustan a lo dispuesto en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos ([1]).

2. **Funciones**

005 El aparato de control deberá garantizar las funciones siguientes:

— control de la inserción y extracción de las tarjetas,

— medición de la velocidad y la distancia,

— medición de la hora,

— supervisión de las actividades del conductor,

— supervisión del régimen de conducción,

— entradas manuales de los conductores:

  — entrada de los lugares donde comienzan o terminan los períodos de trabajo diarios,

  — entrada manual de las actividades del conductor,

  — entrada de condiciones específicas,

([1]) DO L 281 de 23.11.1995, p. 31.

— gestión de los bloqueos introducidos por la empresa,

— supervisión de las actividades de control,

— detección de incidentes o fallos,

— autodiagnóstico y comprobaciones automáticas,

— lectura de los datos almacenados en la memoria,

— registro y almacenamiento de datos en la memoria,

— lectura de las tarjetas de tacógrafo,

— registro y almacenamiento de datos en las tarjetas de tacógrafo,

— visualización,

— impresión,

— advertencias,

— transferencia de datos a medios externos,

— envío de datos a dispositivos externos adicionales,

— calibrado,

— ajuste de la hora.

3. **Modos de funcionamiento**

006 El aparato de control deberá tener cuatro modos de funcionamiento:

— modo operativo,

— modo de control,

— modo de calibrado,

— modo de empresa.

007 El aparato de control pasará al siguiente modo de funcionamiento según las tarjetas de tacógrafo válidas que se inserten en los dispositivos de interfaz:

Modo de funcionamiento		Ranura del conductor				
		Sin tarjeta	Tarjeta del conductor	Tarjeta de control	Tarjeta del centro de ensayo	Tarjeta de la empresa
Ranura del segundo conductor	Sin tarjeta	operativo	operativo	de control	de calibrado	de empresa
	Tarjeta del conductor	operativo	operativo	de control	de calibrado	de empresa
	Tarjeta de control	de control	de control	de control (*)	operativo	operativo
	Tarjeta del centro de ensayo	de calibrado	de calibrado	operativo	de calibrado (*)	operativo
	Tarjeta de la empresa	de empresa	de empresa	operativo	operativo	de empresa (*)

008 (*) En estas situaciones, el aparato de control utilizará exclusivamente la tarjeta de tacógrafo insertada en la ranura del conductor.

009 El aparato de control no tendrá en cuenta las tarjetas no válidas que se inserten, excepto si se visualizan, imprimen o transfieren los datos almacenados en una tarjeta caducada, cosa que deberá ser posible.

010 Todas las funciones enumeradas en el apartado II.2. estarán disponibles en cualquier modo de funcionamiento, con las siguientes excepciones:

— la función de calibrado sólo está disponible en el modo de calibrado,

— la función de ajuste de la hora tiene limitaciones si no se está en el modo de calibrado,

— las funciones de entrada manual del conductor sólo están disponibles en el modo operativo y en el modo de calibrado,

— la función de gestión de los bloqueos introducidos por la empresa sólo está disponible en el modo de empresa,

— la función de supervisión de las actividades de control sólo funciona en el modo de control,

— la función de transferencia no está disponible en el modo operativo (excepto en el caso indicado en el requisito 150).

011 El aparato de control podrá enviar cualquier tipo de datos a la pantalla, a la impresora o a interfaces externas, con las siguientes excepciones:

— en el modo operativo, toda identificación personal (primer apellido y nombre) que no corresponda a una tarjeta de tacógrafo insertada se borrará por completo, y todo número de tarjeta que no corresponda a una tarjeta de tacógrafo insertada se borrará parcialmente (se borrarán los caracteres impares, de izquierda a derecha),

— en el modo de empresa, los datos relativos al conductor (requisitos 081, 084 y 087) sólo podrán enviarse a dispositivos externos durante los períodos que no tenga bloqueados otra empresa (identificada por los 13 primeros dígitos del número de la tarjeta de la empresa),

— si no se ha insertado ninguna tarjeta en el aparato de control, sólo podrán enviarse los datos relativos al conductor que correspondan al día actual y a los 8 días civiles anteriores.

4. **Seguridad**

La seguridad del sistema tiene por objeto proteger la memoria de datos, de manera que se prohíba el acceso a la misma a terceros no autorizados, se excluya la manipulación de información y se detecte cualquier tentativa en ese sentido, así se protege la integridad y autenticidad de los datos intercambiados entre el sensor de movimiento y la unidad intravehicular, y de los datos intercambiados entre el aparato de control y las tarjetas de tacógrafo, y se verifica la integridad y autenticidad de la transferencia de datos.

012 A fin de garantizar la seguridad del sistema, el aparato de control cumplirá los objetivos genéricos de seguridad (apéndice 10) especificados para el sensor de movimiento y la unidad intravehicular.

III. CONDICIONES DE FABRICACIÓN Y FUNCIONAMIENTO DEL APARATO DE CONTROL

1. **Control de la inserción y extracción de las tarjetas**

013 El aparato de control supervisará los dispositivos de interfaz para detectar la inserción y extracción de las tarjetas.

014 Nada más insertar la tarjeta, el aparato de control detectará si se trata de una tarjeta de tacógrafo válida y, en tal caso, identificará el tipo de tarjeta.

015 El aparato de control deberá estar construido de tal modo que las tarjetas de tacógrafo se fijen en su posición al insertarlas correctamente en los dispositivos de interfaz.

016 La liberación de las tarjetas de tacógrafo sólo deberá ser posible con el vehículo parado y después de haberse almacenado en dichas tarjetas los datos pertinentes. La extracción de la tarjeta exigirá la intervención directa del usuario.

2. **Medición de la velocidad y la distancia**

017 Esta función medirá de forma continua y permitirá indicar en el cuentakilómetros el valor correspondiente a la distancia total recorrida por el vehículo.

018 Esta función medirá de forma continua y permitirá indicar la velocidad del vehículo.

019 Asimismo, la función de medición de la velocidad indicará si el vehículo está en movimiento o parado. Se considerará que el vehículo está en movimiento en cuanto la función, a través del sensor de movimiento, detecte más de 1 imp/seg durante al menos 5 segundos. De lo contrario, se considerará que el vehículo está parado.

Los dispositivos indicadores de la velocidad (velocímetro) y de la distancia total recorrida (cuentakilómetros) instalados en un vehículo que incorpore un aparato de control conforme a lo dispuesto en el presente Reglamento, deberán cumplir las condiciones relativas a las tolerancias máximas establecidas en el presente anexo (puntos 2.1 y 2.2 del capítulo III).

2.1. ***Medición de la distancia recorrida***

020 La distancia recorrida podrá medirse:

— bien de forma que se incluyan los movimientos en marcha adelante y en marcha atrás,

— bien de forma que se incluyan solamente los movimientos en marcha adelante.

021 El aparato de control deberá medir la distancia entre 0 y 9 999 999,9 km.

022 La distancia medida estará comprendida en los siguientes límites de tolerancia (distancias de al menos 1 000 m):

— ± 1 % antes de la instalación,

— ± 2 % después de la instalación y de un control periódico,

— ± 4 % durante el uso.

023 La distancia medida tendrá una resolución igual o mejor que 0,1 km.

2.2. ***Medición de la velocidad***

024 El aparato de control deberá medir la velocidad entre 0 y 220 km/h.

025 A fin de garantizar una tolerancia máxima de ± 6 km/h para la indicación de la velocidad, y teniendo en cuenta:

— una tolerancia de ± 2 km/h para posibles variaciones de los valores de entrada (variaciones de los neumáticos, …),

— una tolerancia de ± 1 km/h en las mediciones realizadas durante la instalación o en los controles periódicos,

el aparato de control deberá medir la velocidad con una tolerancia de ± 1 km/h (a velocidad constante), para velocidades entre 20 y 180 km/h y para coeficientes característicos del vehículo entre 4 000 y 25 000 imp/km.

Nota: La resolución de almacenamiento de datos aporta una tolerancia adicional de ± 0,5 km/h a la velocidad registrada por el aparato de control.

025a La velocidad deberá medirse correctamente dentro de las tolerancias normales y antes de que hayan transcurrido 2 segundos tras haberse producido un cambio de velocidad, si dicho cambio no sobrepasa una aceleración de 2 m/s^2.

026 La medición de la velocidad tendrá una resolución igual o mejor que 1 km/h.

3. **Medición de la hora**

027 La función de medición de la hora deberá medir de forma continua y expresar digitalmente la fecha y la hora correspondientes al tiempo universal coordinado (UTC).

028 La fecha y la hora UTC deberán incluirse en las operaciones del aparato de control (registros, documentos impresos, intercambio de datos, indicaciones en pantalla, …).

029 A fin de visualizar la hora local, existirá la posibilidad de cambiar el desfase de la hora indicada, en incrementos de media hora.

030 La desviación de la hora en condiciones de homologación del modelo será de ± 2 segundos por día.

031 La hora medida tendrá una resolución igual o mejor que 1 segundo.

032 En las condiciones de homologación del modelo, la medición de la hora no deberá verse afectada por interrupciones del suministro eléctrico con una duración inferior a 12 meses.

4. **Supervisión de las actividades del conductor**

033 Esta función deberá controlar permanentemente y por separado las actividades de un conductor y un segundo conductor.

034 Las actividades del conductor pueden ser CONDUCCIÓN, TRABAJO, DISPONIBILIDAD o PAUSA/DESCANSO.

035 El conductor o el segundo conductor deberán tener la posibilidad de seleccionar manualmente las actividades de TRABAJO, DISPONIBILIDAD o PAUSA/DESCANSO.

036 Cuando el vehículo esté en movimiento, el aparato seleccionará automáticamente la actividad de CONDUCCIÓN para el conductor y la actividad de DISPONIBILIDAD para el segundo conductor.

037 Cuando el vehículo se detenga, se seleccionará automáticamente la actividad de TRABAJO para el conductor.

038 Si el primer cambio de actividad tiene lugar antes de que hayan transcurrido 120 segundos después de haber cambiado automáticamente a TRABAJO por haberse detenido el vehículo, se entenderá que ha tenido lugar a la hora en que se detuvo el vehículo (por consiguiente, podría cancelar el cambio a TRABAJO).

039 Esta función deberá notificar los cambios de actividad a las funciones de registro con una resolución de un minuto.

040 Dado un minuto cualquiera, si en ese minuto se produce alguna actividad de CONDUCCIÓN, se considerará que todo el minuto es de CONDUCCIÓN.

041 Dado un minuto cualquiera, si se produce alguna actividad de CONDUCCIÓN en los minutos anterior y posterior, se considerará que todo el minuto es de CONDUCCIÓN.

042 Dado un minuto cualquiera que no se considere de CONDUCCIÓN con arreglo a los requisitos antes mencionados, se considerará que todo el minuto será de un mismo tipo de actividad, concretamente la que haya tenido lugar de forma continuada y durante más tiempo dentro de ese minuto (en caso de haber dos actividades de la misma duración, la que se haya producido en último lugar).

043 Esta función también deberá controlar permanentemente el tiempo de conducción continua y el tiempo de descanso acumulado del conductor.

5. **Supervisión del régimen de conducción**

044 Esta función deberá controlar permanentemente el régimen de conducción.

045 Si hay dos tarjetas de conductor insertadas en el aparato, habrá que seleccionar el régimen EN EQUIPO. De otro modo se seleccionará el régimen EN SOLITARIO.

6. **Entradas manuales de los conductores**

6.1. ***Entrada de los lugares donde comienzan o terminan los períodos de trabajo diarios***

046 Esta función deberá permitir la introducción de los lugares donde comienzan o terminan los períodos de trabajo diarios de un conductor o un segundo conductor.

047 Se entiende por lugares el país y, en su caso, la región.

048 En el momento de extraer la tarjeta del conductor (o la tarjeta del centro de ensayo), el aparato de control deberá pedir al conductor (o segundo conductor) que introduzca el "lugar donde termina el período de trabajo diario".

049 El aparato de control debe admitir la posibilidad de que no se haga caso de esta petición.

050 Los lugares donde comiencen o terminen los períodos de trabajo diarios también deben poderse introducir sin necesidad de la tarjeta o en otros momentos que no sea al insertar o extraer la tarjeta.

6.2. ***Entrada manual de las actividades del conductor***

050a Al introducir la tarjeta del conductor (o la tarjeta del centro de ensayo), y exclusivamente en ese momento, el aparato de control deberá:

— recordar al titular de la tarjeta la fecha y la hora en que extrajo la tarjeta por última vez y,

— pedir al titular de la tarjeta que especifique si la inserción actual de la tarjeta representa una continuación del período de trabajo de ese día.

El aparato de control debe permitir al titular de la tarjeta que no conteste a la pregunta, que la conteste afirmativamente o que conteste negativamente:

— Si el titular de la tarjeta no contesta a la pregunta, el aparato de control le pedirá que indique el "lugar donde comienza el período de trabajo diario". El aparato de control debe admitir la posibilidad de que no se conteste esta pregunta. Si se especifica un lugar, éste quedará registrado en la memoria de datos y en la tarjeta de tacógrafo, y se relacionará con la hora de inserción de la tarjeta.

— Si el titular de la tarjeta contesta de forma afirmativa o negativa, el aparato de control le invitará a que introduzca las actividades manualmente, con las fechas y horas de comienzo y final. Sólo podrán introducirse las actividades de TRABAJO, DISPONIBILIDAD o PAUSA/DESCANSO, y en todo caso las que estén comprendidas en el período transcurrido desde que se extrajo la tarjeta por última vez hasta la actual inserción, y sin posibilidad de que dichas actividades se solapen entre sí. Para ello se observarán los procedimientos siguientes:

  — Si el titular de la tarjeta responde a la pregunta afirmativamente, el aparato de control le invitará a que introduzca manualmente y en orden cronológico las actividades que hayan tenido lugar durante el período transcurrido desde que se extrajera la tarjeta por última vez hasta la inserción actual. El procedimiento terminará cuando la hora de finalización de una actividad introducida manualmente coincida con la hora de inserción de la tarjeta.

  — Si el titular de la tarjeta responde a la pregunta negativamente, el aparato de control:

    — Invitará al titular de la tarjeta a que introduzca manualmente y en orden cronológico las actividades que hayan tenido lugar desde el momento en que se extrajera la tarjeta hasta el momento en que finalizara el correspondiente período de trabajo diario (o las actividades relacionadas con ese vehículo, si es que el período de trabajo diario continúa en una hoja de registro). Así pues, antes de permitir al titular de la tarjeta que introduzca cada actividad manualmente, el aparato de control le invitará a que especifique si la hora de finalización de la última actividad registrada representa el final de un período de trabajo anterior (véase la nota a continuación),

      Nota: si el titular de la tarjeta no especifica la hora de finalización del período de trabajo anterior e introduce manualmente una actividad cuya hora de finalización coincide con la hora de inserción de la tarjeta, el aparato de control:

      — supondrá que el período de trabajo diario terminó al comenzar el primer período de DESCANSO (o período INDETERMINADO que haya quedado) después de haberse extraído la tarjeta, o bien en el momento en que se extrajo la tarjeta si no se ha introducido ningún período de descanso (y si no hay ningún período INDETERMINADO),

      — supondrá que la hora de comienzo (véase más abajo) coincide con la hora de inserción de la tarjeta,

      — procederá según se describe a continuación.

    — Seguidamente, si la hora de conclusión del período de trabajo relacionado no coincide con la hora de extracción de la tarjeta, o si en ese momento no se ha introducido un lugar de finalización del período de trabajo diario, pedirá al titular de la tarjeta que "confirme o introduzca el lugar donde terminó el período de trabajo diario" (el aparato de control debe admitir la posibilidad de que no se haga caso de esta petición). Si se introduce un lugar, éste quedará registrado en la tarjeta de tacógrafo exclusivamente, y sólo si no coincide con el lugar que se introdujera al extraer la tarjeta (en caso de haberse introducido uno), y se relacionará con la hora de finalización del período de trabajo,

    — Seguidamente, invitará al titular de la tarjeta a que "introduzca una hora de comienzo" del período de trabajo de ese día (o de las actividades relacionadas con el vehículo en caso de que el titular de la tarjeta hubiera utilizado previamente una hoja de registro durante ese período), y le pedirá que especifique el "lugar donde comienza el período de trabajo diario" (el aparato de control debe admitir la posibilidad de que no se haga caso de esta petición). Si se introduce un lugar, éste quedará registrado en la tarjeta de tacógrafo y se relacionará con esa hora de comienzo. Si dicha hora de comienzo coincide con la hora de inserción de la tarjeta, el lugar también quedará registrado en la memoria de datos,

    — Seguidamente, si dicha hora de comienzo no coincide con la hora de inserción de la tarjeta, invitará al titular de la tarjeta a que introduzca manualmente y en orden cronológico las actividades que hayan tenido lugar desde esa hora de comienzo hasta el momento en que se insertara la tarjeta. El procedimiento terminará cuando la hora de conclusión de una actividad introducida manualmente coincida con la hora de inserción de la tarjeta.

  — A continuación, el aparato de control permitirá que el titular de la tarjeta modifique las actividades introducidas manualmente, hasta que las valide mediante la selección de un comando específico. Una vez validadas las actividades, ya no se podrán realizar modificaciones.

  — Si se responde de cualquiera de estas maneras a la pregunta inicial y luego no se introduce ninguna actividad, el aparato de control entenderá que el titular de la tarjeta ha optado por no responder a la pregunta.

Durante todo este proceso, el aparato de control dejará de esperar una entrada en los siguientes casos:

— si no existe interacción con la interfaz hombre-máquina del aparato durante 1 minuto (con una advertencia visual y quizá auditiva al cabo de 30 segundos), o bien

— si se extrae la tarjeta o se inserta otra tarjeta de conductor (o del centro de ensayo), o bien

— tan pronto el vehículo se ponga en movimiento,

en cuyo caso el aparato de control validará las entradas ya realizadas.

6.3. ***Entrada de condiciones específicas***

050b El aparato de control permitirá que el conductor introduzca en tiempo real las dos condiciones específicas siguientes:

— "FUERA DE ÁMBITO" (comienzo, final)

— "TRAYECTO EN TRANSBORDADOR/TREN"

La condición "TRAYECTO EN TRANSBORDADOR/TREN" no puede darse si está abierta la condición "FUERA DE ÁMBITO".

Si la condición "FUERA DE ÁMBITO" está abierta, el aparato de control tendrá que cerrarla inmediatamente en caso de insertarse o extraerse una tarjeta de conductor.

7. **Gestión de los bloqueos introducidos por la empresa**

051 Esta función deberá permitir la gestión de los bloqueos que haya introducido una empresa con el fin de restringir el acceso a sus propios datos en el modo de empresa.

052 Estos bloqueos consisten en una fecha/hora inicial (activación del bloqueo) y una fecha/hora final (desactivación del bloqueo) asociadas con la identificación de la empresa, indicada por el número de la tarjeta de la empresa (al activarse el bloqueo).

053 Los bloqueos se activan y desactivan siempre en tiempo real.

054 Sólo podrá desactivar el bloqueo la empresa que lo haya activado (identificada por los 13 primeros dígitos del número de la tarjeta de la empresa), o bien

055 El bloqueo se desactivará automáticamente si otra empresa activa un bloqueo.

055a En los casos en los que la empresa que activa el bloqueo es la misma empresa que introdujo el anterior bloqueo, se considerará que el bloqueo previo no ha sido desactivado y se encuentra todavía activo.

8. **Supervisión de las actividades de control**

056 Esta función supervisa las actividades de VISUALIZACIÓN, IMPRESIÓN y TRANSFERENCIA de la VU y de la tarjeta que se lleven a cabo en el modo de control.

057 Esta función también supervisa las actividades de CONTROL DEL EXCESO DE VELOCIDAD en el modo de control. Se entenderá que se ha producido un control del exceso de velocidad cuando, estando en el modo de control, se haya enviado la señal de "exceso de velocidad" a la impresora o a la pantalla, o cuando la memoria de datos VU haya transferido datos sobre "incidentes y fallos".

9. **Detección de incidentes o fallos**

058 Esta función detecta los siguientes incidentes o fallos:

9.1. ***Incidente "Inserción de una tarjeta no válida"***

059 Este incidente se produce al insertar una tarjeta no válida o cuando caduca una tarjeta válida insertada.

9.2. ***Incidente "Conflicto de tarjetas"***

060 Este incidente se produce cuando entran en conflicto dos tarjetas válidas. Las combinaciones que originan este incidente se indican con una X en la tabla siguiente:

Conflicto de tarjetas		Ranura del conductor				
		Sin tarjeta	Tarjeta del conductor	Tarjeta de control	Tarjeta del centro de ensayo	Tarjeta de la empresa
Ranura del segundo conductor	Sin tarjeta					
	Tarjeta del conductor				X	
	Tarjeta de control			X	X	X
	Tarjeta del centro de ensayo		X	X	X	X
	Tarjeta de la empresa			X	X	X

9.3. ***Incidente "Solapamiento temporal"***

061 Este incidente se produce cuando la fecha/hora en que se extrajo por última vez una tarjeta de conductor, según quede registrado en dicha tarjeta, es posterior a la fecha/hora actual del aparato de control donde se inserta la tarjeta.

9.4. ***Incidente "Conducción sin tarjeta adecuada"***

062 Este incidente se produce en determinadas combinaciones de dos tarjetas de tacógrafo (indicadas con una X en la tabla siguiente), cuando la actividad del conductor cambia a CONDUCCIÓN o cuando tiene lugar un cambio del modo de funcionamiento mientras la actividad del conductor es CONDUCCIÓN:

Conducción sin tarjeta adecuada		Ranura del conductor				
		Sin tarjeta (o tarjeta no válida)	Tarjeta del conductor	Tarjeta de control	Tarjeta del centro de ensayo	Tarjeta de la empresa
Ranura del segundo conductor	Sin tarjeta (o tarjeta no válida)	X		X		X
	Tarjeta del conductor	X		X	X	X
	Tarjeta de control	X	X	X	X	X
	Tarjeta del centro de ensayo	X	X	X		X
	Tarjeta de la empresa	X	X	X	X	X

9.5. ***Incidente "Inserción de tarjeta durante la conducción"***

063 Este incidente se produce cuando se inserta una tarjeta de tacógrafo en una de las ranuras mientras la actividad del conductor es CONDUCCIÓN.

9.6. ***Incidente "Error al cerrar la última sesión de la tarjeta"***

064 Este incidente se produce cuando, al insertar la tarjeta, el aparato de control detecta que, a pesar de lo dispuesto en el Capítulo III.1., la sesión anterior de la tarjeta no se ha cerrado correctamente (se ha extraído la tarjeta antes de que pudieran grabarse en ella todos los datos pertinentes). Este incidente afecta exclusivamente a las tarjetas de conductor y a las tarjetas del centro de ensayo.

9.7. ***Incidente "Exceso de velocidad"***

065 Este incidente se produce cada vez que se sobrepasa la velocidad permitida.

9.8. ***Incidente "Interrupción del suministro eléctrico"***

066 Este incidente se produce cuando el suministro eléctrico del sensor de movimiento o de la unidad intravehicular se interrumpe durante más de 200 milisegundos, fuera del modo de calibrado. El umbral de interrupción deberá definirlo el fabricante. La caída de tensión que se produce al arrancar el motor del vehículo no deberá activar este incidente.

9.9. ***Incidente "Error de datos de movimiento"***

067 Este incidente se produce en caso de interrupción del flujo normal de datos entre el sensor de movimiento y la unidad intravehicular o en caso de producirse un error de integridad o de autentificación de datos durante el intercambio entre el sensor de movimiento y la unidad intravehicular.

9.10. ***Incidente "Intento de violación de la seguridad"***

068 Este incidente se produce cuando por algún motivo se ha visto afectada la seguridad del sensor de movimiento o de la unidad intravehicular, según se especifica en los objetivos genéricos de seguridad de dichos componentes, fuera del modo de calibrado.

9.11. ***Fallo "Tarjeta"***

069 Este fallo está asociado al fallo de funcionamiento de una tarjeta de tacógrafo.

9.12. ***Fallo "Aparato de control"***

070 Este fallo está asociado a uno de los fallos siguientes, fuera del modo de calibrado:

— fallo interno de la VU,

— fallo de la impresora,

— fallo de la pantalla,

— fallo de transferencia,

— fallo del sensor.

10. **Autodiagnóstico y comprobaciones automáticas**

071 El aparato de control deberá ser capaz de detectar los fallos ocurridos mediante comprobaciones automáticas y una función de autodiagnóstico, con arreglo a la tabla siguiente:

Subconjunto que se verifica	Comprobación automática	Autodiagnóstico
Software		Integridad
Memoria de datos	Acceso	Acceso, integridad de los datos
Dispositivos de interfaz para tarjetas	Acceso	Acceso
Teclado		Comprobación manual
Impresora	(depende del fabricante)	Documento impreso
Pantalla		Comprobación visual
Transferencia (exclusivamente durante la transferencia)	Funcionamiento correcto	
Sensor	Funcionamiento correcto	Funcionamiento correcto

11. **Lectura de datos de la memoria**

072 El aparato de control deberá ser capaz de leer todos los datos almacenados en su memoria.

12. **Registro y almacenamiento de datos en la memoria**

A efectos del presente apartado,

— Por "365 días" se entienden 365 días civiles de actividad media de un conductor en un vehículo. Por actividad media diaria en un vehículo se entiende al menos 6 conductores o segundos conductores, 6 ciclos de inserción-extracción de tarjeta y 256 cambios de actividad. Por consiguiente, "365 días" incluyen al menos 2 190 (segundos) conductores, 2 190 ciclos de inserción-extracción de tarjeta y 93 440 cambios de actividad.

— Las horas se registran con una resolución de un minuto, a menos que se especifique lo contrario.

— Los valores del cuentakilómetros se registran con una resolución de un kilómetro.

— Las velocidades se registran con una resolución de 1 km/h.

073 En las condiciones de homologación del modelo, los datos almacenados en la memoria no deberán verse afectados por interrupciones del suministro eléctrico de menos de doce meses de duración.

074 El aparato de control deberá ser capaz de registrar y almacenar de forma implícita o explícita en su memoria los datos siguientes:

12.1. ***Datos de identificación de los equipos***

12.1.1. *Datos de identificación de la unidad intravehicular*

075 El aparato de control deberá ser capaz de almacenar en su memoria los siguientes datos de identificación de la unidad intravehicular:

— nombre del fabricante,

— dirección del fabricante,

— número de pieza,

— número de serie,

— versión de software,

— fecha de instalación de la versión de software,

— año de fabricación del equipo,

— número de homologación.

076 El fabricante de la unidad intravehicular registra y almacena de manera permanente, sin posibilidad de alteración, los datos de identificación de dicha unidad, excepto los datos relacionados con el software y el número de homologación, que pueden cambiar en caso de actualizar el software.

12.1.2. *Datos de identificación del sensor de movimiento*

077 El sensor de movimiento deberá ser capaz de almacenar en su memoria los siguientes datos de identificación:

— nombre del fabricante,

— número de pieza,

— número de serie,

— número de homologación,

— identificador del componente de seguridad integrado (por ejemplo, número de pieza del chip/procesador interno),

— identificador del sistema operativo (por ejemplo, versión de software).

078 El fabricante del sensor de movimiento registra y almacena en el propio sensor de manera permanente, sin posibilidad de alteración, los datos de identificación de dicho sensor.

079 La unidad intravehicular deberá ser capaz de registrar y almacenar en su memoria los siguientes datos de identificación del sensor de movimiento al que está acoplada:

— número de serie,

— número de homologación,

— fecha del primer acoplamiento.

12.2. ***Elementos de seguridad***

080 El aparato de control deberá ser capaz de almacenar los siguientes elementos de seguridad:

— clave pública europea,

— certificado del Estado miembro,

— certificado del aparato,

— clave privada del aparato.

Es el fabricante de la unidad intravehicular quien se encarga de introducir los elementos de seguridad del aparato de control.

12.3. ***Datos de inserción y extracción de la tarjeta del conductor***

081 Por cada ciclo de inserción y extracción de una tarjeta del conductor o una tarjeta del centro de ensayo, el aparato de control deberá registrar y almacenar en su memoria:

— el nombre y apellidos del titular de la tarjeta, tal y como constan en la tarjeta,

— el número de la tarjeta, el Estado miembro que la ha expedido y su fecha de caducidad, tal y como consta en la tarjeta,

— la fecha y hora de inserción,

— la lectura del cuentakilómetros del vehículo en el momento de insertar la tarjeta,

— la ranura donde se inserta la tarjeta,

— la fecha y hora de extracción,

— la lectura del cuentakilómetros del vehículo en el momento de extraer la tarjeta,

— la información siguiente acerca del vehículo anterior que utilizara el conductor, tal y como consta en la tarjeta:

  — VRN y Estado miembro donde se matriculó el vehículo,

  — fecha y hora de extracción de la tarjeta,

— una bandera que indique si, en el momento de insertar la tarjeta, el titular ha introducido manualmente alguna actividad.

082 La memoria deberá ser capaz de mantener estos datos almacenados durante al menos 365 días.

083 Cuando se agote la capacidad de almacenamiento, los datos más antiguos se sustituirán por otros nuevos.

12.4. ***Datos sobre la actividad del conductor***

084 Cada vez que cambie la actividad del conductor o del segundo conductor, o cada vez que cambie el régimen de conducción, o cada vez que se inserte o extraiga una tarjeta de conductor o una tarjeta del centro de ensayo, el aparato de control deberá registrar y almacenar en su memoria:

— el régimen de conducción (EN EQUIPO, EN SOLITARIO),

— la ranura (CONDUCTOR, SEGUNDO CONDUCTOR),

— el estado de la tarjeta en la ranura que corresponda (INSERTADA, NO INSERTADA) (véase la nota),

— la actividad (CONDUCCIÓN, DISPONIBILIDAD, TRABAJO, PAUSA/DESCANSO),

— la fecha y hora del cambio.

Nota: INSERTADA significa que se ha insertado en la ranura una tarjeta de conductor o una tarjeta del centro de ensayo válida. NO INSERTADA significa lo contrario, es decir, que no se ha insertado en la ranura una tarjeta de conductor o una tarjeta del centro de ensayo válida (por ejemplo, si se inserta una tarjeta de la empresa).

Nota: Los datos de actividad que introduzca manualmente el conductor no se registran en la memoria.

085 La memoria deberá ser capaz de mantener estos datos almacenados durante al menos 365 días.

086 Cuando se agote la capacidad de almacenamiento, los datos más antiguos se sustituirán por otros nuevos.

12.5. ***Lugares donde comienzan o terminan los períodos de trabajo diarios***

087 Cada vez que un (segundo) conductor introduzca el lugar donde comienza o termina un período de trabajo diario, el aparato de control deberá registrar y almacenar en su memoria la información siguiente:

— en su caso, el número de tarjeta del (segundo) conductor y el Estado miembro que haya expedido la tarjeta,

— la fecha y hora de la entrada (o bien la fecha/hora relacionada con la entrada si ésta tiene lugar durante el procedimiento de entrada manual),

— el tipo de entrada (comienzo o final, condición de entrada),

— el país y la región introducidos,

— la lectura del cuentakilómetros del vehículo.

088 La memoria deberá ser capaz de mantener almacenados durante al menos 365 días los datos sobre el comienzo y el final de los períodos de trabajo diarios (suponiendo que un conductor introduzca dos registros diarios).

089 Cuando se agote la capacidad de almacenamiento, los datos más antiguos se sustituirán por otros nuevos.

12.6. ***Datos del cuentakilómetros***

090 Cada día civil a medianoche, el aparato de control deberá registrar en su memoria la lectura del cuentakilómetros del vehículo y la fecha correspondiente.

091 La memoria deberá ser capaz de almacenar las lecturas de los cuentakilómetros a medianoche durante al menos 365 días civiles.

092 Cuando se agote la capacidad de almacenamiento, los datos más antiguos se sustituirán por otros nuevos.

12.7. ***Datos pormenorizados sobre la velocidad***

093 Para cada segundo de al menos las 24 horas que haya estado el vehículo en movimiento, el aparato de control deberá registrar y almacenar en su memoria la velocidad instantánea del vehículo y la fecha y hora correspondientes.

12.8. ***Datos sobre incidentes***

A efectos del presente subapartado, la hora se registrará con una resolución de 1 segundo.

094 El aparato de control deberá registrar y almacenar en su memoria los datos siguientes para cada incidente detectado, con arreglo a las reglas de almacenamiento descritas a continuación:

Incidente	Reglas de almacenamiento	Datos que hay que registrar en cada incidente
Conflicto de tarjetas	— los 10 incidentes más recientes.	— fecha y hora en que comenzó el incidente, — fecha y hora en que terminó el incidente, — tipo, número y Estado miembro emisor de las dos tarjetas que han entrado en conflicto.
Conducción sin tarjeta adecuada	— el incidente de más duración ocurrido en cada uno de los 10 últimos días en que se hayan producido incidentes de ese tipo, — los 5 incidentes de más duración ocurridos en los últimos 365 días.	— fecha y hora en que comenzó el incidente, — fecha y hora en que terminó el incidente, — tipo, número y Estado miembro emisor de cualquier tarjeta que se haya insertado al comenzar o al terminar el incidente, — número de incidentes similares ocurridos ese día.
Inserción de tarjeta durante la conducción	— el último incidente ocurrido en cada uno de los 10 últimos días en que se hayan producido incidentes de ese tipo,	— fecha y hora del incidente, — tipo, número y Estado miembro emisor de la tarjeta, — número de incidentes similares ocurridos ese día
Error al cerrar la última sesión de la tarjeta	— los 10 incidentes más recientes.	— fecha y hora de inserción de la tarjeta, — tipo, número y Estado miembro emisor, — datos de la última sesión según la lectura de la tarjeta: — fecha y hora de inserción de la tarjeta, — VRN y Estado miembro donde se matriculó el vehículo.
Exceso de velocidad ([1])	— el incidente más grave en cada uno de los 10 últimos días en que se hayan producido incidentes de este tipo (es decir, el que haya ocurrido con la velocidad media más alta), — los 5 incidentes más graves ocurridos en los últimos 365 días. — el primer incidente que haya ocurrido después del último calibrado	— fecha y hora en que comenzó el incidente, — fecha y hora en que terminó el incidente, — velocidad máxima medida durante el incidente, — media aritmética de la velocidad medida durante el incidente, — tipo, número y Estado miembro emisor de la tarjeta del conductor (en su caso), — número de incidentes similares ocurridos ese día.

Incidente	Reglas de almacenamiento	Datos que hay que registrar en cada incidente
Interrupción del suministro eléctrico ([2])	— el incidente de más duración en cada uno de los 10 últimos días en que se hayan producido incidentes de este tipo, — los 5 incidentes de más duración ocurridos en los últimos 365 días.	— fecha y hora en que comenzó el incidente, — fecha y hora en que terminó el incidente, — tipo, número y Estado miembro emisor de cualquier tarjeta que se haya insertado al comenzar o al terminar el incidente, — número de incidentes similares ocurridos ese día.
Error en datos de movimiento	— el incidente de más duración en cada uno de los 10 últimos días en que se hayan producido incidentes de este tipo, — los 5 incidentes de más duración ocurridos en los últimos 365 días.	— fecha y hora en que comenzó el incidente, — fecha y hora en que terminó el incidente, — tipo, número y Estado miembro emisor de cualquier tarjeta que se haya insertado al comenzar o al terminar el incidente, — número de incidentes similares ocurridos ese día.
Intento de violación de la seguridad	— los 10 incidentes más recientes de cada tipo.	— fecha y hora en que comenzó el incidente, — fecha y hora en que terminó el incidente (si es pertinente), — tipo, número y Estado miembro emisor de cualquier tarjeta que se haya insertado al comenzar o al terminar el incidente, — tipo de incidente.

095 ([1]) El aparato de control también deberá registrar y almacenar en su memoria:
— la fecha y hora del último CONTROL DEL EXCESO DE VELOCIDAD,
— la fecha y hora del primer exceso de velocidad ocurrido tras este CONTROL DEL EXCESO DE VELOCIDAD,
— el número de incidentes de exceso de velocidad ocurridos después del último CONTROL DEL EXCESO DE VELOCIDAD.
([2]) Estos datos sólo podrán registrarse al reconectar la alimentación eléctrica. Las horas se determinarán con una precisión de un minuto.

12.9. ***Datos sobre fallos***

A efectos del presente subapartado, la hora se registrará con una resolución de 1 segundo.

096 El aparato de control intentará registrar y almacenar en su memoria los datos siguientes para cada fallo detectado, con arreglo a las reglas de almacenamiento descritas a continuación:

Fallo	Reglas de almacenamiento	Datos que hay que registrar en cada fallo
Fallo de la tarjeta	— los 10 fallos más recientes de la tarjeta del conductor.	— fecha y hora en que comenzó el fallo, — fecha y hora en que terminó el fallo, — tipo, número y Estado miembro emisor de la tarjeta.
Fallos del aparato de control	— los 10 fallos más recientes de cada tipo, — el primer fallo ocurrido después del último calibrado.	— fecha y hora en que comenzó el fallo, — fecha y hora en que terminó el fallo, — tipo de fallo, — tipo, nombre y Estado miembro emisor de cualquier tarjeta que se haya insertado al comenzar o al terminar el fallo.

12.10. ***Datos de calibrado***

097 El aparato de control deberá registrar y almacenar en su memoria los datos correspondientes a:

— los parámetros de calibrado conocidos en el momento de la activación,

— su primer calibrado después de la activación,

— su primer calibrado en el vehículo actual (según conste en el VIN),

— los 5 calibrados más recientes (si el aparato se ha calibrado más de una vez en un mismo día civil, se almacenarán los datos correspondientes al último de estos calibrados).

098 Cada vez que se calibre el aparato de control, se almacenarán los datos siguientes:

— propósito del calibrado (activación, primera instalación, instalación, control periódico),

— nombre y dirección del taller,

— número de la tarjeta del centro de ensayo, Estado miembro que haya expedido la tarjeta y fecha de caducidad de la tarjeta,

— identificación del vehículo,

— parámetros que se actualizan o confirman: w, k, l, tamaño de los neumáticos, valor de ajuste del dispositivo limitador de la velocidad, cuentakilómetros (lectura anterior y nueva lectura), fecha y hora (valor anterior y nuevo valor).

099 El sensor de movimiento deberá registrar y almacenar en su memoria los siguientes datos sobre la instalación del sensor de movimiento:

— primer acoplamiento con una VU (fecha, hora, número de homologación de la VU, número de serie de la VU),

— último acoplamiento con una VU (fecha, hora, número de homologación de la VU, número de serie de la VU).

12.11. ***Datos de ajuste de la hora***

100 El aparato de control deberá registrar y almacenar en su memoria los datos correspondientes a:

— la última ocasión en que se ajustara la hora,

— los 5 casos en que la corrección fuera mayor, desde el último calibrado,

realizado en el modo de calibrado y fuera del marco de un calibrado regular (def. f).

101 Cada vez que se ajuste la hora, se registrarán los datos siguientes:

— fecha y hora, valor anterior,

— fecha y hora, nuevo valor,

— nombre y dirección del taller,

— número de la tarjeta del centro de ensayo, Estado miembro que haya expedido la tarjeta y fecha de caducidad de la tarjeta.

12.12. ***Datos sobre actividades de control***

102 El aparato de control deberá registrar y almacenar en su memoria los siguientes datos correspondientes a las 20 actividades de control más recientes:

— fecha y hora del control,

— número de la tarjeta de control y Estado miembro que haya expedido la tarjeta,

— tipo de control (visualización o impresión o transferencia de los datos de la VU o transferencia de los datos de la tarjeta).

103 En caso de transferencia, también habrá que registrar las fechas correspondientes a los días transferidos más antiguos y más recientes.

12.13. ***Datos sobre los bloqueos introducidos por las empresas***

104 El aparato de control deberá registrar y almacenar en su memoria los siguientes datos correspondientes a los 20 últimos bloqueos introducidos por una empresa:

— fecha y hora de activación del bloqueo,

— fecha y hora de desactivación del bloqueo,

— número de la tarjeta de la empresa y Estado miembro que la haya expedido,

— nombre y dirección de la empresa.

12.14. ***Datos sobre actividades de transferencia***

105 El aparato de control deberá registrar y almacenar en su memoria los siguientes datos correspondientes a la última transferencia de datos de la memoria a medios externos, estando en el modo de empresa o en el modo de calibrado:

— fecha y hora de la transferencia,

— número de la tarjeta de la empresa o de la tarjeta del centro de ensayo y Estado miembro que haya expedido la tarjeta,

— nombre de la empresa o del centro de ensayo.

12.15. ***Datos sobre condiciones específicas***

105a El aparato de control deberá registrar en su memoria los siguientes datos correspondientes a condiciones específicas:

— fecha y hora de la entrada,

— tipo de condición específica.

105b La memoria deberá ser capaz de mantener estos datos almacenados durante al menos 365 días (suponiendo que, como media, cada día se abra y se cierre 1 condición). Cuando se agote la capacidad de almacenamiento, los datos más antiguos se sustituirán por otros nuevos.

13. **Lectura de las tarjetas de tacógrafo**

106 El aparato de control deberá ser capaz de leer las tarjetas de tacógrafo con el fin de obtener, cuando proceda, los datos necesarios para:

— identificar el tipo de tarjeta, al titular de la tarjeta, el anterior vehículo empleado, la fecha y hora en que se retirara la tarjeta por última vez y la actividad seleccionada entonces,

— comprobar que la última sesión de la tarjeta se cerró correctamente,

— calcular el tiempo de conducción continua del conductor, su tiempo de descanso acumulado y sus tiempos de conducción acumulados durante la semana anterior y la actual,

— imprimir, previa solicitud, los datos registrados en una tarjeta de conductor,

— transferir a medios externos la información contenida en una tarjeta de conductor.

107 En caso de producirse un error de lectura, el aparato de control intentará ejecutar de nuevo el mismo comando de lectura. Si no lo consigue después de tres intentos, declarará la tarjeta defectuosa y no válida.

14. **Registro y almacenamiento de datos en las tarjetas de tacógrafo**

108 Nada más introducirse la tarjeta del conductor o del centro de ensayo, el aparato de control deberá configurar los "datos de la sesión" en dicha tarjeta.

109 El aparato de control deberá actualizar los datos almacenados en las tarjetas del conductor, del centro de ensayo o de control, si son válidas. Para ello, escribirá en la tarjeta todos los datos necesarios del titular correspondientes al período en que dicha tarjeta esté insertada. En el capítulo IV se especifican los datos almacenados en cada tipo de tarjeta.

109a El aparato de control deberá actualizar los datos sobre la actividad del conductor y sobre los lugares donde comienzan o terminan los períodos de trabajo diarios (según consta en los apartados 5.2.5 y 5.2.6 del capítulo IV). Estos datos, almacenados en las tarjetas del conductor o en las tarjetas del centro de ensayo, se sustituyen por los datos introducidos manualmente por el titular de la tarjeta.

110 Los datos de las tarjetas de tacógrafo se actualizarán de manera que, cuando sea necesario y teniendo en cuenta la capacidad real de almacenamiento de la tarjeta, los datos más recientes sustituyan a los más antiguos.

111 En caso de producirse un error de escritura, el aparato de control intentará ejecutar de nuevo el mismo comando de escritura. Si no lo consigue después de tres intentos, declarará la tarjeta defectuosa y no válida.

112 Antes de liberar la tarjeta del conductor, y después de haber almacenado en ella todos los datos pertinentes, el aparato de control deberá reiniciar los "datos de la sesión".

15. **Visualización**

113 La pantalla deberá incluir al menos 20 caracteres.

114 Los caracteres tendrán un tamaño mínimo de 5 mm de alto y 3,5 mm de ancho.

114a Tal y como se especifica en el apéndice 1, Capítulo 4 "Conjuntos de caracteres", la pantalla deberá admitir el uso de los conjuntos de caracteres Latin1 y Griego, definidos en las partes 1 y 7 de la norma ISO 8859. La pantalla podrá utilizar glifos simplificados (por ejemplo, los caracteres acentuados podrán aparecer sin acento, o las minúsculas podrán verse como mayúsculas).

115 La pantalla deberá tener una iluminación adecuada que no provoque deslumbramiento.

116 Las indicaciones deberán ser visibles desde fuera del aparato de control.

117 El aparato de control deberá ser capaz de mostrar en pantalla:

— los datos por defecto,

— los datos relacionados con advertencias,

— los datos relacionados con el acceso a los menús,

— otros datos que solicite un usuario.

El aparato de control también podrá mostrar en pantalla otras informaciones, siempre que puedan distinguirse claramente de las arriba exigidas.

118 La pantalla del aparato de control deberá utilizar los pictogramas o las combinaciones de pictogramas enumerados en el apéndice 3. También podrán utilizarse otros pictogramas o combinaciones de pictogramas siempre que puedan distinguirse claramente de los exigidos.

119 La pantalla deberá estar siempre encendida (ON) cuando el vehículo esté en movimiento.

120 El aparato de control podrá incluir una función manual o automática que apague (OFF) la pantalla cuando el vehículo esté parado.

El formato de visualización se especifica en el apéndice 5.

15.1. ***Contenido de la pantalla por defecto***

121 Cuando no sea necesario mostrar otra información, el aparato de control deberá presentar en pantalla, por defecto, los datos siguientes:

— la hora local (hora correspondiente al tiempo universal coordinado + desfase introducido por el conductor),

— el modo de funcionamiento,

— la actividad actual del conductor y la del segundo conductor,

— información relativa al conductor:

  — si su actividad actual es CONDUCCIÓN, el tiempo de conducción continua y el tiempo de descanso acumulado hasta ese momento,

  — si su actividad actual no es CONDUCCIÓN, la duración actual de su actividad (desde que la seleccionara) y el tiempo de descanso acumulado hasta ese momento,

— información relativa al segundo conductor:

  — la duración actual de su actividad (desde que la seleccionara).

122 La presentación en pantalla de los datos relativos a cada conductor será clara, sencilla e inequívoca. Si no fuera posible mostrar en pantalla simultáneamente la información relativa al conductor y la relativa al segundo conductor, el aparato de control deberá mostrar por defecto la información relativa al conductor y ofrecerá al usuario la posibilidad de visualizar la información relativa al segundo conductor.

123 Si el ancho de la pantalla no permite visualizar por defecto el modo de funcionamiento, el aparato de control mostrará unos instantes el nuevo modo de funcionamiento cuando cambie.

124 El aparato de control mostrará unos instantes el nombre del titular de la tarjeta en el momento de insertar la tarjeta.

124a Cuando se abra una condición "FUERA DE ÁMBITO", el contenido de la pantalla por defecto deberá mostrar, con el pictograma correspondiente, que la condición está abierta (se admite que no aparezca simultáneamente en pantalla la actividad actual del conductor).

15.2. ***Visualización de advertencias***

125 Para las advertencias que muestre en pantalla el aparato de control se utilizarán principalmente los pictogramas del apéndice 3, completados cuando sea necesario por información adicional codificada en forma numérica. También se podrá añadir una descripción literal de la advertencia en el idioma que prefiera el conductor.

15.3. ***Acceso a los menús***

126 El aparato de control ofrecerá los comandos necesarios a través de una estructura de menús adecuada.

15.4. ***Otras informaciones en pantalla***

127 Deberá ser posible mostrar en pantalla, de manera selectiva y a voluntad:

— la fecha y la hora correspondientes al tiempo universal coordinado,

— el modo de funcionamiento (si no aparece por defecto),

— el tiempo de conducción continua y el tiempo de descanso acumulado del conductor,

— el tiempo de conducción continua y el tiempo de descanso acumulado del segundo conductor,

— el tiempo de conducción acumulado del conductor durante la semana anterior y la actual,

— el tiempo de conducción acumulado del segundo conductor durante la semana anterior y la actual,

— el contenido de cualquiera de los seis documentos impresos, con el mismo formato que el propio documento.

128 El contenido del documento impreso se mostrará en pantalla de manera secuencial, línea por línea. Si el ancho de la pantalla es menor de 24 caracteres, el usuario dispondrá de un medio adecuado para visualizar la información completa (varias líneas, desplazamiento, …). No es necesario que aparezcan en pantalla las líneas del documento impreso destinadas a informaciones manuscritas.

16. **Impresión**

129 El aparato de control deberá ser capaz de imprimir la información almacenada en su memoria o en las tarjetas de tacógrafo. Habrá al menos seis tipos de documentos de impresión:

— impresión diaria de las actividades del conductor almacenadas en la tarjeta,

— impresión diaria de las actividades del conductor almacenadas en la unidad intravehicular,

— impresión de incidentes y fallos almacenados en la tarjeta,

— impresión de incidentes y fallos almacenados en la unidad intravehicular,

— impresión de datos técnicos,

— impresión de excesos de velocidad.

Los pormenores relativos al formato y al contenido de estos documentos se especifican en el apéndice 4.

Es posible incluir datos adicionales al final de los documentos de impresión.

El aparato de control también podrá imprimir otros documentos, siempre que puedan distinguirse claramente de los seis arriba indicados.

130 La "impresión diaria de las actividades del conductor almacenadas en la tarjeta" y la "impresión de incidentes y fallos almacenados en la tarjeta" sólo estarán disponibles cuando se inserte en el aparato de control una tarjeta del conductor o una tarjeta del centro de ensayo. El aparato de control actualizará los datos almacenados en la tarjeta correspondiente antes de iniciar la impresión.

131 A fin de obtener la "impresión diaria de las actividades del conductor almacenadas en la tarjeta" o la "impresión de incidentes y fallos almacenados en la tarjeta", el aparato de control deberá:

— seleccionar automáticamente la tarjeta del conductor o la tarjeta del centro de ensayo, si solo se ha insertado una de estas dos tarjetas,

— o bien ofrecer un comando para seleccionar la tarjeta de origen o seleccionar la tarjeta en la ranura del conductor, si en el aparato de control se han insertado las dos tarjetas.

132 La impresora deberá ser capaz de imprimir 24 caracteres por línea.

133 Los caracteres tendrán un tamaño mínimo de 2,1 mm de alto y 1,5 mm de ancho.

133a Tal y como se especifica en el apéndice 1, Capítulo 4 "Conjuntos de caracteres", la impresora deberá admitir el uso de los conjuntos de caracteres Latin1 y Griego, definidos en las partes 1 y 7 de la norma ISO 8859.

134 Las impresoras estarán diseñadas de tal forma que faciliten los documentos de impresión arriba mencionados con la definición necesaria para evitar ambigüedades en la lectura.

135 Los documentos de impresión conservarán sus dimensiones y registros en las condiciones normales de humedad (10-90 %) y temperatura.

136 El papel de la impresora llevará la marca de homologación de modelo y la indicación del tipo o tipos de aparato de control con los que se puede utilizar. Si se mantienen las condiciones normales de almacenamiento en lo que respecta a intensidad luminosa, humedad y temperatura, los documentos de impresión seguirán siendo claramente legibles e identificables durante al menos un año.

137 Además, deberá ser posible incluir en los citados documentos inscripciones adicionales hechas a mano, tales como la firma del conductor.

138 En caso de que se acabe el papel durante la impresión de un documento, al cargarse un nuevo rollo el aparato de control deberá reiniciar la impresión desde la primera línea o bien continuar la impresión incluyendo una referencia inequívoca a la parte ya impresa.

17. **Advertencias**

139 El aparato de control deberá avisar al conductor cuando detecte algún incidente o fallo.

140 La advertencia por un incidente de interrupción del suministro eléctrico podrá hacerse cuando se restablezca el suministro.

141 El aparato de control deberá avisar al conductor 15 minutos antes y en el preciso instante en que el tiempo de conducción continua supere 4 h y 30 min.

142 Las señales de advertencia serán visuales, aunque también se podrá instalar señales de tipo acústico.

143 Las señales de advertencia visuales deberán ser perfectamente reconocibles para el usuario, estarán ubicadas dentro del campo de visión del conductor y podrán leerse claramente tanto de día como de noche.

144 Los avisadores luminosos podrán estar incorporados en el aparato de control o separados de él.

145 En este último caso, el avisador llevará una "T" y será de color ámbar o naranja.

146 Las señales de advertencia tendrán una duración de al menos 30 segundos, a menos que el usuario las confirme pulsando una tecla cualquiera del aparato de control. Esta primera confirmación no hará que desaparezca la indicación en pantalla del motivo de la advertencia (véase el párrafo siguiente).

147 El motivo de la advertencia se indicará en la pantalla del aparato de control y permanecerá visible hasta que lo confirme el usuario mediante una tecla o un comando específico del aparato de control.

148 También podrán instalarse otras señales de advertencia, siempre que el conductor no las confunda con las que se han definido anteriormente.

18. **Transferencia de datos a medios externos**

149 El aparato de control, a petición del usuario, deberá ser capaz de transferir a medios de almacenamiento externos los datos contenidos en la memoria o en una tarjeta del conductor, utilizando para ello el conector de calibrado/transferencia. El aparato de control actualizará los datos almacenados en la tarjeta correspondiente antes de iniciar la transferencia.

150 Asimismo, y como característica opcional, el aparato de control podrá, en cualquier modo de funcionamiento, transferir datos por medio de otro conector a una empresa autentificada a través de este canal. En tal caso, dicha transferencia estará sujeta a los derechos de acceso a los datos en el modo de empresa.

151 La transferencia no deberá alterar ni borrar los datos almacenados.

Las características de la interfaz eléctrica del conector de calibrado/transferencia se especifican en el apéndice 6.

Los protocolos de transferencia se especifican en el apéndice 7.

19. **Envío de datos a dispositivos externos adicionales**

152 Si en la pantalla del aparato de control no se indica la velocidad o la lectura del cuentakilómetros, dicho aparato deberá enviar una o más señales de salida que permitan visualizar la velocidad del vehículo (velocímetro) o la distancia total recorrida por el vehículo (cuentakilómetros).

153 Asimismo, la unidad intravehicular deberá ser capaz de enviar los datos que se mencionan a continuación para que puedan procesarlos otras unidades electrónicas instaladas en el vehículo. Los datos se enviarán a través de una conexión en serie adecuada e independiente de una conexión opcional de bus CAN [ISO 11898 Vehículos de carretera — Intercambio de información digital — Red de Área de Controlador (CAN) para comunicaciones de alta velocidad]:

— fecha y hora actuales correspondientes al tiempo universal coordinado,

— velocidad del vehículo,

— distancia total recorrida por el vehículo (cuentakilómetros),

— actividad del conductor y del segundo conductor actualmente seleccionada,

— información de si actualmente hay alguna tarjeta de tacógrafo insertada en la ranura del conductor y en la ranura del segundo conductor, y (en su caso) información sobre la identificación de dichas tarjetas (número de tarjeta y Estado miembro que la haya expedido).

También se podrán enviar otros datos aparte de los arriba mencionados, que constituyen una lista mínima.

Cuando el encendido del vehículo esté activado (ON), estos datos se enviarán de manera permanente. Cuando el encendido del vehículo esté desactivado (OFF), al menos los cambios que se produzcan en la actividad del conductor o del segundo conductor o la inserción o extracción de una tarjeta de tacógrafo generarán una salida de datos correspondiente. Si se ha retenido el envío de datos mientras el encendido del vehículo estaba desactivado, esos datos deberán enviarse en cuanto el encendido del vehículo se active de nuevo.

20. **Calibrado**

154 La función de calibrado deberá permitir:

— el acoplamiento automático del sensor de movimiento con la VU,

— la adaptación digital de la constante del aparato de control (k) al coeficiente característico del vehículo (w) (los vehículos con dos o más multiplicaciones de eje deberán ir provistos de un dispositivo de conmutación que acomode estas multiplicaciones automáticamente a aquélla para la que el aparato se haya adaptado al vehículo),

— el ajuste (sin limitación) de la hora actual,

— el ajuste de la lectura actual del cuentakilómetros,

— la actualización de los datos de identificación del sensor de movimiento que hay almacenados en la memoria,

— la actualización o confirmación de otros parámetros que conozca el aparato de control: identificación del vehículo, w, l, tamaño de los neumáticos y valor de ajuste del dispositivo limitador de la velocidad, en su caso.

155 El acoplamiento del sensor de movimiento con la VU deberá constar al menos de los siguientes pasos:

— actualización (si es preciso) de los datos relativos a la instalación del sensor de movimiento, almacenados en el propio sensor de movimiento,

— copia, en la memoria de la VU, de los datos necesarios para la identificación del sensor de movimiento, almacenados en el propio sensor de movimiento.

156 La función de calibrado deberá ser capaz de introducir todos los datos necesarios a través del conector de calibrado/transferencia, de acuerdo con el protocolo de calibrado definido en el apéndice 8. La función de calibrado también podrá utilizar otros conectores para introducir los datos necesarios.

21. **Ajuste de la hora**

157 La función de ajuste de la hora deberá permitir el ajuste de la hora actual en incrementos de 1 minuto como máximo en intervalos no inferiores a 7 días.

158 La función de ajuste de la hora deberá permitir el ajuste de la hora actual sin limitaciones, en el modo de calibrado.

22. **Características de funcionamiento**

159 La unidad intravehicular deberá funcionar perfectamente en el intervalo de temperaturas que va de - 20 °C a 70 °C, y el sensor de movimiento en el intervalo de - 40 °C a 135 °C. El contenido de la memoria de datos no se borrará aunque la temperatura descienda por debajo de - 40 °C.

160 El aparato de control deberá funcionar perfectamente en el intervalo higrométrico del 10 % al 90 %.

161 El aparato de control deberá estar protegido frente a sobretensiones, inversiones de polaridad de la fuente de alimentación y cortocircuitos.

162 El aparato de control deberá ser conforme a la Directiva 95/54/CE de la Comisión [1], por la que se adapta al progreso técnico la Directiva 72/245/CEE del Consejo [2], relativa a la compatibilidad electromagnética, y deberá estar protegida contra descargas electromagnéticas y fluctuaciones de la tensión.

23. **Materiales**

163 Todos los elementos que formen parte del aparato de control deberán estar fabricados con materiales de estabilidad y resistencia mecánica suficientes y de características eléctricas y magnéticas invariables.

164 Al objeto de garantizar condiciones normales de utilización, todas las partes internas del aparato deberán estar protegidas contra la humedad y el polvo.

165 La unidad intravehicular deberá tener la clase de protección IP 40 y el sensor de movimiento la clase de protección IP 64, según la norma IEC 529.

---

[1] DO L 266 de 8.11.1995, p. 1.
[2] DO L 152 de 6.7.1972, p. 15.

166 El aparato de control deberá ser conforme a todas las especificaciones técnicas aplicables relativas al diseño ergonómico.

167 El aparato de control deberá estar protegido frente a daños accidentales.

24. **Inscripciones**

168 Si el aparato de control permite visualizar la lectura del cuentakilómetros y la velocidad del vehículo, en su pantalla deberán figurar las inscripciones siguientes:

— junto a la cifra que indica la distancia, la unidad de medida de la distancia, indicada mediante la abreviatura "km",

— junto a la cifra que indica la velocidad, la abreviatura "km/h".

El aparato de control también debe ser capaz de mostrar la velocidad en millas por hora, en cuyo caso la unidad de medición de la velocidad se indicará con la abreviatura "mph".

169 Cada uno de los componentes del aparato de control deberá llevar una placa descriptiva con la información siguiente:

— nombre y dirección del fabricante del aparato de control,

— número de pieza del fabricante y año de fabricación del aparato,

— número de serie del aparato,

— marca de homologación del modelo de aparato de control.

170 Cuando el espacio físico disponible no baste para mostrar todas las informaciones arriba mencionadas, en la placa descriptiva deberá figurar al menos: el nombre o el logotipo del fabricante y el número de pieza del aparato de control.

IV. CONDICIONES DE FABRICACIÓN Y FUNCIONAMIENTO DE LAS TARJETAS DE TACÓGRAFO

1. **Datos visibles**

El anverso de la tarjeta contendrá:

171 la mención "Tarjeta del conductor" o "Tarjeta de control" o "Tarjeta del centro de ensayo" o "Tarjeta de la empresa", en caracteres grandes, en la lengua o lenguas oficiales del Estado miembro que expida la tarjeta, según el tipo de tarjeta.

172 Esa misma mención en las demás lenguas oficiales de la Comunidad, impresas de modo que constituyan el fondo de la tarjeta:

ES	TARJETA DEL CONDUCTOR	TARJETA DE CONTROL	TARJETA DEL CENTRO DE ENSAYO	TARJETA DE LA EMPRESA
DK	FØRERKORT	KONTROLKORT	VÆRKSTEDSKORT	VIRKSOMHEDSKORT
DE	FAHRERKARTE	KONTROLLKARTE	WERKSTATTKARTE	UNTERNEHMENSKARTE
EL	ΚΑΡΤΑ ΟΔΗΟΥ	ΚΑΡΤΑ ΕΛΕΓΧΟΥ	ΚΑΡΤΑ ΚΕΝΤΡΟΥ ΔΟΚΙΜΩΝ	ΚΑΡΤΑ ΕΠΙΧΕΙΡΗΣΗΣ
EN	DRIVER CARD	CONTROL CARD	WORKSHOP CARD	COMPANY CARD
FR	CARTE DE CONDUCTEUR	CARTE DE CONTROLEUR	CARTE D'ATELIER	CARTE D'ENTREPRISE
GA	CÁRTA TIOMÁNAÍ	CÁRTA STIÚRTHA	CÁRTA CEARDLAINNE	CÁRTA COMHLACHTA
IT	CARTA DEL CONDUCENTE	CARTA DI CONTROLLO	CARTA DELL'OFFICINA	CARTA DELL'AZIENDA
NL	BESTUURDERS KAART	CONTROLEKAART	WERKSPLAATSKAART	BEDRIJFSKAART
PT	CARTÃO DE CONDUTOR	CARTÃO DE CONTROLO	CARTÃO DO CENTRO DE ENSAIO	CARTÃO DE EMPRESA
FI	KULJETTAJA KORTTILLA	VALVONTA KORTILLA	TESTAUSASEMA KORTILLA	YRITYSKORTILLA
SV	FÖRARKORT	KONTROLLKORT	VERKSTADSKORT	FÖRETAGSKORT

173 El nombre del Estado miembro que expida la tarjeta (opcional);

174 El distintivo del Estado miembro que expida la tarjeta, impreso en negativo en un rectángulo azul rodeado de doce estrellas amarillas. Los distintivos serán los siguientes:

B Bélgica

DK Dinamarca

D Alemania

GR Grecia

E España

F Francia

IRL Irlanda

I Italia

L Luxemburgo

NL Países Bajos

A Austria

P Portugal

FIN Finlandia

S Suecia

UK Reino Unido

175 Las informaciones específicas de la tarjeta expedida, que constarán del siguiente modo:

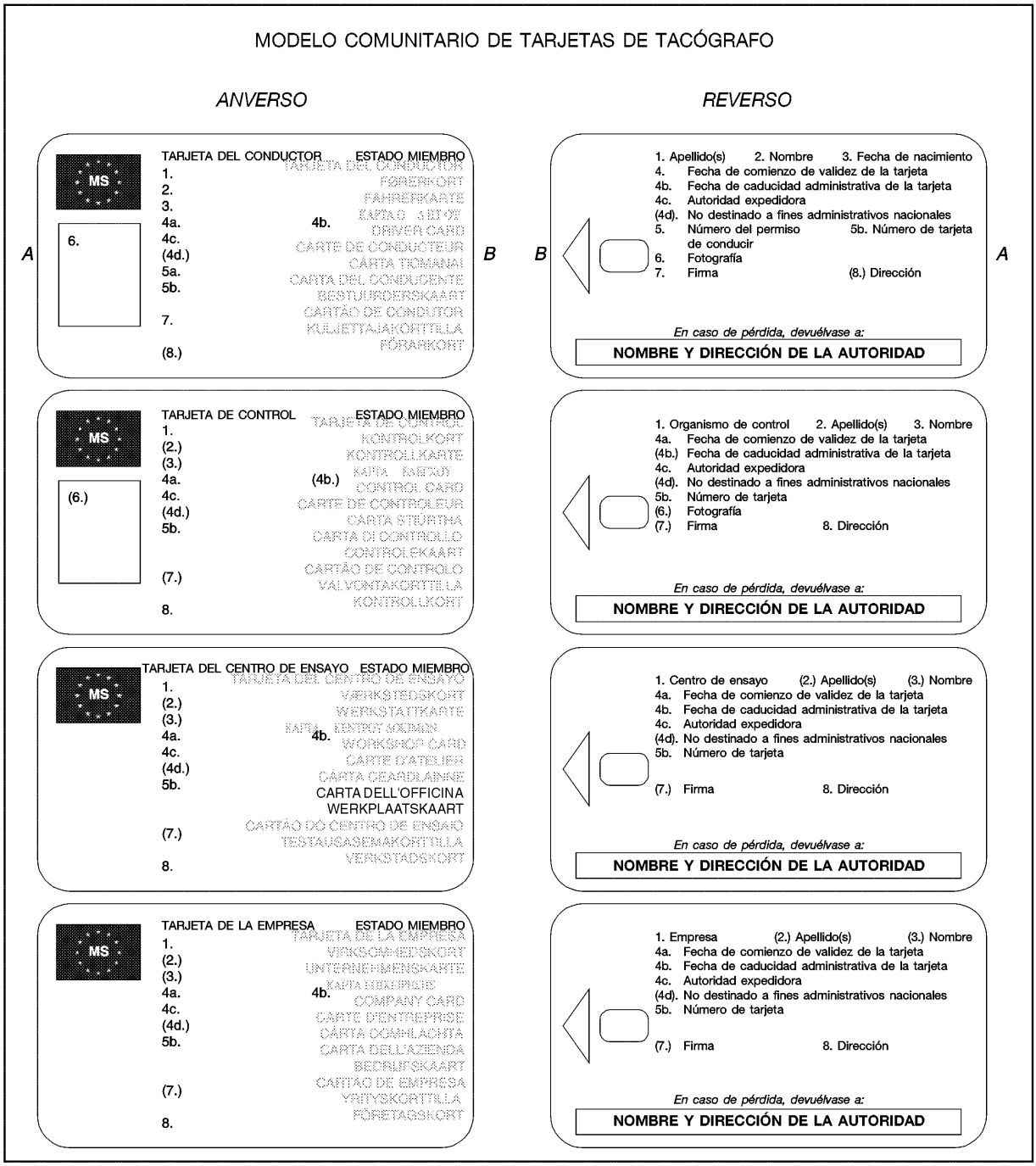
	Tarjeta del conductor	Tarjeta de control	Tarjeta de la empresa o del centro de ensayo
1.	apellido(s) del conductor	nombre del organismo de control	nombre de la empresa o del centro de ensayo
2.	nombre del conductor	apellido del controlador (en su caso)	apellido del titular de la tarjeta (en su caso)
3.	fecha de nacimiento del conductor	nombre del controlador (en su caso)	nombre del titular de la tarjeta (en su caso)
4.(a)	fecha de comienzo de validez de la tarjeta		
(b)	fecha de caducidad de la tarjeta (en su caso)		
(c)	designación de la autoridad que expide la tarjeta (puede figurar en la página 2)		
(d)	un número distinto del que se recoge en la rúbrica 5, que sea útil para la gestión de la tarjeta (opcional)		
5.(a)	número del permiso de conducir (en la fecha de expedición de la tarjeta del conductor)		
5.(b)	Número de tarjeta		
6.	fotografía del conductor	fotografía del controlador (opcional)	—
7.	firma del conductor	firma del titular (opcional)	
8.	lugar de residencia habitual, o dirección postal del titular (opcional)	dirección postal del organismo de control	dirección postal de la empresa o del centro de ensayo

176 Las fechas deberán escribirse con el formato “dd/mm/aaaa” o bien “dd.mm.aaaa” (día, mes, año).

El dorso de la tarjeta contendrá:

177 una explicación de las rúbricas numeradas que aparecen en la primera página de la tarjeta;

178 con autorización expresa por escrito del titular, podrán incluirse también informaciones que no estén relacionadas con la gestión de la tarjeta, pero sin que con ello se modifique en modo alguno la utilización del modelo como tarjeta de tacógrafo.



179 Las tarjetas de tacógrafo deberán imprimirse con los siguientes colores de fondo predominantes:

— tarjeta del conductor: blanco,

— tarjeta de control: azul,

— tarjeta del centro de ensayo: rojo,

— tarjeta de la empresa: amarillo.

180 Las tarjetas de tacógrafo deberán reunir al menos las siguientes características de protección contra intentos de falsificación y manipulación:

— un fondo con diseño de seguridad, fondo labrado e impresión en arco iris,

— en la zona de la fotografía, el fondo con diseño de seguridad y la fotografía deberán solaparse,

— al menos una línea de microimpresión bicolor.

181 Previa consulta a la Comisión, los Estados miembros podrán añadir colores o inscripciones, tales como símbolos nacionales y características de seguridad, sin perjuicio de las demás disposiciones del presente anexo.

2. **Seguridad**

La seguridad del sistema tiene por misión proteger la integridad y autenticidad de los datos que intercambian las tarjetas y el aparato de control, proteger la integridad y la autenticidad de los datos que se transfieren de las tarjetas, permitir determinadas operaciones de escritura en las tarjetas por parte del aparato de control exclusivamente, descartar toda posibilidad de falsificación de los datos almacenados en las tarjetas, impedir la manipulación y detectar todo intento en este sentido.

182 Al objeto de lograr la seguridad del sistema, las tarjetas de tacógrafo deberán cumplir los requisitos de seguridad que se definen en sus objetivos genéricos de seguridad (apéndice 10).

183 Las tarjetas de tacógrafo podrán leerse con otros equipos, como por ejemplo ordenadores personales.

3. **Normas**

184 Las tarjetas de tacógrafo deberán ajustarse a las normas siguientes:

— ISO/IEC 7810 Tarjetas de identificación — Características físicas,

— ISO/IEC 7816 Tarjetas de identificación — Circuitos integrados con contactos:

  — Parte 1: Características físicas,

  — Parte 2: Dimensiones y ubicación de los contactos,

  — Parte 3: Señales electrónicas y protocolos de transmisión,

  — Parte 4: Comandos intersectoriales de intercambio,

  — Parte 8: Comandos intersectoriales relacionados con la seguridad,

— ISO/IEC 10373 Tarjetas de identificación — Métodos de ensayo.

4. **Especificaciones ambientales y eléctricas**

185 Las tarjetas de tacógrafo deberán estar en condiciones de funcionar correctamente bajo cualquier condición climática habitual en el territorio de la Comunidad y al menos en el intervalo de temperaturas comprendido entre – 25 °C y + 70 °C, con picos ocasionales de hasta + 85 °C ("ocasional" significa no más de 4 horas cada vez y no más de 100 veces durante la vida útil de la tarjeta).

186 Las tarjetas de tacógrafo deberán poder funcionar correctamente en el intervalo higrométrico comprendido entre el 10 % y el 90 %.

187 Las tarjetas de tacógrafo deberán poder funcionar correctamente durante cinco años si se utilizan con arreglo a las especificaciones ambientales y eléctricas.

188 Por lo que respecta a su funcionamiento, las tarjetas de tacógrafo deberán ser conformes a la Directiva 95/54/CE relativa a la compatibilidad electromagnética, y deberán estar protegidas contra descargas electromagnéticas.

5. **Almacenamiento de datos**

A efectos del presente apartado,

— las horas se registran con una resolución de un minuto, a menos que se especifique lo contrario,

— las lecturas del cuentakilómetros se registran con una resolución de un kilómetro,

— las velocidades se registran con una resolución de 1 km/h.

Las funciones, comandos y estructuras lógicas de las tarjetas de tacógrafo, por lo que respecta al cumplimiento de las condiciones de almacenamiento de datos, se especifican en el apéndice 2.

189 En este apartado se especifica la capacidad mínima de almacenamiento de los diferentes archivos de datos de la aplicación. Las tarjetas de tacógrafo deberán ser capaces de indicar al aparato de control la capacidad real de almacenamiento de dichos archivos.

Todos los datos adicionales que puedan contener las tarjetas de tacógrafo, relativos a otras aplicaciones que soporte la tarjeta, deberán estar almacenados con arreglo a la Directiva 95/46/CE.

5.1. ***Identificación de la tarjeta y datos de seguridad***

5.1.1. *Identificación de la aplicación*

190 Las tarjetas de tacógrafo deberán ser capaces de almacenar los siguientes datos para la identificación de la aplicación:

— identificación de la aplicación del tacógrafo,

— identificación del tipo de tarjeta de tacógrafo.

5.1.2. *Identificación del chip*

191 Las tarjetas de tacógrafo deberán ser capaces de almacenar los siguientes datos para la identificación del circuito integrado (CI):

— número de serie del CI,

— referencias de fabricación del CI.

5.1.3. *Identificación de la tarjeta CI*

192 Las tarjetas de tacógrafo deberán ser capaces de almacenar los siguientes datos para la identificación de la tarjeta inteligente:

— número de serie de la tarjeta (incluidas referencias de fabricación),

— número de homologación del modelo de tarjeta,

— identificación personal de la tarjeta (ID),

— ID del fabricante de la tarjeta,

— Identificador del CI.

5.1.4. *Elementos de seguridad*

193 Las tarjetas de tacógrafo deberán ser capaces de almacenar los siguientes datos sobre elementos de seguridad:

— clave pública europea,

— certificado del Estado miembro,

— certificado de la tarjeta,

— clave privada de la tarjeta.

5.2. ***Tarjeta del conductor***

5.2.1. *Identificación de la tarjeta*

194 La tarjeta del conductor deberá ser capaz de almacenar los siguientes datos relativos a la identificación de la tarjeta:

— número de tarjeta,

— nombre del Estado miembro y de la autoridad que expidió la tarjeta, fecha de expedición,

— fecha de comienzo de validez de la tarjeta, fecha de caducidad de la tarjeta.

5.2.2. *Identificación del titular de la tarjeta*

195 La tarjeta del conductor deberá ser capaz de almacenar los siguientes datos relativos a la identificación del titular de la tarjeta:

— apellido(s) del titular,

— nombre del titular,

— fecha de nacimiento,

— idioma preferido.

5.2.3. *Información sobre el permiso de conducir*

196 La tarjeta del conductor deberá ser capaz de almacenar los siguientes datos sobre el permiso de conducir:

— designación del Estado miembro y la autoridad que haya expedido el permiso,

— número del permiso de conducir (en la fecha de expedición de la tarjeta).

5.2.4. *Datos sobre vehículos empleados*

197 La tarjeta del conductor deberá ser capaz de almacenar, para cada día civil que se haya utilizado la tarjeta y para cada período de uso del vehículo en ese día (un período de uso incluye todos los ciclos consecutivos de inserción/extracción de la tarjeta en el vehículo, visto desde el punto de vista de la tarjeta), los siguientes datos:

— fecha y hora en que se utiliza el vehículo por primera vez (es decir, primera inserción de la tarjeta en ese período de uso del vehículo, o bien 00h00 si el vehículo se está utilizando en ese momento),

— lectura del cuentakilómetros del vehículo en ese momento,

— fecha y hora en que se utiliza el vehículo por última vez, (es decir, última extracción de la tarjeta en ese período de uso del vehículo, o bien 23h59 si el vehículo se está utilizando en ese momento),

— valor del cuentakilómetros del vehículo en ese momento,

— VRN y Estado miembro donde se matriculó el vehículo.

198 La tarjeta del conductor deberá ser capaz de almacenar al menos 84 de estos registros.

5.2.5. *Datos sobre la actividad del conductor*

199 La tarjeta del conductor deberá ser capaz de almacenar, para cada día civil que se haya utilizado la tarjeta o para el cual el conductor haya introducido actividades manualmente, los siguientes datos:

— la fecha,

— un contador de presencia diaria (incrementado en una unidad por cada uno de estos días civiles),

— la distancia total recorrida por el conductor durante ese día,

— el régimen de conducción a las 00:00,

— cada vez que el conductor cambie de actividad, o cambie el régimen de conducción, o inserte o extraiga su tarjeta:

  — el régimen de conducción (EN EQUIPO, EN SOLITARIO),

  — la ranura (CONDUCTOR, SEGUNDO CONDUCTOR),

  — el estado de la tarjeta (INSERTADA, NO INSERTADA),

  — la actividad (CONDUCCIÓN, DISPONIBILIDAD, TRABAJO, PAUSA/DESCANSO),

  — la hora del cambio.

200 La memoria de la tarjeta del conductor deberá ser capaz de mantener almacenados durante al menos 28 días los datos sobre la actividad del conductor (la actividad media de un conductor se define como 93 cambios de actividad por día).

201 Los datos enumerados en los epígrafes 197 y 199 deberán almacenarse de manera que las actividades puedan recuperarse en su orden de ocurrencia, incluso en una situación de solapamiento temporal.

5.2.6. *Lugares donde comienzan o terminan los períodos de trabajo diarios*

202 La tarjeta del conductor deberá ser capaz de almacenar los siguientes datos, que introduce el conductor, relativos a los lugares donde comienzan o terminan los períodos de trabajo diarios:

— la fecha y hora de la entrada (o la fecha/hora relacionada con la entrada si ésta tiene lugar durante el procedimiento de entrada manual),

— el tipo de entrada (comienzo o final, condición de entrada),

— el país y la región introducidos,

— la lectura del cuentakilómetros del vehículo.

203 La memoria de la tarjeta del conductor deberá ser capaz de mantener almacenados al menos 42 pares de estos registros.

5.2.7. *Datos sobre incidentes*

A efectos del presente subapartado, la hora se almacenará con una resolución de 1 segundo.

204 La tarjeta del conductor deberá ser capaz de almacenar los datos relativos a los siguientes incidentes detectados por el aparato de control con la tarjeta insertada:

— solapamiento temporal (cuando esa tarjeta sea la causa del incidente),

— inserción de la tarjeta durante la conducción (cuando esa tarjeta sea el objeto del incidente),

— error al cerrar la última sesión de la tarjeta (cuando esa tarjeta sea el tema del incidente),

— interrupción del suministro eléctrico,

— error en los datos de movimiento,

— intentos de violación de la seguridad.

205 La tarjeta del conductor deberá ser capaz de almacenar los siguientes datos sobre dichos incidentes:

— código del incidente,

— fecha y hora en que comenzó el incidente (o en que se insertó la tarjeta, si el incidente estaba ocurriendo en ese momento),

— fecha y hora en que terminó el incidente (o en que se extrajo la tarjeta, si el incidente estaba ocurriendo en ese momento),

— VRN y Estado miembro donde se matriculó el vehículo en el que ocurrió el incidente.

Nota: por lo que respecta al incidente de "solapamiento temporal":

— la fecha y hora en que comenzó el incidente deberán coincidir con la fecha y hora en que se retirara la tarjeta del vehículo anterior,

— la fecha y hora en que terminó el incidente deberán coincidir con la fecha y hora en que se insertara la tarjeta en el vehículo actual,

— los datos del vehículo deberán coincidir con los del vehículo en que se produce el incidente.

Nota: por lo que respecta al incidente de "error al cerrar la última sesión de la tarjeta":

— la fecha y hora en que comenzó el incidente deberán coincidir con la fecha de inserción de la tarjeta y la hora de la sesión que no se cerrara correctamente,

— la fecha y hora en que terminó el incidente deberán coincidir con la fecha de inserción de la tarjeta y la hora de la sesión durante la que se detectara el incidente (sesión actual),

— los datos del vehículo deberán coincidir con los del vehículo en que la sesión no se cerró correctamente.

206 La tarjeta del conductor deberá ser capaz de almacenar los datos correspondientes a los seis incidentes más recientes de cada tipo (es decir, un total de 36 incidentes).

5.2.8. *Datos sobre fallos*

A efectos del presente subapartado, la hora se registrará con una resolución de 1 segundo.

207 La tarjeta del conductor deberá ser capaz de almacenar los datos relativos a los siguientes fallos detectados por el aparato de control estando la tarjeta insertada:

— fallo de la tarjeta (cuando esa tarjeta sea el tema del incidente),

— fallo del aparato de control.

208 La tarjeta del conductor deberá ser capaz de almacenar los siguientes datos sobre dichos fallos:

— código del fallo,

— fecha y hora en que comenzó el fallo (o en que se introdujo la tarjeta, si el fallo estaba ocurriendo en ese momento),

— fecha y hora en que terminó el fallo (o en que se extrajo la tarjeta, si el fallo estaba ocurriendo en ese momento),

— VRN y Estado miembro donde se matriculó el vehículo en el que ocurrió el fallo.

209 La tarjeta del conductor deberá ser capaz de almacenar los datos correspondientes a los doce fallos más recientes de cada tipo (es decir, un total de 24 fallos).

5.2.9. *Datos sobre actividades de control*

210 La tarjeta del conductor deberá ser capaz de almacenar los siguientes datos relativos a las actividades de control:

— fecha y hora del control,

— número de la tarjeta de control y Estado miembro que haya expedido la tarjeta,

— tipo de control [visualización o impresión o transferencia de los datos de la VU o transferencia de los datos de la tarjeta (véase la nota)],

— período transferido, en caso de transferencia,

— VRN y Estado miembro donde se matriculó el vehículo en el que se produjera el control.

Nota: las condiciones de seguridad implican que la transferencia de los datos de la tarjeta sólo quedará registrada si se lleva a cabo con un aparato de control.

211 La tarjeta del conductor deberá ser capaz de mantener almacenado uno de dichos registros.

5.2.10. *Datos de la sesión*

212 La tarjeta del conductor deberá ser capaz de almacenar los datos relativos al vehículo que abrió la sesión actual:

— fecha y hora en que se abrió la sesión (es decir, inserción de la tarjeta), con una resolución de un segundo,

— VRN y Estado miembro donde se matriculó el vehículo.

5.2.11. *Datos sobre condiciones específicas*

212a La tarjeta del conductor deberá ser capaz de almacenar los siguientes datos relativos a las condiciones específicas que se introdujeron al insertar la tarjeta (en la ranura que fuese):

— fecha y hora de la entrada,

— tipo de condición específica.

212b La tarjeta del conductor deberá ser capaz de mantener almacenados 56 de estos registros.

5.3. ***Tarjeta del centro de ensayo***

5.3.1. *Elementos de seguridad*

213 La tarjeta del centro de ensayo deberá ser capaz de almacenar un número de identificación personal (código PIN).

214 La tarjeta del centro de ensayo deberá poder almacenar las claves criptográficas necesarias para acoplar sensores de movimiento con unidades intravehiculares.

5.3.2. *Identificación de la tarjeta*

215 La tarjeta del centro de ensayo deberá ser capaz de almacenar los siguientes datos relativos a la identificación de la tarjeta:

— número de tarjeta,

— nombre del Estado miembro y de la autoridad que expidió la tarjeta, fecha de expedición,

— fecha de comienzo de validez de la tarjeta, fecha de caducidad de la tarjeta.

5.3.3. *Identificación del titular de la tarjeta*

216 La tarjeta del centro de ensayo deberá ser capaz de almacenar los siguientes datos relativos a la identificación del titular de la tarjeta:

— nombre del centro de ensayo,

— dirección del centro de ensayo,

— apellido(s) del titular,

— nombre del titular,

— idioma preferido.

5.3.4. *Datos sobre vehículos empleados*

217 La tarjeta del centro de ensayo deberá ser capaz de almacenar registros de datos sobre los vehículos empleados, del mismo modo que una tarjeta del conductor.

218 La tarjeta del centro de ensayo deberá ser capaz de almacenar al menos 4 de estos registros.

5.3.5. *Datos sobre la actividad del conductor*

219 La tarjeta del centro de ensayo deberá ser capaz de almacenar datos sobre la actividad del conductor, del mismo modo que una tarjeta del conductor.

220 La tarjeta del centro de ensayo deberá ser capaz de mantener almacenados los datos sobre la actividad del conductor durante al menos 1 día de actividad media.

5.3.6. *Datos sobre el comienzo y el final de los períodos de trabajo diarios*

221 La tarjeta del centro de ensayo deberá ser capaz de almacenar los registros de datos sobre las horas de comienzo o final de los períodos de trabajo diarios, del mismo modo que una tarjeta del conductor.

222 La tarjeta del centro de ensayo deberá ser capaz de mantener almacenados al menos 3 pares de estos registros.

5.3.7. *Datos sobre fallos e incidentes*

223 La tarjeta del centro de ensayo deberá ser capaz de almacenar los registros de datos sobre fallos e incidentes, del mismo modo que una tarjeta del conductor.

224 La tarjeta del centro de ensayo deberá ser capaz de almacenar los datos de los tres incidentes más recientes de cada tipo (es decir, 18 incidentes) y de los seis fallos más recientes de cada tipo (es decir, 12 fallos).

5.3.8. *Datos sobre actividades de control*

225 La tarjeta del centro de ensayo deberá ser capaz de almacenar un registro de datos sobre actividades de control, del mismo modo que una tarjeta del conductor.

5.3.9. *Datos de calibrado y de ajuste de la hora*

226 La tarjeta del centro de ensayo deberá ser capaz de mantener almacenados los registros de los calibrados o ajustes de hora que se hayan realizado mientras la tarjeta está insertada en el aparato de control.

227 Cada registro de calibrado deberá ser capaz de mantener almacenados los datos siguientes:

— propósito del calibrado (primera instalación, instalación, control periódico),

— identificación del vehículo,

— parámetros que se actualizan o confirman (w, k, l, tamaño de los neumáticos, valor de ajuste del dispositivo limitador de la velocidad, cuentakilómetros (lectura anterior y nueva lectura), fecha y hora (valor anterior y nuevo valor),

— identificación del aparato de control (número de pieza de la VU, número de serie de la VU, número de serie del sensor de movimiento).

228 La tarjeta del centro de ensayo deberá ser capaz de almacenar al menos 88 de estos registros.

229 La tarjeta del centro de ensayo deberá tener un contador que indique el número total de calibrados que se hayan realizado con la tarjeta.

230 La tarjeta del centro de ensayo deberá tener un contador que indique el número de calibrados que se hayan realizado desde la última transferencia.

5.3.10. *Datos sobre condiciones específicas*

230a La tarjeta del centro de ensayo deberá ser capaz de almacenar los datos correspondientes a las condiciones específicas, del mismo modo que la tarjeta del conductor. La tarjeta del centro de ensayo deberá ser capaz de almacenar 2 de estos registros.

5.4. ***Tarjeta de control***

5.4.1. *Identificación de la tarjeta*

231 La tarjeta de control deberá ser capaz de almacenar los siguientes datos relativos a la identificación de la tarjeta:

— número de tarjeta,

— nombre del Estado miembro y de la autoridad que expidió la tarjeta, fecha de expedición,

— fecha de comienzo de validez de la tarjeta, fecha de caducidad de la tarjeta (en su caso).

5.4.2. *Identificación del titular de la tarjeta*

232 La tarjeta de control deberá ser capaz de almacenar los siguientes datos relativos a la identificación del titular de la tarjeta:

— nombre del organismo de control,

— dirección del organismo de control,

— apellido(s) del titular,

— nombre del titular,

— idioma preferido.

5.4.3. *Datos sobre actividades de control*

233 La tarjeta de control deberá ser capaz de almacenar los siguientes datos sobre actividades de control:

— fecha y hora del control,

— tipo de control (visualización o impresión o transferencia de los datos de la VU o transferencia de los datos de la tarjeta),

— período transferido (en su caso),

— VRN y autoridad del Estado miembro donde se matriculó el vehículo controlado,

— número de tarjeta y Estado miembro que haya expedido la tarjeta de conductor que se controla.

234 La tarjeta de control deberá ser capaz de mantener almacenados al menos 230 de estos registros.

5.5. ***Tarjeta de la empresa***

5.5.1. *Identificación de la tarjeta*

235 La tarjeta de la empresa deberá ser capaz de almacenar los siguientes datos relativos a la identificación de la tarjeta:

— número de tarjeta,

— nombre del Estado miembro y de la autoridad que expidió la tarjeta, fecha de expedición,

— fecha de comienzo de validez de la tarjeta, fecha de caducidad de la tarjeta (en su caso).

5.5.2. *Identificación del titular de la tarjeta*

236 La tarjeta de la empresa deberá ser capaz de almacenar los siguientes datos relativos a la identificación del titular de la tarjeta:

— nombre de la empresa,

— dirección de la empresa.

5.5.3. *Datos sobre la actividad de la empresa*

237 La tarjeta de la empresa deberá ser capaz de almacenar los siguientes datos sobre la actividad de la empresa:

— fecha y hora de la actividad,

— tipo de actividad (activación o desactivación del bloqueo de la VU, o transferencia de los datos de la VU o transferencia de los datos de la tarjeta),

— período transferido (en su caso),

— VRN y autoridad del Estado miembro donde se matriculó el vehículo,

— número de tarjeta y Estado miembro que haya expedido la tarjeta (en caso de transferencia de los datos de la tarjeta).

238 La tarjeta de la empresa deberá ser capaz de mantener almacenados al menos 230 de estos registros.

V. INSTALACIÓN DEL APARATO DE CONTROL

1. **Instalación**

239 El aparato de control deberá entregarse desactivado al instalador o al fabricante del vehículo, con todos los parámetros de calibrado que se relacionan en el capítulo III.20 configurados según sus valores por defecto. Si no existe un valor en particular que deba considerarse adecuado por defecto, los parámetros literales deberán configurarse con cadenas de interrogantes ("?") y los valores numéricos deberán ajustarse a cero ("0").

240 Antes de ser activado, el aparato de control tendrá que dar acceso a la función de calibrado, aunque no se encuentre en el modo de calibrado.

241 Antes de ser activado, el aparato de control no deberá registrar ni almacenar los datos mencionados en III.12.3. a III.12.9. y III.12.12 a III.12.14. inclusive.

242 Durante la instalación, el fabricante del vehículo deberá preconfigurar todos los parámetros conocidos.

243 El fabricante del vehículo o el instalador deberá activar el aparato de control antes de que el vehículo salga de la nave donde se haya llevado a cabo la instalación.

244 El aparato de control se activa automáticamente al insertar por primera vez una tarjeta del centro de ensayo en cualquiera de los dispositivos de interfaz para tarjetas.

245 Las operaciones específicas de acoplamiento que se precisan entre el sensor de movimiento y la unidad intravehicular, si las hay, deberán producirse automáticamente antes o durante la activación.

246 Una vez activado, el aparato de control deberá permitir el uso de todas las funciones y derechos de acceso a los datos.

247 Una vez activado el aparato de control, las funciones de registro y almacenamiento serán totalmente operativas.

248 La instalación deberá ir seguida de un calibrado. El primer calibrado incluirá la introducción del número de matrícula (VRN) y tendrá lugar en un plazo máximo de 2 semanas tras esta instalación o tras la asignación del número de matrícula, si ésta es posterior.

248a El aparato de control deberá colocarse en el vehículo de modo que el conductor pueda acceder a las funciones necesarias desde su sitio.

2. **Placa de instalación**

249 Después de haber instalado y verificado el aparato de control, se colocará en el mismo, o junto a él, una placa de instalación bien visible y de fácil acceso. Después de cada nueva intervención del instalador o del centro de ensayo autorizado, la placa deberá sustituirse por una nueva.

250 En la placa deberán figurar, como mínimo, los datos siguientes:

— nombre completo y domicilio o nombre comercial del instalador o del centro de ensayo autorizado,

— coeficiente característico del vehículo, en la forma “w = … imp/km”,

— constante del aparato de control, en la forma “k = … imp/km”,

— circunferencia efectiva de los neumáticos de las ruedas, en la forma “l = … mm”,

— tamaño de los neumáticos,

— fecha en la que se determinó el coeficiente característico del vehículo y se midió la circunferencia efectiva de los neumáticos de las ruedas,

— el número de bastidor del vehículo (VIN).

3. **Precintos**

251 Deberán precintarse los elementos siguientes:

— cualquier conexión que, de estar desconectada, ocasionaría modificaciones o pérdidas de datos imposibles de descubrir,

— la placa de instalación, salvo que esté sujeta de tal modo que no pueda retirarse sin destruir las inscripciones que figuran en ella.

252 Los precintos anteriormente mencionados podrán quitarse:

— en caso de urgencia,

— para instalar, ajustar o reparar un dispositivo de limitación de velocidad o cualquier otro dispositivo que contribuya a la seguridad vial, siempre que el aparato de control siga funcionando de forma fiable y correcta y vuelva a ser precintado por un instalador o taller autorizado (de acuerdo con lo dispuesto en el capítulo VI) inmediatamente después de que se haya instalado el limitador de velocidad o cualquier otro dispositivo que contribuya a la seguridad en carretera, o en el plazo de 7 días en otros casos.

253 Siempre que se retiren estos precintos deberá redactarse y ponerse a disposición de la autoridad competente una justificación de esta medida.

VI. VERIFICACIONES, CONTROLES Y REPARACIONES

En el capítulo V.3 del presente anexo se definen las circunstancias en las que pueden quitarse los precintos, según se indica en el apartado 5 del artículo 12 del Reglamento (CEE) nº 3821/85, cuya última modificación la constituye el Reglamento (CE) nº 2135/98.

1. **Aprobación de instaladores o centros de ensayo**

Los Estados miembros aprobarán, inspeccionarán periódicamente y certificarán los organismos encargados de realizar:

— instalaciones,

— verificaciones,

— controles,

— reparaciones.

En el marco de lo dispuesto en el apartado 1 del artículo 12 de este Reglamento, las tarjetas de centro de ensayo se expedirán únicamente a los instaladores o centros de ensayo que hayan sido autorizados para proceder a la activación o calibrado del aparato de control de conformidad con el presente anexo y que además, salvo justificación:

— no puedan optar a recibir una tarjeta de la empresa,

— sus actividades profesionales restantes no supongan un compromiso potencial de la seguridad general del sistema tal y como se define en el apéndice 10.

2. **Verificación de instrumentos nuevos o reparados**

254 Cada dispositivo, tanto nuevo como reparado, deberá verificarse individualmente en lo que se refiere a su correcto funcionamiento y a la exactitud de sus indicaciones y registros, dentro de los límites establecidos en los puntos 2.1 y 2.2 del capítulo III, mediante la colocación de un precinto, de acuerdo con lo dispuesto en el capítulo V.3., y la realización de un calibrado.

3. **Inspección de la instalación**

255 En el momento de su instalación en un vehículo, el aparato de control y la instalación en su conjunto deberán ajustarse a las disposiciones sobre las tolerancias máximas establecidas en los puntos 2.1 y 2.2 del capítulo III.

4. **Controles periódicos**

256 Los aparatos instalados en los vehículos se someterán a un control periódico cada vez que se repare el aparato o se efectúe cualquier modificación del coeficiente característico del vehículo o de la circunferencia efectiva de los neumáticos de las ruedas, o si la hora UTC del aparato presenta un retraso o un adelanto de más de 20 minutos, o si cambia el número de matrícula, o al menos en el plazo de dos años desde el último control.

257 En estos controles se verificará al menos:

— que el aparato de control ejecute correctamente todas sus funciones, incluida la función de almacenamiento de datos en las tarjetas de tacógrafo,

— que se cumpla lo dispuesto en los puntos 2.1 y 2.2 del capítulo III sobre tolerancias máximas al realizarse la instalación,

— que el aparato de control lleve la marca de homologación,

— que se haya colocado la placa de instalación,

— que estén intactos los precintos del aparato y de las demás partes de la instalación,

— el tamaño y la circunferencia real de los neumáticos.

258 Dichos controles deberán incluir un calibrado.

5. **Determinación de errores**

259 La determinación de los errores de instalación y de uso deberá efectuarse en las condiciones siguientes, que se considerarán condiciones normales de ensayo:

— vehículo vacío, en condiciones normales de marcha,

— presión de los neumáticos conforme a las instrucciones del fabricante,

— desgaste de los neumáticos dentro de los límites admitidos por las normas nacionales en vigor,

— movimiento del vehículo:

  — éste deberá desplazarse, movido por su propio motor, en línea recta por una superficie plana a una velocidad de 50 ± 5 km/h. La distancia de medición será de al menos 1 000 m,

— la prueba podrá realizarse también en un banco de pruebas adecuado o con otros métodos, si garantizan una precisión similar.

6. **Reparaciones**

260 Los centros de ensayo deberán ser capaces de extraer los datos del aparato de control para facilitarlos a la empresa de transportes que corresponda.

261 Los centros de ensayo autorizados deberán expedir para las empresas de transportes un certificado de intransferibilidad de datos donde se atestigüe que los datos previamente registrados no se pueden transferir en caso de producirse un fallo de funcionamiento del aparato, ni siquiera después de una reparación por un centro de ensayo. Los centros de ensayo conservarán en su poder durante al menos un año una copia de cada certificado que hayan expedido.

VII. EXPEDICIÓN DE TARJETAS

Los procedimientos de expedición de tarjetas que establezcan los Estados miembros deberán cumplir las condiciones siguientes:

262 En el número de la primera tarjeta de tacógrafo expedida para un solicitante, el índice consecutivo (en su caso), el índice de sustitución y el índice de renovación serán "0".

263 Los números de todas las tarjetas de tacógrafo no personales que se expidan para un mismo organismo de control, centro de ensayo o empresa de transportes empezarán por los mismos 13 dígitos, y todos ellos tendrán un índice consecutivo diferente.

264 Cuando se expida una tarjeta de tacógrafo en sustitución de otra ya existente, la nueva llevará el mismo número de tarjeta con excepción del índice de sustitución, que se verá incrementado en una unidad (en el orden 0, …, 9, A, …, Z).

265 Cuando se expida una tarjeta de tacógrafo en sustitución de otra ya existente, la nueva tendrá la misma fecha de caducidad.

266 Cuando se expida una tarjeta de tacógrafo para renovar otra ya existente, la nueva llevará el mismo número de tarjeta con excepción del índice de sustitución, que se pondrá a "0", y el índice de renovación, que se verá incrementado en una unidad (en el orden 0, …, 9, A, …, Z).

267 Cuando se sustituya una tarjeta de tacógrafo existente para modificar datos administrativos, se observarán las reglas de renovación si el cambio se efectúa en el mismo Estado miembro, o las reglas de primera expedición, si el cambio lo efectúa otro Estado miembro.

268 En el caso de las tarjetas de centro de ensayo o de control que no sean personales, en la rúbrica "apellido(s) del titular de la tarjeta" se anotará el nombre del centro de ensayo o del organismo de control.

VIII. HOMOLOGACIÓN DEL APARATO DE CONTROL Y DE LAS TARJETAS DE TACÓGRAFO

1. **Generalidades**

A efectos del presente capítulo, por "aparato de control" se entenderá el "aparato de control o sus componentes". No es preciso homologar el cable o cables que conectan el sensor de movimiento y la VU. El papel que utilice el aparato de control se considerará un componente de dicho aparato.

269 El aparato de control deberá presentarse a la homologación provisto de los dispositivos complementarios pertinentes.

270 La homologación del aparato de control y de las tarjetas de tacógrafo deberá incluir pruebas relacionadas con la seguridad, pruebas funcionales y pruebas de interoperabilidad. El resultado positivo de cada una de estas pruebas se consignará en un certificado.

271 Las autoridades de homologación de los Estados miembros no concederán el certificado de homologación del modelo, de conformidad con el artículo 5 del presente Reglamento, si no se les hace entrega de:

— un certificado de seguridad,

— un certificado funcional, y

— un certificado de interoperabilidad

para el aparato de control o la tarjeta de tacógrafo cuya homologación se solicite.

272 Todo cambio que se introduzca en el software o el hardware del aparato de control o en la naturaleza de los materiales empleados en su fabricación deberá notificarse, antes de su utilización, a la autoridad que haya homologado el aparato. Dicha autoridad deberá confirmar al fabricante el alcance de la homologación, o bien podrá exigir una actualización o confirmación del certificado funcional, de seguridad o de interoperabilidad.

273 Los procesos de actualización del software empleado por el aparato de control precisarán la aprobación de la autoridad que haya homologado el aparato. La actualización del software no deberá alterar ni borrar los datos sobre la actividad del conductor que haya almacenados en el aparato de control. El software sólo podrá actualizarse bajo la responsabilidad del fabricante del aparato.

2. **Certificado de seguridad**

274 El certificado de seguridad se entrega según lo dispuesto en el apéndice 10 del presente anexo.

3. **Certificado funcional**

275 Cada candidato al recibir una homologación deberá facilitar a la autoridad de homologación del Estado miembro que corresponda todo el material y la documentación que dicha autoridad estime necesario.

276 El certificado funcional deberá entregarse al fabricante sólo después de haberse superado como mínimo todas las pruebas funcionales especificadas en el apéndice 9.

277 El certificado funcional lo entrega la autoridad de homologación. Dicho certificado deberá incluir, además del nombre de su beneficiario y la identificación del modelo, una relación pormenorizada de las pruebas que se hayan realizado, junto con los resultados obtenidos.

4. **Certificado de interoperabilidad**

278 Las pruebas de interoperabilidad las lleva a cabo un único laboratorio bajo la autoridad y la responsabilidad de la Comisión Europea.

279 Dicho laboratorio deberá registrar en el orden cronológico de recepción las solicitudes de prueba que presenten los fabricantes.

280 Las solicitudes sólo se registrarán oficialmente cuando el laboratorio esté en posesión de:

— todo el material y los documentos necesarios para dichas pruebas de interoperabilidad,

— el correspondiente certificado de seguridad,

— el correspondiente certificado funcional.

La fecha de registro de la solicitud deberá notificarse al fabricante.

281 El laboratorio no deberá realizar pruebas de interoperabilidad con aparatos de control o tarjetas de tacógrafo para los que no se haya concedido un certificado de seguridad y un certificado funcional.

282 Todo el material y los documentos facilitados por el fabricante que solicite pruebas de interoperabilidad quedarán en manos del laboratorio encargado de dichas pruebas.

283 Las pruebas de interoperabilidad deberán llevarse a cabo con arreglo a lo dispuesto en el apartado 5 del apéndice 9 del presente anexo e incluirán todos los tipos de aparatos de control o tarjetas de tacógrafo:

— que dispongan de un certificado de homologación válido, o bien

— que estén pendientes de ser homologados y dispongan de un certificado de interoperabilidad válido.

284 El laboratorio no entregará el certificado de interoperabilidad al fabricante hasta que se hayan superado todas las pruebas de interoperabilidad exigidas.

285 Si uno o varios aparatos de control o tarjetas de tacógrafo no superan las pruebas de interoperabilidad, tal y como se especifica en el epígrafe 283, el certificado de interoperabilidad no se entregará hasta que el fabricante que presente la solicitud haya realizado las modificaciones necesarias y superado las pruebas de interoperabilidad. El laboratorio deberá identificar la causa del problema con ayuda de los fabricantes que se vean afectados por dicho fallo de interoperabilidad, y procurará ayudar al fabricante que presente la solicitud a encontrar una solución técnica. Si el fabricante ha modificado su producto, será responsabilidad suya comprobar, mediante consulta a las autoridades pertinentes, que el certificado de seguridad y los certificados funcionales siguen siendo válidos.

286 El certificado de interoperabilidad es válido durante seis meses y queda revocado al finalizar este período si el fabricante no ha recibido el correspondiente certificado de homologación del modelo. El fabricante entrega el certificado de interoperabilidad a la autoridad de homologación del Estado miembro que ha otorgado el certificado funcional.

287 El elemento o elementos que pudieran haber causado un fallo de interoperabilidad no deberán utilizarse con afán de lucro o para lograr una posición dominante.

5. **Certificado de homologación del modelo**

288 La autoridad de homologación del Estado miembro podrá entregar el certificado de homologación del modelo en cuanto esté en posesión de los tres certificados necesarios.

289 Cuando entregue el certificado de homologación al fabricante, la autoridad de homologación deberá facilitar una copia al laboratorio encargado de las pruebas de interoperabilidad.

290 El laboratorio competente para las pruebas de interoperabilidad deberá mantener un sitio web público donde se pueda consultar una relación actualizada de los modelos de aparato de control o de tarjetas de tacógrafo:

— para los que se haya registrado una solicitud de pruebas de interoperabilidad,

— que hayan recibido un certificado de interoperabilidad (aunque sea provisional),

— que hayan recibido un certificado de homologación.

6. **Procedimiento de excepción: primeros certificados de interoperabilidad**

291 Hasta cuatro meses después de haberse certificado que el primer acoplamiento constituido por el aparato de control y las tarjetas de tacógrafo (tarjeta del conductor, tarjeta del centro de ensayo, tarjeta de control y tarjeta de la empresa) es interoperable, se considerarán provisionales los certificados de interoperabilidad que puedan haberse entregado (incluido este primero) en relación con las solicitudes registradas durante este período.

292 Si al finalizar este período todos los productos afectados interoperan sin problemas entre sí, los certificados de interoperabilidad correspondientes adquirirán un carácter definitivo.

293 Si durante este período se detectan fallos de interoperabilidad, el laboratorio encargado de las pruebas de interoperabilidad deberá identificar las causas de los problemas con ayuda de todos los fabricantes implicados, y les invitará a realizar las modificaciones necesarias.

294 Si al finalizar este período persisten los problemas de interoperabilidad, el laboratorio encargado de las pruebas de interoperabilidad, con la colaboración de los fabricantes implicados y con las autoridades de homologación que otorguen los correspondientes certificados funcionales, deberán determinar las causas de los fallos de interoperabilidad y establecer las modificaciones que debería introducir cada uno de los fabricantes. La búsqueda de soluciones técnicas deberá prolongarse un máximo de dos meses. Si transcurre este plazo sin haberse hallado una solución común, la Comisión, previa consulta al laboratorio encargado de las pruebas de interoperabilidad, deberá decidir qué aparato(s) y tarjetas obtienen un certificado de interoperabilidad definitivo, y fundamentar su decisión.

295 Deberá posponerse hasta que se hayan resuelto los problemas de interoperabilidad iniciales cualquier solicitud de pruebas de interoperabilidad que registre el laboratorio entre el final del período de cuatro meses posterior al primer certificado de interoperabilidad provisional y la fecha en que la Comisión adopta la decisión mencionada en el epígrafe 294. Dichas solicitudes se procesarán luego en el orden cronológico en que se registraron.

Apéndice 1

DICCIONARIO DE DATOS

ÍNDICE

1. INTRODUCCIÓN

En el presente apéndice se especifican diversos formatos, elementos y estructuras para su uso en el aparato de control y las tarjetas de tacógrafo.

1.1. **Enfoque de la definición de los tipos de datos**

En el presente apéndice se utiliza la Notación de Sintaxis Abstracta Uno (NSA.1) para definir los tipos de datos. Ello permite definir datos simples y estructurados sin necesidad de una sintaxis específica de transferencia (reglas de codificación), que dependerá de la aplicación y del entorno.

Las convenciones sobre la denominación de los tipos NSA.1 se ajustan a la norma ISO/IEC 8824-1. Esto significa que:

— siempre que sea posible, el significado de un tipo de datos se deduce de los nombres seleccionados,

— cuando un tipo de datos se compone de otros tipos, el nombre del tipo de datos sigue siendo una secuencia única de caracteres alfabéticos que comienzan con una mayúscula, aunque las mayúsculas se utilizan en el nombre para transmitir el correspondiente significado,

— en general, los nombres de los tipos de datos están relacionados con el nombre de los tipos de datos de los que se derivan, con el equipo en que se almacenan los datos y con la función asociada a dichos datos.

Si un tipo NSA.1 ya se ha definido como parte de otra norma y si es pertinente para uso en el aparato de control, entonces ese tipo NSA.1 se definirá en el presente apéndice.

Para que pueda haber diferentes tipos de reglas de codificación, algunos tipos NSA.1 del presente apéndice están limitados por identificadores de intervalos de valores. Dichos identificadores se definen en el apartado 3.

1.2. **Referencias**

En el presente apéndice aparecen las siguientes referencias:

ISO 639	Código para la representación de nombres de lenguas. Primera edición: 1988.
EN 726-3	Sistemas de tarjetas de identificación — Tarjetas de circuito(s) integrados y terminales para las telecomunicaciones — Parte 3: Requisitos de la tarjeta independientes de las aplicaciones. Diciembre 1994.
ISO 3779	Vehículos de carretera — Número de identificación del vehículo (VIN) — Contenido y estructura. Edición 3: 1983.
ISO/IEC 7816-5	Tecnología de la información — Tarjetas de identificación — Tarjetas de circuitos(s) integrado(s) con contactos — Parte 5: Sistema de numeración y procedimiento de registro para identificadores de aplicación. Primera edición: 1994 + Modificación 1: 1996.
ISO/IEC 8824-1	Tecnología de la información — Notación de Sintaxis Abstracta 1 (NSA.1): Especificación de la notación básica. Edición 2: 1998.
ISO/IEC 8825-2	Tecnología de la información — Reglas de codificación NSA.1: Especificación de las Reglas de Codificación por Paquetes (PER). Edición 2: 1998.
ISO/IEC 8859-1	Tecnología de la información — Conjuntos de caracteres gráficos codificados con un solo byte de 8 bits — Parte 1: Alfabeto latino nº 1. Primera edición: 1998.
ISO/IEC 8859-7	Tecnología de la información — Conjuntos de caracteres gráficos codificados con un solo byte de 8 bits — Parte 7: Alfabeto latino/griego. Primera edición: 1987.
ISO 16844-3	Vehículos de carretera — Sistemas de tacógrafo — Interfaz del sensor de movimiento. WD 3-20/05/99.

2. DEFINICIONES DE TIPOS DE DATOS

En todos los tipos de datos que se describen a continuación, el valor por defecto para un contenido "desconocido" o "no aplicable" consistirá en rellenar el elemento de datos con bytes 'FF'.

2.1. **ActivityChangeInfo**

Este tipo de datos permite codificar, en una palabra de dos bytes, el estado de la ranura a las 00.00 o el estado del conductor a las 00.00 y/o los cambios de actividad y/o los cambios del régimen de conducción y/o los cambios del estado de la tarjeta para un conductor o un segundo conductor. Este tipo de datos está relacionado con los requisitos 084, 109a, 199 y 219.

```
ActivityChangeInfo ::= OCTET STRING (SIZE(2))
```

Asignación de valor — Alineación de octeto: 'scpaatttttttttttt'B (16 bits)

Para registros en la memoria de datos (o estado de la ranura):

's'B Ranura:

'0'B: CONDUCTOR,

'1'B: SEGUNDO CONDUCTOR,

'c'B Régimen de conducción:

'0'B: EN SOLITARIO,

'1'B: EN EQUIPO,

'p'B Estado de la tarjeta del conductor (o del centro de ensayo) en la ranura que corresponda:

'0'B: INSERTADA, hay una tarjeta insertada,

'1'B: NO INSERTADA, no hay tarjeta insertada (o se ha extraído una tarjeta),

'aa'B Actividad:

'00'B: PAUSA/DESCANSO,

'01'B: DISPONIBILIDAD,

'10'B: TRABAJO,

'11'B: CONDUCCIÓN,

'ttttttttttt'B Hora del cambio: minutos transcurridos desde las 00.00 horas de ese día.

Para registros en la tarjeta del conductor (o del centro de ensayo) (y estado del conductor):

's'B Ranura (irrelevante cuando 'p' = 1, excepto en el caso que se cita en la nota siguiente):

'0'B: CONDUCTOR,

'1'B: SEGUNDO CONDUCTOR,

'c'B Régimen de conducción (caso 'p' = 0) o Régimen en la actividad siguiente (caso 'p' = 1):

'0'B: EN SOLITARIO, '0'B: INDETERMINADO

'1'B: EN EQUIPO, '1'B: DETERMINADO (= entrada manual)

'p'B Estado de la tarjeta:

'0'B: INSERTADA, la tarjeta está insertada en un equipo de control,

'1'B: NO INSERTADA, la tarjeta no está insertada (o se ha extraído),

'aa'B Actividad (irrelevante cuando 'p' = 1 y 'c' = 0, excepto en el caso citado en la nota siguiente):

'00'B: PAUSA/DESCANSO,

'01'B: DISPONIBILIDAD,

'10'B: TRABAJO,

'11'B: CONDUCCIÓN,

'ttttttttttt'B Hora del cambio: minutos transcurridos desde las 00h00 de ese día.

Nota sobre el caso "extracción de la tarjeta":

Cuando se extrae la tarjeta:

— 's' es relevante e indica la ranura de la que se extrae la tarjeta,

— 'c' debe configurarse a 0,

— 'p' debe configurarse a 1,

— 'aa' debe codificar la actividad que esté seleccionada en ese momento,

Como resultado de una entrada manual, los bits 'c' y 'aa' de la palabra (almacenada en una tarjeta) se pueden sobrescribir posteriormente para reflejar la entrada.

2.2. **Address**

Una dirección.

```
Address ::= SEQUENCE {
   codePage                                    INTEGER (0..255),
   address                                     OCTET STRING (SIZE(35))
}
```

codePage especifica qué parte de la norma ISO/IEC 8859 se utiliza para codificar la dirección,

address es una dirección codificada con arreglo a la norma ISO/IEC 8859-codePage.

2.3. **BCDString**

La cadena BCDString se aplica para la representación decimal de codificación binaria (BCD). Este tipo de datos se utiliza para representar un dígito decimal en un semiocteto (4 bits). La cadena BCDString se basa en el 'CharacterStringType' de la norma ISO/IEC 8824-1.

```
BCDString ::= CHARACTER STRING (WITH COMPONENTS {
   identification ( WITH COMPONENTS {
   fixed PRESENT }) })
```

La cadena BCDString emplea una notación "hstring". El dígito hexadecimal situado más a la izquierda deberá ser el semiocteto más significativo del primer octeto. Para obtener un múltiplo de octetos habrá que insertar semioctetos a la derecha, según sea necesario, a partir de la posición del semiocteto situado más a la izquierda en el primer octeto.

Los dígitos permitidos son : 0, 1, … 9.

2.4. **CalibrationPurpose**

Código que explica por qué se registró un conjunto de parámetros de calibrado. Este tipo de datos está relacionado con los requisitos 097 y 098.

```
CalibrationPurpose ::= OCTET STRING (SIZE(1))
```

Asignación de valor:

'00'H valor reservado,

'01'H activación: registro de los parámetros de calibrado conocidos en el momento de la activación de la VU,

'02'H primera instalación: primer calibrado de la VU después de su activación,

'03'H instalación: primer calibrado de la VU en el vehículo actual,

'04'H control periódico.

2.5. **CardActivityDailyRecord**

Información almacenada en una tarjeta y relativa a las actividades del conductor en un día civil concreto. Este tipo de datos está relacionado con los requisitos 199 y 219.

```
CardActivityDailyRecord ::= SEQUENCE {
   activityPreviousRecordLength            INTEGER(0..CardActivityLengthRange),
   activityRecordDate                      TimeReal,
   activityDailyPresenceCounter            DailyPresenceCounter,
   activityDayDistance                     Distance,
   activityChangeInfo                      SET SIZE(1..1440) OF ActivityChangeInfo
}
```

activityPreviousRecordLength es la longitud total del registro diario anterior, expresada en bytes. El valor máximo viene dado por la longitud de la CADENA DE OCTETOS que contiene dichos registros (véase CardActivityLengthRange, apartado 3). Cuando este registro es el registro diario más antiguo, el valor de activityPreviousRecordLength debe configurarse a 0.

activityRecordLength es la longitud total de este registro, expresada en bytes. El valor máximo viene dado por la longitud de la CADENA DE OCTETOS que contiene dichos registros.

activityRecordDate es la fecha del registro.

activityDailyPresenceCounter es el contador de presencia diaria para esa tarjeta en ese día.

activityDayDistance es la distancia total recorrida ese día.

activityChangeInfo es el conjunto de datos de ActivityChangeInfo correspondientes al conductor en ese día. Puede contener 1 440 valores como máximo (un cambio de actividad cada minuto). Este conjunto incluye siempre la ActivityChangeInfo que codifica el estado del conductor a las 00:00.

2.6. **CardActivityLengthRange**

Número de bytes disponibles en una tarjeta de conductor o en una tarjeta del centro de ensayo para almacenar registros sobre las actividades del conductor.

```
CardActivityLengthRange ::= INTEGER(0..2^16-1)
```

Asignación de valor: véase el apartado 3.

2.7. **CardApprovalNumber**

Número de homologación de la tarjeta.

```
CardApprovalNumber ::= IA5String(SIZE(8))
```

Asignación de valor: sin especificar.

2.8. **CardCertificate**

Certificado de la clave pública de una tarjeta.

```
CardCertificate ::= Certificate
```

2.9. **CardChipIdentification**

Información almacenada en una tarjeta y relativa a la identificación del circuito integrado (CI) de dicha tarjeta (requisito 191).

```
CardChipIdentification ::= SEQUENCE {
   icSerialNumber                          OCTET STRING (SIZE(4)),
   icManufacturingReferences               OCTET STRING (SIZE(4))
}
```

icSerialNumber es el número de serie del CI, tal y como se define en la norma EN 726-3.

icManufacturingReferences es el identificador del fabricante del CI y los elementos de fabricación, tal y como se definen en la norma EN 726-3.

2.10. **CardConsecutiveIndex**

El índice consecutivo de una tarjeta [definición h)].

```
CardConsecutiveIndex ::= IA5String(SIZE(1))
```

Asignación de valor: (véase el capítulo VII del presente anexo)

Orden de incremento: '0, …, 9, A, … , Z, a, … , z'

2.11. **CardControlActivityDataRecord**

Información almacenada en una tarjeta de conductor o en una tarjeta del centro de ensayo y relativa al último control que ha pasado el conductor (requisitos 210 y 225).

```
CardControlActivityDataRecord ::= SEQUENCE {
   controlType                          controlType,
   controlTime                          TimeReal,
   controlCardNumber                    FullCardNumber,
   controlVehicleRegistration           VehicleRegistrationIdentification,
   controlDownloadPeriodBegin           TimeReal,
   controlDownloadPeriodEnd             TimeReal,
}
```

controlType es el tipo de control.

controlTime es la fecha y la hora del control.

controlCardNumber es el FullCardNumber del funcionario que ha realizado el control.

controlVehicleRegistration es el VRN y el nombre del Estado miembro donde se matriculó el vehículo que ha sido objeto del control.

controlDownloadPeriodBegin y **controlDownloadPeriodEnd** es el período transferido, en caso de transferencia.

2.12. **CardCurrentUse**

Información acerca del uso actual de la tarjeta (requisito 212).

```
CardCurrentUse ::= SEQUENCE {
   sessionOpenTime                      TimeReal,
   sessionOpenVehicle                   VehicleRegistrationIdentification
}
```

sessionOpenTime es la hora en que se inserta la tarjeta para el uso actual. Este elemento se pone a cero al extraer la tarjeta.

sessionOpenVehicle es la identificación del vehículo que se está utilizando actualmente. Este elemento se configura al insertar la tarjeta y se pone a cero al extraer la tarjeta.

2.13. **CardDriverActivity**

Información almacenada en una tarjeta de conductor o en una tarjeta del centro de ensayo y relativa a las actividades del conductor (requisitos 199 y 219).

```
CardDriverActivity ::= SEQUENCE {
   activityPointerOldestDayRecord       INTEGER(0..CardActivityLengthRange-1),
   activityPointerNewestRecord          INTEGER(0..CardActivityLengthRange-1),
   activityDailyRecords                 OCTET STRING
                                        (SIZE(CardActivityLengthRange))
}
```

activityPointerOldestDayRecord es un elemento que señala el comienzo del espacio de almacenamiento (número de bytes a partir del principio de la cadena) que corresponde al registro completo más antiguo de ese día en la cadena activityDailyRecords. El valor máximo viene dado por la longitud de la cadena.

activityPointerNewestRecord es un elemento que señala el comienzo del espacio de almacenamiento (número de bytes a partir del principio de la cadena) que corresponde al registro más reciente de ese día en la cadena activityDailyRecords. El valor máximo viene dado por la longitud de la cadena.

activityDailyRecords es el espacio disponible para almacenar los datos sobre la actividad del conductor (estructura de datos: CardActivityDailyRecord) en cada uno de los días civiles en que se ha utilizado la tarjeta.

Asignación de valor: esta cadena de octetos se va llenando cíclicamente con registros del tipo CardActivityDailyRecord. En el primer uso, el almacenamiento comienza en el primer byte de la cadena. Cada nuevo registro se añade al final del anterior. Cuando la cadena está llena, el almacenamiento continúa en el primer byte de la cadena, con independencia de si hay alguna pausa dentro de un elemento de datos. Antes de introducir en la cadena nuevos datos de actividad (ampliando el actual activityDailyRecord, o introduciendo un nuevo activityDailyRecord) que sustituyan a datos antiguos, es preciso actualizar el activityPointerOldestDayRecord para reflejar la nueva ubicación del registro completo más antiguo de ese día, y además es preciso poner a 0 la longitud activityPreviousRecordLength de este (nuevo) registro completo más antiguo del día.

2.14. **CardDrivingLicenceInformation**

Información almacenada en una tarjeta de conductor y relativa a los datos correspondientes al permiso de conducir del titular de la tarjeta (requisito 196).

```
CardDrivingLicenceInformation ::= SEQUENCE {

   drivingLicenceIssuingAuthority           Name,

   drivingLicenceIssuingNation              NationNumeric,

   drivingLicenceNumber                     IA5String(SIZE(16))

}
```

drivingLicenceIssuingAuthority es la autoridad que expidió el permiso de conducir.

drivingLicenceIssuingNation es la nacionalidad de la autoridad que expidió el permiso de conducir.

drivingLicenceNumber es el número del permiso de conducir.

2.15. **CardEventData**

Información almacenada en una tarjeta de conductor o en una tarjeta del centro de ensayo y relativa a los incidentes asociados al titular de la tarjeta (requisitos 204 y 223).

```
CardEventData ::= SEQUENCE SIZE(6) OF {

   cardEventRecords SET                     SIZE(NoOfEventsPerType) OF
                                            CardEventRecord

}
```

CardEventData es una secuencia de cardEventRecords ordenada por valor ascendente del código EventFaultType (excepto los registros relacionados con intentos de violación de la seguridad, que se incluyen en el último conjunto de la secuencia).

cardEventRecords es un conjunto de registros de incidentes de un tipo en particular (o de una categoría en particular, en el caso de los intentos de violación de la seguridad).

2.16. **CardEventRecord**

Información almacenada en una tarjeta de conductor o en una tarjeta del centro de ensayo y relativa a un incidente asociado al titular de la tarjeta (requisitos 205 y 223).

```
CardEventRecord ::= SEQUENCE {

   eventType                                EventFaultType,

   eventBeginTime                           TimeReal,

   eventEndTime                             TimeReal,

   eventVehicleRegistration                 VehicleRegistrationIdentification

}
```

eventType es el tipo de incidente.

eventBeginTime es la fecha y la hora en que comenzó el incidente.

eventEndTime es la fecha y la hora en que terminó el incidente.

eventVehicleRegistration es el VRN y el nombre del Estado miembro donde se matriculó el vehículo en el que se produjo el incidente.

2.17. **CardFaultData**

Información almacenada en una tarjeta de conductor o en una tarjeta del centro de ensayo y relativa a los fallos asociados al titular de la tarjeta (requisitos 207 y 223).

```
CardFaultData ::= SEQUENCE SIZE(2) OF {
   cardFaultRecords                    SET SIZE(NoOfFaultsPerType) OF
                                       CardFaultRecord
}
```

CardFaultData es una secuencia integrada por un conjunto con los registros de los fallos del aparato de control, seguido de un conjunto con los registros de los fallos de la tarjeta.

cardFaultRecords es un conjunto de registros de fallos de una categoría determinada (del aparato de control o de la tarjeta).

2.18. **CardFaultRecord**

Información almacenada en una tarjeta de conductor o en una tarjeta del centro de ensayo y relativa a un fallo asociado al titular de la tarjeta (requisitos 208 y 223).

```
CardFaultRecord ::= SEQUENCE {
   faultType                           EventFaultType,
   faultBeginTime                      TimeReal,
   faultEndTime                        TimeReal,
   faultVehicleRegistration            VehicleRegistrationIdentification
}
```

faultType es el tipo de fallo.

faultBeginTime es la fecha y la hora de comienzo del fallo.

faultEndTime es la fecha y la hora en que termina el fallo.

faultVehicleRegistration es el VRN y el nombre del Estado miembro donde se matriculó el vehículo en el que ocurrió el fallo.

2.19. **CardIccIdentification**

Información almacenada en una tarjeta y relativa a la identificación de la tarjeta con circuito integrado (CI) (requisito 192).

```
CardIccIdentification ::= SEQUENCE {
   clockStop                           OCTET STRING (SIZE(1)),
   cardExtendedSerialNumber            ExtendedSerialNumber,
   cardApprovalNumber                  CardApprovalNumber
   cardPersonaliserID                  OCTET STRING (SIZE(1)),
   embedderIcAssemblerId               OCTET STRING (SIZE(5)),
   icIdentifier                        OCTET STRING (SIZE(2))
}
```

clockStop es el modo de paro de reloj, tal y como se define en la norma EN 726-3.

cardExtendedSerialNumber es el número de serie y la referencia de fabricación de la tarjeta CI, tal y como se definen en la norma EN 726-3. Esta información se completa con el tipo de datos ExtendedSerialNumber.

cardApprovalNumber es el número de homologación del modelo de tarjeta.

cardPersonaliserID es la identificación personal de la tarjeta, tal y como se define en la norma EN 726-3.

embedderIcAssemblerId es la identificación del fabricante de la tarjeta/encargado de integrar el CI, tal y como se define en la norma EN 726-3.

icIdentifier es el identificador del CI que incorpora la tarjeta y del fabricante de dicho CI, tal y como se define en la norma EN 726-3.

2.20. **CardIdentification**

Información almacenada en una tarjeta y relativa a la identificación de la tarjeta (requisitos 194, 215, 231, 235).

```
CardIdentification ::= SEQUENCE
   cardIssuingMemberState                  NationNumeric,
   cardNumber                              CardNumber,
   cardIssuingAuthorityName                Name,
   cardIssueDate                           TimeReal,
   cardValidityBegin                       TimeReal,
   cardExpiryDate                          TimeReal
}
```

cardIssuingMemberState es el código del Estado miembro que expide la tarjeta.

cardNumber es el número de la tarjeta.

cardIssuingAuthorityName es el nombre de la autoridad que ha expedido la tarjeta.

cardIssueDate es la fecha en que se expidió la tarjeta al titular actual.

cardValidityBegin es la fecha correspondiente al primer día de validez de la tarjeta.

cardExpiryDate es la fecha en que termina la validez de la tarjeta.

2.21. **CardNumber**

Un número de tarjeta, según se indica en la definición g).

```
CardNumber ::= CHOICE {
   SEQUENCE {
      driverIdentification                 IA5String(SIZE(14)),
      cardReplacementIndex                 CardReplacementIndex,
      cardRenewalIndex                     CardRenewalIndex
   }
   SEQUENCE {
      ownerIdentification                  IA5String(SIZE(13)),
      cardConsecutiveIndex                 CardConsecutiveIndex,
      cardReplacementIndex                 CardReplacementIndex,
      cardRenewalIndex                     CardRenewalIndex
   }
}
```

driverIdentification es la identificación exclusiva de un conductor en un Estado miembro.

ownerIdentification es la identificación exclusiva de una empresa, de un centro de ensayo o de un organismo de control en un Estado miembro.

cardConsecutiveIndex es el índice consecutivo de la tarjeta.

cardReplacementIndex es el índice de sustitución de la tarjeta.

cardRenewalIndex es el índice de renovación de la tarjeta.

La primera de las dos secuencias a elegir sirve para codificar el número de una tarjeta de conductor, mientras que la segunda secuencia sirve para codificar el número de una tarjeta de centro de ensayo, de una tarjeta de control y de una tarjeta de empresa.

2.22. **CardPlaceDailyWorkPeriod**

Información almacenada en una tarjeta de conductor o en una tarjeta del centro de ensayo y relativa a los lugares donde comienzan y/o terminan los períodos de trabajo diarios (requisitos 202 y 221).

```
CardPlaceDailyWorkPeriod ::= SEQUENCE {
   placePointerNewestRecord                INTEGER(0..NoOfCardPlaceRecords-1),
   placeRecords SET                        SIZE(NoOfCardPlaceRecords) OF PlaceRecord
}
```

placePointerNewestRecord es el índice del último registro actualizado de un lugar.

Asignación de valor: número que corresponde al numerador del registro de un lugar. Al primer registro de la estructura se le asigna el número '0'.

placeRecords es el conjunto de registros que contiene la información relativa a los lugares introducidos.

2.23. **CardPrivateKey**

La clave privada de una tarjeta.

```
CardPrivateKey ::= RSAKeyPrivateExponent
```

2.24. **CardPublicKey**

La clave pública de una tarjeta.

```
CardPublicKey ::= PublicKey
```

2.25. **CardRenewalIndex**

El índice de renovación de una tarjeta [definición i)].

```
CardRenewalIndex ::= IA5String(SIZE(1))
```

Asignación de valor: (véase el capítulo VII del presente anexo).

'0' Primera expedición.

Orden de incremento: '0, …, 9, A, …, Z'

2.26. **CardReplacementIndex**

El índice de sustitución de una tarjeta [definición j)].

```
CardReplacementIndex ::= IA5String(SIZE(1))
```

Asignación de valor: (véase el capítulo VII del presente anexo).

'0' Tarjeta original.

Orden de incremento: '0, …, 9, A, …, Z'

2.27. **CardSlotNumber**

Código para distinguir entre las dos ranuras de una unidad intravehicular.

```
CardSlotNumber ::= INTEGER {
   driverSlot                              (0),
   co-driverSlot                           (1)
}
```

Asignación de valor: no hay más especificaciones.

2.28. **CardSlotsStatus**

Código que indica el tipo de tarjetas insertadas en las dos ranuras de la unidad intravehicular.

```
CardSlotsStatus ::= OCTET STRING (SIZE(1))
```

Asignación de valor — Alineación de octeto: 'ccccdddd'B:

'cccc'B Identificación del tipo de tarjeta insertada en la ranura del segundo conductor,

'dddd'B Identificación del tipo de tarjeta insertada en la ranura del conductor,

con los siguientes códigos de identificación:

'0000'B no hay tarjeta insertada,

'0001'B se ha insertado una tarjeta de conductor,

'0010'B se ha insertado una tarjeta del centro de ensayo,

'0011'B se ha insertado una tarjeta de control,

'0100'B se ha insertado una tarjeta de empresa.

2.29. **CardStructureVersion**

Código que indica la versión de la estructura empleada en una tarjeta de tacógrafo.

```
CardStructureVersion ::= OCTET STRING (SIZE(2))
```

Asignación de valor: 'aabb'H:

'aa'H índice para cambios de la estructura,

'bb'H índice para cambios relativos al uso de los elementos de datos definidos para la estructura que viene dada por el byte alto.

2.30. **CardVehicleRecord**

Información almacenada en una tarjeta de conductor o en una tarjeta del centro de ensayo y relativa a un período de uso de un vehículo durante un día civil (requisitos 197 y 217).

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                    OdometerShort,
   vehicleOdometerEnd                      OdometerShort,
   vehicleFirstUse                         TimeReal,
   vehicleLastUse                          TimeReal,
   vehicleRegistration                     VehicleRegistrationIdentification,
   vuDataBlockCounter                      VuDataBlockCounter
}
```

vehicleOdometerBegin es la lectura del cuentakilómetros del vehículo al comenzar el período de uso del vehículo.

vehicleOdometerEnd es la lectura del cuentakilómetros del vehículo al terminar el período de uso del vehículo.

vehicleFirstUse es la fecha y la hora en que comienza el período de uso del vehículo.

vehicleLastUse es la fecha y la hora en que termina el período de uso del vehículo.

vehicleRegistration es el VRN y el Estado miembro donde se ha matriculado el vehículo.

vuDataBlockCounter es el valor del VuDataBlockCounter en el momento de extraer la tarjeta por última vez en el período de uso del vehículo.

2.31. **CardVehiclesUsed**

Información almacenada en una tarjeta de conductor o en una tarjeta del centro de ensayo y relativa a los vehículos utilizados por el titular de la tarjeta (requisitos 197 y 217).

```
CardVehiclesUsed := SEQUENCE {
   vehiclePointerNewestRecord              INTEGER(0..NoOfCardVehicleRecords-1),
   cardVehicleRecords                      SET SIZE(NoOfCardVehicleRecords) OF
                                           CardVehicleRecord
}
```

vehiclePointerNewestRecord es el índice del último registro actualizado de un vehículo.

Asignación de valor: número correspondiente al numerador del registro de un vehículo. Al primer registro de la estructura se le asigna el número '0'.

cardVehicleRecords es el conjunto de registros con información sobre los vehículos utilizados.

2.32. **Certificate**

El certificado de una clave pública expedido por una autoridad de certificación.

```
Certificate ::= OCTET STRING (SIZE(194))
```

Asignación de valor: firma digital con recuperación parcial del contenido del certificado, según lo dispuesto en el Apéndice 11 "Mecanismos de seguridad comunes": firma (128 bytes) || resto de la clave pública (58 bytes) || referencia a la autoridad de certificación (8 bytes).

2.33. **CertificateContent**

El contenido (sin cifrar) del certificado de una clave pública, según lo dispuesto en el Apéndice 11 "Mecanismos de seguridad comunes".

```
CertificateContent ::= SEQUENCE {
   certificateProfileIdentifier             INTEGER(0..255),
   certificationAuthorityReference          KeyIdentifier,
   certificateHolderAuthorisation           CertificateHolderAuthorisation,
   certificateEndOfValidity                 TimeReal,
   certificateHolderReference               KeyIdentifier,
   publicKey                                PublicKey
}
```

certificateProfileIdentifier es la versión del certificado que corresponda.

Asignación de valor: '01h' para esta versión.

CertificationAuthorityReference identifica a la autoridad de certificación que expide el certificado. También es una referencia a la clave pública de dicha autoridad de certificación.

certificateHolderAuthorisation identifica los derechos que asisten al titular del certificado.

certificateEndOfValidity es la fecha en que el certificado caduca administrativamente.

certificateHolderReference identifica al titular del certificado. También es una referencia a su clave pública.

publicKey es la clave pública que se certifica con este certificado.

2.34. **CertificateHolderAuthorisation**

Identificación de los derechos que asisten al titular de un certificado.

```
CertificateHolderAuthorisation ::= SEQUENCE {
   tachographApplicationID                  OCTET STRING(SIZE(6))
   equipmentType                            EquipmentType
}
```

tachographApplicationID es el identificador de la aplicación de tacógrafo.

Asignación de valor: 'FFh' '54h' '41h' '43h' '48h' '4Fh'. Este AID es un identificador propio y no registrado de la aplicación, con arreglo a la norma ISO/IEC 7816-5.

equipmentType es la identificación del tipo de equipo al que se refiere el certificado.

Asignación de valor: de acuerdo con el tipo de datos EquipmentType. 0 si el certificado es de un Estado miembro.

2.35. **CertificateRequestID**

Identificacion exclusiva de una solicitud de certificado. También puede utilizarse como identificador de la clave pública de una unidad intravehicular si en el momento de generar el certificado se desconoce el número de serie de la unidad intravehicular a la que se refiere la clave.

```
CertificateRequestID ::= SEQUENCE {
   requestSerialNumber                    INTEGER(0..2^32-1)
   requestMonthYear                       BCDString(SIZE(2))
   crIdentifier                           OCTET STRING(SIZE(1))
   manufacturerCode                       ManufacturerCode
}
```

requestSerialNumber es un número de serie para la solicitud de certificado, exclusivo para el fabricante y para el mes a que se refiere la línea siguiente.

requestMonthYear es la identificación del mes y el año de la solicitud de certificado.

Asignación de valor: codificación BCD del mes (dos dígitos) y el año (dos últimos dígitos).

crIdentifier: es un identificador para distinguir entre una solicitud de certificado y un número de serie ampliado.

Asignación de valor: 'FFh'.

manufacturerCode: es el código numérico del fabricante que solicita el certificado.

2.36. **CertificationAuthorityKID**

Identificador de la clave pública de una autoridad de certificación (un Estado miembro o la autoridad de certificación europea).

```
CertificationAuthorityKID ::= SEQUENCE {
   nationNumeric                          NationNumeric
   nationAlpha                            NationAlpha
   keySerialNumber                        INTEGER(0..255)
   additionalInfo OCTET STRING(SIZE(2))
   caIdentifier OCTET STRING(SIZE(1))
}
```

nationNumeric es el código numérico de nación de la autoridad de certificación.

nationAlpha es el código alfanumérico de nación de la autoridad de certificación.

keySerialNumber es un número de serie para distinguir las diferentes claves de la autoridad de certificación en caso de que éstas se cambien.

additionalInfo es un campo de dos bytes para codificación adicional (específica de la autoridad de certificación).

caIdentifier es un identificador para distinguir entre el identificador de clave de una autoridad de certificación y otros identificadores de clave.

Asignación de valor: '01h'.

2.37. **CompanyActivityData**

Información almacenada en una tarjeta de empresa y relativa a las actividades que se realizan con la tarjeta (requisito 237).

```
CompanyActivityData ::= SEQUENCE {
  companyPointerNewestRecord          INTEGER(0..NoOfCompanyActivityRecords-1),
  companyActivityRecords              SET SIZE(NoOfCompanyActivityRecords) OF
    companyActivityRecord               SEQUENCE {
      companyActivityType                 CompanyActivityType,
      companyActivityTime                 TimeReal,
      cardNumberInformation               FullCardNumber,
```

```
        vehicleRegistrationInformation      VehicleRegistrationIdentification,
        downloadPeriodBegin                 TimeReal,
        downloadPeriodEnd                   TimeReal
    }
}
```

companyPointerNewestRecord es el índice del último registro actualizado de una actividad de la empresa.

Asignación de valor: número correspondiente al numerador del registro de una actividad de la empresa. Al primer registro de la estructura se le asigna el número '0'.

companyActivityRecords es el conjunto de todos los registros de actividades de la empresa.

companyActivityRecord es la secuencia de información relativa a una actividad de la empresa.

companyActivityType es el tipo de actividad de la empresa.

companyActivityTime es la fecha y la hora de la actividad de la empresa.

cardNumberInformation es el número de tarjeta y el nombre del Estado miembro que ha expedido la tarjeta cuyos datos se han transferido, en tal caso.

vehicleRegistrationInformation es el VRN y el nombre del Estado miembro donde se ha matriculado el vehículo cuyos datos se han transferido o cuyo bloqueo se ha activado o desactivado.

downloadPeriodBegin y **downloadPeriodEnd** es el período transferido de la VU, en tal caso.

2.38. **CompanyActivityType**

Código que indica una actividad realizada por una empresa haciendo uso de su tarjeta de empresa.

```
CompanyActivityType ::= INTEGER {
    card downloading                    (1),
    VU downloading                      (2),
    VU lock-in                          (3),
    VU lock-out                         (4)
}
```

2.39. **CompanyCardApplicationIdentification**

Información almacenada en una tarjeta de empresa y relativa a la identificación de la aplicación de la tarjeta (requisito 190).

```
CompanyCardApplicationIdentification ::= SEQUENCE {
    typeOfTachographCardId              EquipmentType,
    cardStructureVersion                CardStructureVersion,
    noOfCompanyActivityRecords          NoOfCompanyActivityRecords
}
```

typeOfTachographCardId especifica el tipo de tarjeta utilizado.

cardStructureVersion especifica la versión de la estructura que se utiliza en la tarjeta.

noOfCompanyActivityRecords es el número de registros de actividades de la empresa que puede almacenar la tarjeta.

2.40. **CompanyCardHolderIdentification**

Información almacenada en una tarjeta de empresa y relativa a la identificación del titular de dicha tarjeta (requisito 236).

```
CompanyCardHolderIdentification ::= SEQUENCE {
    companyName                         Name,
    companyAddress                      Address,
    cardHolderPreferredLanguage         Language
}
```

companyName es el nombre de la empresa titular.

companyAddress es la dirección de la empresa titular.

cardHolderPreferredLanguage es el idioma preferido por el titular de la tarjeta.

2.41. **ControlCardApplicationIdentification**

Información almacenada en una tarjeta de control y relativa a la identificación de la aplicación de la tarjeta (requisito 190).

```
ControlCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId                  EquipmentType,
   cardStructureVersion                    CardStructureVersion,
   noOfControlActivityRecords              NoOfControlActivityRecords
}
```

typeOfTachographCardId especifica el tipo de tarjeta de que se trata.

cardStructureVersion especifica la versión de la estructura que se utiliza en la tarjeta.

noOfControlActivityRecords es el número de registros de actividades de control que puede almacenar la tarjeta.

2.42. **ControlCardControlActivityData**

Información almacenada en una tarjeta de control y relativa a las actividades de control realizadas con dicha tarjeta (requisito 233).

```
ControlCardControlActivityData ::= SEQUENCE {
   controlPointerNewestRecord              INTEGER(0..NoOfControlActivityRecords-1),
   controlActivityRecords                  SET SIZE(NoOfControlActivityRecords) OF
     controlActivityRecord                   SEQUENCE {
       controlType                             ControlType,
       controlTime                             TimeReal,
       controlledCardNumber                    FullCardNumber,
       controlledVehicleRegistration           VehicleRegistrationIdentification,
       controlDownloadPeriodBegin              TimeReal,
       controlDownloadPeriodEnd                TimeReal
     }
}
```

controlPointerNewestRecord es el índice del último registro actualizado de una actividad de control.

Asignación de valor: número correspondiente al numerador del registro de una actividad de control. Al primer registro de la estructura se le asigna el número '0'.

controlActivityRecords es el conjunto de todos los registros de actividades de control.

controlActivityRecord es la secuencia de información relativa a un control.

controlType es el tipo de control.

controlTime es la fecha y la hora del control.

controlledCardNumber es el número de tarjeta y el nombre del Estado miembro que ha expedido la tarjeta que es objeto del control.

controlledVehicleRegistration es el VRN y el nombre del Estado miembro donde se ha matriculado el vehículo en el que ocurrió el control.

controlDownloadPeriodBegin y **controlDownloadPeriodEnd** es el período cuyos datos se transfieren.

2.43. **ControlCardHolderIdentification**

Información almacenada en una tarjeta de control y relativa a la identificación del titular de dicha tarjeta (requisito 232).

```
ControlCardHolderIdentification ::= SEQUENCE {
   controlBodyName                          Name,
   controlBodyAddress                       Address,
   cardHolderName                           HolderName,
   cardHolderPreferredLanguage              Language
}
```

controlBodyName es el nombre del organismo de control que corresponde al titular de la tarjeta.

controlBodyAddress es la dirección del organismo de control que corresponde al titular de la tarjeta.

cardHolderName es el nombre y los apellidos del titular de la tarjeta de control.

cardHolderPreferredLanguage es el idioma preferido por el titular de la tarjeta.

2.44. **ControlType**

Código que indica las actividades realizadas durante un control. Este tipo de datos está relacionado con los requisitos 102, 210 y 225.

```
ControlType ::= OCTET STRING (SIZE(1))
```

Asignación de valor — Alineación de octeto: 'cvpdxxxx'B (8 bits)

'c'B transferencia de los datos de la tarjeta:

'0'B: datos de la tarjeta no transferidos durante esta actividad de control,

'1'B: datos de la tarjeta transferidos durante esta actividad de control

'v'B transferencia de los datos de la VU:

'0'B: datos de la VU no transferidos durante esta actividad de control,

'1'B: datos de la VU transferidos durante esta actividad de control

'p'B impresión:

'0'B: no se imprimen datos durante esta actividad de control,

'1'B: se imprimen datos durante esta actividad de control

'd'B visualización:

'0'B: no se visualizan datos durante esta actividad de control,

'1'B: se visualizan datos durante esta actividad de control

'xxxx'B No se utiliza.

2.45. **CurrentDateTime**

La fecha y la hora actuales del aparato de control.

```
CurrentDateTime ::= TimeReal
```

Asignación de valor: no hay más especificaciones.

2.46. **DailyPresenceCounter**

Contador que está almacenado en una tarjeta de conductor o en una tarjeta del centro de ensayo y que se incrementa en una unidad por cada día civil que se haya insertado la tarjeta en una VU. Este tipo de datos está relacionado con los requisitos 199 y 219.

```
DailyPresenceCounter ::= BCDString(SIZE(2))
```

Asignación de valor: número consecutivo con un valor máximo de 9999, y que vuelve a comenzar desde 0. La primera vez que se expide la tarjeta, el número se pone a 0.

2.47. **Datef**

Fecha expresada en un formato numérico fácil de imprimir.

```
Datef ::= SEQUENCE {
   year       BCDString(SIZE(2)),
   month      BCDString(SIZE(1)),
   day        BCDString(SIZE(1))
}
```

Asignación de valor:

yyyy	Año
mm	Mes
dd	Día

'00000000'H denota explícitamente la ausencia de fecha.

2.48. **Distance**

Una distancia recorrida (resultado de calcular la diferencia en kilómetros entre dos lecturas del cuentakilómetros del vehículo).

```
Distance ::= INTEGER(0..2^16-1)
```

Asignación de valor: número binario sin signo. Valor en km en el intervalo operativo de 0 a 9999 km.

2.49. **DriverCardApplicationIdentification**

Información almacenada en una tarjeta de conductor y relativa a la identificación de la aplicación de la tarjeta (requisito 190).

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId                  EquipmentType,
   cardStructureVersion                    CardStructureVersion,
   noOfEventsPerType                       NoOfEventsPerType,
   noOfFaultsPerType                       NoOfFaultsPerType,
   activityStructureLength                 CardActivityLengthRange,
   noOfCardVehicleRecords                  NoOfCardVehicleRecords,
   noOfCardPlaceRecords                    NoOfCardPlaceRecords
}
```

typeOfTachographCardId especifica el tipo de tarjeta utilizado.

cardStructureVersion especifica la versión de la estructura que se utiliza en la tarjeta.

noOfEventsPerType es el número de incidentes de cada tipo que puede registrar la tarjeta.

noOfFaultsPerType es el número de fallos de cada tipo que puede registrar la tarjeta.

activityStructureLength indica el número de bytes disponibles para almacenar registros de actividad.

noOfCardVehicleRecords es el número de registros del vehículo que caben en la tarjeta.

noOfCardPlaceRecords es el número de lugares que puede registrar la tarjeta.

2.50. **DriverCardHolderIdentification**

Información almacenada en una tarjeta de conductor y relativa a la identificación del titular de dicha tarjeta (requisito 195).

```
DriverCardHolderIdentification ::= SEQUENCE {
   cardHolderName                          HolderName,
   cardHolderBirthDate                     Datef,
   cardHolderPreferredLanguage             Language
}
```

cardHolderName es el nombre y los apellidos del titular de la tarjeta de conductor.

cardHolderBirthDate es la fecha de nacimiento del titular de la tarjeta de conductor.

cardHolderPreferredLanguage es el idioma preferido por el titular de la tarjeta.

2.51. **EntryTypeDailyWorkPeriod**

Código para distinguir entre el comienzo y el final cuando se introduce un período diario de trabajo, el lugar y la condición de la entrada.

```
EntryTypeDailyWorkPeriod ::= INTEGER
   Begin,  related time = card insertion time or time of entry          (0),
   End,    related time = card withdrawal time or time of entry        (1),
   Begin,  related time manually entered (start time)                   (2),
   End,    related time manually entered (end of work period)           (3),
   Begin,  related time assumed by VU                                   (4),
   End,    related time assumed by VU                                   (5)
}
```

Asignación de valor: con arreglo a la norma ISO/IEC8824-1.

2.52. **EquipmentType**

Código para distinguir diferentes tipos de equipos para la aplicación de tacógrafo.

```
EquipmentType ::= INTEGER(0..255)
- - Reserved                          (0),
- - Driver Card                       (1),
- - Workshop Card                     (2),
- - Control Card                      (3),
- - Company Card                      (4),
- - Manufacturing Card                (5),
- - Vehicle Unit                      (6),
- - Motion Sensor                     (7),
- - RFU                               (8..255)
```

Asignación de valor: con arreglo a la norma ISO/IEC8824-1.

El valor 0 se reserva para designar a un Estado miembro o a Europa en el campo CHA de los certificados.

2.53. **EuropeanPublicKey**

La clave pública europea.

```
EuropeanPublicKey ::= PublicKey
```

2.54. **EventFaultType**

Código que califica un incidente o un fallo.

```
EventFaultType ::= OCTET STRING (SIZE(1))
```

Asignación de valor:

'0x'H	Incidentes de carácter general,
'00'H	No hay más información,
'01'H	Inserción de una tarjeta no válida,
'02'H	Conflicto de tarjetas,
'03'H	Solapamiento temporal,
'04'H	Conducción sin tarjeta adecuada,
'05'H	Inserción de tarjeta durante la conducción,
'06'H	Error al cerrar la última sesión de la tarjeta,
'07'H	Exceso de velocidad,

'08'H	Interrupción del suministro eléctrico,
'09'H	Error en datos de movimiento,
'0A'H .. '0F'H	RFU,
'1x'H	Intentos de violación de la seguridad relacionados con la unidad intravehicular,
'10'H	No hay más información,
'11'H	Fallo de autentificación del sensor de movimiento,
'12'H	Fallo de autentificación de la tarjeta de tacógrafo,
'13'H	Cambio no autorizado del sensor de movimiento,
'14'H	Error de integridad en la entrada de los datos de la tarjeta
'15'H	Error de integridad en los datos de usuario almacenados,
'16'H	Error en una transferencia interna de datos,
'17'H	Apertura no autorizada de la carcasa,
'18'H	Sabotaje del hardware,
'19'H .. '1F'H	RFU,
'2x'H	Intentos de violación de la seguridad relacionados con el sensor,
'20'H	No hay más información,
'21'H	Fallo de autentificación,
'22'H	Error de integridad en los datos almacenados,
'23'H	Error en una transferencia interna de datos,
'24'H	Apertura no autorizada de la carcasa,
'25'H	Sabotaje del hardware,
'26'H .. '2F'H	RFU,
'3x'H	Fallos del aparato de control,
'30'H	No hay más información,
'31'H	Fallo interno de la VU,
'32'H	Fallo de la impresora,
'33'H	Fallo de la pantalla,
'34'H	Fallo de transferencia,
'35'H	Fallo del sensor,
'36'H .. '3F'H	RFU,
'4x'H	Fallos de las tarjetas,
'40'H	No hay más información,
'41'H .. '4F'H	RFU,
'50'H .. '7F'H	RFU,
'80'H .. 'FF'H	Específicos del fabricante.

2.55. **EventFaultRecordPurpose**

Código que explica por qué se ha registrado un incidente o fallo.

```
EventFaultRecordPurpose ::= OCTET STRING (SIZE(1))
```

Asignación de valor:

'00'H	uno de los 10 incidentes o fallos más recientes (o de los 10 últimos)
'01'H	el incidente de más duración ocurrido en uno de los 10 últimos días en que se hayan producido incidentes de este tipo
'02'H	uno de los 5 incidentes de más duración ocurridos en los últimos 365 días
'03'H	el último incidente ocurrido en uno de los 10 últimos días en que se hayan producido incidentes de este tipo
'04'H	el incidente más grave en uno de los últimos días en que se hayan producido incidentes de este tipo
'05'H	uno de los 5 incidentes más graves ocurridos en los últimos 365 días
'06'H	el primer incidente o fallo ocurrido tras el último calibrado
'07'H	un incidente o fallo activo/en curso
'08'H .. '7F'H	RFU
'80'H .. 'FF'H	específicos del fabricante

2.56. **ExtendedSerialNumber**

Identificación exclusiva de un equipo. También puede utilizarse como el identificador de clave pública de un equipo.

```
ExtendedSerialNumber ::= SEQUENCE {
   serialNumber                          INTEGER(0..2^32-1)
   monthYear                             BCDString(SIZE(2))
   type OCTET                            STRING(SIZE(1))
   manufacturerCode                      ManufacturerCode
}
```

serialNumber es el número de serie de un equipo; exclusivo para el fabricante, para el tipo de equipo y para el mes a que se refiere la línea siguiente.

monthYear es la identificación del mes y el año de fabricación (o de la asignación del número de serie).

Asignación de valor: codificación BCD del mes (dos dígitos) y el año (dos últimos dígitos).

type es un identificador del tipo de equipo.

Asignación de valor: específica del fabricante, con 'FFh' valor reservado.

manufacturerCode es el código numérico del fabricante del equipo.

2.57. **FullCardNumber**

Código que identifica por completo a una tarjeta de tacógrafo.

```
FullCardNumber ::= SEQUENCE {
   cardType                              EquipmentType,
   cardIssuingMemberState                NationNumeric,
   cardNumber                            CardNumber
}
```

cardType es el tipo de tarjeta de tacógrafo.

cardIssuingMemberState es el código del Estado miembro que ha expedido la tarjeta.

cardNumber es el número de la tarjeta.

2.58. **HighResOdometer**

Lectura del cuentakilómetros del vehículo: distancia acumulada que ha recorrido el vehículo durante su funcionamiento.

```
HighResOdometer ::= INTEGER(0..2^32-1)
```

Asignación de valor: número binario sin signo. Valor en 1/200 km en el intervalo operativo de 0 a 21 055 406 km.

2.59. **HighResTripDistance**

La distancia recorrida durante todo o parte de un viaje.

```
HighResTripDistance ::= INTEGER(0..2^32-1)
```

Asignación de valor: número binario sin signo. Valor en 1/200 km en el intervalo operativo de 0 a 21 055 406 km.

2.60. **HolderName**

El nombre y apellidos del titular de una tarjeta.

```
HolderName ::= SEQUENCE {
   holderSurname                         Name,
   holderFirstNames                      Name
}
```

holderSurname son los apellidos del titular, sin incluir sus títulos.

Asignación de valor: cuando una tarjeta no es personal, holderSurname contiene la misma información que companyName o workshopName o controlBodyName.

holderFirstNames es el nombre y las iniciales del titular.

2.61. **K-ConstantOfRecordingEquipment**

Constante del aparato de control [definición m)].

```
K-ConstantOfRecordingEquipment ::= INTEGER(0..2^16-1)
```

Asignación de valor: impulsos por kilómetro en el intervalo operativo de 0 a 64 255 impulsos/km.

2.62. **KeyIdentifier**

Un identificador exclusivo de una clave pública, empleado para hacer referencia a dicha clave y seleccionarla. También identifica al titular de la clave.

```
KeyIdentifier ::= CHOICE {

   extendedSerialNumber                    ExtendedSerialNumber,

   certificateRequestID                    CertificateRequestID,

   certificationAuthorityKID               CertificationAuthorityKID

}
```

La primera opción sirve para hacer referencia a la clave pública de una unidad intravehicular o de una tarjeta de tacógrafo.

La segunda opción sirve para hacer referencia a la clave pública de una unidad intravehicular (en caso de que el número de serie de dicha unidad intravehicular no pueda conocerse en el momento de generarse el certificado).

La tercera opción sirve para hacer referencia a la clave pública de un Estado miembro.

2.63. **L-TyreCircumference**

Circunferencia efectiva de los neumáticos de las ruedas [definición u)].

```
L-TyreCircumference ::= INTEGER(0..2^16-1)
```

Asignación de valor: número binario sin signo, valor en 1/8 mm en el intervalo operativo de 0 a 8 031 mm.

2.64. **Language**

Código que identifica un idioma.

```
Language ::= IA5String(SIZE(2))
```

Asignación de valor: codificación mediante dos letras en minúsculas con arreglo a la norma ISO 639.

2.65. **LastCardDownload**

Fecha y hora, almacenadas en la tarjeta del conductor, de la última transferencia de los datos de la tarjeta (para fines distintos de los de control). Esta fecha puede ser actualizada por una VU o por cualquier lector de tarjetas.

```
LastCardDownload ::= TimeReal
```

Asignación de valor: no hay más especificaciones.

2.66. **ManualInputFlag**

Código que identifica si el titular de una tarjeta, en el momento de insertar dicha tarjeta, ha introducido o no manualmente alguna actividad del conductor (requisito 081).

```
ManualInputFlag ::= INTEGER {
   noEntry                          (0)
   manualEntries                    (1)
}
```

Asignación de valor: no hay más especificaciones.

2.67. **ManufacturerCode**

Código que identifica a un fabricante.

```
ManufacturerCode ::= INTEGER(0..255)
```

Asignación de valor:

'00'H	No hay información disponible
'01'H	Valor reservado
'02'H .. '0F'H	Reservado para uso futuro
'10'H	ACTIA
'11'H .. '17'H	Reservado para fabricantes cuyo nombre comience por 'A'
'18'H .. '1F'H	Reservado para fabricantes cuyo nombre comience por 'B'
'20'H .. '27'H	Reservado para fabricantes cuyo nombre comience por 'C'
'28'H .. '2F'H	Reservado para fabricantes cuyo nombre comience por 'D'
'30'H .. '37'H	Reservado para fabricantes cuyo nombre comience por 'E'
'38'H .. '3F'H	Reservado para fabricantes cuyo nombre comience por 'F'
'40'H	Giesecke & Devrient GmbH
'41'H	GEM plus
'42'H .. '47'H	Reservado para fabricantes cuyo nombre comience por 'G'
'48'H .. '4F'H	Reservado para fabricantes cuyo nombre comience por 'H'
'50'H .. '57'H	Reservado para fabricantes cuyo nombre comience por 'I'
'58'H .. '5F'H	Reservado para fabricantes cuyo nombre comience por 'J'
'60'H .. '67'H	Reservado para fabricantes cuyo nombre comience por 'K'
'68'H .. '6F'H	Reservado para fabricantes cuyo nombre comience por 'L'
'70'H .. '77'H	Reservado para fabricantes cuyo nombre comience por 'M'
'78'H .. '7F'H	Reservado para fabricantes cuyo nombre comience por 'N'
'80'H	OSCARD
'81'H .. '87'H	Reservado para fabricantes cuyo nombre comience por 'O'
'88'H .. '8F'H	Reservado para fabricantes cuyo nombre comience por 'P'
'90'H .. '97'H	Reservado para fabricantes cuyo nombre comience por 'Q'
'98'H .. '9F'H	Reservado para fabricantes cuyo nombre comience por 'R'
'A0'H	SETEC
'A1'H	SIEMENS VDO
'A2'H	STONERIDGE
'A3'H .. 'A7'H	Reservado para fabricantes cuyo nombre comience por 'S'
'AA'H	TACHOCONTROL
'AB'H .. 'AF'H	Reservado para fabricantes cuyo nombre comience por 'T'
'B0'H .. 'B7'H	Reservado para fabricantes cuyo nombre comience por 'U'
'B8'H .. 'BF'H	Reservado para fabricantes cuyo nombre comience por 'V'
'C0'H .. 'C7'H	Reservado para fabricantes cuyo nombre comience por 'W'
'C8'H .. 'CF'H	Reservado para fabricantes cuyo nombre comience por 'X'
'D0'H .. 'D7'H	Reservado para fabricantes cuyo nombre comience por 'Y'
'D8'H .. 'DF'H	Reservado para fabricantes cuyo nombre comience por 'Z'

2.68. **MemberStateCertificate**

El certificado de la clave pública de un Estado miembro, expedido por la autoridad de certificación europea.

```
MemberStateCertificate ::= Certificate
```

2.69. **MemberStatePublicKey**

La clave pública de un Estado miembro.

```
MemberStatePublicKey ::= PublicKey
```

2.70. **Name**

Un nombre.

```
Name ::= SEQUENCE {
   codePage                                    INTEGER (0..255),
   name                                        OCTET STRING (SIZE(35))
}
```

codePage especifica la parte de la norma ISO/IEC 8859 que se utiliza para codificar el nombre,

name es un nombre codificado con arreglo a la norma ISO/IEC 8859-codePage.

2.71. **NationAlpha**

Referencia alfabética a un país, con arreglo a la codificación convencional de países que se utiliza en los adhesivos de parachoques y/o en los documentos de seguro armonizados internacionalmente (tarjeta verde).

```
NationAlpha ::= IA5String(SIZE(3))
```

Asignación de valor:

' '	No hay información disponible
'A'	Austria,
'AL'	Albania,
'AND'	Andorra,
'ARM'	Armenia,
'AZ'	Azerbaiyán,
'B'	Bélgica,
'BG'	Bulgaria,
'BIH'	Bosnia y Hercegovina,
'BY'	Bielorrusia,
'CH'	Suiza,
'CY'	Chipre,
'CZ'	República Checa,
'D'	Alemania,
'DK'	Dinamarca,
'E'	España,
'EST'	Estonia,
'F'	Francia,
'FIN'	Finlandia,
'FL'	Liechtenstein,
'FR'	Islas Feroe,
'UK'	Reino Unido, Alderney, Guernsey, Jersey, Isla de Man, Gibraltar,
'GE'	Georgia,
'GR'	Grecia,
'H'	Hungría,
'HR'	Croacia,
'I'	Italia,
'IRL'	Irlanda,
'IS'	Islandia,
'KZ'	Kazajistán,
'L'	Luxemburgo,
'LT'	Lituania,
'LV'	Letonia,
'M'	Malta,
'MC'	Mónaco,

'MD' República de Moldavia,
'MK' Macedonia,
'N' Noruega,
'NL' Países Bajos,
'P' Portugal,
'PL' Polonia,
'RO' Rumania,
'RSM' San Marino,
'RUS' Federación Rusa,
'S' Suecia,
'SK' Eslovaquia,
'SLO' Eslovenia,
'TM' Turkmenistán,
'TR' Turquía,
'UA' Ucrania,
'V' Vaticano,
'YU' Yugoslavia,
'UNK' Desconocido,
'EC' Comunidad Europea,
'EUR' Resto de Europa,
'WLD' Resto del mundo.

2.72. **NationNumeric**

Referencia numérica a un país.

```
NationNumeric ::= INTEGER(0..255)
```

Asignación de valor:

-- No hay información disponible (00)H,
-- Austria (01)H,
-- Albania (02)H,
-- Andorra (03)H,
-- Armenia (04)H,
-- Azerbaiyán (05)H,
-- Bélgica (06)H,
-- Bulgaria (07)H,
-- Bosnia y Hercegovina (08)H,
-- Bielorrusia (09)H,
-- Suiza (0A)H,
-- Chipre (0B)H,
-- República Checa (0C)H,
-- Alemania (0D)H,
-- Dinamarca (0E)H,
-- España (0F)H,
-- Estonia (10)H,
-- Francia (11)H,
-- Finlandia (12)H,
-- Liechtenstein (13)H,
-- Islas Feroe (14)H,
-- Reino Unido (15)H,
-- Georgia (16)H,
-- Grecia (17)H,
-- Hungría (18)H,
-- Croacia (19)H,
-- Italia (1A)H,
-- Irlanda (1B)H,
-- Islandia (1C)H,

- - Kazajistán	(1D)H,
- - Luxemburgo	(1E)H,
- - Lituania	(1F)H,
- - Letonia	(20)H,
- - Malta	(21)H,
- - Mónaco	(22)H,
- - República de Moldavia	(23)H,
- - Macedonia	(24)H,
- - Noruega	(25)H,
- - Países Bajos	(26)H,
- - Portugal	(27)H,
- - Polonia	(28)H,
- - Rumania	(29)H,
- - San Marino	(2A)H,
- - Federación Rusa	(2B)H,
- - Suecia	(2C)H,
- - Eslovaquia	(2D)H,
- - Eslovenia	(2E)H,
- - Turkmenistán	(2F)H,
- - Turquía	(30)H,
- - Ucrania	(31)H,
- - Vaticano	(32)H,
- - Yugoslavia	(33)H,
- - RFU	(34..FC)H,
- - Comunidad Europea	(FD)H,
- - Resto de Europa	(FE)H,
- - Resto del mundo	(FF)H

2.73. **NoOfCalibrationRecords**

Número de registros de calibrado que puede almacenar una tarjeta del centro de ensayo.

NoOfCalibrationRecords ::= INTEGER(0..255)

Asignación de valor: véase el apartado 3.

2.74. **NoOfCalibrationsSinceDownload**

Contador que indica el número de calibrados realizados con una tarjeta del centro de ensayo desde que se transfirieran por última vez sus datos (requisito 230).

NoOfCalibrationsSinceDownload ::= INTEGER(0..2^{16}-1),

Asignación de valor: no hay más especificaciones.

2.75. **NoOfCardPlaceRecords**

Número de registros de lugares que puede almacenar una tarjeta de conductor o una tarjeta del centro de ensayo.

NoOfCardPlaceRecords ::= INTEGER(0..255)

Asignación de valor: véase el apartado 3.

2.76. **NoOfCardVehicleRecords**

Número de registros sobre vehículos usados que puede almacenar una tarjeta de conductor o una tarjeta del centro de ensayo.

NoOfCardVehicleRecords ::= INTEGER(0..2^{16}-1)

Asignación de valor: véase el apartado 3.

2.77. **NoOfCompanyActivityRecords**

Número de registros sobre actividades de empresa que puede almacenar una tarjeta de empresa.

NoOfCompanyActivityRecords ::= INTEGER(0..2^{16}-1)

Asignación de valor: véase el apartado 3.

2.78. **NoOfControlActivityRecords**

Número de registros sobre actividades de control que puede almacenar una tarjeta de control.

```
NoOfControlActivityRecords ::= INTEGER(0..2^16-1)
```

Asignación de valor: véase el apartado 3.

2.79. **NoOfEventsPerType**

Número de incidentes de cada tipo que puede almacenar una tarjeta.

```
NoOfEventsPerType ::= INTEGER(0..255)
```

Asignación de valor: véase el apartado 3.

2.80. **NoOfFaultsPerType**

Número de fallos de cada tipo que puede almacenar una tarjeta.

```
NoOfFaultsPerType ::= INTEGER(0..255)
```

Asignación de valor: véase el apartado 3.

2.81. **OdometerValueMidnight**

La lectura del cuentakilómetros del vehículo a medianoche de un día determinado (requisito 090).

```
OdometerValueMidnight ::= OdometerShort
```

Asignación de valor: no hay más especificaciones.

2.82. **OdometerShort**

Lectura del cuentakilómetros del vehículo en forma abreviada.

```
OdometerShort ::= INTEGER(0..2^24-1)
```

Asignación de valor: número binario sin signo. Valor en km en el intervalo operativo de 0 a 9 999 999 km.

2.83. **OverspeedNumber**

Número de incidentes de exceso de velocidad ocurridos desde el último control del exceso de velocidad.

```
OverspeedNumber ::= INTEGER(0..255)
```

Asignación de valor: 0 significa que no se ha producido ningún incidente de exceso de velocidad desde el último control, 1 significa que se ha producido un incidente de exceso de velocidad desde el último control … 255 significa que se han producido 255 o más incidentes de exceso de velocidad desde el último control.

2.84. **PlaceRecord**

Información relativa al lugar donde comienza o termina un período de trabajo diario (requisitos 087, 202, 221).

```
PlaceRecord ::= SEQUENCE {
   entryTime                          TimeReal,
   entryTypeDailyWorkPeriod           EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry             NationNumeric,
   dailyWorkPeriodRegion              RegionNumeric,
   vehicleOdometerValue               OdometerShort
}
```

entryTime es una fecha y una hora relacionadas con la entrada.

entryTypeDailyWorkPeriod es el tipo de entrada.

dailyWorkPeriodCountry es el país introducido.

dailyWorkPeriodRegion es la región introducida

vehicleOdometerValue es la lectura del cuentakilómetros en el momento de introducir el lugar.

2.85. **PreviousVehicleInfo**

Información relativa al vehículo que utilizara previamente un conductor, cuando inserta su tarjeta en una unidad intra-vehicular (requisito 081).

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification        VehicleRegistrationIdentification,
   cardWithdrawalTime                       TimeReal
}
```

vehicleRegistrationIdentification es el VRN y el nombre del Estado miembro donde se matriculara el vehículo.

cardWithdrawalTime es la fecha y la hora de extracción de la tarjeta.

2.86. **PublicKey**

Una clave RSA pública.

```
PublicKey ::= SEQUENCE {
   rsaKeyModulus                            RSAKeyModulus,
   rsaKeyPublicExponent                     RSAKeyPublicExponent
}
```

rsaKeyModulus es el módulo del par de claves.

rsaKeyPublicExponent es el exponente público del par de claves.

2.87. **RegionAlpha**

Referencia alfabética a una región perteneciente a un país especificado.

```
RegionAlpha ::= IA5STRING(SIZE(3))
```

Asignación de valor:

' '	No hay información disponible,
España:	
'AN'	Andalucía,
'AR'	Aragón,
'AST'	Asturias,
'C'	Cantabria,
'CAT'	Cataluña,
'CL'	Castilla-León,
'CM'	Castilla-La-Mancha,
'CV'	Valencia,
'EXT'	Extremadura,
'G'	Galicia,
'IB'	Baleares,
'IC'	Canarias,
'LR'	La Rioja,
'M'	Madrid,
'MU'	Murcia,
'NA'	Navarra,
'PV'	País Vasco

2.88. **RegionNumeric**

Referencia numérica a una región perteneciente a un país especificado.

```
RegionNumeric ::= OCTET STRING (SIZE(1))
```

Asignación de valor:

'00'H	No hay información disponible,

España:

'01'H	Andalucía,
'02'H	Aragón,
'03'H	Asturias,
'04'H	Cantabria,
'05'H	Cataluña,
'06'H	Castilla-León,
'07'H	Castilla-La-Mancha,
'08'H	Valencia,
'09'H	Extremadura,
'0A'H	Galicia,
'0B'H	Baleares,
'0C'H	Canarias,
'0D'H	La Rioja,
'0E'H	Madrid,
'0F'H	Murcia,
'10'H	Navarra,
'11'H	País Vasco

2.89. **RSAKeyModulus**

El módulo de un par de claves RSA.

```
RSAKeyModulus ::= OCTET STRING (SIZE(128))
```

Asignación de valor: sin especificar.

2.90. **RSAKeyPrivateExponent**

El exponente privado de un par de claves RSA.

```
RSAKeyPrivateExponent ::= OCTET STRING (SIZE(128))
```

Asignación de valor: sin especificar.

2.91. **RSAKeyPublicExponent**

El exponente público de un par de claves RSA.

```
RSAKeyPublicExponent ::= OCTET STRING (SIZE(8))
```

Asignación de valor: sin especificar.

2.92. **SensorApprovalNumber**

Número de homologación del sensor.

```
SensorApprovalNumber ::= IA5String(SIZE(8))
```

Asignación de valor: sin especificar.

2.93. **SensorIdentification**

Información almacenada en un sensor de movimiento y relativa a la identificación de dicho sensor (requisito 077).

```
SensorIdentification ::= SEQUENCE {
   sensorSerialNumber                    SensorSerialNumber,
   sensorApprovalNumber                  SensorApprovalNumber,
   sensorSCIdentifier                    SensorSCIdentifier,
   sensorOSIdentifier                    SensorOSIdentifier
}
```

sensorSerialNumber es el número de serie ampliado del sensor de movimiento (incluye el número de pieza y el código del fabricante).

sensorApprovalNumber es el número de homologación del sensor de movimiento.

sensorSCIdentifier es el identificador del componente de seguridad del sensor de movimiento.

sensorOSIdentifier es el identificador del sistema operativo del sensor de movimiento.

2.94. **SensorInstallation**

Información almacenada en un sensor de movimiento y relativa a la instalación de dicho sensor (requisito 099).

```
SensorInstallation ::= SEQUENCE {
   sensorPairingDateFirst                  SensorPairingDate,
   firstVuApprovalNumber                   VuApprovalNumber,
   firstVuSerialNumber                     VuSerialNumber,
   sensorPairingDateCurrent                SensorPairingDate,
   currentVuApprovalNumber                 VuApprovalNumber,
   currentVUSerialNumber                   VuSerialNumber
}
```

sensorPairingDateFirst es la fecha del primer acoplamiento del sensor de movimiento con una unidad intravehicular.

firstVuApprovalNumber es el número de homologación de la primera unidad intravehicular acoplada con el sensor de movimiento.

firstVuSerialNumber es el número de serie de la primera unidad intravehicular acoplada con el sensor de movimiento.

sensorPairingDateCurrent es la fecha del acoplamiento actual entre el sensor de movimiento y la unidad intravehicular.

currentVuApprovalNumber es el número de homologación de la unidad intravehicular que está acoplada actualmente con el sensor de movimiento.

currentVUSerialNumber es el número de serie de la unidad intravehicular que está acoplada actualmente con el sensor de movimiento.

2.95. **SensorInstallationSecData**

Información almacenada en una tarjeta del centro de ensayo y relativa a los datos de seguridad necesarios para acoplar sensores de movimiento a unidades intravehiculares (requisito 214).

```
SensorInstallationSecData ::= TDesSessionKey
```

Asignación de valor: con arreglo a la norma ISO 16844-3.

2.96. **SensorOSIdentifier**

Identificador del sistema operativo del sensor de movimiento.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Asignación de valor: específica del fabricante.

2.97. **SensorPaired**

Información almacenada en una unidad intravehicular y relativa a la identificación del sensor de movimiento acoplado a la unidad intravehicular (requisito 079).

```
SensorPaired ::= SEQUENCE {
   sensorSerialNumber                      SensorSerialNumber,
   sensorApprovalNumber                    SensorApprovalNumber,
   sensorPairingDateFirst                  SensorPairingDate
}
```

sensorSerialNumber es el número de serie del sensor de movimiento que está acoplado actualmente a la unidad intravehicular.

sensorApprovalNumber es el número de homologación del sensor de movimiento que está acoplado actualmente a la unidad intravehicular.

sensorPairingDateFirst es la fecha en que el sensor de movimiento acoplado actualmente a la unidad intravehicular se acopló por primera vez a una unidad intravehicular.

2.98. **SensorPairingDate**

Fecha de un acoplamiento entre el sensor de movimiento y la unidad intravehicular.

```
SensorPairingDate ::= TimeReal
```

Asignación de valor: sin especificar.

2.99. **SensorSerialNumber**

Número de serie del sensor de movimiento.

```
SensorSerialNumber ::= ExtendedSerialNumber
```

2.100. **SensorSCIdentifier**

Identificador del componente de seguridad del sensor de movimiento.

```
SensorSCIdentifier ::= IA5String(SIZE(8))
```

Asignación de valor: específica del fabricante del componente.

2.101. **Signature**

Una firma digital.

```
Signature ::= OCTET STRING (SIZE(128))
```

Asignación de valor: con arreglo a lo dispuesto en el Apéndice 11 (Mecanismos de seguridad comunes).

2.102. **SimilarEventsNumber**

El número de incidentes similares ocurridos en un día determinado (requisito 094).

```
SimilarEventsNumber ::= INTEGER(0..255)
```

Asignación de valor: el 0 no se utiliza, el 1 significa que ese día sólo ha ocurrido y se ha almacenado un incidente de ese tipo, el 2 significa que ese día han ocurrido 2 incidentes de ese tipo (y sólo se ha almacenado uno), … 255 significa que ese día han ocurrido 255 o más incidentes de ese tipo.

2.103. **SpecificConditionType**

Código que identifica una condición específica (requisitos 050b, 105a, 212a y 230a).

```
SpecificConditionType ::= INTEGER(0..255)
```

Asignación de valor:

'00'H	RFU
'01'H	Fuera de ámbito — Comienzo
'02'H	Fuera de ámbito — Final
'03'H	Puente/Paso a nivel
'04'H .. 'FF'H	RFU

2.104. **SpecificConditionRecord**

Información almacenada en una tarjeta de conductor, una tarjeta del centro de ensayo o una unidad intravehicular y relativa a una condición específica (requisitos 105a, 212a y 230a).

```
SpecificConditionRecord ::= SEQUENCE {
   entryTime                                TimeReal,
   specificConditionType                    SpecificConditionType
}
```

entryTime es la fecha y la hora de la entrada.

specificConditionType es el código que identifica a la condición específica.

2.105. **Speed**

Velocidad del vehículo (km/h).

```
Speed ::= INTEGER(0..255)
```

Asignación de valor: kilómetros por hora en el intervalo operativo de 0 a 220 km/h.

2.106. **SpeedAuthorised**

Velocidad máxima autorizada para el vehículo [definición bb)].

```
SpeedAuthorised ::= Speed
```

2.107. **SpeedAverage**

Velocidad media en un lapso de tiempo previamente definido (km/h).

```
SpeedAverage ::= Speed
```

2.108. **SpeedMax**

Velocidad máxima medida en un lapso de tiempo previamente definido.

```
SpeedMax ::= Speed
```

2.109. **TDesSessionKey**

Una clave de sesión triple DES.

```
TDesSessionKey ::= SEQUENCE {
   tDesKeyA                                 OCTET STRING (SIZE(8))
   tDesKeyB                                 OCTET STRING (SIZE(8))
}
```

Asignación de valor: no hay más especificaciones.

2.110. **TimeReal**

Código para un campo combinado de fecha y hora, donde ambos parámetros se expresan como los segundos transcurridos desde las 00h.00m.00s. del 1 de enero de 1970, tiempo medio de Greenwich.

```
TimeReal{INTEGER:TimeRealRange} ::= INTEGER(0..TimeRealRange)
```

Asignación de valor — Alineación de octeto: número de segundos transcurridos a partir de la medianoche del día 1 de enero de 1970, tiempo medio de Greenwich.

La fecha/hora máxima posible es en el año 2106.

2.111. **TyreSize**

Designación de las dimensiones de los neumáticos.

```
TyreSize ::= IA5String(SIZE(15))
```

Asignación de valor: con arreglo a la Directiva 92/23CEE.

2.112. **VehicleIdentificationNumber**

Número de identificación del vehículo (VIN) referido al vehículo completo, generalmente el número de serie del chasis o el número de bastidor.

```
VehicleIdentificationNumber ::= IA5String(SIZE(17))
```

Asignación de valor: tal y como se define en la norma ISO 3779.

2.113. **VehicleRegistrationIdentification**

Identificación de un vehículo, exclusiva para Europa (VRN y Estado miembro).

```
VehicleRegistrationIdentification ::= SEQUENCE {
   vehicleRegistrationNation                NationNumeric,
   vehicleRegistrationNumber                VehicleRegistrationNumber
}
```

vehicleRegistrationNation es la nación donde se matriculó el vehículo.

vehicleRegistrationNumber es el número de matrícula del vehículo (VRN).

2.114. **VehicleRegistrationNumber**

Número de matrícula del vehículo (VRN). El número de matrícula lo asigna la autoridad de matriculación de vehículos.

```
VehicleRegistrationNumber ::= SEQUENCE {
   codePage                                 INTEGER (0..255),
   vehicleRegNumber                         OCTET STRING (SIZE(13))
}
```

codePage especifica la parte de la norma ISO/IEC 8859 que se utiliza para codificar el vehicleRegNumber.

vehicleRegNumber es un VRN codificado con arreglo a la norma ISO/IEC 8859-codePage.

Asignación de valor: específica de cada país.

2.115. **VuActivityDailyData**

Información almacenada en una VU y relativa a los cambios de actividad y/o los cambios del régimen de conducción y/o los cambios del estado de la tarjeta que tengan lugar en un día civil determinado (requisito 084) y a los estados de las ranuras a las 00.00 de ese día.

```
VuActivityDailyData ::= SEQUENCE {
   noOfActivityChanges                      INTEGER SIZE(0..1440),
   activityChangeInfos                      SET SIZE(noOfActivityChanges) OF
                                            ActivityChangeInfo
}
```

noOfActivityChanges es el número de palabras que hay en el conjunto activityChangeInfos.

activityChangeInfos es un conjunto de palabras que se almacenan en la VU a lo largo del día y contiene información sobre los cambios de actividad realizados ese día. Siempre incluye dos palabras de activityChangeInfo que dan el estado de las dos ranuras a las 00.00 de ese día.

2.116. **VuApprovalNumber**

Número de homologación de la unidad intravehicular.

```
VuApprovalNumber ::= IA5String(SIZE(8))
```

Asignación de valor: sin especificar.

2.117. **VuCalibrationData**

Información almacenada en una unidad intravehicular y relativa a los calibrados del aparato de control (requisito 098).

```
VuCalibrationData ::= SEQUENCE {
   noOfVuCalibrationRecords                 INTEGER(0..255),
   vuCalibrationRecords SET                 SIZE(noOfVuCalibrationRecords) OF
                                            VuCalibrationRecord
}
```

noOfVuCalibrationRecords es el número de registros que hay en el conjunto vuCalibrationRecords.

vuCalibrationRecords es el conjunto de registros de calibrado.

2.118. **VuCalibrationRecord**

Información almacenada en una unidad intravehicular y relativa a un calibrado del aparato de control (requisito 098).

```
VuCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                    CalibrationPurpose,
   workshopName                          Name,
   workshopAddress Address,
   workshopCardNumber                    FullCardNumber,
   workshopCardExpiryDate                TimeReal,
   vehicleIdentificationNumber           VehicleIdentificationNumber,
   vehicleRegistrationIdentification     VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant        W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment         K-ConstantOfRecordingEquipment,
   lTyreCircumference                    L-TyreCircumference,
   tyreSize                              TyreSize,
   authorisedSpeed                       SpeedAuthorised,
   oldOdometerValue                      OdometerShort,
   newOdometerValue                      OdometerShort,
   oldTimeValue                          TimeReal,
   newTimeValue                          TimeReal,
   nextCalibrationDate                   TimeReal
}
```

calibrationPurpose es el propósito del calibrado.

workshopName, workshopAddress son el nombre y la dirección del centro de ensayo.

workshopCardNumber identifica la tarjeta del centro de ensayo empleada durante el calibrado.

workshopCardExpiryDate es la fecha de caducidad de la tarjeta.

vehicleIdentificationNumber es el VIN.

vehicleRegistrationIdentification contiene el VRN y el nombre del Estado miembro donde se matriculó el vehículo.

wVehicleCharacteristicConstant es el coeficiente característico del vehículo.

kConstantOfRecordingEquipment es la constante del aparato de control.

lTyreCircumference es la circunferencia efectiva de los neumáticos de las ruedas.

tyreSize son las dimensiones de las ruedas montadas en el vehículo.

authorisedSpeed es la velocidad autorizada del vehículo.

oldOdometerValue, newOdometerValue son la lectura anterior y la nueva lectura del cuentakilómetros.

oldTimeValue, newTimeValue son el valor anterior y el nuevo valor de la fecha y la hora.

nextCalibrationDate es la fecha del próximo calibrado del tipo especificado en CalibrationPurpose, a cargo de una autoridad de inspección autorizada.

2.119. **VuCardIWData**

Información almacenada en una unidad intravehicular y relativa a los ciclos de inserción y extracción de tarjetas de conductor o tarjetas del centro de ensayo en la unidad intravehicular (requisito 081).

```
VuCardIWData ::= SEQUENCE {
   noOfIWRecords                         INTEGER(0..216-1),
   vuCardIWRecords SET                   SIZE(noOfIWRecords) OF
                                         VuCardIWRecord
}
```

noOfIWRecords es el número de registros que hay en el conjunto vuCardIWRecords.

vuCardIWRecords es el conjunto de registros relativos a los ciclos de inserción y extracción de la tarjeta.

2.120. **VuCardIWRecord**

Información almacenada en una unidad intravehicular y relativa a un ciclo de inserción y extracción de una tarjeta de conductor o de una tarjeta del centro de ensayo en la unidad intravehicular (requisito 081).

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                          HolderName,
   fullCardNumber                          FullCardNumber,
   cardExpiryDate                          TimeReal,
   cardInsertionTime                       TimeReal,
   vehicleOdometerValueAtInsertion         OdometerShort,
   cardSlotNumber                          CardSlotNumber,
   cardWithdrawalTime                      TimeReal,
   vehicleOdometerValueAtWithdrawal        OdometerShort,
   previousVehicleInfo                     PreviousVehicleInfo
   manualInputFlag                         ManualInputFlag
}
```

cardHolderName es el nombre y los apellidos del titular de la tarjeta de conductor o de la tarjeta del centro de ensayo, según los datos almacenados en la propia tarjeta.

fullCardNumber es el tipo de tarjeta, el nombre del Estado miembro que la expidió y el número de tarjeta, según los datos almacenados en la propia tarjeta.

cardExpiryDate es la fecha de caducidad de la tarjeta, según los datos almacenados en la propia tarjeta.

cardInsertionTime es la fecha y la hora de inserción.

vehicleOdometerValueAtInsertion es la lectura del cuentakilómetros del vehículo en el momento de insertar la tarjeta.

cardSlotNumber es la ranura donde se inserta la tarjeta.

cardWithdrawalTime es la fecha y la hora de extracción.

vehicleOdometerValueAtWithdrawal es la lectura del cuentakilómetros del vehículo en el momento de extraer la tarjeta.

previousVehicleInfo contiene información sobre el vehículo anterior que utilizara el conductor, según los datos almacenados en la tarjeta.

manualInputFlag es una bandera que indica si el titular de la tarjeta ha introducido manualmente alguna actividad del conductor en el momento de insertar la tarjeta.

2.121. **VuCertificate**

Certificado de la clave pública de una unidad intravehicular.

```
VuCertificate ::= Certificate
```

2.122. **VuCompanyLocksData**

Información almacenada en una unidad intravehicular y relativa a bloqueos introducidos por empresas (requisito 104).

```
VuCompanyLocksData ::= SEQUENCE {
   noOfLocks                               INTEGER(0..20),
   vuCompanyLocksRecords                   SET SIZE(noOfLocks) OF
                                           VuCompanyLocksRecord
}
```

noOfLocks es el número de bloqueos incluidos en el conjunto vuCompanyLocksRecords.

vuCompanyLocksRecords es el conjunto de registros de bloqueos introducidos por empresas.

2.123. **VuCompanyLocksRecord**

Información almacenada en una unidad intravehicular y relativa a un bloqueo introducido por una empresa (requisito 104).

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                          TimeReal,
   lockOutTime                         TimeReal,
   companyName                         Name,
   companyAddress                      Address,
   companyCardNumber                   FullCardNumber
}
```

lockInTime, lockOutTime son la fecha y la hora de activación y desactivación del bloqueo.

companyName, companyAddress son el nombre y la dirección de la empresa relacionada con la activación del bloqueo.

companyCardNumber identifica la tarjeta empleada para la activación del bloqueo.

2.124. **VuControlActivityData**

Información almacenada en una unidad intravehicular y relativa a los controles efectuados con dicha VU (requisito 102).

```
VuControlActivityData ::= SEQUENCE {
   noOfControls                        INTEGER(0..20),
   vuControlActivityRecords            SET SIZE(noOfControls) OF
                                       VuControlActivityRecord
}
```

noOfControls es el número de controles incluidos en el conjunto vuControlActivityRecords.

vuControlActivityRecords es el conjunto de registros sobre actividades de control.

2.125. **VuControlActivityRecord**

Información almacenada en una unidad intravehicular y relativa a un control efectuado con dicha VU (requisito 102).

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                         ControlType,
   controlTime                         TimeReal,
   controlCardNumber                   FullCardNumber,
   downloadPeriodBeginTime             TimeReal,
   downloadPeriodEndTime               TimeReal
}
```

controlType es el tipo de control.

controlTime es la fecha y la hora del control.

ControlCardNumber identifica la tarjeta de control empleada para el control.

downloadPeriodBeginTime es la hora de comienzo del período cuyos datos se transfieren, en caso de transferencia.

downloadPeriodEndTime es la hora de conclusión del período cuyos datos se transfieren, en caso de transferencia.

2.126. **VuDataBlockCounter**

Contador, almacenado en una tarjeta, que identifica secuencialmente los ciclos de inserción/extracción de la tarjeta en unidades intravehiculares.

```
VuDataBlockCounter ::= BCDString(SIZE(2))
```

Asignación de valor: número consecutivo con un valor máximo de 9 999, y que vuelve a comenzar desde 0.

2.127. **VuDetailedSpeedBlock**

Información pormenorizada almacenada en una unidad intravehicular y relativa a la velocidad del vehículo durante un minuto que haya estado en movimiento (requisito 093).

```
VuDetailedSpeedBlock ::= SEQUENCE {
   speedBlockBeginDate                    TimeReal,
   speedsPerSecond                        SEQUENCE SIZE(60) OF Speed
}
```

speedBlockBeginDate es la fecha y la hora del primer valor de velocidad comprendido en ese bloque.

speedsPerSecond es la secuencia cronológica de las velocidades medidas cada segundo de ese minuto, empezando desde speedBlockBeginDate (inclusive).

2.128. **VuDetailedSpeedData**

Información pormenorizada almacenada en una unidad intravehicular y relativa a la velocidad del vehículo.

```
VuDetailedSpeedData ::= SEQUENCE
   noOfSpeedBlocks                        INTEGER(0.2^16-1),
   vuDetailedSpeedBlocks                  SET SIZE(noOfSpeedBlocks) OF
                                          VuDetailedSpeedBlock
}
```

noOfSpeedBlocks es el número de bloques con datos de velocidad que hay en el conjunto vuDetailedSpeedBlocks.

vuDetailedSpeedBlocks es el conjunto de bloques con datos pormenorizados sobre la velocidad.

2.129. **VuDownloadablePeriod**

La fecha más antigua y la más reciente para las que una unidad intravehicular conserva datos relativos a las actividades de los conductores (requisitos 081, 084 o 087).

```
VuDownloadablePeriod ::= SEQUENCE {
   minDownloadableTime                    TimeReal
   maxDownloadableTime                    TimeReal
}
```

minDownloadableTime es la fecha y la hora más antiguas en que se insertó una tarjeta, ocurrió un cambio de actividad o se introdujo un lugar; según los datos almacenados en la VU.

maxDownloadableTime es la fecha y la hora más recientes en que se insertó una tarjeta, ocurrió un cambio de actividad o se introdujo un lugar; según los datos almacenados en la VU.

2.130. **VuDownloadActivityData**

Información almacenada en una unidad intravehicular y relativa a la última transferencia de sus datos (requisito 105).

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                        TimeReal,
   fullCardNumber                         FullCardNumber,
   companyOrWorkshopName                  Name
}
```

downloadingTime es la fecha y la hora de la transferencia.

fullCardNumber identifica la tarjeta empleada para autorizar la transferencia.

companyOrWorkshopName es el nombre de la empresa o del centro de ensayo.

2.131. **VuEventData**

Información almacenada en una unidad intravehicular y relativa a incidentes (requisito 094, salvo el incidente de exceso de velocidad).

```
VuEventData ::= SEQUENCE {
   noOfVuEvents                           INTEGER(0..255),
   vuEventRecords                         SET SIZE(noOfVuEvents) OF VuEventRecord
}
```

noOfVuEvents es el número de incidentes incluidos en el conjunto vuEventRecords.

vuEventRecords es un conjunto de registros sobre incidentes.

2.132. **VuEventRecord**

Información almacenada en una unidad intravehicular y relativa a un incidente (requisito 094, salvo el incidente de exceso de velocidad).

```
VuEventRecord ::= SEQUENCE {
   eventType                              EventFaultType,
   eventRecordPurpose                     EventFaultRecordPurpose,
   eventBeginTime                         TimeReal,
   eventEndTime                           TimeReal,
   cardNumberDriverSlotBegin              FullCardNumber,
   cardNumberCodriverSlotBegin            FullCardNumber,
   cardNumberDriverSlotEnd                FullCardNumber,
   cardNumberCodriverSlotEnd              FullCardNumber,
   similarEventsNumber                    SimilarEventsNumber
}
```

eventType es el tipo de incidente.

eventRecordPurpose es el propósito con que se ha registrado ese incidente.

eventBeginTime es la fecha y la hora de comienzo del incidente.

eventEndTime es la fecha y la hora en que termina el incidente.

cardNumberDriverSlotBegin identifica la tarjeta que estaba insertada en la ranura del conductor en el momento en que comenzó el incidente.

cardNumberCodriverSlotBegin identifica la tarjeta que estaba insertada en la ranura del segundo conductor en el momento en que comenzó el incidente.

cardNumberDriverSlotEnd identifica la tarjeta que estaba insertada en la ranura del conductor en el momento en que finalizó el incidente.

cardNumberCodriverSlotEnd identifica la tarjeta que estaba insertada en la ranura del segundo conductor en el momento en que finalizó el incidente.

similarEventsNumber es el número de incidentes similares ocuridos ese día.

Esta secuencia puede utilizarse para todos los incidentes, excepto los de exceso de velocidad.

2.133. **VuFaultData**

Información almacenada en una unidad intravehicular y relativa a los fallos (requisito 096).

```
VuFaultData ::= SEQUENCE {
noOfVuFaults                            INTEGER(0..255),
vuFaultRecords SET                      SIZE(noOfVuFaults) OF VuFaultRecord
}
```

noOfVuFaults es el número de fallos incluidos en el conjunto vuFaultRecords.

vuFaultRecords es un conjunto de registros sobre fallos.

2.134. **VuFaultRecord**

Información almacenada en una unidad intravehicular y relativa a un fallo (requisito 096).

```
VuFaultRecord ::= SEQUENCE {
   faultType                              EventFaultType,
   faultRecordPurpose                     EventFaultRecordPurpose,
   faultBeginTime                         TimeReal,
   faultEndTime                           TimeReal,
   cardNumberDriverSlotBegin              FullCardNumber,
   cardNumberCodriverSlotBegin            FullCardNumber,
   cardNumberDriverSlotEnd                FullCardNumber,
   cardNumberCodriverSlotEnd              FullCardNumber
}
```

faultType es el tipo de fallo del aparato de control.

faultRecordPurpose es el propósito con que se ha registrado ese fallo.

faultBeginTime es la fecha y la hora de comienzo del fallo.

faultEndTime es la fecha y la hora en que termina el fallo.

cardNumberDriverSlotBegin identifica la tarjeta que estaba insertada en la ranura del conductor en el momento en que comenzó el fallo.

cardNumberCodriverSlotBegin identifica la tarjeta que estaba insertada en la ranura del segundo conductor en el momento en que comenzó el fallo.

cardNumberDriverSlotEnd identifica la tarjeta que estaba insertada en la ranura del conductor en el momento en que terminó el fallo.

cardNumberCodriverSlotEnd identifica la tarjeta que estaba insertada en la ranura del segundo conductor en el momento en que terminó el fallo.

2.135. **VuIdentification**

Información almacenada en una unidad intravehicular y relativa a la identificación de dicha unidad intravehicular (requisito 075).

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                  VuManufacturerName,
   vuManufacturerAddress               VuManufacturerAddress,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   vuSoftwareIdentification            VuSoftwareIdentification,
   vuManufacturingDate                 VuManufacturingDate,
   vuApprovalNumber                    VuApprovalNumber
}
```

vuManufacturerName es el nombre del fabricante de la unidad intravehicular.

vuManufacturerAddress es la dirección del fabricante de la unidad intravehicular.

vuPartNumber es el número de pieza de la unidad intravehicular.

vuSerialNumber es el número de serie de la unidad intravehicular.

vuSoftwareIdentification identifica el software instalado en la unidad intravehicular.

vuManufacturingDate es la fecha de fabricación de la unidad intravehicular.

vuApprovalNumber es el número de homologación de la unidad intravehicular.

2.136. **VuManufacturerAddress**

Dirección del fabricante de la unidad intravehicular.

```
VuManufacturerAddress ::= Address
```

Asignación de valor: sin especificar.

2.137. **VuManufacturerName**

Nombre del fabricante de la unidad intravehicular.

```
VuManufacturerName ::= Name
```

Asignación de valor: sin especificar.

2.138. **VuManufacturingDate**

Fecha de fabricación de la unidad intravehicular.

```
VuManufacturingDate ::= TimeReal
```

Asignación de valor: sin especificar.

2.139. **VuOverSpeedingControlData**

Información almacenada en una unidad intravehicular y relativa a incidentes de exceso de velocidad ocurridos desde el último control del exceso de velocidad (requisito 095).

```
VuOverSpeedingControlData ::= SEQUENCE {
   lastOverspeedControlTime                TimeReal,
   firstOverspeedSince                     TimeReal,
   numberOfOverspeedSince                  OverspeedNumber
}
```

lastOverspeedControlTime es la fecha y la hora del último control del exceso de velocidad.

firstOverspeedSince es la fecha y la hora del primer exceso de velocidad ocurrido tras este control.

numberOfOverspeedSince es el número de incidentes de exceso de velocidad ocurridos después del último control del exceso de velocidad.

2.140. **VuOverSpeedingEventData**

Información almacenada en una unidad intravehicular y relativa a incidentes de exceso de velocidad (requisito 094).

```
VuOverSpeedingEventData ::= SEQUENCE {
   noOfVuOverSpeedingEvents                INTEGER(0..255),
   vuOverSpeedingEventRecords              SET SIZE(noOfVuOverSpeedingEvents) OF
                                           VuOverSpeedingEventRecord
}
```

noOfVuOverSpeedingEvents es el número de incidentes incluidos en el conjunto vuOverSpeedingEventRecords.

vuOverSpeedingEventRecords es el conjunto de registros sobre incidentes de exceso de velocidad.

2.141. **VuOverSpeedingEventRecord**

Información almacenada en una unidad intravehicular y relativa a incidentes de exceso de velocidad (requisito 094).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                               EventFaultType,
   eventRecordPurpose                      EventFaultRecordPurpose,
   eventBeginTime                          TimeReal,
   eventEndTime                            TimeReal,
   maxSpeedValue                           SpeedMax,
   averageSpeedValue                       SpeedAverage,
   cardNumberDriverSlotBegin               FullCardNumber,
   similarEventsNumber                     SimilarEventsNumber
}
```

eventType es el tipo de incidente.

eventRecordPurpose es el propósito con que se ha registrado ese incidente.

eventBeginTime es la fecha y la hora de comienzo del incidente.

eventEndTime es la fecha y la hora en que termina el incidente.

maxSpeedValue es la velocidad máxima medida durante el incidente.

averageSpeedValue es la media aritmética de las velocidades medidas durante el incidente.

cardNumberDriverSlotBegin identifica la tarjeta que estaba insertada en la ranura del conductor en el momento en que comenzó el incidente.

similarEventsNumber es el número de incidentes similares ocurridos ese día.

2.142. **VuPartNumber**

Número de pieza de la unidad intravehicular.

```
VuPartNumber ::= IA5String(SIZE(16))
```

Asignación de valor: específica del fabricante de la VU.

2.143. **VuPlaceDailyWorkPeriodData**

Información almacenada en una unidad intravehicular y relativa a los lugares donde los conductores comienzan o terminan los períodos de trabajo diarios (requisito 087).

```
VuPlaceDailyWorkPeriodData ::= SEQUENCE {

   noOfPlaceRecords                          INTEGER(0..255),

   vuPlaceDailyWorkPeriodRecords             SET SIZE(noOfPlaceRecords) OF
                                             VuPlaceDailyWorkPeriodRecord

}
```

noOfPlaceRecords es el número de registros incluidos en el conjunto vuPlaceDailyWorkPeriodRecords.

vuPlaceDailyWorkPeriodRecords es el conjunto de registros relativos a lugares.

2.144. **VuPlaceDailyWorkPeriodRecord**

Información almacenada en una unidad intravehicular y relativa a un lugar donde un conductor comienza o termina un período de trabajo diario (requisito 087).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {

   fullCardNumber                            FullCardNumber,

   placeRecord                               PlaceRecord

}
```

fullCardNumber es el tipo de tarjeta del conductor, el Estado miembro que la ha expedido y el número de tarjeta.

placeRecord contiene la información relativa al lugar introducido.

2.145. **VuPrivateKey**

La clave privada de una unidad intravehicular.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.146. **VuPublicKey**

La clave pública de una unidad intravehicular.

```
VuPublicKey ::= PublicKey
```

2.147. **VuSerialNumber**

Número de serie de la unidad intravehicular (requisito 075).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.148. **VuSoftInstallationDate**

Fecha de instalación de la versión de software que lleva instalada la unidad intravehicular.

```
VuSoftInstallationDate ::= TimeReal
```

Asignación de valor: sin especificar.

2.149. **VuSoftwareIdentification**

Información almacenada en una unidad intravehicular y relativa al software instalado.

```
VuSoftwareIdentification ::= SEQUENCE {

   vuSoftwareVersion                         VuSoftwareVersion,

   vuSoftInstallationDate                    VuSoftInstallationDate

}
```

vuSoftwareVersion es el número de la versión de software que lleva instalado la unidad intravehicular.

vuSoftInstallationDate es la fecha de instalación de la versión de software.

2.150. **VuSoftwareVersion**

Número de la versión de software que lleva instalado la unidad intravehicular.

```
VuSoftwareVersion ::= IA5String(SIZE(4))
```

Asignación de valor: sin especificar.

2.151. **VuSpecificConditionData**

Información almacenada en una unidad intravehicular y relativa a condiciones específicas.

```
VuSpecificConditionData ::= SEQUENCE {
   noOfSpecificConditionRecords              INTEGER(0..2^16-1)
   specificConditionRecords                  SET SIZE (noOfSpecificConditionRecords) OF
                                             SpecificConditionRecord
}
```

noOfSpecificConditionRecords es el número de registros incluidos en el conjunto specificConditionRecords set.

specificConditionRecords es el conjunto de registros relativos a condiciones específicas.

2.152. **VuTimeAdjustmentData**

Información almacenada en una unidad intravehicular y relativa a los ajustes de hora que se han efectuado fuera del marco de un calibrado regular (requisito 101).

```
VuTimeAdjustmentData ::= SEQUENCE {
   noOfVuTimeAdjRecords                      INTEGER(0..6),
   vuTimeAdjustmentRecords                   SET SIZE(noOfVuTimeAdjRecords) OF
                                             VuTimeAdjustmentRecord
}
```

noOfVuTimeAdjRecords es el número de registros que hay en el conjunto vuTimeAdjustmentRecords.

vuTimeAdjustmentRecords es el conjunto de registros sobre ajustes de la hora.

2.153. **VuTimeAdjustmentRecord**

Información almacenada en una unidad intravehicular y relativa a un ajuste de la hora efectuado fuera del marco de un calibrado regular (requisito 101).

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                              TimeReal,
   oldTimeValue                              TimeReal,
   newTimeValue                              TimeReal,
   workshopName                              Name,
   workshopAddress                           Address,
   workshopCardNumber                        FullCardNumber
}
```

oldTimeValue, newTimeValue son el valor anterior y el nuevo valor de la fecha y la hora.

workshopName, workshopAddress son el nombre y la dirección del centro de ensayo.

workshopCardNumber identifica la tarjeta del centro de ensayo empleada para realizar el ajuste de la hora.

2.154. **W-VehicleCharacteristicConstant**

Coeficiente característico del vehículo [definición k)].

```
W-VehicleCharacteristicConstant ::= INTEGER(0..2^16-1))
```

Asignación de valor: impulsos por kilómetro en el intervalo operativo de 0 a 64 255 impulsos/km.

2.155. **WorkshopCardApplicationIdentification**

Información almacenada en una tarjeta del centro de ensayo y relativa a la identificación de la aplicación de dicha tarjeta (requisito 190).

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId                  EquipmentType,
   cardStructureVersion                    CardStructureVersion,
   noOfEventsPerType                       NoOfEventsPerType,
   noOfFaultsPerType                       NoOfFaultsPerType,
   activityStructureLength                 CardActivityLengthRange,
   noOfCardVehicleRecords                  NoOfCardVehicleRecords,
   noOfCardPlaceRecords                    NoOfCardPlaceRecords,
   noOfCalibrationRecords                  NoOfCalibrationRecords
}
```

typeOfTachographCardId especifica el tipo de tarjeta utilizado.

cardStructureVersion especifica la versión de la estructura que se utiliza en la tarjeta.

noOfEventsPerType es el número de incidentes de cada tipo que puede registrar la tarjeta.

noOfFaultsPerType es el número de fallos de cada tipo que puede registrar la tarjeta.

activityStructureLength indica el número de bytes disponibles para almacenar registros de actividad.

noOfCardVehicleRecords es el número de registros del vehículo que caben en la tarjeta.

noOfCardPlaceRecords es el número de lugares que puede registrar la tarjeta.

noOfCalibrationRecords es el número de registros de calibrado que puede almacenar la tarjeta.

2.156. **WorkshopCardCalibrationData**

Información almacenada en una tarjeta del centro de ensayo y relativa a las actividades del centro de ensayo realizadas con dicha tarjeta (requisitos 227 y 229).

```
WorkshopCardCalibrationData ::= SEQUENCE {
   calibrationTotalNumber                  INTEGER(0..2^16-1),
   calibrationPointerNewestRecord          INTEGER(0..NoOfCalibrationRecords-1),
   calibrationRecords                      SET SIZE(NoOfCalibrationRecords) OF
                                           WorkshopCardCalibrationRecord
}
```

calibrationTotalNumber es el número total de calibrados realizados con la tarjeta.

calibrationPointerNewestRecord es el índice del último registro actualizado de calibrado.

Asignación de valor: número correspondiente al numerador del registro de calibrado. Al primer registro de la estructura se le asigna el número '0'.

calibrationRecords es el conjunto de registros que contienen información sobre calibrados y/o ajustes de hora.

2.157. **WorkshopCardCalibrationRecord**

Información almacenada en una tarjeta del centro de ensayo y relativa a un calibrado realizado con dicha tarjeta (requisito 227).

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                      CalibrationPurpose,
   vehicleIdentificationNumber             VehicleIdentificationNumber,
   vehicleRegistration                     VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant          W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment           K-ConstantOfRecordingEquipment,
   lTyreCircumference                      L-TyreCircumference,
   tyreSize                                TyreSize,
```

```
   authorisedSpeed                    SpeedAuthorised,
   oldOdometerValue                   OdometerShort,
   newOdometerValue                   OdometerShort,
   oldTimeValue                       TimeReal,
   newTimeValue                       TimeReal,
   nextCalibrationDate                TimeReal,
   vuPartNumber                       VuPartNumber,
   vuSerialNumber                     VuSerialNumber,
   sensorSerialNumber                 SensorSerialNumber
}
```

calibrationPurpose es el propósito del calibrado.

vehicleIdentificationNumber es el VIN.

vehicleRegistration contiene el VRN y el nombre del Estado miembro donde se matriculó el vehículo.

wVehicleCharacteristicConstant es el coeficiente característico del vehículo.

kConstantOfRecordingEquipment es la constante del aparato de control.

lTyreCircumference es la circunferencia efectiva de los neumáticos de las ruedas.

tyreSize son las dimensiones de los neumáticos montados en el vehículo.

authorisedSpeed es la velocidad máxima autorizada del vehículo.

oldOdometerValue, newOdometerValue son la lectura anterior y la nueva lectura del cuentakilómetros.

oldTimeValue, newTimeValue son el valor anterior y el nuevo valor de la fecha y la hora.

nextCalibrationDate es la fecha del próximo calibrado del tipo especificado en CalibrationPurpose, a cargo de una autoridad de inspección autorizada.

vuPartNumber, vuSerialNumber y **sensorSerialNumber** son los elementos de datos para la identificación del aparato de control.

2.158. **WorkshopCardHolderIdentification**

Información almacenada en una tarjeta del centro de ensayo y relativa a la identificación del titular de dicha tarjeta (requisito 216).

```
WorkshopCardHolderIdentification ::= SEQUENCE {
   workshopName                       Name,
   workshopAddress                    Address,
   cardHolderName                     HolderName,
   cardHolderPreferredLanguage        Language
}
```

workshopName es el nombre del centro de ensayo que corresponde al titular de la tarjeta.

workshopAddress es la dirección del centro de ensayo que corresponde al titular de la tarjeta.

cardHolderName es el nombre y los apellidos del titular (por ejemplo, el nombre del mecánico).

cardHolderPreferredLanguage es el idioma preferido por el titular de la tarjeta.

2.159. **WorkshopCardPIN**

Número de identificación personal de la tarjeta del centro de ensayo (requisito 213).

```
WorkshopCardPIN ::= IA5String(SIZE(8))
```

Asignación de valor: el PIN que conoce el titular de la tarjeta, rellenado por la derecha con bytes 'FF' hasta llegar a 8 bytes.

3. DEFINICIONES DE LOS INTERVALOS DE VALORES Y TAMAÑOS ADMISIBLES

Definición de valores variables empleados en las definiciones del apartado 2.

`TimeRealRange ::= 2^32-1`

3.1. **Definiciones para la tarjeta del conductor:**

Nombre del valor variable	Mín.	Máx.
`CardActivityLengthRange`	5 544 bytes (28 días, 93 cambios de actividad cada día)	13 776 bytes (28 días, 240 cambios de actividad cada día)
`NoOfCardPlaceRecords`	84	112
`NoOfCardVehicleRecords`	84	200
`NoOfEventsPerType`	6	12
`NoOfFaultsPerType`	12	24

3.2. **Definiciones para la tarjeta del centro de ensayo:**

Nombre del valor variable	Mín.	Máx.
`CardActivityLengthRange`	198 bytes (1 día, 93 cambios de actividad)	492 bytes (1 día, 240 cambios de actividad)
`NoOfCardPlaceRecords`	6	8
`NoOfCardVehicleRecords`	4	8
`NoOfEventsPerType`	3	3
`NoOfFaultsPerType`	6	6
`NoOfCalibrationRecords`	88	255

3.3. **Definiciones para la tarjeta de control:**

Nombre del valor variable	Mín.	Máx.
`NoOfControlActivityRecords`	230	520

3.4. **Definiciones para la tarjeta de empresa:**

Nombre del valor variable	Mín.	Máx.
`NoOfCompanyActivityRecords`	230	520

4. CONJUNTOS DE CARACTERES

Las cadenas IA5 utilizan los caracteres ASCII que se definen en la norma ISO/IEC 8824-1. Para facilitar la lectura y las referencias, a continuación se ofrece la asignación de valores. La norma ISO/IEC 8824-1 prevalece sobre esta nota informativa en caso de discrepancia.

```
! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ?
@ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [ \ ] ^ _
` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~
```

Otras cadenas de caracteres (Address, Name, VehicleRegistrationNumber) uutilizan además los caracteres definidos en los códigos 192 a 255 de la norma ISO/IEC 8859-1 (conjunto de caracteres Latín1) o de la norma ISO/IEC 8859-7 (conjunto de caracteres griegos):

5. CODIFICACIÓN

Si se aplican las reglas de codificación NSA.1, todos los tipos de datos definidos deberán codificarse con arreglo a la norma ISO/IEC 8825-2, variante alineada.

Apéndice 2

ESPECIFICACIONES DE LAS TARJETAS DE TACÓGRAFO

ÍNDICE

1. INTRODUCCIÓN

1.1. **Siglas**

A efectos del presente apéndice se utilizan las siguientes siglas:

AC	Condiciones de acceso
AID	Identificador de aplicación
ALW	Siempre
APDU	Unidad de datos de protocolo de una aplicación (estructura de un comando)
ATR	Respuesta a reinicio
AUT	Autentificado
C6, C7	Contactos nº 6 y 7 de la tarjeta, tal y como se describen en la norma ISO/CEI 7816-2
cc	Ciclos de reloj
CHV	Información para la verificación del titular de la tarjeta
CLA	Byte de clase de un comando APDU
DF	Archivo dedicado. Un DF puede contener otros archivos (EF o DF)
EF	Archivo elemental
ENC	Cifrado: el acceso sólo es posible mediante la codificación de datos
etu	Unidad de tiempo elemental
IC	Circuito integrado
ICC	Tarjeta de circuito integrado
ID	Identificador
IFD	Dispositivo de interfaz
IFS	Tamaño del campo de información
IFSC	Tamaño del campo de información para la tarjeta
IFSD	Dispositivo de tamaño del campo de información (para el terminal)
INS	Byte de instrucción de un comando APDU
Lc	Longitud de los datos de entrada para un comando APDU
Le	Longitud de los datos esperados (datos de salida para un comando)
MF	Archivo principal (DF raíz)
P1-P2	Bytes de parámetros
NAD	Dirección de nodo empleada en el protocolo T=1
NEV	Nunca
PIN	Número de identificación personal
PRO SM	Protegido con mensajería segura
PTS	Selección de la transmisión de protocolo
RFU	Reservado para uso futuro

RST	Reinicio (de la tarjeta)
SM	Mensajería segura
SW1-SW2	Bytes de estado
TS	Carácter ATR inicial
VPP	Tensión de programación
XXh	Valor XX en notación hexadecimal
||	Símbolo de concatenación 03||04=0304

1.2. **Referencias**

En el presente apéndice aparecen las siguientes referencias:

EN 726-3	Sistemas de tarjetas de identificación — Tarjetas con circuito(s) integrados y terminales para telecomunicaciones — Parte 3: Requisitos de la tarjeta independientes de las aplicaciones. Diciembre 1994.
ISO/CEI 7816-2	Tecnología de la información — Tarjetas de identificación — Tarjetas de circuito(s) integrado(s) con contactos — Parte 2: Dimensiones y ubicación de los contactos. Primera edición: 1999.
ISO/CEI 7816-3	Tecnología de la información — Tarjetas de identificación — Tarjetas de circuito(s) integrado(s) con contactos — Parte 3: Señales electrónicas y protocolo de transmisión. Segunda edición: 1997.
ISO/CEI 7816-4	Tecnología de la información — Tarjetas de identificación — Tarjetas de circuito(s) integrado(s) con contactos — Parte 4: Comandos interindustriales para intercambio. Primera edición: 1995 + Modificación 1: 1997.
ISO/CEI 7816-6	Tecnología de la información — Tarjetas de identificación — Tarjetas de circuito(s) integrado(s) con contactos — Parte 6: Elementos de datos interindustriales. Primera edición: 1996 + Cor 1: 1998.
ISO/CEI 7816-8	Tecnología de la información — Tarjetas de identificación — Tarjetas de circuito(s) integrado(s) con contactos — Parte 8: Comandos interindustriales relacionados con la seguridad. Primera edición: 1999.
ISO/CEI 9797	Tecnología de la información — Técnicas de seguridad — Mecanismo de integridad de los datos mediante una función de comprobación criptográfica que utiliza un algoritmo de cifrado en bloques. Segunda edición: 1994.

2. CARACTERÍSTICAS ELÉCTRICAS Y FÍSICAS

TCS_200 Todas las señales electrónicas deberán ser conformes a la norma ISO/CEI 7816-3, a menos que se especifique otra cosa.

TCS_201 La ubicación y dimensiones de los contactos de las tarjetas se ajustarán a lo dispuesto en la norma ISO/CEI 7816-2.

2.1. **Tensión de alimentación y consumo de corriente**

TCS_202 La tarjeta deberá trabajar con arreglo a las especificaciones, dentro de los límites de consumo especificados en la norma ISO/CEI 7816-3.

TCS_203 La tarjeta deberá trabajar con una tensión V_{cc} = 3 V (+/− 0,3 V) o V_{cc} = 5 V (+/− 0,5 V).

La tensión deberá seleccionarse con arreglo a lo dispuesto en la norma ISO/CEI 7816-3.

2.2. **Tensión de programación V_{pp}**

TCS_204 La tarjeta no precisará una tensión de programación en la patilla C6. Se espera que la patilla C6 no esté conectada a un IFD. El contacto C6 podrá estar conectado a la tensión V_{cc} de la tarjeta, pero no a masa. Dicha tensión no deberá interpretarse en ningún caso.

2.3. **Generación y frecuencia del reloj**

TCS_205 La tarjeta deberá funcionar el intervalo de frecuencias de 1 a 5 MHz. La frecuencia del reloj podrá experimentar una variación del ± 2 % dentro de una sesión de la tarjeta. La frecuencia del reloj la genera la unidad intravehicular y no la propia tarjeta. El ciclo de trabajo puede variar entre el 40 y el 60 %.

TCS_206 El reloj externo puede ser detenido en las condiciones que especifica el archivo EF_{ICC} de la tarjeta. El primer byte que hay en el cuerpo del archivo EF_{ICC} codifica las condiciones del modo de paro del reloj (más información en la norma EN 726-3):

Bajo	Alto		
Bit 3	Bit 2	Bit 1	
0	0	1	Se permite el paro del reloj, no hay un nivel preferido
0	1	1	Se permite el paro del reloj, preferiblemente en el nivel alto
1	0	1	Se permite el paro del reloj, preferiblemente en el nivel bajo
0	0	0	No se permite el paro del reloj
0	1	0	Se permite el paro del reloj, exclusivamente en el nivel alto
1	0	0	Se permite el paro del reloj, exclusivamente en el nivel bajo

Los bits 4 a 8 no se utilizan.

2.4. **Contacto de entrada/salida**

TCS_207 El contacto C7 de entrada/salida sirve para recibir y transmitir datos al IFD. Durante el funcionamiento de dicho contacto, tan solo podrán estar en modo de transmisión la tarjeta o el IFD. Si ambas unidades estuvieran en el modo de transmisión, la tarjeta no deberá sufrir daños. A menos que se esté transmitiendo, la tarjeta deberá entrar en el modo de recepción.

2.5. **Estados de la tarjeta**

TCS_208 La tarjeta trabaja en dos estados mientras se aplica la tensión de alimentación:

— estado de funcionamiento mientras se ejecutan los comandos o se mantiene la interconexión con la unidad digital,

— estado de reposo en el resto de casos; en este estado la tarjeta deberá retener todos los datos.

3. SOPORTE FÍSICO Y COMUNICACIONES

3.1. **Introducción**

El presente apartado describe la funcionalidad mínima que precisan las tarjetas de tacógrafo y las VUs para garantizar un correcto funcionamiento e interoperabilidad.

Las tarjetas de tacógrafo cumplen en todo lo posible las normas ISO/CEI aplicables (en especial la norma ISO/CEI 7816). No obstante, a continuación se ofrece una descripción completa de los comandos y protocolos a fin de especificar algunos casos de uso restringido o determinadas diferencias que puedan existir. Los comandos especificados son totalmente conformes a las normas citadas, salvo en los casos que se indican.

3.2. **Protocolo de transmisión**

TCS_300 El protocolo de transmisión deberá ser conforme a la norma ISO/CEI 7816-3. En particular, la VU deberá reconocer las extensiones de tiempo de espera que envíe la tarjeta.

3.2.1. ***Protocolos***

TCS_301 La tarjeta deberá ofrecer los protocolos T=0 y T=1.

TCS_302 T=0 es el protocolo por defecto, de modo que se precisa un comando PTS para cambiar al protocolo T=1.

TCS_303 Los dispositivos deberán admitir la convención directa en ambos protocolos: por consiguiente, la convención directa es obligatoria para la tarjeta.

TCS_304 Dentro de la respuesta ATR, el byte correspondiente al tamaño del campo de información para la tarjeta deberá presentarse en el carácter TA3. Este valor deberá ser al menos 'F0h' (= 240 bytes).

Los protocolos estarán sujetos a las restricciones siguientes:

TCS_305 T=0

— El dispositivo de interfaz deberá admitir una respuesta en la entrada/salida después del flanco ascendente de la señal en RST a partir de 400 cc.

— El dispositivo de interfaz deberá ser capaz de leer caracteres separados por 12 etu.

— El dispositivo de interfaz deberá leer un carácter erróneo y su repetición cuando estén separados por 13 etu. Si se detecta un carácter erróneo, la señal de error en la entrada/salida puede ocurrir entre 1 etu y 2 etu más tarde. El dispositivo deberá admitir un retardo de 1 etu.

— El dispositivo de interfaz deberá aceptar una respuesta ATR de 33 bytes (TS+32).

— Si TC1 está presente en la respuesta ATR, el tiempo adicional de seguridad deberá estar presente para los caracteres que envíe el dispositivo de interfaz, aunque los caracteres que envíe la tarjeta igualmente podrán estar separados por 12 etu. Este principio también es cierto para el carácter ACK que envía la tarjeta después de que el dispositivo de interfaz haya emitido un carácter P3.

— El dispositivo de interfaz deberá tener en cuenta los caracteres NUL que pueda emitir la tarjeta.

— El dispositivo de interfaz deberá aceptar el modo complementario de ACK.

— El comando GET RESPONSE no se puede utilizar en el modo de encadenamiento para obtener un dato cuya longitud podría sobrepasar 255 bytes.

TCS_306 T=1

— NAD Byte: no se utiliza (la dirección NAD deberá configurarse a '00').

— S-block ABORT: no se utiliza.

— S-block VPP state error: no se utiliza.

— La longitud total de encadenamiento de un campo de datos no sobrepasará 255 bytes (de ello se asegurará el IFD).

— El IFD deberá indicar el dispositivo de tamaño del campo de información (IFSD) inmediatamente después de la respuesta ATR: el IFD deberá transmitir la petición de IFS del bloque S después de la respuesta ATR y la tarjeta deberá enviar el IFS del bloque S. El valor recomendado para el IFSD es 254 bytes.

— La tarjeta no pedirá un reajuste del IFS.

3.2.2. ***ATR***

TCS_307 El dispositivo comprueba los bytes ATR, de acuerdo con la norma ISO/CEI 7816-3. No se verificarán los caracteres históricos ATR.

Ejemplo de biprotocolo básico ATR con arreglo a la norma ISO/CEI 7816-3

Carácter	Valor	Observaciones
TS	'3Bh'	Indica convención directa
T0	'85h'	TD1 presente; hay 5 bytes históricos presentes
TD1	'80h'	TD2 presente; ha de utilizarse T=0
TD2	'11h'	TA3 presente; ha de utilizarse T=1
TA3	'XXh' (al menos 'F0h')	Tamaño del campo de información para la tarjeta (IFSC)
TH1 a TH5	'XXh'	Caracteres históricos
TCK	'XXh'	Comprobar carácter (OR exclusivo)

TCS_308 Después de la respuesta a reinicio (ATR), el archivo principal (MF) se selecciona de manera implícita y pasa a ser el directorio actual.

3.2.3. ***PTS***

TCS_309 El protocolo por defecto es T=0. Para configurar el protocolo T=1, es preciso que el dispositivo envíe a la tarjeta una selección PTS (también denominada PPS).

TCS_310 Dado que tanto el protocolo T=0 como el T=1 son obligatorios para la tarjeta, la selección PTS básica de conmutación de protocolos es obligatoria para la tarjeta.

La selección PTS se puede utilizar, tal y como se indica en la norma ISO/CEI 7816-3, para cambiar a una velocidad en baudios más alta que la velocidad que propone por defecto la tarjeta en la respuesta ATR, en su caso [byte TA(1)].

Opcionalmente, la tarjeta puede funcionar a velocidad en baudios más altas.

TCS_311 Si no se admiten otras velocidades en baudios aparte de la que se ajusta por defecto (o si la velocidad en baudios seleccionada es inadmisible), la tarjeta deberá responder a la selección PTS en la forma correcta según la norma ISO/CEI 7816-3, es decir, omitiendo el byte PPS1.

A continuación se ofrecen varios ejemplos de PTS básica selección de protocolo:

Carácter	Valor	Observaciones
PPSS	'FFh'	El carácter de inicio
PPS0	'00h' o bien '01h'	PPS1 a PPS3 no están presentes; '00h' para seleccionar T0, '01h' para seleccionar T1
PK	'XXh'	Comprobar carácter: 'XXh' = 'FFh' si PPS0 = '00h', 'XXh' = 'FEh' si PPS0 = '01h'

3.3. **Condiciones de acceso (AC)**

Las condiciones de acceso (AC) para los comandos UPDATE_BINARY y READ_BINARY se definen para cada archivo elemental.

TCS_312 Es preciso que se cumplan las condiciones AC del archivo actual antes de acceder al archivo a través de estos comandos.

A continuación se ofrecen las definiciones de las condiciones de acceso disponibles:

— ALW: la acción siempre es posible y se puede ejecutar sin restricciones.

— NEV: la acción nunca es posible.

— AUT: es preciso abrir el derecho correspondiente a una autentificación externa con resultado positivo (se encarga de ello el comando EXTERNAL AUTHENTICATE).

— PRO SM: es preciso transmitir el comando con una suma de control criptográfica por medio de mensajería segura (véase el apéndice 11).

— AUT y PRO SM (combinados).

En los comandos de proceso (UPDATE BINARY y READ BINARY), es posible seleccionar en la tarjeta las siguientes condiciones de acceso:

	UPDATE BINARY	READ BINARY
ALW	Sí	Sí
NEV	Sí	Sí
AUT	Sí	Sí
PRO SM	Sí	No
AUT y PRO SM	Sí	No

La condición de acceso PRO SM no está disponible para el comando READ BINARY, lo que significa que la presencia de una suma de control criptográfica para un comando READ nunca es obligatoria. No obstante, si se utiliza el valor 'OC' para la clase, es posible utilizar el comando READ BINARY con mensajería segura, tal y como se describe en el apartado 3.6.2.

3.4. **Cifrado de datos**

Cuando es preciso proteger la confidencialidad de unos datos que se van a leer, el archivo que los contiene se marca como "cifrado". El cifrado se lleva a cabo utilizando mensajería segura (véase el apéndice 11).

3.5. **Visión general de los comandos y los códigos de error**

Los comandos y la organización de archivos se deducen de la norma ISO/CEI 7816-4.

TCS_313 En esta sección se describen los siguientes pares comando APDU-respuesta:

Comando	INS
SELECT FILE	A4
READ BINARY	B0
UPDATE BINARY	D6
GET CHALLENGE	84
VERIFY	20
GET RESPONSE	C0
PERFORM SECURITY OPERATION: VERIFY CERTIFICATE COMPUTE DIGITAL SIGNATURE VERIFY DIGITAL SIGNATURE HASH	2A
INTERNAL AUTHENTICATE	88
EXTERNAL AUTHENTICATE	82
MANAGE SECURITY ENVIRONMENT: SETTING A KEY	22
PERFORM HASH OF FILE	2A

TCS_314 Las palabras de estado SW1 SW2 aparecen en todos los mensajes de respuesta e indican el estado de procesado del comando.

SW1	SW2	Significado
90	00	Procesamiento normal
61	XX	Procesamiento normal. XX = número de bytes de respuesta disponibles
62	81	Procedimiento de aviso. Una parte de los datos devueltos puede estar dañada
63	CX	CHV (PIN) incorrecto. 'X' indica el contador de intentos restantes
64	00	Error de ejecución. No ha variado el estado de la memoria permanente. Error de integridad
65	00	Error de ejecución. Ha variado el estado de la memoria permanente
65	81	Error de ejecución. Ha variado el estado de la memoria permanente. Fallo de memoria
66	88	Error de seguridad: suma de control criptográfica incorrecta (durante la mensajería segura) o bien certificado incorrecto (durante la verificación del certificado) o bien criptograma incorrecto (durante la autentificación externa) o bien firma incorrecta (durante la verificación de la firma)
67	00	Longitud incorrecta (Lc o Le incorrecta)
69	00	Comando prohibido (no hay respuesta disponible en T=0)
69	82	Estado de seguridad no satisfecho
69	83	Método de autentificación bloqueado
69	85	Condiciones de uso no satisfechas
69	86	Comando no autorizado (falta el EF actual)
69	87	Faltan objetos de datos de mensajería segura que se esperaban
69	88	Objetos de datos de mensajería segura incorrectos
6A	82	Archivo no encontrado
6A	86	Parámetros P1-P2 incorrectos
6A	88	Datos referenciados no encontrados
6B	00	Parámetros incorrectos (desviación fuera del EF)

SW1	SW2	Significado
6C	XX	Longitud incorrecta, SW2 indica la longitud exacta. No se devuelve un campo de datos
6D	00	Código de instrucción inadmisible o no válido
6E	00	Clase inadmisible
6F	00	Otros errores de comprobación

3.6. **Descripción de los comandos**

En el presente capítulo se describen los comandos obligatorios para las tarjetas de tacógrafo.

En el apéndice 11 (Mecanismos de seguridad comunes) hallará otros pormenores relevantes relacionados con las operaciones criptográficas que es preciso realizar.

Todos los comandos se describen con independencia del protocolo utilizado (T=0 o T=1). Los bytes APDU CLA, INS, P1, P2, Lc y Le siempre se indican. Si el byte Lc o Le no es necesario para el comando descrito, entonces la longitud, el valor y la descripción asociados están vacíos.

TCS_315 Si se solicitan los dos bytes de longitud (Lc y Le) y además el IFD está utilizando el protocolo T=0, es preciso dividir en dos partes el comando descrito: el IFD envía el comando del modo descrito con P3=Lc+data y seguidamente envía un comando GET RESPONSE (véase el apartado 3.6.6) con P3=Le.

TCS_316 Si se solicitan los dos bytes de longitud y Le=0 (mensajería segura)

— en caso de utilizarse el protocolo T=1, la tarjeta deberá responder a Le=0 enviando todos los datos de salida disponibles,

— en caso de utilizarse el protocolo T=0, la tarjeta deberá responder a Le=0 con los bytes de estado '61La', donde La es el número de bytes de respuesta disponibles. A continuación, el IFD deberá generar un comando GET RESPONSE con P3= La para leer los datos.

3.6.1. ***Select File (seleccionar archivo)***

Este comando cumple con lo dispuesto en la norma ISO/CEI 7816-4, pero tiene un uso restringido en comparación con el comando que se define en dicha norma.

El comando SELECT FILE se utiliza:

— para seleccionar un DF de la aplicación (es preciso utilizar la selección por nombre),

— para seleccionar un archivo elemental que corresponda al ID de archivo enviado.

3.6.1.1. *Selección por nombre (AID)*

Este comando permite seleccionar un DF de la aplicación en la tarjeta.

TCS_317 Este comando puede ejecutarse desde cualquier punto de la estructura de archivos (después de la respuesta ATR o en cualquier momento).

TCS_318 Al seleccionar una aplicación se reinicia el entorno de seguridad actual. A partir de ese momento ya no se vuelve a seleccionar una clave pública actual y la clave de la sesión anterior deja de estar disponible para mensajería segura. También se pierde la condición de acceso AUT.

TCS_319 Mensaje de comando

Byte	Long.	Valor	Descripción
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'04h'	Selección por nombre (AID)
P2	1	'0Ch'	No se espera respuesta
Lc	1	'NNh'	Número de bytes enviados a la tarjeta (longitud del AID): '06h' para la aplicación de tacógrafo
#6-#(5+NN)	NN	'XX..XXh'	AID: 'FF 54 41 43 48 4F' para la aplicación de tacógrafo

No se precisa respuesta para el comando SELECT FILE (Le ausente en T=1, o no se pide respuesta en T=0).

TCS_320 Mensaje de respuesta (no se pide respuesta)

Byte	Long.	Valor	Descripción
SW	2	'XXXXh'	Palabras de estado (SW1, SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '9000'.

— Si no se encuentra la aplicación que corresponde al AID, se contesta con el estado de procesado '6A82'.

— En T=1, si está presente el byte Le, se contesta con el estado '6700'.

— En T=0, si se pide una respuesta después del comando SELECT FILE, se contesta con el estado '6900'.

— Si se considera que la aplicación seleccionada está dañada (se detecta un error de integridad dentro de los atributos del archivo), se contesta con el estado de procesado '6400' o '6581'.

3.6.1.2. *Selección de un archivo elemental utilizando su identificador*

TCS_321 Mensaje de comando

Byte	Long.	Valor	Descripción
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'02h'	Selección de un EF bajo el DF actual
P2	1	'0Ch'	No se espera respuesta
Lc	1	'02h'	Número de bytes enviados a la tarjeta
#6-#7	2	'XXXXh'	Identificador de archivo

No se precisa respuesta para el comando SELECT FILE (Le ausente en T=1, o no se pide respuesta en T=0).

TCS_322 Mensaje de respuesta (no se pide respuesta)

Byte	Long.	Valor	Descripción
SW	2	'XXXXh'	Palabras de estado (SW1, SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '9000'.

— Si no se encuentra el archivo que corresponde al identificador, se contesta con el estado de procesado '6A82'.

— En T=1, si está presente el byte Le, se contesta con el estado '6700'.

— En T=0, si se pide una respuesta después del comando SELECT FILE, se contesta con el estado '6900'.

— Si se considera que el archivo seleccionado está dañado (se detecta un error de integridad dentro de los atributos del archivo), se contesta con el estado de procesado '6400' o '6581'.

3.6.2. ***Read Binary (leer archivo binario)***

Este comando cumple con lo dispuesto en la norma ISO/CEI 7816-4, pero tiene un uso restringido en comparación con el comando que se define en dicha norma.

El comando READ BINARY sirve para leer datos de un archivo transparente.

La respuesta de la tarjeta consiste en devolver los datos leídos, opcionalmente encapsulados en una estructura de mensajería segura.

TCS_323 El comando sólo puede ejecutarse si el estado de seguridad satisface los atributos de seguridad definidos para el EF de la función READ.

3.6.2.1. *Comando sin mensajería segura*

Este comando permite al IFD leer datos del EF actualmente seleccionado, sin mensajería segura.

TCS_324 Este comando no deberá permitir que se lean datos de un archivo marcado como "cifrado".

TCS_325 Mensaje de comando

Byte	Long.	Valor	Descripción
CLA	1	'00h'	No se pide mensajería segura
INS	1	'B0h'	
P1	1	'XXh'	Desviación en bytes desde el comienzo del archivo: byte más significativo
P2	1	'XXh'	Desviación en bytes desde el comienzo del archivo: byte menos significativo
Le	1	'XXh'	Longitud de los datos esperados. Número de bytes que se han de leer

Nota: el bit 8 de P1 debe ponerse a 0.

TCS_326 Mensaje de respuesta

Byte	Long.	Valor	Descripción
#1-#X	X	'XX..XXh'	Datos leídos
SW	2	'XXXXh'	Palabras de estado (SW1, SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '9000'.

— Si no se selecciona un EF, se contesta con el estado de procesado '6986'.

— Si no se satisface el control de accesos del archivo seleccionado, se interrumpe el comando con '6982'.

— Si la desviación no es compatible con el tamaño del EF (desviación > tamaño del EF), se contesta con el estado de procesado '6B00'.

— Si el tamaño de los datos que se han de leer no es compatible con el tamaño del EF (desviación + Le > tamaño del EF), se contesta con el estado de procesado '6700' o '6Cxx' donde 'xx' indica la longitud exacta.

— Si se detecta un error de integridad dentro de los atributos del archivo, la tarjeta considerará el archivo dañado e irrecuperable, se contesta con el estado de procesado '6400' o '6581'.

— Si se detecta un error de integridad dentro de los datos almacenados, la tarjeta devuelve los datos solicitados y contesta con el estado de procesado '6281'.

3.6.2.2. *Comando con mensajería segura*

Este comando permite al IDF leer datos del EF actualmente seleccionado, con mensajería segura, a fin de verificar la integridad de los datos recibidos y proteger la confidencialidad de los datos en caso de que el EF se haya marcado como "cifrado".

TCS_327 Mensaje de comando

Byte	Long.	Valor	Descripción
CLA	1	'0Ch'	Se pide mensajería segura
INS	1	'B0h'	INS
P1	1	'XXh'	P1 (desviación en bytes desde el comienzo del archivo): byte más significativo
P2	1	'XXh'	P2 (desviación en bytes desde el comienzo del archivo): byte menos significativo
Lc	1	'09h'	Longitud de los datos de entrada para mensajería segura
#6	1	'97h'	T_{LE}: Etiqueta para especificación de la longitud esperada
#7	1	'01h'	L_{LE}: Longitud de la longitud esperada
#8	1	'NNh'	Especificación de la longitud esperada (Le original): Número de bytes que se han de leer

Byte	Long.	Valor	Descripción
#9	1	'8Eh'	T_{CC}: Etiqueta para suma de control criptográfica
#10	1	'04h'	L_{CC}: Longitud de la siguiente suma de control criptográfica
#11-#14	4	'XX..XXh'	Suma de control criptográfica (4 bytes más significativos)
Le	1	'00h'	Según se especifica en la norma ISO/CEI 7816-4

TCS_328 Mensaje de respuesta si el EF no está marcado como "cifrado" y si el formato de entrada de mensajería segura es correcto:

Byte	Long.	Valor	Descripción
#1	1	'81h'	T_{PV}: Etiqueta para datos del valor plano
#2	L	'NNh' or '81 NNh'	L_{PV}: longitud de los datos devueltos (=Le original). L es 2 bytes si L_{PV}>127 bytes.
#(2+L)-#(1+L+NN)	NN	'XX..XXh'	Valor de datos planos
#(2+L+NN)	1	'8Eh'	T_{CC}: Etiqueta para suma de control criptográfica
#(3+L+NN)	1	'04h'	L_{CC}: Longitud de la siguiente suma de control criptográfica
#(4+L+NN)-#(7+L+NN)	4	'XX..XXh'	Suma de control criptográfica (4 bytes más significativos)
SW	2	'XXXXh'	Palabras de estado (SW1, SW2)

TCS_329 Mensaje de respuesta si el EF está marcado como "cifrado" y si el formato de entrada de mensajería segura es correcto:

Byte	Long.	Valor	Descripción
#1	1	'87h'	$T_{PI\ CG}$: Etiqueta para datos cifrados (criptograma)
#2	L	'MMh' or '81 MMh'	$L_{PI\ CG}$: longitud de los datos cifrados que se devuelven (distinta de la Le original del comando, debido al relleno). L es 2 bytes si $L_{PI\ CG}$ > 127 bytes
#(2+L)-#(1+L+MM)	MM	'01XX..XXh'	Datos cifrados: Indicador de relleno y criptograma
#(2+L+MM)	1	'8Eh'	T_{CC}: Etiqueta para suma de control criptográfica
#(3+L+MM)	1	'04h'	L_{CC}: Longitud de la siguiente suma de control criptográfica
#(4+L+MM)-#(7+L+MM)	4	'XX..XXh'	Suma de control criptográfica (4 bytes más significativos)
SW	2	'XXXXh'	Palabras de estado (SW1, SW2)

Los datos cifrados que se devuelven contienen un primer byte que indica el modo de relleno utilizado. Para la aplicación de tacógrafo, el indicador de relleno siempre toma el valor '01h', para indicar que se utiliza el modo de relleno especificado en la norma ISO/CEI 7816-4 (un byte con valor '80h' seguido de varios bytes nulos: ISO/CEI 9797 método 2).

Los estados de procesado "normales", descritos para el comando READ BINARY sin mensajería segura (véase el apartado 3.6.2.1), se pueden devolver utilizando las estructuras de mensaje de respuesta descritas anteriormente.

Asimismo, es posible que se produzcan algunos errores específicamente relacionados con la mensajería segura. En tal caso, el estado de procesado se devuelve tal cual, sin la intervención de una estructura de mensajería segura.

TCS_330 Mensaje de respuesta si el formato de entrada de mensajería segura es incorrecto

Byte	Long.	Valor	Descripción
SW	2	'XXXXh'	Palabras de estado (SW1, SW2)

— Si no hay una clave disponible para la sesión actual, se devuelve el estado de procesado '6A88'. Esto ocurre si la clave de la sesión no se ha generado todavía o si ha expirado la validez de dicha clave (en tal caso, el IFD debe ejecutar de nuevo un proceso de autentificación mutua para establecer una nueva clave de sesión).

— Si en el formato de mensajería segura faltan algunos de los objetos de datos que se esperaban (anteriormente especificados), se devuelve el estado de procesado '6987': este error se produce si falta una etiqueta esperada o si el cuerpo del comando no está bien construido.

— Si algunos de los objetos de datos son incorrectos, se contesta con el estado de procesado '6988': este error se produce si están presentes todas las etiquetas necesarias pero algunas longitudes no coinciden con las esperadas.

— Si falla la verificación de la suma de control criptográfica, se contesta con el estado de procesado '6688'.

3.6.3. ***Update Binary (actualizar archivo binario)***

Este comando cumple con lo dispuesto en la norma ISO/CEI 7816-4, pero tiene un uso restringido en comparación con el comando que se define en dicha norma.

El mensaje de comando UPDATE BINARY inicia la actualización (borrar + escribir) de los bits ya presentes en un EF binario, para sustituirlos por los bits dados en el comando APDU.

TCS_331 El comando sólo puede ejecutarse si el estado de seguridad satisface los atributos de seguridad definidos para el EF de la función UPDATE (si el control de acceso de la función UPDATE incluye PRO SM, habrá que añadir una mensajería segura en el comando).

3.6.3.1. *Comando sin mensajería segura*

Este comando permite al IFD escribir datos en el EF actualmente seleccionado, sin que la tarjeta verifique la integridad de los datos recibidos. Este modo directo sólo se permite si el archivo relacionado no se ha marcado como "cifrado".

TCS_332 Mensaje de comando

Byte	Long.	Valor	Descripción
CLA	1	'00h'	No se pide mensajería segura
INS	1	'D6h'	
P1	1	'XXh'	Desviación en bytes desde el comienzo del archivo: byte más significativo
P2	1	'XXh'	Desviación en bytes desde el comienzo del archivo: byte menos significativo
Lc	1	'NNh'	Lc Longitud de los datos que se han de actualizar. Número de bytes que se han de escribir
#6-#(5+NN)	NN	'XX..XXh'	Datos que se han de escribir

Nota: el bit 8 de P1 debe ponerse a 0.

TCS_333 Mensaje de respuesta

Byte	Long.	Valor	Descripción
SW	2	'XXXXh'	Palabras de estado (SW1, SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '9000'.

— Si no se selecciona un EF, se contesta con el estado de procesado '6986'.

— Si no se satisface el control de accesos del archivo seleccionado, se interrumpe el comando con '6982'.

— Si la desviación no es compatible con el tamaño del EF (desviación > tamaño del EF), se contesta con el estado de procesado '6B00'.

— Si el tamaño de los datos que se han de escribir no es compatible con el tamaño del EF (desviación + Le > tamaño del EF), se contesta con el estado de procesado '6700'.

— Si se detecta un error de integridad dentro de los atributos del archivo, la tarjeta considerará el archivo dañado e irrecuperable, se contesta con el estado de procesado '6400' o '6500'.

— Si falla la escritura, se contesta con el estado de procesado '6581'.

3.6.3.2. *Comando con mensajería segura*

Este comando permite al IFD escribir datos en el EF actualmente seleccionado, de modo que la tarjeta verifica la integridad de los datos recibidos. Dado que no se precisa confidencialidad, los datos no están cifrados.

TCS_334 Mensaje de comando

Byte	Long.	Valor	Descripción
CLA	1	'0Ch'	Se pide mensajería segura
INS	1	'D6h'	INS
P1	1	'XXh'	Desviación en bytes desde el comienzo del archivo: Byte más significativo
P2	1	'XXh'	Desviación en bytes desde el comienzo del archivo: Byte menos significativo
Lc	1	'XXh'	Longitud del campo de datos seguro
#6	1	'81h'	T_{PV}: Etiqueta para datos del valor plano
#7	L	'NNh' or '81 NNh'	L_{PV}: longitud de los datos transmitidos L es 2 bytes si L_{PV} > 127 bytes
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Valor de datos planos (datos que se han de escribir)
#(7+L+NN)	1	'8Eh'	T_{CC}: Etiqueta para suma de control criptográfica
#(8+L+NN)	1	'04h'	L_{CC}: Longitud de la siguiente suma de control criptográfica
#(9+L+NN)-#(12+L+NN)	4	'XX..XXh'	Suma de control criptográfica (4 bytes más significativos)
Le	1	'00h'	Según se especifica en la norma ISO/CEI 7816-4

TCS_335 Mensaje de respuesta si el formato de entrada de mensajería segura es correcto

Byte	Long.	Valor	Descripción
#1	1	'99h'	T_{SW}: Etiqueta para palabras de estado (con la protección de CC)
#2	1	'02h'	L_{SW}: longitud de las palabras de estado devueltas
#3-#4	2	'XXXXh'	Palabras de estado (SW1, SW2)
#5	1	'8Eh'	T_{CC}: Etiqueta para suma de control criptográfica
#6	1	'04h'	L_{CC}: Longitud de la siguiente suma de control criptográfica
#7-#10	4	'XX..XXh'	Suma de control criptográfica (4 bytes más significativos)
SW	2	'XXXXh'	Palabras de estado (SW1, SW2)

Los estados de procesado "normales", descritos para el comando UPDATE BINARY sin mensajería segura (véase el apartado 3.6.3.1), se pueden devolver utilizando las estructuras de mensaje de respuesta descritas anteriormente.

Asimismo, es posible que se produzcan algunos errores específicamente relacionados con la mensajería segura. En tal caso, el estado de procesado se devuelve tal cual, sin la intervención de una estructura de mensajería segura.

TCS_336 Mensaje de respuesta si se produce un error de mensajería segura

Byte	Long.	Valor	Descripción
SW	2	'XXXXh'	Palabras de estado (SW1, SW2)

— Si no hay una clave disponible para la sesión actual, se devuelve el estado de procesado '6A88'.

— Si en el formato de mensajería segura faltan algunos de los objetos de datos que se esperaban (anteriormente especificados), se devuelve el estado de procesado '6987': este error se produce si falta una etiqueta esperada o si el cuerpo del comando no está bien construido.

— Si algunos de los objetos de datos son incorrectos, se contesta con el estado de procesado '6988': este error se produce si están presentes todas las etiquetas necesarias pero algunas longitudes no coinciden con las esperadas.

— Si falla la verificación de la suma de control criptográfica, se contesta con el estado de procesado '6688'.

3.6.4. ***Get Challenge (obtener interrogación)***

Este comando cumple con lo dispuesto en la norma ISO/CEI 7816-4, pero tiene un uso restringido en comparación con el comando que se define en dicha norma.

El comando GET CHALLENGE pide a la tarjeta que envíe una interrogación para usarla en un procedimiento relacionado con la seguridad que incluya el envío de un criptograma o de unos datos cifrados a la tarjeta.

TCS_337 La interrogación que envía la tarjeta tan solo es válida para el siguiente comando que utilice una interrogación y se envíe a la tarjeta.

TCS_338 Mensaje de comando

Byte	Long.	Valor	Descripción
CLA	1	'00h'	CLA
INS	1	'84h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Le	1	'08h'	Le (Longitud de la interrogación esperada)

TCS_339 Mensaje de respuesta

Byte	Long.	Valor	Descripción
#1-#8	8	'XX..XXh'	Interrogación
SW	2	'XXXXh'	Palabras de estado (SW1, SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '9000'.

— Si Le es distinto de '08h', el estado de procesado es '6700'.

— Si los parámetros P1-P2 son incorrectos, el estado de procesado es '6A86'.

3.6.5. ***Verify (verificar)***

Este comando cumple con lo dispuesto en la norma ISO/CEI 7816-4, pero tiene un uso restringido en comparación con el comando que se define en dicha norma.

El comando VERIFY inicia una comparación en la tarjeta, confrontando los datos CHV (PIN) enviados desde el comando con la referencia CHV almacenada en la tarjeta.

Nota: el IFD debe añadir bytes 'FFh' para rellenar por la derecha el PIN que introduzca el usuario, hasta llegar a una longitud de 8 bytes.

TCS_340 Si el comando se ejecuta correctamente, los derechos correspondientes a la presentación CHV se abren y el contador de intentos CHV restantes se reinicializa.

TCS_341 Si la comparación no tiene éxito, queda registrada en la tarjeta a fin de limitar el número de intentos que quedan para utilizar la información CHV de referencia.

TCS_342 Mensaje de comando

Byte	Long.	Valor	Descripción
CLA	1	'00h'	CLA
INS	1	'20h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (la CHV verificada se conoce implícitamente)
Lc	1	'08h'	Longitud del código CHV transmitido
#6-#13	8	'XX..XXh'	CHV

TCS_343 Mensaje de respuesta

Byte	Long.	Valor	Descripción
SW	2	'XXXXh'	Palabras de estado (SW1, SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '9000'.

— S no se encuentra la referencia CHV, se contesta con el estado de procesado '6A88'.

— Si la información CHV está bloqueada (el contador de intentos restantes de la CHV es cero), se contesta con el estado de procesado '6983'. Una vez en ese estado, ya no se puede volver a presentar la información CHV.

— Si la comparación no tiene éxito, se resta una unidad a la lectura del contador de intentos restantes y se devuelve el estado '63CX' (X > 0 y X es igual al contador de intentos CHV restantes. Si X = 'F', el contador de intentos CHV es mayor que 'F').

— Si se considera que la información CHV de referencia está dañada, se contesta con el estado de procesado '6400' o '6581'.

3.6.6. ***Get Response (obtener respuesta)***

Este comando cumple con lo dispuesto en la norma ISO/CEI 7816-4.

Este comando (exclusivamente necesario y disponible en el protocolo T=0) sirve para transmitir datos preparados de la tarjeta al dispositivo de interfaz (cuando el comando incluye las longitudes Lc y Le).

El comando GET RESPONSE tiene que enviarse inmediatamente después del comando que prepara los datos. De lo contrario, los datos se pierden. Una vez ejecutado el comando GET RESPONSE (salvo si se produce el error '61xx', véase más abajo), los datos preparados previamente dejan de estar disponibles.

TCS_344 Mensaje de comando

Byte	Long.	Valor	Descripción
CLA	1	'00h'	
INS	1	'C0h'	
P1	1	'00h'	
P2	1	'00h'	
Le	1	'XXh'	Número de bytes esperados

TCS_345 Mensaje de respuesta

Byte	Long.	Valor	Descripción
#1-#X	X	'XX..XXh'	Datos
SW	2	'XXXXh'	Palabras de estado (SW1,SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '9000'.

— Si la tarjeta no ha preparado ningún dato, se contesta con el estado de procesado '6900'.

— Si la longitud Le sobrepasa el número de bytes disponibles o es igual a cero, se contesta con el estado de procesado '6Cxx', donde xx es el número exacto de bytes disponibles. En ese caso, y exclusivamente en ese caso, los datos preparados siguen estando disponibles para un comando GET RESPONSE posterior.

— Si la longitud Le es distinta de cero y menor que el número de bytes disponibles, la tarjeta normalmente envía los datos necesarios, y se contesta con el estado de procesado '61xx' donde xx indica el número de bytes extra todavía disponibles para un comando GET RESPONSE posterior. El resto de datos (que no se pidieron) ya no están disponibles.

— Si el comando no se admite (protocolo T=1), la tarjeta contesta con el estado '6D00'.

3.6.7. ***PSO: Verify Certificate (realizar operación de seguridad: verificar certificado)***

Este comando cumple con lo dispuesto en la norma ISO/CEI 7816-8, pero tiene un uso restringido en comparación con el comando que se define en dicha norma.

El comando VERIFY CERTIFICATE lo utiliza la tarjeta para obtener una clave pública del exterior y para comprobar su validez.

TCS_346 Cuando un comando VERIFY CERTIFICATE se ejecuta correctamente, la clave pública queda almacenada para su uso posterior en el entorno de seguridad. Esta clave debe crearla de forma explícita el comando MSE utilizando su identificador de clave (véase el apartado 3.6.10), para uso en comandos relacionados con la seguridad (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE o VERIFY CERTIFICATE).

TCS_347 En cualquier caso, el comando VERIFY CERTIFICATE utiliza la clave pública previamente seleccionada por el comando MSE para abrir el certificado.

TCS_348 Mensaje de comando

Byte	Long.	Valor	Descripción
CLA	1	'00h'	CLA
INS	1	'2Ah'	Realizar operación de seguridad
P1	1	'00h'	P1
P2	1	'AEh'	P2: datos sin codificación BER-TLV (concatenación de elementos de datos)
Lc	1	'CEh'	Lc: Longitud del certificado, 206 Bytes
#6-#199	194	'XX..XXh'	Certificado: concatenación de elementos de datos (como se describe en el Apéndice 11)

TCS_349 Mensaje de respuesta

Byte	Long.	Valor	Descripción
SW	2	'XXXXh'	Palabras de estado (SW1, SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '9000'.

— Si la verificación del certificado falla, se contesta con el estado de procesado '6688'. El proceso de verificación y desenvolvimiento del certificado se describe en el apéndice 11.

— Si no hay una clave pública presente en el entorno de seguridad, se devuelve '6A88'.

— Si se considera que la clave publica seleccionada (utilizada para desenvolver el certificado) está dañada, se contesta con el estado de procesado '6400' o '6581'.

— Si la clave pública seleccionada (utilizada para desenvolver el certificado) tiene un CHA.LSB (`CertificateHolderAuthorisation.equipmentType`) diferente de '00' (es decir, no es el de un Estado miembro o el de Europa), se contesta con el estado de procesado '6985'.

3.6.8. ***Internal Authenticate (autentificación interna)***

Este comando cumple con lo dispuesto en la norma ISO/CEI 7816-4.

Por medio del comando INTERNAL AUTHENTICATE, el IFD puede autentificar la tarjeta.

El proceso de autentificación se describe en el apéndice 11 e incluye las afirmaciones siguientes:

TCS_350 El comando INTERNAL AUTHENTICATE utiliza la clave privada de la tarjeta (seleccionada implícitamente) para firmar datos de autentificación, incluidos K1 (el primer elemento para acordar la clave de la sesión) y RND1, y utiliza la clave pública actualmente seleccionada (a través del último comando MSE) para cifrar la firma y formar el testigo de autentificación (hallará información más detallada al respecto en el apéndice 11).

TCS_351 Mensaje de comando

Byte	Long.	Valor	Descripción
CLA	1	'00h'	CLA
INS	1	'88h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Lc	1	'10h'	Longitud de los datos enviados a la tarjeta
#6-#13	8	'XX..XXh'	Interrogación empleada para autentificar la tarjeta
#14-#21	8	'XX..XXh'	VU.CHR (véase el apéndice 11)
Le	1	'80h'	Longitud de los datos que se esperan de la tarjeta

TCS_352 Mensaje de respuesta

Byte	Long.	Valor	Descripción
#1-#128	128	'XX..XXh'	Testigo de autentificación de la tarjeta (véase el apéndice 11)
SW	2	'XXXXh'	Palabras de estado (SW1, SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '9000'.

— Si no hay una clave pública presente en el entorno de seguridad, se contesta con el estado de procesado '6A88'.

— Si no hay una clave privada presente en el entorno de seguridad, se contesta con el estado de procesado '6A88'.

— Si VU.CHR no coincide con el identificador actual de clave pública, se contesta con el estado de procesado '6A88'.

— Si se considera que la clave privada seleccionada está dañada, se contesta con el estado de procesado '6400' o '6581'.

TCS_353 Si el comando INTERNAL AUTHENTICATE se ejecuta correctamente, la clave de la sesión actual, si la hay, se borra y deja de estar disponible. Para disponer de una nueva clave de sesión, es preciso que el comando EXTERNAL_ AUTHENTICATE se ejecute correctamente.

3.6.9. ***External Authenticate (autentificación externa)***

Este comando cumple con lo dispuesto en la norma ISO/CEI 7816-4.

Por medio del comando EXTERNAL AUTHENTICATE, la tarjeta puede autentificar el IFD.

El proceso de autentificación se describe en el apéndice 11, e incluye las siguientes afirmaciones:

TCS_354 El comando EXTERNAL AUTHENTICATE debe ir inmediatamente precedido por un comando GET CHALLENGE. La tarjeta envía un interrogación al exterior (RND3).

TCS_355 La verificación del criptograma utiliza RND3 (interrogación enviada por la tarjeta), la clave privada de la tarjeta (seleccionada implícitamente) y la clave pública previamente seleccionada por el comando MSE.

TCS_356 La tarjeta verifica el criptograma y, en caso de ser correcto, se abre la condición de acceso AUT.

TCS_357 El criptograma de entrada incluye K2, el segundo elemento para acordar la clave de la sesión.

TCS_358 Mensaje de comando

Byte	Long.	Valor	Descripción
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (la clave pública que se va a utilizar se conoce implícitamente, y la ha determinado previamente el comando MSE)
Lc	1	'80h'	Lc (Longitud de los datos enviados a la tarjeta)
#6-#133	128	'XX..XXh'	Criptograma (véase el apéndice 11)

TCS_359 Mensaje de respuesta

Byte	Long.	Valor	Descripción
SW	2	'XXXXh'	Palabras de estado [Palabras de estado (SW1, SW2)]

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '9000'.

— Si no hay una clave pública presente en el entorno de seguridad, se devuelve '6A88'.

— Si el CHA de la clave pública actualmente configurada no es la concatenación del AID de la aplicación de tacógrafo y de un tipo de equipo VU, se contesta con el estado de procesado '6F00' (véase el apéndice 11).

— Si no hay una clave privada presente en el entorno de seguridad, se contesta con el estado de procesado '6A88'.

— Si la verificación del criptograma es incorrecta, se contesta con el estado de procesado '6688'.

— Si el comando no va precedido inmediatamente de un comando GET CHALLENGE, se contesta con el estado de procesado '6985'.

— Si se considera que la clave privada seleccionada está dañada, se contesta con el estado de procesado '6400' o '6581'.

TCS_360 Si el comando EXTERNAL AUTHENTICATE se ejecuta correctamente, y si la primera parte de la clave de sesión está disponible a partir de un comando INTERNAL AUTHENTICATE que se haya ejecutado recientemente, la clave de sesión queda configurada para futuros comandos que utilicen mensajería segura.

TCS_361 Si la primera parte de la clave de sesión no está disponible a partir de un comando INTERNAL AUTHENTICATE anterior, la segunda parte de la clave de sesión, enviada por el IFD, no se almacena en la tarjeta. Este mecanismo garantiza que el proceso de autentificación mutua se lleva a cabo en el orden especificado en el apéndice 11.

3.6.10. ***Manage Security Environment (gestión del entorno de seguridad)***

Este comando se utiliza para determinar una clave pública con fines de autentificación.

Este comando cumple con lo dispuesto en la norma ISO/CEI 7816-8, pero tiene un uso restringido en relación con dicha norma.

TCS_362 La clave a que se hace referencia en el campo de datos MSE es válida para todos los archivos del DF Tacógrafo.

TCS_363 La clave a que se hace referencia en el campo de datos MSE sigue siendo la clave pública actual hasta el siguiente comando MSE correcto.

TCS_364 Si la clave a que se hace referencia no está (ya) presente en la tarjeta, el entorno de seguridad no experimenta cambio alguno.

TCS_365 Mensaje de comando

Byte	Long.	Valor	Descripción
CLA	1	'00h'	CLA
INS	1	'22h'	INS
P1	1	'C1h'	P1: clave a que se hace referencia, válida para todas las operaciones criptográficas
P2	1	'B6h'	P2 (datos a que se hace referencia, relativos a la firma digital)
Lc	1	'0Ah'	Lc: longitud del campo de datos subsiguiente
#6	1	'83h'	Etiqueta para hacer referencia a una clave pública en casos asimétricos
#7	1	'08h'	Longitud de la referencia de la clave (identificador de clave)
#8-#15	08h	'XX..XXh'	Identificador de clave según se especifica en el apéndice 11

TCS_366 Mensaje de respuesta

Byte	Long.	Valor	Descripción
SW	2	'XXXXh'	Palabras de estado (SW1, SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '9000'.

— Si la clave a que se hace referencia no está presente en la tarjeta, se contesta con el estado de procesado '6A88'.

— Si en el formato de mensajería segura faltan algunos de los objetos de datos que se esperaban, se devuelve el estado de procesado '6987'. Esto puede ocurrir si falta la etiqueta '83h'.

— Si algunos objetos de datos son incorrectos, se contesta con el estado de procesado '6988'. Esto puede ocurrir si la longitud del identificador de clave no es '08h'.

— Si se considera que la clave seleccionada está dañada, se contesta con el estado de procesado '6400' o '6581'.

3.6.11. ***PSO: Hash (realizar operación de seguridad: comprobación aleatoria)***

Este comando sirve para transferir a la tarjeta el resultado de un cálculo de comprobación aleatoria con unos datos determinados. Este comando se utiliza para la verificación de firmas digitales. El valor de comprobación aleatoria se almacena en la memoria EEPROM para el comando verificación de firma numérica subsiguiente.

Este comando cumple con lo dispuesto en la norma ISO/CEI 7816-8, pero tiene un uso restringido en relación con dicha norma.

TCS_367 Mensaje de comando

Byte	Longitud	Valor	Descripción
CLA	1	'00h'	CLA
INS	1	'2Ah'	Realizar operación de seguridad
P1	1	'90h'	Devolver código de comprobación aleatoria
P2	1	'A0h'	Etiqueta: campo de datos contiene DOs relevantes para comprobación aleatoria
Lc	1	'16h'	Longitud Lc del campo de datos subsiguiente
#6	1	'90h'	Etiqueta para el código de comprobación aleatoria
#7	1	'14h'	Longitud del código de comprobación aleatoria
#8-#27	20	'XX..XXh'	Código de comprobación aleatoria

TCS_368 Mensaje de respuesta

Byte	Longitud	Valor	Descripción
SW	2	'XXXXh'	Palabras de estado (SW1, SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '9000'.

— Si faltan algunos de los objetos de datos que se esperaban (anteriormente especificados), se devuelve el estado de procesado '6987' Esto puede ocurrir si falta una de las etiquetas '90h'.

— Si algunos objetos de datos son incorrectos, se contesta con el estado de procesado '6988'. Este error ocurre si la etiqueta necesaria está presente pero su longitud es distinta de '14h'.

3.6.12. ***Perform Hash of File (realizar comprobación aleatoria de archivo)***

Este comando no cumple la norma ISO/CEI 7816-8. Por consiguiente, el byte CLA de este comando indica que hay un uso propio del comando PERFORM SECURITY OPERATION/HASH.

TCS_369 El comando PERFORM HASH OF FILE sirve para realizar una comprobación aleatoria en la zona de datos del EF transparente actualmente seleccionado.

TCS_370 El resultado de la operación de comprobación aleatoria se almacena en la tarjeta y posteriormente se puede utilizar para obtener una firma digital del archivo, mediante el comando PSO: COMPUTE DIGITAL SIGNATURE. Este resultado sigue disponible para el comando COMPUTE DIGITAL SIGNATURE hasta el siguiente comando PERFORM HASH OF FILE que se ejecute correctamente.

TCS_371 Mensaje de comando

Byte	Long.	Valor	Descripción
CLA	1	'80h'	CLA
INS	1	'2Ah'	Realizar operación de seguridad
P1	1	'90h'	Etiqueta: Hash
P2	1	'00h'	P2: Comprobación aleatoria de los datos del archivo transparente actualmente seleccionado

TCS_372 Mensaje de respuesta

Byte	Long.	Valor	Descripción
SW	2	'XXXXh'	Palabras de estado (SW1, SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '9000'.

— Si no se ha seleccionado una aplicación, se devuelve el estado de procesado '6985'.

— Si se considera que el EF seleccionado está dañado (errores de integridad en los atributos del archivo o los datos almacenados), se contesta con el estado de procesado '6400' o '6581'.

— Si el archivo seleccionado no es transparente, se contesta con el estado de procesado '6986'.

3.6.13. ***PSO: Compute Digital Signature (realizar operación de seguridad: calcular firma digital)***

Este comando sirve para calcular la firma digital de un código de comprobación aleatoria calculado previamente (véase Perform Hash of File, apartado 3.6.12).

Este comando cumple con lo dispuesto en la norma ISO/CEI 7816-8, pero tiene un uso restringido en relación con dicha norma.

TCS_373 La tarjeta conoce implícitamente su clave privada, que se utiliza para calcular la firma digital.

TCS_374 La tarjeta realiza una firma digital utilizando un método de relleno conforme a la norma PKCS1 (hallará más información en el apéndice 11).

TCS_375 Mensaje de comando

Byte	Long.	Valor	Descripción
CLA	1	'00h'	CLA
INS	1	'2Ah'	Realizar operación de seguridad
P1	1	'9Eh'	Firma digital que se ha de devolver
P2	1	'9Ah'	Etiqueta: el campo de datos contiene los datos que se han de firmar. Como se incluye ningún campo de datos, se supone que los datos ya están presentes en la tarjeta (comprobación aleatoria del archivo)
Le	1	'80h'	Longitud de la firma esperada

TCS_376 Mensaje de respuesta

Byte	Long.	Valor	Descripción
#1-#128	128	'XX..XXh'	Firma de la comprobación aleatoria calculada previamente
SW	2	'XXXXh'	Palabras de estado (SW1, SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '9000'.

— Si se considera que la clave privada seleccionada implícitamente está dañada, se contesta con el estado de procesado '6400' o '6581'.

3.6.14. ***PSO: Verify Digital Signature (realizar operación de seguridad: verificar firma digital)***

Este comando sirve para verificar la firma digital, disponible como entrada, de acuerdo con la norma PKCS1, de un mensaje cuya comprobación aleatoria conoce la tarjeta. La tarjeta conoce implícitamete el algoritmo de la firma.

Este comando cumple con lo dispuesto en la norma ISO/CEI 7816-8, pero tiene un uso restringido en relación con dicha norma.

TCS_377 El comando VERIFY DIGITAL SIGNATURE utiliza siempre la clave pública seleccionada por el anterior comando MANAGE SECURITY ENVIRONMENT, y el anterior código de comprobación aleatoria introducido por un comando PSO: HASH.

TCS_378 Mensaje de comando

Byte	Longitud	Valor	Descripción
CLA	1	'00h'	CLA
INS	1	'2Ah'	Realizar operación de seguridad
P1	1	'00h'	
P2	1	'A8h'	Etiqueta: el campo de datos contiene DOs relevantes para verificación
Lc	1	'83h'	Longitud Lc del campo de datos subsiguiente
#28	1	'9Eh'	Etiqueta para firma digital
#29-#30	2	'8180h'	Longitud de la firma digital (128 bytes, codificados según la norma ISO/CEI 7816-6)
#31-#158	128	'XX..XXh'	Contenido de la firma digital

TCS_379 Mensaje de respuesta

Byte	Longitud	Valor	Descripción
SW	2	'XXXXh'	Palabras de estado (SW1, SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '9000'.

— Si la verificación de la firma falla, se contesta con el estado de procesado '6688'. El proceso de verificación se describe en el apéndice 11.

— Si no se selecciona una clave pública, se contesta con el estado de procesado '6A88'.

— Si faltan algunos de los objetos de datos que se esperaban (anteriormente especificados), se devuelve el estado de procesado '6987'. Esto puede ocurrir si falta una de las etiquetas necesarias.

— Si no hay disponible un código de comprobación aleatoria para procesar el comando (como resultado de un comando anterior PSO: HASH), se contesta con el estado de procesado '6985'.

— Si algunos de los objetos de datos son incorrectos, se contesta con el estado de procesado '6988'. Esto puede ocurrir si la longitud de uno de los objetos de datos necesarios es incorrecta.

— Si se considera que la clave pública seleccionada está dañada, se contesta con el estado de procesado '6400' o '6581'.

4. ESTRUCTURA DE LAS TARJETAS DE TACÓGRAFO

El presente apartado especifica las estructuras de archivos de las tarjetas de tacógrafo para el almacenamiento de datos accesibles.

No se especifican las estructuras internas que dependen del fabricante de la tarjeta, como por ejemplo las cabeceras de archivos, ni el almacenamiento y la manipulación de elementos de datos necesarios para uso interno excluisvamente, como `EuropeanPublicKey`, `CardPrivateKey`, `TDesSessionKey` o bien `WorkshopCardPin`.

La capacidad útil de almacenamiento de una tarjeta de tacógrafo será de 11 kbytes como mínimo. También podrán utilizarse capacidades mayores, en cuyo caso la estructura de la tarjeta será la misma, aunque aumentará el número de registros de ciertos elementos. El presente apartado especifica los valores máximo y mínimo de dichos números de registro.

4.1. **Estructura de la tarjeta de conductor**

TCS_400 Una vez personalizada la tarjeta de conductor, su estructura permanente de archivos y las condiciones de acceso a dichos archivos serán las siguientes:

Archivo	ID Archivo	Condiciones de acceso		
		Lectura	Actualización	Cifrado
MF	3F00			
├─EF ICC	0002	ALW	NEV	No
├─EF IC	0005	ALW	NEV	No
└─DF Tachograph	0500			
├─EF Application_Identification	0501	ALW	NEV	No
├─EF Card_Certificate	C100	ALW	NEV	No
├─EF CA_Certificate	C108	ALW	NEV	No
├─EF Identification	0520	ALW	NEV	No
├─EF Card_Download	050E	ALW	ALW	No
├─EF Driving_Licence_Info	0521	ALW	NEV	No
├─EF Events_Data	0502	ALW	PRO SM / AUT	No
├─EF Faults_Data	0503	ALW	PRO SM / AUT	No
├─EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	No
├─EF Vehicles_Used	0505	ALW	PRO SM / AUT	No
├─EF Places	0506	ALW	PRO SM / AUT	No
├─EF Current_Usage	0507	ALW	PRO SM / AUT	No
├─EF Control_Activity_Data	0508	ALW	PRO SM / AUT	No
└─EF Specific_Conditions	0522	ALW	PRO SM / AUT	No

TCS_401 La estructura de todos los EF deberá ser transparente.

TCS_402 La lectura con mensajería segura deberá ser posible para todos los archivos del DF Tacógrafo.

TCS_403 La tarjeta de conductor deberá tener la siguiente estructura de datos:

Archivo/Elemento de datos	Nº de registros	Tamaño (bytes) Mín.	Tamaño (bytes) Max.	Valores por defecto
MF		*11411*	*24959*	
╠EF ICC		*25*	*25*	
└CardIccIdentification		*25*	*25*	
├clockStop		1	1	{00}
├cardExtendedSerialNumber		8	8	{00..00}
├cardApprovalNumber		8	8	{20..20}
├cardPersonaliserID		1	1	{00}
├embedderIcAssemblerId		5	5	{00..00}
└icIdentifier		2	2	{00 00}
╠EF IC		*8*	*8*	
└CardChipIdentification		*8*	*8*	
├icSerialNumber		4	4	{00..00}
└icManufacturingReferences		4	4	{00..00}
╚DF Tachograph		*11378*	*24926*	
╠EF Application_Identification		*10*	*10*	
└DriverCardApplicationIdentification		*10*	*10*	
├typeOfTachographCardId		1	1	{00}
├cardStructureVersion		2	2	{00 00}
├noOfEventsPerType		1	1	{00}
├noOfFaultsPerType		1	1	{00}
├activityStructureLength		2	2	{00 00}
├noOfCardVehicleRecords		2	2	{00 00}
└noOfCardPlaceRecords		1	1	{00}
╠EF Card_Certificate		*194*	*194*	
└CardCertificate		194	194	{00..00}
╠EF CA_Certificate		*194*	*194*	
└MemberStateCertificate		194	194	{00..00}
╠EF Identification		*143*	*143*	
├CardIdentification		*65*	*65*	
├cardIssuingMemberState		1	1	{00}
├cardNumber		16	16	{20..20}
├cardIssuingAuthorityName		36	36	{20..20}
├cardIssueDate		4	4	{00..00}
├cardValidityBegin		4	4	{00..00}
└cardExpiryDate		4	4	{00..00}
└DriverCardHolderIdentification		*78*	*78*	
├cardHolderName		*72*	*72*	
├holderSurname		36	36	{00, 20..20}
└holderFirstNames		36	36	{00, 20..20}
├cardHolderBirthDate		4	4	{00..00}
└cardHolderPreferredLanguage		2	2	{20 20}

EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*864*	*1728*	
CardEventData		*864*	*1728*	
cardEventRecords	6	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
CardDriverActivity		*5548*	*13780*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*2606*	*6202*	
CardVehiclesUsed		*2606*	*6202*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*2604*	*6200*	
CardVehicleRecord	n_3	*31*	*31*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
EF Places		*841*	*1121*	
CardPlaceDailyWorkPeriod		*841*	*1121*	
placePointerNewestRecord		1	1	{00}
placeRecords		*840*	*1120*	
PlaceRecord	n_4	*10*	*10*	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
CardCurrentUse		*19*	*19*	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*280*	*280*	
SpecificConditionRecord	56	*5*	*5*	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

TCS_404 Los valores siguientes, empleados para indicar tamaños en la tabla anterior, son los valores máximo y mínimo que la estructura de datos de la tarjeta de conductor debe utilizar para los números de registro:

		Mín.	Máx.
n_1	NoOfEventsPerType	**6**	12
n_2	NoOfFaultsPerType	**12**	24
n_3	NoOfCardVehicleRecords	**84**	200
n_4	NoOfCardPlaceRecords	**84**	112
n_6	CardActivityLengthRange	5544 bytes (28 días * 93 cambios de actividad)	13776 bytes (28 días * 240 cambios de actividad)

4.2. **Estructura de la tarjeta del centro de ensayo**

TCS_405 Una vez personalizada la tarjeta del centro de ensayo, su estructura permanente de archivos y las condiciones de acceso a dichos archivos serán las siguientes:

		Condiciones de acceso		
Archivo	ID Archivo	Lectura	Actualización	Cifrado
MF	3F00			
├─EF ICC	0002	ALW	NEV	No
├─EF IC	0005	ALW	NEV	No
└─DF Tachograph	0500			
├─EF Application_Identification	0501	ALW	NEV	No
├─EF Card_Certificate	C100	ALW	NEV	No
├─EF CA_Certificate	C108	ALW	NEV	No
├─EF Identification	0520	ALW	NEV	No
├─EF Card_Download	0509	ALW	ALW	No
├─EF Calibration	050A	ALW	PRO SM / AUT	No
├─EF Sensor_Installation_Data	050B	ALW	NEV	Sí
├─EF Events_Data	0502	ALW	PRO SM / AUT	No
├─EF Faults_Data	0503	ALW	PRO SM / AUT	No
├─EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	No
├─EF Vehicles_Used	0505	ALW	PRO SM / AUT	No
├─EF Places	0506	ALW	PRO SM / AUT	No
├─EF Current_Usage	0507	ALW	PRO SM / AUT	No
├─EF Control_Activity_Data	0508	ALW	PRO SM / AUT	No
└─EF Specific_Conditions	0522	ALW	PRO SM / AUT	No

TCS_406 La estructura de todos los EF deberá ser transparente.

TCS_407 La lectura con mensajería segura deberá ser posible para todos los archivos del DF Tacógrafo.

TCS_408 La tarjeta del centro de ensayo deberá tener la siguiente estructura de datos:

Archivo/Elemento de datos	Nº de registros	Tamaño (Bytes) Mín.	Tamaño (Bytes) Máx.	Valores por defecto
MF		*11088*	*29061*	
╠═EF ICC		*25*	*25*	
╚═CardIccIdentification		*25*	*25*	
├─clockStop		1	1	{00}
├─cardExtendedSerialNumber		8	8	{00..00}
├─cardApprovalNumber		8	8	{20..20}
├─cardPersonaliserID		1	1	{00}
├─embedderIcAssemblerId		5	5	{00..00}
└─icIdentifier		2	2	{00 00}
╠═EF IC		*8*	*8*	
╚═CardChipIdentification		*8*	*8*	
├─icSerialNumber		4	4	{00..00}
└─icManufacturingReferences		4	4	{00..00}
╚═DF Tachograph		*11055*	*29028*	
╠═EF Application_Identification		*11*	*11*	
╚═WorkshopCardApplicationIdentification		*11*	*11*	
├─typeOfTachographCardId		1	1	{00}
├─cardStructureVersion		2	2	{00 00}
├─noOfEventsPerType		1	1	{00}
├─noOfFaultsPerType		1	1	{00}
├─activityStructureLength		2	2	{00 00}
├─noOfCardVehicleRecords		2	2	{00 00}
├─noOfCardPlaceRecords		1	1	{00}
└─noOfCalibrationRecords		1	1	{00}

EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*9243*	*26778*	
WorkshopCardCalibrationData		*9243*	*26778*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		1	1	{00}
calibrationRecords		*9240*	*26775*	
WorkshopCardCalibrationRecord	n_5	*105*	*105*	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}
oldTimeValue		4	4	{00..00}
newTimeValue		4	4	{00..00}
nextCalibrationDate		4	4	{00..00}
vuPartNumber		16	16	{20..20}
vuSerialNumber		8	8	{00..00}
sensorSerialNumber		8	8	{00..00}
EF Sensor_Installation_Data		*16*	*16*	
SensorInstallationSecData		16	16	{00..00}
EF Events_Data		*432*	*432*	
CardEventData		*432*	*432*	
cardEventRecords	6	*72*	*72*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
CardFaultData		*288*	*288*	
cardFaultRecords	2	*144*	*144*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
CardDriverActivity		*202*	*496*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*126*	*250*	
CardVehiclesUsed		*126*	*250*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*124*	*248*	
CardVehicleRecord	n_3	*31*	*31*	
vehicleOdometerBegin		3	3	{00..00}

├─vehicleOdometerEnd		3	3	{00..00}
├─vehicleFirstUse		4	4	{00..00}
├─vehicleLastUse		4	4	{00..00}
├─vehicleRegistration				
│ ├─vehicleRegistrationNation		1	1	{00}
│ └─vehicleRegistrationNumber		14	14	{00, 20..20}
└─vuDataBlockCounter		2	2	{00 00}
═EF Places		*61*	*81*	
└─CardPlaceDailyWorkPeriod		*61*	*81*	
├─placePointerNewestRecord		1	1	{00}
└─placeRecords		*60*	*80*	
└─PlaceRecord	n_4	*10*	*10*	
├─entryTime		4	4	{00..00}
├─entryTypeDailyWorkPeriod		1	1	{00}
├─dailyWorkPeriodCountry		1	1	{00}
├─dailyWorkPeriodRegion		1	1	{00}
└─vehicleOdometerValue		3	3	{00..00}
═EF Current_Usage		*19*	*19*	
└─CardCurrentUse		*19*	*19*	
├─sessionOpenTime		4	4	{00..00}
└─sessionOpenVehicle				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
═EF Control_Activity_Data		*46*	*46*	
└─CardControlActivityDataRecord		*46*	*46*	
├─controlType		1	1	{00}
├─controlTime		4	4	{00..00}
├─controlCardNumber				
│ ├─cardType		1	1	{00}
│ ├─cardIssuingMemberState		1	1	{00}
│ └─cardNumber		16	16	{20..20}
├─controlVehicleRegistration				
│ ├─vehicleRegistrationNation		1	1	{00}
│ └─vehicleRegistrationNumber		14	14	{00, 20..20}
├─controlDownloadPeriodBegin		4	4	{00..00}
└─controlDownloadPeriodEnd		4	4	{00..00}
═EF Specific_Conditions		*10*	*10*	
└─SpecificConditionRecord	2	*5*	*5*	
├─entryTime		4	4	{00..00}
└─SpecificConditionType		1	1	{00}

TCS_409 Los valores siguientes, empleados para indicar tamaños en la tabla anterior, son los valores máximo y mínimo que la estructura de datos de la tarjeta del centro de ensayo debe utilizar para los números de registro:

		Mín.	Máx.
n_1	NoOfEventsPerType	**3**	3
n_2	NoOfFaultsPerType	**6**	6
n_3	NoOfCardVehicleRecords	**4**	8
n_4	NoOfCardPlaceRecords	**6**	8
n_6	CardActivityLengthRange	88	255
n_5	NoOfCalibrationRecords	198 bytes (1 día * 93 cambios de actividad)	492 bytes (1 día * 240 cambios de actividad)

4.3. **Estructura de la tarjeta de control**

TCS_410 Una vez personalizada la tarjeta de control, su estructura permanente de archivos y las condiciones de acceso a dichos archivos serán las siguientes:

		Condiciones de acceso		
Archivo	ID Archivo	Lectura	Actualización	Cifrado
MF	3F00			
├─EF ICC	0002	ALW	NEV	No
├─EF IC	0005	ALW	NEV	No
└─DF Tachograph	0500			
├─EF Application_Identification	0501	ALW	NEV	No
├─EF Card_Certificate	C100	ALW	NEV	No
├─EF CA_Certificate	C108	ALW	NEV	No
├─EF Identification	0520	AUT	NEV	No
└─EF Controller_Activity_Data	050C	ALW	PRO SM / AUT	No

TCS_411 La estructura de todos los EF deberá ser transparente.

TCS_412 La lectura con mensajería segura deberá ser posible para los archivos del DF Tacógrafo.

TCS_413 La tarjeta de control deberá tener la siguiente estructura de datos:

Archivo/Elemento de datos	Nº de registros	Tamaño (Bytes) Mín.	Tamaño (Bytes) Máx.	Valores por defecto
MF		*11219*	*24559*	
╠EF ICC		*25*	*25*	
╚CardIccIdentification		*25*	*25*	
├clockStop		1	1	{00}
├cardExtendedSerialNumber		8	8	{00..00}
├cardApprovalNumber		8	8	{20..20}
├cardPersonaliserID		1	1	{00}
├embedderIcAssemblerId		5	5	{00..00}
└icIdentifier		2	2	{00 00}
╠EF IC		*8*	*8*	
╚CardChipIdentification		*8*	*8*	
├icSerialNumber		4	4	{00..00}
└icManufacturingReferences		4	4	{00..00}
╠DF Tachograph		*11186*	*24526*	
╠EF Application_Identification		*5*	*5*	
╚ControlCardApplicationIdentification		*5*	*5*	
├typeOfTachographCardId		1	1	{00}
├cardStructureVersion		2	2	{00 00}
└noOfControlActivityRecords		2	2	{00 00}
╠EF Card_Certificate		*194*	*194*	
╚CardCertificate		194	194	{00..00}
╠EF CA_Certificate		*194*	*194*	
╚MemberStateCertificate		194	194	{00..00}
╠EF Identification		*211*	*211*	
├CardIdentification		*65*	*65*	
├cardIssuingMemberState		1	1	{00}
├cardNumber		16	16	{20..20}
├cardIssuingAuthorityName		36	36	{00, 20..20}
├cardIssueDate		4	4	{00..00}
├cardValidityBegin		4	4	{00..00}
└cardExpiryDate		4	4	{00..00}
└ControlCardHolderIdentification		*146*	*146*	
├controlBodyName		36	36	{00, 20..20}
├controlBodyAddress		36	36	{00, 20..20}
├cardHolderName				
├holderSurname		36	36	{00, 20..20}
└holderFirstNames		36	36	{00, 20..20}
└cardHolderPreferredLanguage		2	2	{20 20}
╠EF Controller_Activity_Data		*10582*	*23922*	
└ControlCardControlActivityData		*10582*	*23922*	
├controlPointerNewestRecord		2	2	{00 00}
└controlActivityRecords		*10580*	*23920*	
└controlActivityRecord	n_7	*46*	*46*	
├controlType		1	1	{00}
├controlTime		4	4	{00..00}
├controlledCardNumber				
├cardType		1	1	{00}
├cardIssuingMemberState		1	1	{00}
└cardNumber		16	16	{20..20}
├controlledVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├controlDownloadPeriodBegin		4	4	{00..00}
└controlDownloadPeriodEnd		4	4	{00..00}

TCS_414 Los valores siguientes, empleados para indicar tamaños en la tabla anterior, son los valores máximo y mínimo que la estructura de datos de la tarjeta de control debe utilizar para los números de registro:

		Mín.	Máx.
n_7	NoOfControlActivityRecords	230	520

4.4. **Estructura de la tarjeta de empresa**

TCS_415 Una vez personalizada la tarjeta de empresa, su estructura permanente de archivos y las condiciones de acceso a dichos archivos serán las siguientes:

		Condiciones de acceso		
Archivo	ID Archivo	Lectura	Actualización	Cifrado
MF	3F00			
├─EF ICC	0002	ALW	NEV	No
├─EF IC	0005	ALW	NEV	No
└─DF Tachograph	0500			
├─EF Application_Identification	0501	ALW	NEV	No
├─EF Card_Certificate	C100	ALW	NEV	No
├─EF CA_Certificate	C108	ALW	NEV	No
├─EF Identification	0520	AUT	NEV	No
└─EF Company_Activity_Data	050D	ALW	PRO SM / AUT	No

TCS_416 La estructura de todos los EF deberá ser transparente.

TCS_417 La lectura con mensajería segura deberá ser posible para todos los archivos del DF Tacógrafo.

TCS_418 La tarjeta de empresa deberá tener la siguiente estructura de datos:

Archivo/Elemento de datos	Nº de registros	Tamaño (Bytes) Mín.	Tamaño (Bytes) Máx.	Valores por defecto
MF		*11147*	*24487*	
╠═EF ICC		*25*	*25*	
╚═CardIccIdentification		*25*	*25*	
├─clockStop		1	1	{00}
├─cardExtendedSerialNumber		8	8	{00..00}
├─cardApprovalNumber		8	8	{20..20}
├─cardPersonaliserID		1	1	{00}
├─embedderIcAssemblerId		5	5	{00..00}
└─icIdentifier		2	2	{00 00}
╠═EF IC		*8*	*8*	
╚═CardChipIdentification		*8*	*8*	
├─icSerialNumber		4	4	{00..00}
└─icManufacturingReferences		4	4	{00..00}
╚═DF Tachograph		*11114*	*24454*	
╠═EF Application_Identification		*5*	*5*	
╚═CompanyCardApplicationIdentification		*5*	*5*	
├─typeOfTachographCardId		1	1	{00}
├─cardStructureVersion		2	2	{00 00}
└─noOfCompanyActivityRecords		2	2	{00 00}
╠═EF Card_Certificate		*194*	*194*	
╚═CardCertificate		194	194	{00..00}
╠═EF CA_Certificate		*194*	*194*	
╚═MemberStateCertificate		194	194	{00..00}
╠═EF Identification		*139*	*139*	
├─CardIdentification		*65*	*65*	
├─cardIssuingMemberState		1	1	{00}
├─cardNumber		16	16	{20..20}
├─cardIssuingAuthorityName		36	36	{00, 20..20}
├─cardIssueDate		4	4	{00..00}
├─cardValidityBegin		4	4	{00..00}
└─cardExpiryDate		4	4	{00..00}
└─CompanyCardHolderIdentification		*74*	*74*	
├─companyName		36	36	{00, 20..20}
├─companyAddress		36	36	{00, 20..20}
└─cardHolderPreferredLanguage		2	2	{20 20}
╚═EF Company_Activity_Data		*10582*	*23922*	
└─CompanyActivityData		*10582*	*23922*	
├─companyPointerNewestRecord		2	2	{00 00}
└─companyActivityRecords		*10580*	*23920*	
└─companyActivityRecord	n_8	46	46	
├─companyActivityType		1	1	{00}
├─companyActivityTime		4	4	{00..00}
├─cardNumberInformation				
├─cardType		1	1	{00}
├─cardIssuingMemberState		1	1	{00}
└─cardNumber		16	16	{20..20}
├─vehicleRegistrationInformation				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}

├─cardNumberInformation			
│ ├─cardType	1	1	{00}
│ ├─cardIssuingMemberState	1	1	{00}
│ └─cardNumber	16	16	{20..20}
├─downloadPeriodBegin	4	4	{00..00}
└─downloadPeriodEnd	4	4	{00..00}

TCS_419 Los valores siguientes, empleados para indicar tamaños en la tabla anterior, son los valores máximo y mínimo que la estructura de datos de la tarjeta de empresa debe utilizar para los números de registro:

		Mín.	Máx.
n8	NoOfCompanyActivityRecords	230	520

Apéndice 3

PICTOGRAMAS

PIC_001 El aparato de control podrá utilizar los siguientes pictogramas y combinaciones de pictogramas:

1. PICTOGRAMAS BÁSICOS

	Personas	**Acciones**	**Modos de funcionamiento**
	Empresa		Modo de empresa
	Controlador	Control	Modo de control
	Conductor	Conducción	Modo operativo
	Taller/centro de ensayo	Inspección/calibrado	Modo de calibrado
	Fabricante		

	Actividades	**Duración**
	Disponible	Período de disponibilidad actual
	Conducción	Tiempo de conducción continua
	Descanso	Período de descanso actual
	Trabajo	Período de trabajo actual
	Pausa	Tiempo de pausa acumulado
	Indeterminado	

	Aparato	**Funciones**
	Ranura del conductor	
	Ranura del segundo conductor	
	Tarjeta	
	Reloj	
	Pantalla	Visualización
	Almacenamiento externo	Transferencia
	Fuente de alimentación	
	Impresora/doc. impreso	Impresión
	Sensor	
	Tamaño de los neumáticos	
	Vehículo/unidad intravehicular	

	Condiciones específicas
	Fuera de ámbito
	Puente/paso a nivel

	Diversos		
	Incidentes		Fallos
	Comienzo del período de trabajo diario		Final del período de trabajo diario
	Lugar		Entrada manual de las actividades del conductor
	Seguridad		Velocidad
	Hora		Total/resumen

	Calificadores
	Diario
	Semanal
	Dos semanas
	Desde o hasta

2. Combinaciones de pictogramas

	Diversos		
	Lugar de control		
	Lugar donde comienza el período de trabajo diario		Lugar donde termina el período de trabajo diario
	Hora de comienzo		Hora de conclusión
	Desde el vehículo		
	Comienzo condición Fuera de ámbito		Final condición Fuera de ámbito

Tarjetas

Tarjeta del conductor
Tarjeta de la empresa
Tarjeta de control
Tarjeta del centro de ensayo
Sin tarjeta

Conducción

Conducción en equipo
Tiempo de conducción en una semana
Tiempo de conducción en dos semanas

Documentos impresos

Impresión diaria de las actividades del conductor almacenadas en la tarjeta
Impresión diaria de las actividades del conductor almacenadas en la VU
Impresión de incidentes y fallos almacenados en la tarjeta
Impresión de incidentes y fallos almacenados en la VU
Impresión de datos técnicos
Impresión por exceso de velocidad

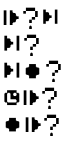
Incidentes

Inserción de una tarjeta no válida
Conflicto de tarjetas
Solapamiento temporal
Conducción sin tarjeta adecuada
Inserción de tarjeta durante la conducción
Error al cerrar la última sesión de la tarjeta
Exceso de velocidad
Interrupción del suministro eléctrico
Error en datos de movimiento
Violación de la seguridad
Ajuste de la hora (por el centro de ensayo)
Control del exceso de velocidad

Fallos

Fallo de tarjeta (ranura del conductor)
Fallo de tarjeta (ranura del segundo conductor)
Fallo de la pantalla
Fallo de transferencia
Fallo de la impresora
Fallo del sensor
Fallo interno de la VU

Procedimiento de entrada manual



¿Continúa el mismo período de trabajo diario?
¿Final del anterior período de trabajo?
Confirme o introduzca el lugar donde termina el período de trabajo
Introduzca la hora de comienzo
Introduzca el lugar donde comienza el período de trabajo.

Nota: En el apéndice 4 se definen otras combinaciones de pictogramas con las que se forman identificadores de bloque o de registro en documentos impresos.

Apéndice 4

DOCUMENTOS IMPRESOS

ÍNDICE

1. GENERALIDADES

Cada documento impreso es una concatenación de varios bloques de datos, posiblemente identificados con un identificador de bloque.

Un bloque de datos contiene uno o más registros, posiblemente identificados con un identificador de registro.

PRT_001 Cuando un identificador de bloque precede inmediatamente a un identificador de registro, el identificador de registro no se imprime.

PRT_002 Cuando una unidad de información se desconoce o no debe imprimirse por motivos relacionados con los derechos de acceso a los datos, en su lugar se imprimen espacios.

PRT_003 Si el contenido de una línea entera es desconocido o no tiene que imprimirse, se omite toda la línea.

PRT_004 Los campos de datos numéricos se imprimen alineados a la derecha, con un espacio como separador de las unidades de millar y de millón, y sin ceros a la izquierda.

PRT_005 Los campos de datos en cadena se imprimen alineados a la izquierda. Cuando es preciso (en nombres y direcciones), se rellenan con espacios hasta alcanzar la longitud de la unidad de información, o bien se truncan para no sobrepasar dicha longitud.

2. ESPECIFICACIÓN DE LOS BLOQUES DE DATOS

En este capítulo se han utilizado las siguientes convenciones para la notación de formatos:

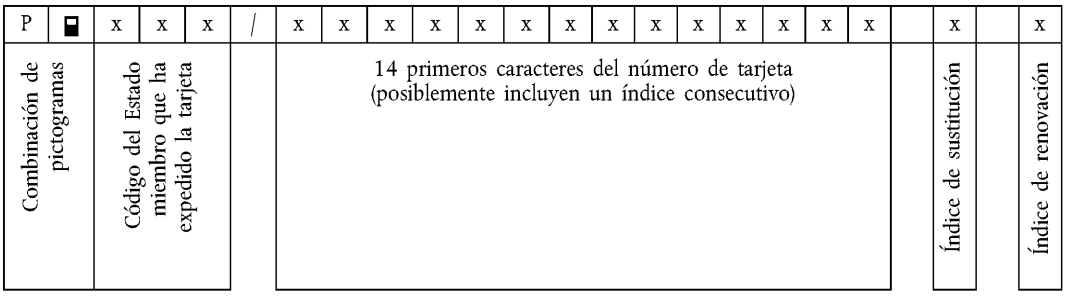
— los caracteres impresos en **negrita** indican texto legible que hay que imprimir (en caracteres normales),

— los caracteres normales indican variables (pictogramas o datos) que hay que sustituir por sus valores antes de proceder a la impresión,

— los nombres de las variables se han acabado de llenar con guiones bajos con el fin de mostrar la longitud disponible para la variable en ese elemento de información,

— las fechas se especifican con el formato “dd/mm/aaaa”" (día, mes, año). También se puede utilizar el formato “dd.mm.aaaa”,

— el término “identificación de la tarjeta” indica la composición de: el tipo de tarjeta (mediante una combinación de pictogramas), el código del Estado miembro que ha expedido la tarjeta, un carácter de barra oblicua y el número de tarjeta con el índice de sustitución y el índice de renovación separados por espacios:



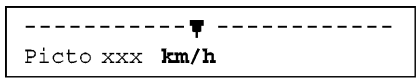
PRT_006 Los documentos impresos deberán utilizar los siguientes bloques de datos o registros de datos, con arreglo a los significados y formatos que se exponen a continuación:

Número de bloque o de registro Significado	Formato de los datos
1 **Fecha y hora en que se imprime el documento**	dd/mm/aaaa hh:mm **(UTC)**

2 **Tipo de documento impreso**

Identificador de bloque

Combinación de pictogramas impresos (véase el apéndice 3), Valor de ajuste del dispositivo limitador de la velocidad (exclusivamente en caso de impresión por exceso de velocidad)



3 **Identificación del titular de la tarjeta**

Identificador de bloque. P = pictograma de persona

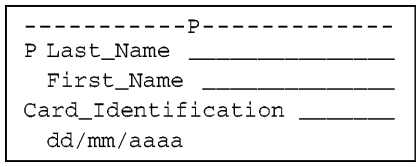
Apellido(s) del titular

Nombre del titular (en su caso)

Identificación de la tarjeta

Fecha de caducidad de la tarjeta (en su caso)

Cuando la tarjeta no sea personal y no especifique los apellidos del titular, en su lugar deberá imprimirse el nombre de la empresa, del centro de ensayo o del organismo de control

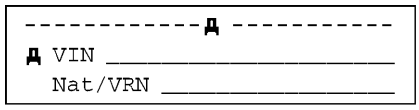


4 **Identificación del vehículo**

Identificador de bloque

Número de bastidor (VIN)

Estado miembro donde se matriculó y número de matrícula (VRN)

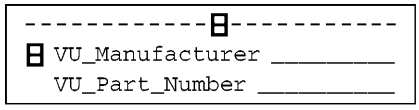


5 **Identificación de la VU**

Identificador de bloque

Nombre del fabricante de la VU

Número de pieza de la VU



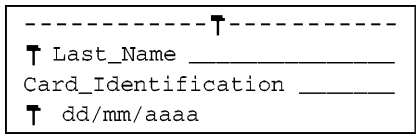
6 **Último calibrado del aparato de control**

Identificador de bloque

Nombre del centro de ensayo

Identificación de la tarjeta del centro de ensayo

Fecha del calibrado



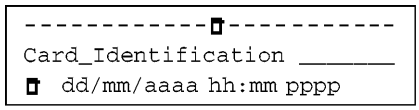
7 **Último control (a cargo de un agente responsable)**

Identificador de bloque

Identificación de la tarjeta del controlador

Fecha, hora y tipo de control

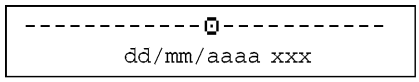
Tipo de control: hasta cuatro pictogramas. El tipo de control puede ser (una combinación de):
: Transferencia de la tarjeta, : Transferencia de la VU, : Impresión, : Visualización



8 **Actividades del conductor almacenadas en una tarjeta en orden de ocurrencia**

Identificador de bloque

Fecha que se consulta (día civil que es objeto de la impresión) + Contador de presencia diaria de la tarjeta



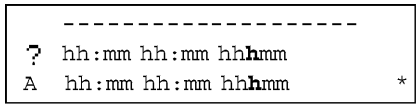
8.1 *Período durante el que no estuvo insertada la tarjeta*

8.1a Identificador de registro (comienzo del período)

8.1b *Período indeterminado*. Hora de comienzo y de final, duración

8.1c *Actividad introducida manualmente*

Pictograma de actividad, hora de comienzo y de final (incluida), duración, los períodos de descanso de al menos una hora se marcan con un asterisco.



8.2 *Inserción de la tarjeta en la ranura S*

Identificador de registro; S = pictograma de la ranura

Estado miembro donde se matriculó el vehículo y número de matrícula (VRN)

Lectura del cuentakilómetros del vehículo al insertar la tarjeta

```
----------S----------
Nat/VRN _______________
x xxx xxx km
```

8.3 *Actividad (mientras estuvo insertada la tarjeta)*

Pictograma de la actividad, hora de comienzo y de final (incluida), duración, régimen de conducción (pictograma de equipo si es EN EQUIPO, espacios en blanco si es EN SOLITARIO), los períodos de descanso de al menos una hora se marcan con un asterisco

```
A hh:mm hh:mm hhhmm OO      *
```

8.3a *Condición específica*. Hora de entrada, pictograma (o combinación de pictogramas) de la condición específica

```
hh:mm ----- pppp -----
```

8.4 *Extracción de la tarjeta*

Lectura del cuentakilómetros y distancia recorrida desde la última inserción para la que se conoce la lectura del cuentakilómetros

```
x xxx xxx km; x xxx km
```

9 **Actividades del conductor almacenadas en una VU por cada ranura y en orden cronológico**

Identificador de bloque

Fecha que se consulta (día civil que es objeto de la impresión)

Lectura del cuentakilómetros del vehículo a las 00:00 y a las 24:00

```
-----------O-----------
        dd/mm/aaaa
x xxx xxx - x xxx xxx km
```

10 **Actividades realizadas en la ranura S**

Identificador de bloque

```
---------- S ---------
```

10.1 *Período en que no hubo ninguna tarjeta insertada en la ranura S*

Identificador de registro

No hay tarjeta insertada

Lectura del cuentakilómetros al comenzar el período

```
--------------------
O --
x xxx xxx km
```

10.2 *Inserción de la tarjeta*

Identificador del registro de inserción de la tarjeta

Apellido(s) del conductor

Nombre del conductor

Identificación de la tarjeta del conductor

Fecha de caducidad de la tarjeta del conductor

Estado miembro donde se matriculó el vehículo utilizado anteriormente y número de matrícula de dicho vehículo

Fecha y hora de extracción de la tarjeta del vehículo anterior

Línea en blanco

Lectura del cuentakilómetros del vehículo al insertar la tarjeta, bandera indicadora de si el conductor ha introducido sus actividades de forma manual (M en caso afirmativo, en blanco en caso negativo)

```
--------------------
O Last_Name _____________
  First_Name _____________
Card_Identification _______
   dd/mm/aaaa
Nat/VRN _______________
   dd/mm/aaaa hh:mm

   x xxx xxx km          M
```

10.3 *Actividad*

Pictograma de la actividad, hora de comienzo y de final (incluida), duración, régimen de conducción (pictograma de equipo si es EN EQUIPO, espacios en blanco si es EN SOLITARIO), los períodos de descanso de al menos una hora se marcan con un asterisco

```
A hh:mm hh:mm hhhmm OO      *
```

10.3a *Condición específica*. Hora de entrada, pictograma (o combinación de pictogramas) de la condición específica

```
hh:mm ----- pppp -----
```

10.4 *Extracción de la tarjeta o Final del período "sin tarjeta"*

Lectura del cuentakilómetros al extraer la tarjeta o al terminar el período "sin tarjeta", y distancia recorrida desde que se insertara la tarjeta o desde que comenzara el período "sin tarjeta"

```
x xxx xxx km; x xxx km
```

11 **Resumen diario**

Identificador de bloque

```
----------Σ ---------
```

11.1 *Resumen VU de períodos sin tarjeta en la ranura del conductor*

Identificador de bloque

```
10■ - - -
```

11.2 *Resumen VU de períodos sin tarjeta en la ranura del segundo conductor*

Identificador de bloque 2

```
20■ - - -
```

11.3 *Resumen diario VU para cada conductor*

Identificador de registro

Apellido(s) del conductor

Nombre del conductor

Identificación de la tarjeta del conductor

```
  --------------------
0 Last_Name ________________
  First_Name ________________
Card_Identification _______
```

11.4 *Entrada del lugar donde comienza o termina un período de trabajo diario*

pi = pictograma del lugar de comienzo/final, hora, país, región,

Lectura del cuentakilómetros

```
pihh:mm  Cou  Reg
  x xxx  xxx  km
```

11.5 *Totales de la actividad (en una tarjeta)*

Tiempo total de conducción, distancia recorrida

Tiempo total de trabajo y de disponibilidad

Tiempo total de descanso e indeterminado

Duración total de las actividades del equipo

```
  0 hhhmm x xxx km
  ⚒ hhhmm ⧈ hhhmm
  ⊢ hhhmm ? hhhmm
00 hhhmm
```

11.6 *Totales de la actividad (períodos sin tarjeta en la ranura del conductor)*

Tiempo total de conducción, distancia recorrida

Tiempo total de trabajo y de disponibilidad

Tiempo total de descanso

```
  0 hhhmm x xxx km
  ⚒ hhhmm ⧈ hhhmm
  ⊢ hhhmm
```

11.7 *Totales de la actividad (períodos sin tarjeta en la ranura del segundo conductor)*

Tiempo total de trabajo y de disponibilidad

Tiempo total de descanso

```
  ⚒ hhhmm ⧈ hhhmm
  ⊢ hhhmm
```

11.8 *Totales de la actividad (para cada conductor, ambas ranuras incluidas)*

Tiempo total de conducción, distancia recorrida

Tiempo total de trabajo y de disponibilidad

Tiempo total de descanso

Duración total de las actividades del equipo

Cuando se precisa un documento impreso con la información de todo el día, la información del resumen diario se computa con los datos disponibles en el momento de imprimir el documento.

```
hhhmm x xxx km
hhhmm hhhmm
hhhmm
hhhmm
```

12 **Incidentes o fallos almacenados en una tarjeta**

12.1 Identificador de bloque para los 5 últimos "Incidentes y fallos" en una tarjeta

```
-------- !x -------- 
```

12.2 Identificador de bloque para todos los "Incidentes" registrados en una tarjeta

```
--------- !---------
```

12.3 Identificador de bloque para todos los "Fallos" registrados en una tarjeta

```
--------- x---------
```

12.4 *Registro de incidente o fallo*

Identificador de registro

Pictograma del incidente/fallo, propósito del registro, fecha y hora de comienzo,

Código del incidente/fallo adicional (en su caso), duración

Estado miembro en que se matriculó el vehículo donde se produjo el incidente o fallo, y número de matrícula de dicho vehículo

```
---------------------
Pic (p)     dd/mm/aaaa hh:mm

!xxx                   hhhmm
Nat/VRN _____
```

13 **Incidentes o fallos almacenados en una VU**

13.1 Identificador de bloque para los 5 últimos "Incidentes y fallos" en la VU

```
-------- !x -------- 
```

13.2 Identificador de bloque para todos los "Incidentes" registrados o en curso en una VU

```
--------- !---------
```

13.3 Identificador de bloque para todos los "Fallos" registrados o en curso en una VU

```
--------- x---------
```

13.4 *Registro de incidente o fallo*

Identificador de registro

Pictograma del incidente/fallo, propósito del registro, fecha y hora de comienzo

Código del incidente/fallo adicional (en su caso), número de incidentes similares ocurridos ese día, duración

Identificación de las tarjetas insertadas al comenzar o terminar el incidente o fallo (hasta 4 líneas sin repetir dos veces los mismos números de tarjeta)

Caso en que no se insertó ninguna tarjeta

El propósito del registro (p) es un código numérico que explica por qué se registró el incidente o fallo, y se codifica con arreglo al elemento de información `EventFaultRecordPurpose`.

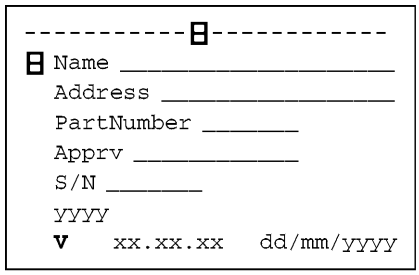
```
---------------------
Pic  (p)  dd/mm/aaaa  hh:mm

!xxx      (xxx)       hhhmm

Card_Identification _______
Card_Identification _______
Card_Identification _______
Card_Identification _______
 ---
```

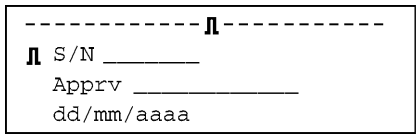
14 **Identificación de la VU**

Identificador de bloque
Nombre del fabricante de la VU
Dirección del fabricante de la VU
Número de pieza de la VU
Número de homologación de la VU
Número de serie de la VU
Año de fabricación de la VU
Versión y fecha de instalación del software de la VU



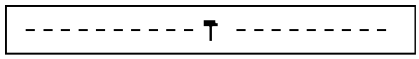
15 **Identificación del sensor**

Identificador de bloque
Número de serie del sensor
Número de homologación del sensor
Fecha de la primera instalación del sensor



16 **Datos de calibrado**

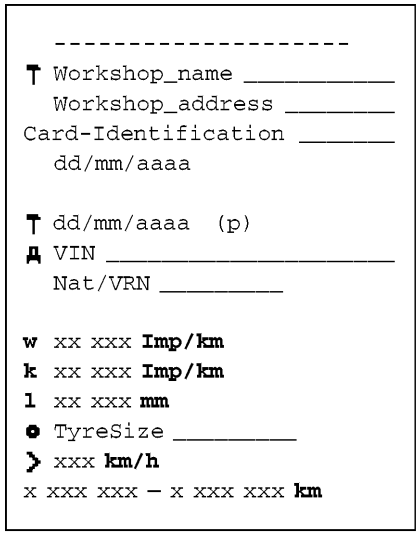
Identificador de bloque



16.1 *Registro de calibrado*

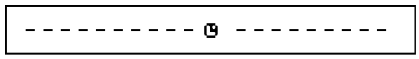
Identificador de registro
Centro de ensayo que haya efectuado el calibrado
Dirección del centro de ensayo
Identificación de la tarjeta del centro de ensayo
Fecha de caducidad de la tarjeta del centro de ensayo
Línea en blanco
Fecha del calibrado + propósito del calibrado
Número de bastidor
Estado miembro donde se matriculó el vehículo y número de matrícula
Coeficiente característico del vehículo
Constante del aparato de control
Circunferencia efectiva de los neumáticos de las ruedas
Tamaño de los neumáticos montados
Valor de ajuste del dispositivo limitador de la velocidad
Lectura anterior y actual del cuentakilómetros

El propósito del calibrado (p) es un código numérico que explica por qué se registraron esos parámetros de calibrado, y se codifica con arreglo al elemento de información `CalibrationPurpose`.



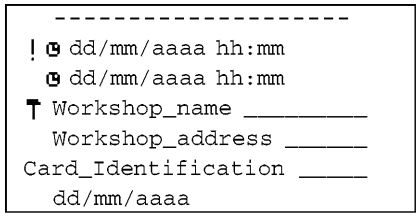
17 **Ajuste de la hora**

Identificador de bloque



17.1 *Registro de ajuste de la hora*

Identificador de registro
Fecha y hora antiguas
Fecha y hora nuevas
Centro de ensayo que ha efectuado el ajuste de la hora
Dirección del centro de ensayo
Identificación de la tarjeta del centro de ensayo
Fecha de caducidad de la tarjeta del centro de ensayo



18 **Incidente y fallo más recientes registrados en la VU**

Identificador de bloque

Fecha y hora del incidente más reciente

Fecha y hora del fallo más reciente

```
---------- ! ✕ ---------
!  dd/mm/aaaa  hh:mm
✕  dd/mm/aaaa  hh:mm
```

19 **Información de control del exceso de velocidad**

Identificador de bloque

Fecha y hora del último CONTROL DEL EXCESO DE VELOCIDAD

Fecha y hora del primer exceso de velocidad y número de incidentes de este tipo que han ocurrido desde entonces

```
----------  ----------
   dd/mm/aaaa  hh:mm
   dd/mm/aaaa  hh:mm (nnn)
```

20 **Registro del exceso de velocidad**

20.1 Identificador de bloque "Primer exceso de velocidad después del último calibrado"

```
--------  --------
```

20.2 Identificador de bloque "Los 5 más graves en los últimos 365 días"

```
-------  (365) -------
```

20.3 Identificador de bloque "El más grave en cada uno de los 10 últimos días en que hayan ocurrido incidentes de este tipo"

```
-------  (10) -------
```

20.4 Identificador de registro

Fecha, hora y duración

Velocidad máxima y velocidad media, número de incidentes similares ocurridos ese día

Apellido(s) del conductor

Nombre del conductor

Identificación de la tarjeta del conductor

```
   ------------------
   dd/mm/aaaa hh:mm hhhmm
   xxx km/h xxx km/h (xxx)
   Last_Name _____________
   First_Name _____________
Card_Identification _______
```

20.5 Si el bloque no incluye ningún registro de exceso de velocidad

```
  - - -
```

21 **Información manuscrita**

Identificador de bloque

21.1 Lugar de control

21.2 Firma del controlador

21.3 Hora de inicio

21.4 Hora de conclusión

21.5 Firma del conductor

"Información manuscrita"; inserte un número suficiente de líneas en blanco encima de un elemento manuscrito, para así poder escribir la información necesaria o firmar el documento.

```
------------------------
  .....
  .....
  .....
  .....
  .....
```

3. ESPECIFICACIONES DE LOS DOCUMENTOS IMPRESOS

En este capítulo se han empleado las siguientes convenciones para la notación:

N	Imprimir bloque o registro número N
N	Imprimir bloque o registro número N, repetido tantas veces como sea necesario
X/Y	Imprimir bloques o registros X o Y según proceda, y repetidos tantas veces como sea necesario

3.1. **Impresión diaria de las actividades del conductor almacenadas en la tarjeta**

PRT_007 La impresión diaria de las actividades del conductor almacenadas en la tarjeta deberá efectuarse con arreglo al formato siguiente:

1	Fecha y hora en la que se imprime el documento
2	Tipo de documento impreso
3	Identificación del controlador (si se inserta una tarjeta de control en la VU)
3	Identificación del conductor (según la tarjeta cuyos datos se imprimen)
4	Identificación del vehículo (vehículo del que se obtiene el documento impreso)
5	Identificación de la VU (VU de la que se obtiene el documento impreso)
6	Último calibrado de esta VU
7	Último control al que se ha sometido el conductor investigado
8	Delimitador de las actividades del conductor
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Actividades del conductor en orden de ocurrencia
11	Delimitador del resumen diario
11.4	Lugares introducidos en orden cronológico
11.5	Totales de la actividad
12.1	Incidentes o fallos procedentes del delimitador de la tarjeta
12.4	Registros de incidentes/fallos (5 últimos incidentes o fallos almacenados en la tarjeta)
13.1	Incidentes o fallos procedentes del delimitador de la VU
13.4	Registros de incidentes/fallos (5 últimos incidentes o fallos almacenados o en curso en la VU)
21.1	Lugar de control
21.2	Firma del controlador
21.5	Firma del conductor

3.2. **Impresión diaria de las actividades del conductor almacenadas en la VU**

PRT_008 La impresión diaria de las actividades del conductor almacenadas en la VU deberá efectuarse con arreglo al formato siguiente:

1	Fecha y hora en la que se imprime el documento
2	Tipo de documento impreso
3	Identificación del titular de la tarjeta (para todas las tarjetas insertadas en la VU)
4	Identificación del vehículo (vehículo del que se obtiene el documento impreso)
5	Identificación de la VU (VU de la que se obtiene el documento impreso)
6	Último calibrado de esta VU
7	Último control de este aparato de control
9	Delimitador de las actividades del conductor
10	Delimitador de la ranura del conductor (ranura 1)
10.1 / 10.2 / 10.3 /10.3a / 10.4	Actividades en orden cronológico (ranura del conductor)
10	Delimitador de la ranura del segundo conductor (ranura 2)
10.1 / 10.2 / 10.3 /10.3a / 10.4	Actividades en orden cronológico (ranura del segundo conductor)
11	Delimitador del resumen diario
11.1	Resumen de períodos sin tarjeta en la ranura del conductor
11.4	Lugares introducidos en orden cronológico
11.6	Totales de la actividad

11.2	Resumen de períodos sin tarjeta en la ranura del segundo conductor
11.4	Lugares introducidos en orden cronológico
11.7	Totales de la actividad
11.3	Resumen de actividades de un conductor, ambas ranuras incluidas
11.4	Lugares introducidos por este conductor en orden cronológico
11.7	Totales de la actividad para este conductor
13.1	Delimitador de incidentes/fallos
13.4	Registros de incidentes/fallos (5 últimos incidentes o fallos almacenados o en curso en la VU)
21.1	Lugar de control
21.2	Firma del controlador
21.3	Hora de comienzo (espacio disponible para un conductor que no disponga de tarjeta para indicar los períodos que le corresponden)
21.4	Hora de conclusión
21.5	Firma del conductor

3.3. **Impresión de incidentes y fallos almacenados en la tarjeta**

PRT_009 La impresión de incidentes y fallos almacenados en la tarjeta deberá efectuarse con arreglo al formato siguiente:

1	Fecha y hora en la que se imprime el documento
2	Tipo de documento impreso
3	Identificación del controlador (si se inserta una tarjeta de control en la VU)
3	Identificación del conductor (según la tarjeta cuyos datos se imprimen)
4	Identificación del vehículo (vehículo del que se obtiene el documento impreso)
12.2	Delimitador de incidentes
12.4	Registros de incidentes (todos los incidentes almacenados en la tarjeta)
12.3	Delimitador de fallos
12.4	Registros de fallos (todos los fallos almacenados en la tarjeta)
21.1	Lugar de control
21.2	Firma del controlador
21.5	Firma del conductor

3.4. **Impresión de incidentes y fallos almacenados en la VU**

PRT_010 La impresión de incidentes y fallos almacenados en la VU deberá efectuarse con arreglo al formato siguiente:

1	Fecha y hora en la que se imprime el documento
2	Tipo de documento impreso
3	Identificación del titular de la tarjeta (para todas las tarjetas insertadas en la VU)
4	Identificación del vehículo (vehículo del que se obtiene el documento impreso)
13.2	Delimitador de incidentes
13.4	Registros de incidentes (todos los incidentes almacenados o en curso en la VU)
13.3	Delimitador de fallos
13.4	Registros de fallos (todos los fallos almacenados o en curso en la VU)
21.1	Lugar de control
21.2	Firma del controlador
21.5	Firma del conductor

3.5. **Impresión de datos técnicos**

PRT_011 La impresión de datos técnicos deberá efectuarse con arreglo al formato siguiente:

1	Fecha y hora en la que se imprime el documento
2	Tipo de documento impreso
3	Identificación del titular de la tarjeta (para todas las tarjetas insertadas en la VU)
4	Identificación del vehículo (vehículo del que se obtiene el documento impreso)
14	Identificación de la VU
15	Identificación del sensor
16	Delimitador de los datos de calibrado
16.1	Registros de calibrado (todos los registros disponibles en orden cronológico)
17	Delimitador del ajuste de hora
17.1	Registros de ajuste de hora (todos los registros disponibles acerca del ajuste de hora y de los registros de los datos de calibrado)
18	El incidente y el fallo más recientes registrados en la VU

3.6. **Impresión por exceso de velocidad**

PRT_012 La impresión por exceso de velocidad deberá efectuarse con arreglo al formato siguiente:

1	Fecha y hora en la que se imprime el documento
2	Tipo de documento impreso
3	Identificación del titular de la tarjeta (para todas las tarjetas insertadas en la VU)
4	Identificación del vehículo (vehículo del que se obtiene el documento impreso)
19	Información sobre el control del exceso de velocidad
20.1	Identificador de los datos sobre el exceso de velocidad
20.4 / 20.5	Primer exceso de velocidad después del último calibrado
20.2	Identificador de los datos sobre el exceso de velocidad
20.4 / 20.5	Los 5 incidentes más graves de exceso de velocidad ocurridos en los últimos 365 días
20.3	Identificador de los datos sobre el exceso de velocidad
20.4 / 20.5	El incidente más grave de exceso de velocidad en cada uno de los 10 últimos días en que hayan ocurrido incidentes de este tipo
21.1	Lugar de control
21.2	Firma del controlador
21.5	Firma del conductor

Apéndice 5

PANTALLA

En este apéndice se utilizan las siguientes convenciones para la notación de formatos:

— los caracteres impresos en **negrita** indican texto legible que hay que imprimir (las informaciones en pantalla se siguen visualizando en caracteres normales),

— los caracteres normales indican variables (pictogramas o datos) que hay que sustituir por sus valores antes de presentarlos en pantalla:

dd mm aaaa: día, mes, año,

hh: horas,

mm: minutos,

D: pictograma de duración,

EF: combinación de pictogramas de incidente o fallo,

O: pictograma de modo de funcionamiento.

DIS_001 Cuando muestre los datos en pantalla, el aparato de control deberá utilizar los formatos siguientes:

Datos	Formato
Contenido de la pantalla por defecto	
Hora local	hh:mm
Modo de funcionamiento	O
Información relativa al conductor	1 Dhh**h**mm ▮▮hh**h**mm
Información relativa al segundo conductor	2 Dhh**h**mm
Condición fuera de ámbito abierta	OUT
Visualización de advertencias	
Sobrepasado el tiempo de conducción continua	10 hh**h**mm ▮▮hh**h**mm
Incidente o fallo	EF
Otras informaciones en pantalla	
Fecha UTC	UTC dd/mm/aaaa o bien UTC dd.mm.aaaa
Hora	hh:mm
Tiempo de conducción continua y tiempo de descanso acumulado del conductor	10 hh**h**mm ▮▮hh**h**mm
Tiempo de conducción continua y tiempo de descanso acumulado del segundo conductor	20 hh**h**mm ▮▮hh**h**mm
Tiempo de conducción acumulado del conductor durante la semana anterior y la actual	10 ‖ hhh**h**mm
Tiempo de conducción acumulado del segundo conductor durante la semana anterior y la actual	20 ‖ hhh**h**mm

Apéndice 6

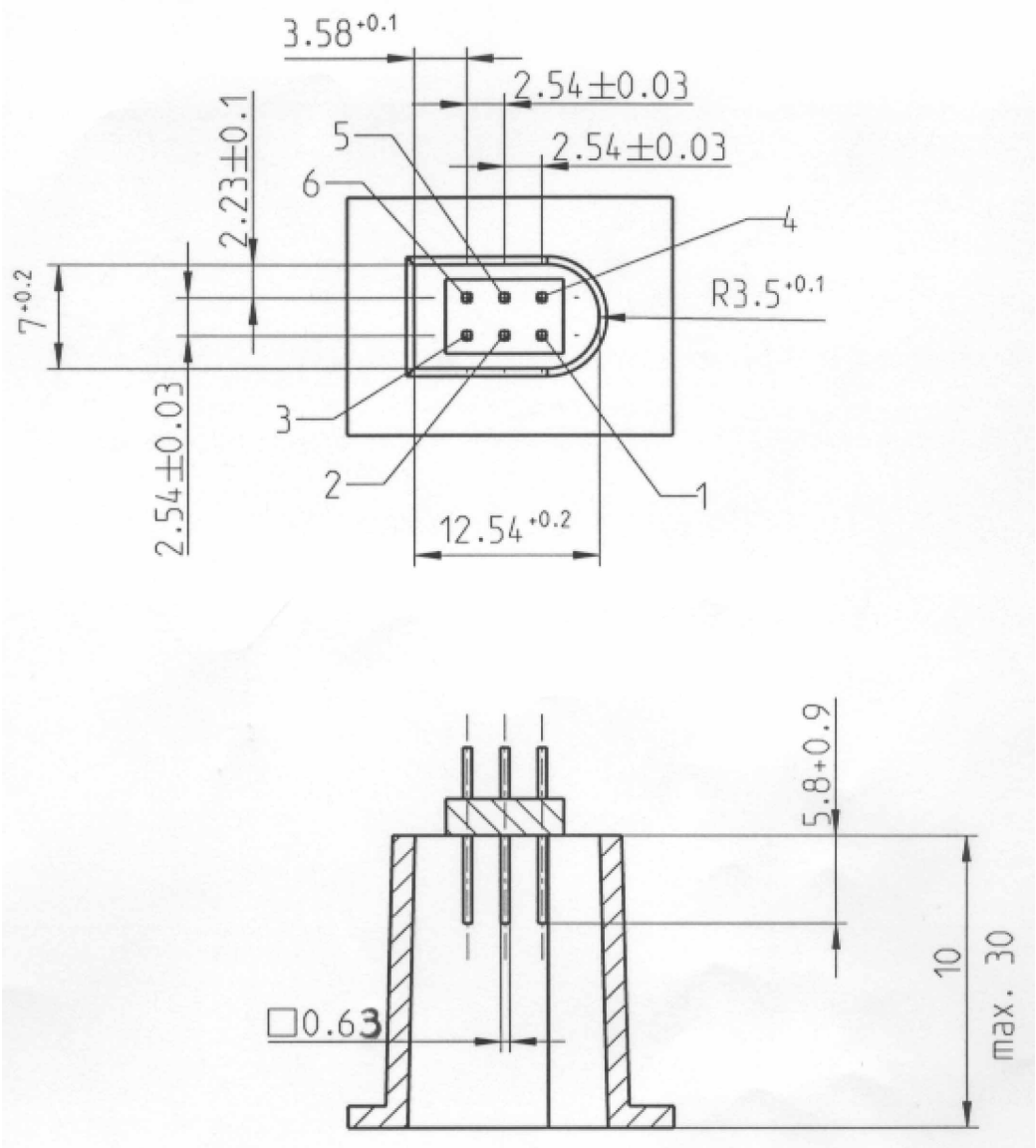
INTERFACES EXTERNAS

ÍNDICE

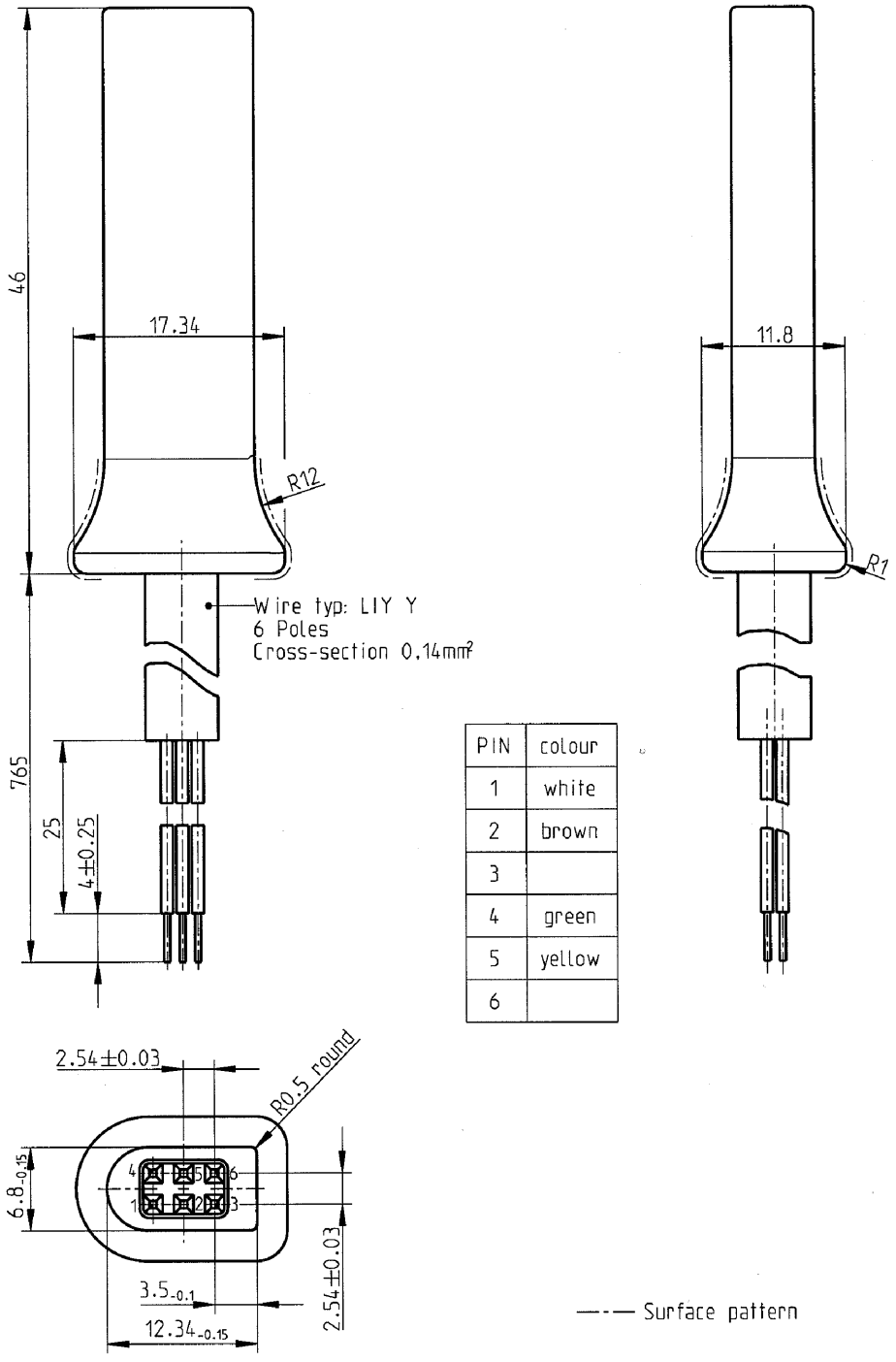
1. HARDWARE

1.1. **Conector**

INT_001 El conector de transferencia/calibrado deberá tener 6 patillas y ser accesible en el panel frontal sin necesidad de desconectar ninguno de los elementos del aparato de control, y sus dimensiones se ajustarán al siguiente esquema (dimensiones en milímetros):



La siguiente ilustración muestra una clavija de acoplamiento típica de 6 patillas:



PIN	colour
1	white
2	brown
3	
4	green
5	yellow
6	

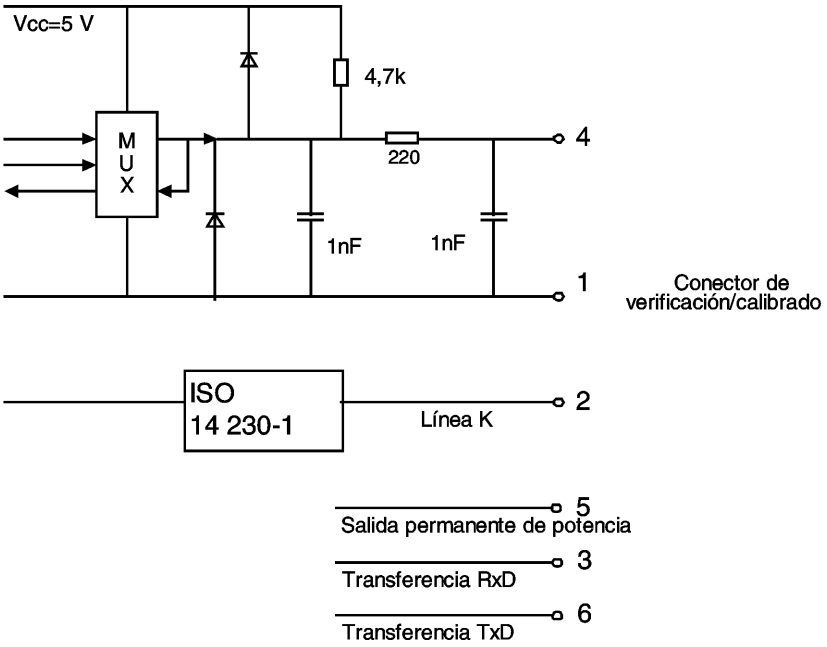
1.2. **Asignación de contactos**

INT_002 Los contactos se asignarán de acuerdo con la tabla siguiente:

Patilla	Descripción	Observaciones
1	Polo negativo batería	Conectado al polo negativo de la batería del vehículo
2	Comunicación de datos	Línea K (ISO 14230-1)
3	Transferencia RxD	Entrada de datos en el aparato de control
4	Señal de entrada/salida	Calibrado
5	Salida permanente de potencia	Se especifica que el intervalo de tensiones debe ser el de la potencia del vehículo menos 3 V que permitan una caída de tensión en los circuitos de protección. Salida 40 mA
6	Transferencia TxD	Salida de datos del aparato de control

1.3. **Diagrama de conjunto**

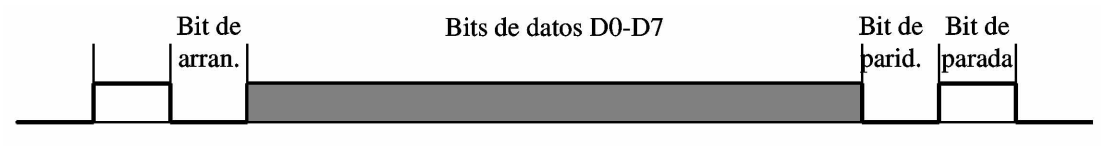
INT_003 El diagrama de conjunto será el siguiente:



2. INTERFAZ DE TRANSFERENCIA

INT_004 La interfaz de transferencia deberá cumplir las especificaciones RS232.

INT_005 La interfaz de transferencia deberá utilizar un bit de arranque, 8 bits de datos con LSB primero, un bit de paridad par y 1 bit de parada.



Organización de los bytes de datosBit de arranque un bit de nivel lógico 0;

Bits de datos: transmitidos con LSB primero;

Bit de paridad: paridad par

Bit de parada: un bit de nivel lógico 1

Cuando se transmitan datos numéricos compuestos de más de un byte, el byte más significativo se transmitirá el primero, y el byte menos significativo el último.

INT_006 La velocidad de transmisión deberá poder ajustarse entre 9 600 bps y 115 200 bps. La transmisión deberá efectuarse a la velocidad más alta posible. La velocidad inicial en baudios al comenzar la comunicación se fija en 9 600 bps.

3. INTERFAZ DE CALIBRADO

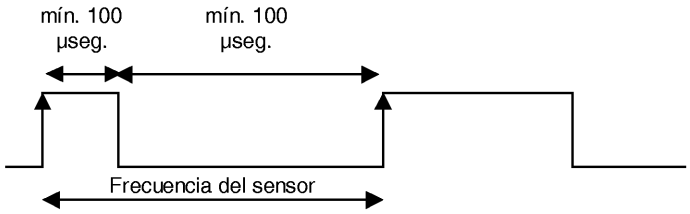
INT_007 La comunicación de datos deberá cumplir lo dispuesto en la norma ISO 14230-1 Vehículos de carretera — Sistemas de diagnóstico — Protocolo Keyword 2000 — Parte 1: Nivel físico, Primera edición: 1999.

INT_008 La señal de entrada/salida deberá cumplir las siguientes especificaciones eléctricas:

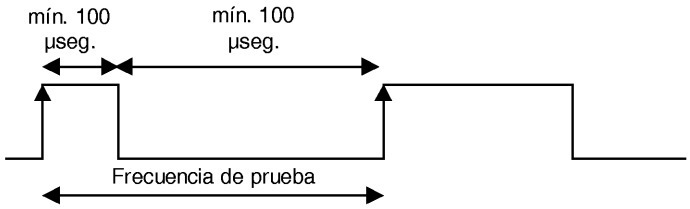
Parámetro	Mínimo	Típico	Máximo	Observaciones
U_{low} (entrada)			1,0 V	I = 750 µA
$U_{U\ high}$ (entrada)	4 V			I = 200 µA
Frecuencia			4 kHz	
U_{low} (salida)			1,0 V	I = 1 mA
U_{high} (salida)	4 V			I = 1 mA

INT_009 La señal de entrada/salida deberá cumplir los siguientes diagramas de relaciones de tiempo:

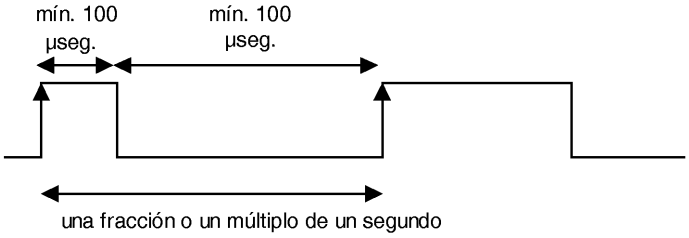
Señal del sensor (salida)



Señal de prueba (entrada)



Señal de reloj UTC (salida)



Apéndice 7

PROTOCOLOS DE TRANSFERENCIA DE DATOS

ÍNDICE

1. INTRODUCCIÓN

En el presente apéndice se especifican los procedimientos que se deben utilizar para llevar a cabo los diferentes tipos de transferencia de datos a un medio de almacenamiento externo (ESM), así como los protocolos que es preciso aplicar para garantizar la corrección de dichas transferencias y la total compatibilidad del formato de los datos transferidos, a fin de que un controlador cualquiera pueda inspeccionar dichos datos y comprobar su autenticidad e integridad antes de analizarlos.

1.1. **Ámbito de aplicación**

Se pueden transferir datos a un ESM:

— desde una unidad intravehicular, mediante un equipo dedicado inteligente (IDE) conectado a la VU,

— desde una tarjeta de tacógrafo, mediante un IDE que incorpore un dispositivo de interfaz de tarjeta (IFD),

— desde una tarjeta de tacógrafo y a través de una unidad intravehicular, mediante un IDE conectado a la VU.

Para poder verificar la autenticidad y la integridad de los datos transferidos que se encuentran almacenados en un ESM, dichos datos se transfieren con una firma añadida según lo dispuesto en el apéndice 11 (Mecanismos de seguridad comunes). También se transfieren la identificación del equipo de origen (VU o tarjeta) y sus certificados de seguridad (Estado miembro y equipamiento). La persona encargada de verificar los datos debe estar en posesión de una clave pública europea de confianza.

DDP_001 Los datos transferidos durante una sesión de transferencia deben almacenarse en el ESM en un solo archivo.

1.2. **Acrónimos y notaciones**

En el presente apéndice se utilizan los acrónimos siguientes:

AID	Identificador de aplicación
ATR	Respuesta a reinicio
CS	Byte de la suma de control
DF	Archivo dedicado
DS	Sesión de diagnóstico
EF	Archivo elemental
ESM	Medio de almacenamiento externo
FID	Identificador de archivo (file ID)
FMT	Byte de formato (primer byte de la cabecera del mensaje)
ICC	Tarjeta de circuito integrado
IDE	Equipo dedicado inteligente: el equipo empleado para realizar la transferencia de datos al ESM (por ejemplo un ordenador personal)
IFD	Dispositivo de interfaz
KWP	Protocolo Keyword 2000
LEN	Byte de longitud (el último byte de la cabecera del mensaje)
PPS	Selección de los parámetros de protocolo
PSO	Realizar operación de seguridad
SID	Identificador de servicio
SRC	Byte de origen
TGT	Byte de destino
TLV	Valor de longitud de la etiqueta
TREP	Parámetro de la respuesta a la petición de transferencia
TRTP	Parámetro de la petición de transferencia
VU	Unidad intravehicular

2. TRANSFERENCIA DE LOS DATOS DE LA VU

2.1. **Procedimiento de transferencia**

A fin de realizar una transferencia de los datos de la VU, el operario debe efectuar las operaciones siguientes:

— introducir su tarjeta de tacógrafo en una ranura de la VU ([1]),

— conectar el IDE al conector de transferencia de la VU,

— establecer la conexión entre el IDE y la VU,

— seleccionar en el IDE los datos que se van a transferir y enviar la petición a la VU,

— cerrar la sesión de transferencia.

2.2. **Protocolo de transferencia de datos**

El protocolo presenta una estructura maestro-esclavo, de modo que el IDE actúa como maestro y la VU como esclavo.

La estructura, los tipos y el flujo de los mensajes se basan principalmente en el protocolo Keyword 2000 (KWP) (ISO 14230-2 Vehículos de carretera — Sistemas de diagnóstico — Protocolo Keyword 2000 — Parte 2: Nivel de enlace de datos).

La capa de aplicación se basa principalmente en el proyecto actual de norma ISO 14229-1 (Vehículos de carretera — Sistemas de diagnóstico — Parte 1: Servicios de diagnóstico, versión 6 de 22 de febrero de 2001).

2.2.1. ***Estructura de los mensajes***

DDP_002 El formato de todos los mensajes que intercambian el IDE y la VU presenta una estructura de tres partes:

— una cabecera compuesta de un byte de formato (FMT), un byte de destino (TGT), un byte de origen (SRC) y posiblemente un byte de longitud (LEN),

— un campo de datos compuesto de un byte identificador de servicio (SID) y un número variable de bytes de datos, que puede incluir un byte opcional de sesión de diagnóstico (dS) o un byte opcional de parámetro de transferencia (TRTP o TREP),

— una suma de control consistente en un byte de suma de control (CS).

Cabecera				Campo de datos					Suma de control
FMT	TGT	SRC	LEN	SID	DATA	…	…	…	CS
4 bytes				Máx. 255 bytes					1 byte

Los bytes TGT y SRC representan la dirección física del destinatario y del emisor del mensaje. Los valores son F0 Hex para el IDE y EE Hex para la VU.

El byte LEN es la longitud de la parte correspondiente al campo de datos.

El byte de suma de control es la suma de todos los bytes del mensaje tomados de 8 bits en 8 bits, en módulo 256, excluido el propio CS.

Los bytes FMT, SID, DS, TRTP y TREP se definen más adelante en este mismo documento.

([1]) La tarjeta introducida activará los correspondientes derechos de acceso a la función de transferencia y a los datos.

DDP_003 Cuando la longitud de los datos que deba incluir el mensaje es mayor que el espacio disponible en la parte correspondiente al campo de datos, el mensaje se envía dividido en varios submensajes. Cada submensaje incorpora una cabecera, los mismos SID y TREP, y un contador de 2 bytes que indica el número de submensaje dentro del mensaje total. Al objeto de permitir la verificación de errores y la cancelación, el IDE confirma cada uno de los submensajes. El IDE puede aceptar el submensaje, solicitar su retransmisión, pedir a la VU que comience de nuevo o cancelar la transmisión.

DDP_004 Si el último submensaje contiene exactamente 255 bytes en el campo de datos, habrá que añadir un submensaje final con un campo de datos vacío (exceptuando los identificadores SID y TREP y el contador de submensaje) para indicar el final del mensaje.

Ejemplo:

Cabecera	SID	TREP	Mensaje	CS
4 bytes	Más largo que 255 bytes			

Se transmitirá como:

Cabecera	SID	TREP	00	01	Submensaje 1	CS
4 bytes	255 bytes					

Cabecera	SID	TREP	00	02	Submensaje 2	CS
4 bytes	255 bytes					

…

Cabecera	SID	TREP	xx	yy	Submensaje n	CS
4 bytes	Menos que 255 bytes					

o bien como:

Cabecera	SID	TREP	00	01	Submensaje 1	CS
4 bytes	255 bytes					

Cabecera	SID	TREP	00	02	Submensaje 2	CS
4 bytes	255 bytes					

…

Cabecera	SID	TREP	xx	yy	Submensaje n	CS
4 bytes	255 bytes					

Cabecera	SID	TREP	xx	yy+1	CS
4 bytes	4 bytes				

2.2.2. ***Tipos de mensajes***

El protocolo de comunicaciones para la transferencia de datos entre la VU y el IDE exige el intercambio de 14 tipos de mensajes diferentes.

La tabla siguiente resume dichos mensajes.

Estructura del mensaje IDE -> <- VU	Máx. 4 bytes Cabecera				Máx. 255 bytes Datos			1 byte Suma de control
IDE -> <- FE	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATOS	CS
Petición de inicio de comunicación	81	EE	F0		81			E0
Respuesta positiva a la petición de inicio de comunicación	80	F0	EE	03	C1		8F,EA	9B
Petición de inicio de la sesión de diagnóstico	80	EE	F0	02	10	81		F1
Respuesta positiva a la petición de inicio de diagnóstico	80	F0	EE	02	50	81		31
Servicio de control del enlace								
Verificar la velocidad en baudios								
9 600 Bd	80	EE	F0	04	87		01,01,01	EC
19 200 Bd	80	EE	F0	04	87		01,01,02	ED
38 400 Bd	80	EE	F0	04	87		01,01,03	ED
57 600 Bd	80	EE	F0	04	87		01,01,04	EF
115 200 Bd	80	EE	F0	04	87		01,01,05	F0
Respuesta positiva a la petición de verificar la velocidad en baudios	80	F0	EE	02	C7		01	28
Velocidad de baudios de transición (fase 2)	80	EE	F0	03	87		02,03	ED
Envío de petición	80	EE	F0	0A	35		00,00,00,0-0,00,FF,FF,-FF,FF	99
Respuesta positiva al envío de petición	80	F0	EE	03	75		00,FF	D5
Petición de transferencia de datos								
Resumen	80	EE	F0	02	36	01		97
Actividades	80	EE	F0	06	36	02	Fecha	CS
Incidentes y fallos	80	EE	F0	02	36	03		99
Datos pormenorizados sobre la velocidad	80	EE	F0	02	36	04		9A
Datos técnicos	80	EE	F0	02	36	05		9B
Transferencia de los datos de la tarjeta	80	EE	F0	02	36	06		9C
Respuesta positiva a la petición de transferencia de datos	80	F0	EE	Len	76	TREP	Datos	CS
Petición de salida de la transferencia	80	EE	F0	01	37			96
Respuesta positiva a la petición de salida de la transferencia	80	F0	EE	01	77			D6
Petición de interrupción de la comunicación	80	EE	F0	01	82			E1
Respuesta positiva a la petición de interrupción de la comunicación	80	F0	EE	01	C2			21
Confirmación de submensaje	80	EE	F0	Len	83		Datos	CS
Respuestas negativas								
Envío no aceptado	80	F0	EE	03	7F	Sid pet.	10	CS
Servicio no admitido	80	F0	EE	03	7F	Sid pet.	11	CS
Subfunción no admitida	80	F0	EE	03	7F	Sid pet.	12	CS
Longitud del mensaje incorrecta	80	F0	EE	03	7F	Sid pet.	13	CS
Condiciones incorrectas o error en la secuencia de la petición	80	F0	EE	03	7F	Sid pet.	22	CS
Petición no admisible	80	F0	EE	03	7F	Sid pet.	31	CS
Falta respuesta	80	F0	EE	03	7F	Sid pet.	50	CS
Datos no disponibles	80	F0	EE	03	7F	Sid pet.	78	CS
Rechazo general	80	F0	EE	03	7F	Sid pet.	FA	CS

Notas:
— Sid pet. = el Sid de la petición que corresponda, Lid pet. = el Lid de la petición que corresponda.
— TREP = el TRTP de la petición correspondiente.
— Las casillas en negro significan que no se transmite ningún dato.
— El término envío (entendido desde el IDE) se utiliza para compatibilidad con ISO 14229. Significa lo mismo que transferencia (entendida desde la VU).
— Los contadores de submensaje potenciales de 2 bytes no aparecen en la tabla.

2.2.2.1. *Petición de inicio de comunicación (SID 81)*

DDP_005 El IDE envía este mensaje para establecer el enlace de comunicación con la VU. Las comunicaciones iniciales se hacen siempre a 9600 baudios (hasta que la velocidad en baudios se cambia utilizando los servicios adecuados de control del enlace.

2.2.2.2. *Respuesta positiva a la petición de inicio de comunicación (SID C1)*

DDP_006 La VU envía este mensaje para responder positivamente a una petición de inicio de comunicación. Incluye los 2 bytes de clave '8F' y 'EA' , indicativos de que la unidad admite un protocolo con una cabecera que incluya información sobre el destino, el origen y la longitud del mensaje.

2.2.2.3. *Petición de inicio de la sesión de diagnóstico (SID 10)*

DDP_007 El IDE envía el mensaje de petición de inicio de la sesión de diagnóstico para solicitar una nueva sesión de diagnóstico con la VU. La subfunción "sesión de fallos" (fault session) (81 Hex) indica que va a abrirse una sesión de diagnóstico estándar.

2.2.2.4. *Respuesta positiva a la petición de inicio de diagnóstico (SID 50)*

DDP_008 La VU envía el mensaje de respuesta positiva a la petición de inicio de diagnóstico para responder positivamente a la solicitud de sesión de diagnóstico.

2.2.2.5. *Servicio de control del enlace (SID 87)*

DDP_052 El servicio de control del enlace es utilizado por el IDE para iniciar un cambio en la velocidad en baudios. Este cambio se lleva a cabo en dos etapas. En la primera el IDE propone el cambio en la velocidad en baudios, indicando la nueva velocidad. Al recibir un mensaje positivo de la VU, el IDE envía a la VU, una confirmación del cambio en la velocidad en baudios (etapa 2). A continuación el IDE cambia a la nueva velocidad en baudios. Tras recibir la confirmación la VU cambia a la nueva velocidad en baudios.

2.2.2.6. *Respuesta positiva al control del enlace (SID C7)*

DDP_053 La respuesta positiva al control del enlace es enviada por la VU para contestar positivamente a la petición de servicio del control del enlace (etapa 1). Téngase en cuenta que no se da respuesta a la solicitud de confirmación (etapa 2).

2.2.2.7. *Envío de petición (SID 35)*

DDP_009 El IDE envía el mensaje de envío de petición para especificar a la VU que se solicita una operación de transferencia. Para cumplir los requisitos de ISO 14229, se incluyen entre los datos: la dirección y el tamaño y el formato de los datos solicitados. Dado que el IDE no los conoce antes de la transferencia, la dirección de la memoria se pone a 0, el formato está descifrado y descomprimido y el tamaño de la memoria se fija en el máximo.

2.2.2.8. *Respuesta positiva al envío de petición (SID 75)*

DDP_010 La VU envía el mensaje de respuesta positiva al envío de petición para indicar al IDE que la VU está preparada para transferir datos. Para cumplir los requisitos de ISO 14229, se incluyen datos en este mensaje de respuesta positiva, indicando al IDE que los ulteriores mensajes de respuesta positiva a la transferencia de datos incluirán un máximo de 00FF hex bytes.

Junto con el mensaje la VU envía datos que ayudan al operario del IDE a seleccionar los datos que quiere transferir. La información contenida en este mensaje es la siguiente:

2.2.2.9. *Petición de transferencia de datos (SID 36)*

DDP_011 El IDE envía la petición de transferencia de datos para especificar a la VU el tipo de datos que se van a transferir. Un parámetro de petición de transferencia (TRTP) de un byte indica el tipo de transferencia.

Existen cinco tipos de transferencias de datos:

— Resumen (TRTP 01),

— Actividades de una fecha específica (TRTP02),

— Incidentes y fallos (TRTP 03),

— Datos pormenorizados sobre la velocidad (TRTP 04),

— Datos técnicos (TRTP 05),

— Transferencia de datos de la tarjeta (TRTP 06).

DDP_054 Es obligatorio que el IDE solicite la transferencia de datos "resumen" (TRTP 01) durante una sesión de transferencia ya que sólo eso asegurará que los certificados de la VU se registran con el archivo transferido (y permiten la verificación de la firma digital).

En el segundo caso (TRTP 02), el mensaje de petición de transferencia de datos incluye la indicación del día natural (en formato `TimeReal`) cuyos datos se van a transferir.

2.2.2.10. *Respuesta positiva a la petición de transferencia de datos (SID 76)*

DDP_012 La VU envía la respuesta positiva a la petición de transferencia de datos como contestación a la petición de transferencia de datos. Este mensaje contiene los datos solicitados, junto con un parámetro de respuesta a la solicitud de transferencia (TREP) correspondiente al TRTP de la petición.

DDP_055 En el primer caso (TREP 01), la VU envía datos que ayudan al operario del IDE a seleccionar los datos que quiere transferir. La información contenida en este mensaje es la siguiente:

— certificados de seguridad,

— identificación del vehículo,

— fecha y hora actuales de la VU,

— fecha máxima y mínima transferible (datos de la VU),

— indicación de presencia de tarjetas en la VU,

— transferencia previa a una empresa,

— bloqueos introducidos por empresas,

— controles anteriores.

2.2.2.11. *Petición de salida de la transferencia (SID 37)*

DDP_013 El IDE envía el mensaje de petición de salida de la transferencia para informar a la VU de que la sesión de transferencia ha terminado.

2.2.2.12. *Respuesta positiva a la petición de salida de la transferencia (SID 77)*

DDP_014 La VU envía el mensaje de respuesta positiva a la petición de salida de la transferencia para confirmar la petición de salida de la transferencia.

2.2.2.13. *Petición de interrupción de la comunicación (SID 82)*

DDP_015 El IDE envía el mensaje de petición de interrupción de la comunicación para desconectar el enlace de comunicación con la VU.

2.2.2.14. *Respuesta positiva a la petición de interrupción de la comunicación (SID C2)*

DDP_016 La VU envía el mensaje de respuesta positiva a la petición de interrupción de la comunicación para confirmar la petición de interrupción de la comunicación.

2.2.2.15. *Confirmación de submensaje (SID 83)*

DDP_017 El IDE envía el mensaje de confirmación de submensaje para confirmar la recepción de cada una de las partes de un mensaje que se transmiten como diversos submensajes. El campo de datos contiene el SID recibido de la VU y un código de 2 bytes que se interpreta de la manera siguiente:

— MsgC +1 confirma la correcta recepción del submensaje número MsgC.

El IDE solicita a la VU que envíe el siguiente submensaje.

— MsgC indica un problema en la recepción del submensaje número MsgC.

El IDE solicita a la VU que envíe de nuevo ese submensaje.

— FFFF solicita la terminación del mensaje

El IDE puede utilizar este código para terminar la transmisión del mensaje de la VU por el motivo que fuere.

El último submensaje de un mensaje (byte LEN < 255) se puede confirmar con cualquiera de estos códigos, o bien puede dejarse sin confirmar.

Respuestas de la VU que se componen de varios submensajes:

— Respuesta positiva a la petición de transferencia de datos (SID 76).

2.2.2.16. *Respuesta negativa (SID 7F)*

DDP_018 La VU envía el mensaje de respuesta negativa como contestación a los mensajes de petición anteriores cuando no puede satisfacer la petición de que se trate. Los campos de datos del mensaje incluyen el SID de la respuesta (7F), el SID de la petición y un código que especifica el motivo de la respuesta negativa. Están disponibles los códigos siguientes:

— 10 rechazo general

La acción solicitada no se puede llevar a cabo por un motivo distinto de los enumerados a continuación.

— 11 servicio no admitido

No se entiende el SID de la petición.

— 12 subfunción no admitida

No se entiende el DS o el TRTP de la petición, o bien no hay más submensajes que transmitir.

— 13 longitud del mensaje incorrecta

La longitud del mensaje es incorrecta.

— 22 condiciones incorrectas o error en la secuencia de la petición

El servicio requerido no está activo o la secuencia de mensajes de petición es incorrecta.

— 31 solicitud no admisible

El registro del parámetro de la solicitud (campo de datos) no es válido.

— 50 envío no aceptado

No se puede llevar a cabo la petición (la VU se encuentra en un modo de funcionamiento inadecuado o tiene un fallo interno).

— 78 falta respuesta

La acción solicitada no se puede llevar a cabo a tiempo y la VU no está preparada para aceptar otra petición.

— FA datos no disponibles

El objeto de datos de una petición de transferencia de datos no está disponible en la VU (por ejemplo, no se ha introducido una tarjeta, …).

2.2.3. ***Flujo del mensaje***

A continuación se describe el flujo normal de un mensaje durante un procedimiento normal de transferencia de datos:

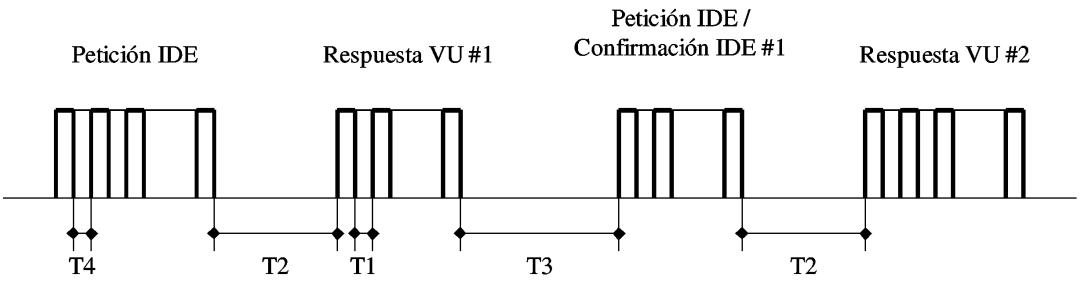
IDE		VU
Petición de inicio de comunicación	⇨	
	⇦	Respuesta positiva
Petición de inicio del servicio de diagnóstico	⇨	
	⇦	Respuesta positiva
Envío de petición	⇨	
	⇦	Respuesta positiva
Petición de transferencia de datos #1	⇨	
	⇦	Respuesta positiva
Petición de transferencia de datos #2	⇨	
	⇦	Respuesta positiva #1
Confirmación de submensaje #1	⇨	
	⇦	Respuesta positiva #2
Confirmación de submensaje #2	⇨	
	⇦	Respuesta positiva #m
Confirmación de submensaje #m	⇨	
	⇦	Respuesta positiva (Campo de datos < 255 bytes)
Confirmación de submensaje (opcional)	⇨	
	…	
Petición de transferencia de datos #n	⇨	
	⇦	Respuesta positiva
Petición de salida de la transferencia	⇨	
	⇦	Respuesta positiva
Petición de interrupción de la comunicación	⇨	
	⇦	Respuesta positiva

2.2.4. ***Sincronización***

DDP_019 Los parámetros de sincronización que aparecen en el gráfico siguiente son importantes durante el funcionamiento normal:

Figura 1

Flujo del mensaje, sincronización



Donde:

P1 = Tiempo entre dos bytes para la respuesta VU.

P2 = Tiempo transcurrido desde el final de la petición IDE hasta el comienzo de la respuesta VU, o desde el final de la confirmación IDE hasta el comienzo de la siguiente respuesta VU.

P3 = Tiempo transcurrido desde el final de la respuesta VU hasta el comienzo de una nueva petición IDE, o desde el final de la respuesta VU hasta el principio de la confirmación IDE, o desde el final de la petición IDE hasta el comienzo de una nueva petición IDE si la VU no puede responder.

P4 = Tiempo entre 2 bytes para la petición IDE.

P5 = Valor ampliado de P3 para la transferencia de los datos de la tarjeta.

La tabla siguiente muestra los valores admisibles para los parámetros de sincronización (conjunto de parámetros de sincronización ampliados KWP, empleado en caso de direccionamiento físico para lograr una comunicación más rápida).

Parámetro de sincronización	Límite inferior del valor (ms)	Límite superior del valor (ms)
P1	0	20
P2	20	1 000 (*)
P3	10	5 000
P4	5	20
P5	10 minutos	20 minutos

(*) Si la VU contesta con una respuesta negativa que contiene un código con el significado "petición recibida correctamente, falta respuesta", este valor se amplía hasta el límite superior del valor correspondiente al parámetro P3.

2.2.5. ***Gestión de errores***

Si se produce un error durante el intercambio, el esquema de flujo del mensaje se modifica en función de qué equipo haya detectado el error y qué mensaje haya generado el error.

Las figuras 2 y 3 muestran los procedimientos de gestión de errores para la VU y para el IDE, respectivamente.

2.2.5.1. *Fase de inicio de la comunicación*

DDP_020 Si el IDE detecta un error durante la fase de Inicio de la comunicación, ya sea por sincronización o por la corriente de bits, esperará durante un período P3 mín. antes de enviar de nuevo la petición.

DDP_021 Si la VU detecta un error en la secuencia procedente del IDE, no enviará respuesta y esperará durante un período P3 máx. a recibir otro mensaje de petición de inicio de comunicación.

2.2.5.2. *Fase de comunicación*

Se pueden definir dos zonas distintas de gestión de errores:

1. La VU detecta un error en la transmisión del IDE

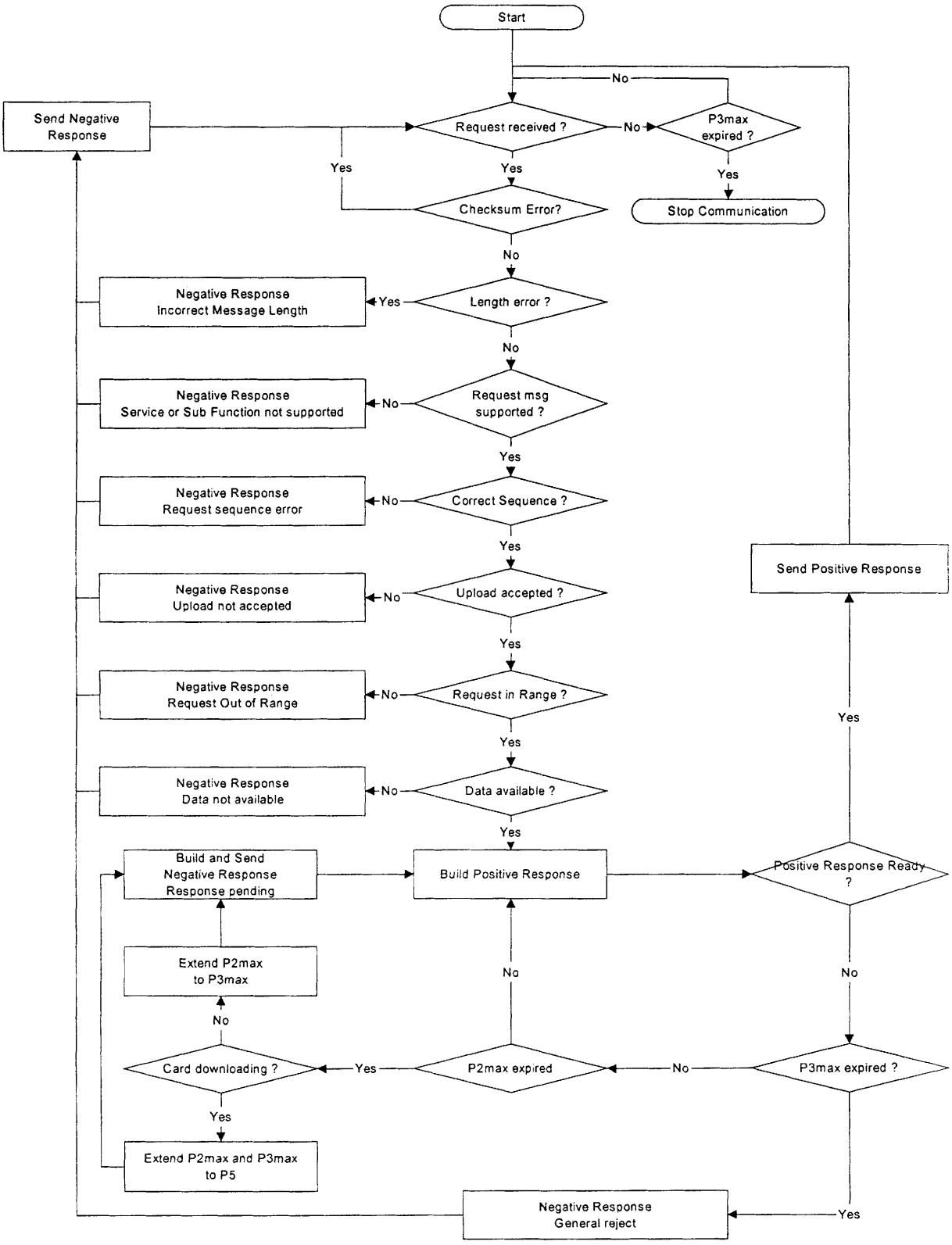
DDP_022 Por cada mensaje que reciba, la VU detectará errores de sincronización, errores de formato de byte (por ejemplo, violaciones de los bits de inicio y de paro) y errores de trama (el número de bytes recibidos es incorrecto, el byte de la suma de control es incorrecto).

DDP_023 Si la VU detecta uno de los errores anteriores, no envía respuesta ni hace caso del mensaje recibido.

DDP_024 La VU puede detectar otros errores en el formato o en el contenido del mensaje recibido (por ejemplo, tipo de mensaje inadmisible), aunque el mensaje cumpla los requisitos en cuanto a longitud y suma de control; en tal caso, la VU deberá contestar al IDE con un mensaje de respuesta negativa que especifique la naturaleza del error.

Figura 2

Gestión de errores para la VU



2. El IDE detecta un error en la transmisión de la VU

DDP_025 Por cada mensaje que reciba, el IDE detectará errores de sincronización, errores de formato de byte (por ejemplo, violaciones de los bits de inicio y de paro) y errores de trama (el número de bytes recibidos es incorrecto, el byte de la suma de control es incorrecto).

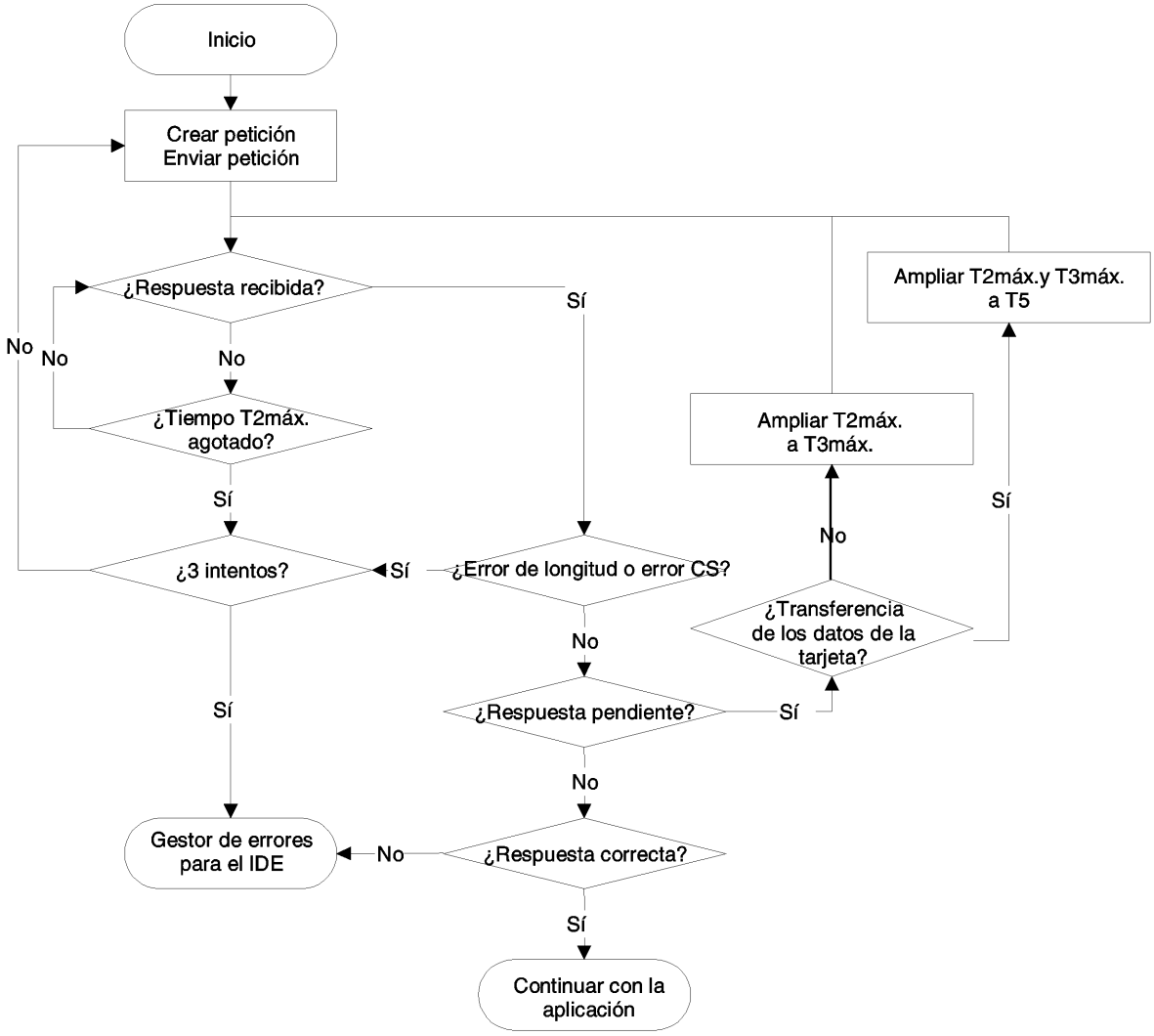
DDP_026 El IDE deberá detectar errores de secuencia; es decir, errores en los incrementos del contador de submensajes en mensajes sucesivos.

DDP_027 Si el IDE detecta un error o transcurre el período P2máx. sin que se haya recibido contestación de la VU, el mensaje de petición se envía de nuevo para un máximo de tres transmisiones en total. A efectos de esta detección de errores, una confirmación de submensaje se considerará una petición a la VU.

DDP_028 El IDE deberá esperar durante al menos un período P3mín. antes de comenzar cada transmisión; el período de espera se medirá a partir del momento de ocurrencia del último bit de paro calculado después de haberse detectado el error.

Figura 3

Gestión de errores para el IDE



2.2.6. ***Contenido del mensaje de respuesta***

En este apartado se especifica el contenido de los campos de datos incluidos en los diferentes mensajes de respuesta positiva.

Los elementos de datos se definen en el apéndice 1 (Diccionario de datos).

2.2.6.1. *Respuesta positiva a la petición de transferencia de datos "resumen"*

DDP_029 El campo de datos del mensaje respuesta positiva a la petición de transferencia de datos "resumen" contiene los datos siguientes en este orden, con el SID 76 Hex y el método adecuado de división y recuento de submensajes:

Elemento de datos	Longitud (Bytes)	Observaciones
MemberStateCertificate	194	Certificados de seguridad de la VU
VUCertificate	194	
VehicleIdentificationNumber	17	Identificación del vehículo
VehicleRegistrationIdentification		
vehicleRegistrationNation	1	
vehicleRegistrationNumber	14	
CurrentDateTime	4	Fecha y hora actuales de la VU
VuDownloadablePeriod		Período transferible
minDownloadableTime	4	
maxDownloadableTime	4	
CardSlotsStatus	1	Tipo de tarjetas insertadas en la VU
VuDownloadActivityData		Transferencia anterior de la VU
downloadingTime	4	
fullCardNumber	18	
companyOrWorkshopName	36	
VuCompanyLocksData		Todos los bloqueos de empresa almacenados. Si la sección está vacía, tan solo se envía noOfLocks = 0
noOfLocks	1	
...	(98)	
VuCompanyLocksRecord: lockInTime	4	
VuCompanyLocksRecord: lockOutTime	4	
VuCompanyLocksRecord: companyName	36	
VuCompanyLocksRecord: companyAddress	36	
VuCompanyLocksRecord: companyCardNumber	18	
...		
VuControlActivityData		Todos los registros de control almacenados en la VU. Si la sección está vacía, tan solo se envía noOfControls = 0
noOfControls	1	
...	(31)	
VuControlActivityRecord: controlType	1	
VuControlActivityRecord: controlTime	4	
VuControlActivityRecord: controlCardNumber	18	
VuControlActivityRecord: downloadPeriodBeginTime	4	
VuControlActivityRecord: downloadPeriodEndTime	4	
...		
Signature	128	Firma RSA de todos los datos (excepto los certificados), desde el VehicleIdentificationNumber hasta el último byte del último VuControlActivityRecord

2.2.6.2. *Respuesta positiva a la petición de transferencia de datos sobre actividades*

DDP_030 El campo de datos del mensaje "Respuesta positiva a la petición de transferencia de datos sobre actividades" contiene los datos siguientes en este orden, con el SID 76 Hex, el LID 01 Hex y el método adecuado de división y recuento de submensajes:

Elemento de datos	Longitud (Bytes)	Observaciones
TimeReal	4	Fecha correspondiente al día cuyos datos se transfieren
OdometerValueMidnight	3	Lectura del cuentakilómetros al terminar el día cuyos datos se transfieren
VuCardIWData		Datos sobre los ciclos de inserción y extracción de tarjetas.
noOfVuCardIWRecords	2	
...	(129)	— Si esta sección no contiene datos disponibles, tan solo se envía noOfVuCardIWRecords = 0
VuCardIWRecord: cardHolderName		— Cuando un registro VuCardIWRecord es anterior a las 00:00 (la tarjeta se insertó el día de antes) o posterior a las 24:00 (la tarjeta se extrajo el día después), deberá constar en los dos días
holderSurname	36	
holderFirstNames	36	
fullCardNumber	18	
cardExpiryDate	4	
cardInsertionTime	4	
vehicleOdometerValueAtInsertion	3	
cardSlotNumber	1	
cardWithdrawalTime	4	
vehicleOdometerValueAtWithdrawal	3	
previousVehicleInfo		
vehicleRegistrationIdentification		
vehicleRegistrationNation	1	
vehicleRegistrationNumber	14	
cardWithdrawalTime	4	
manualInputFlag	1	
...		
VuActivityDailyData		Estado de la ranura a las 00:00 y cambios de actividad registrados durante el día cuyos datos se transfieren
noOfActivityChanges	2	
...		
ActivityChangeInfo	2	
...		
VuPlaceDailyWorkPeriodData		Datos relativos a lugares y registrados durante el día cuyos datos se transfieren. Si la sección está vacía, tan solo se envía noOfPlaceRecords = 0
noOfPlaceRecords	1	
...	(28)	
VuPlaceDailyWorkPeriodRecord: fullCardNumber	18	
placeRecord		
entryTime	4	
entryTypeDailyWorkPeriod	1	
dailyWorkPeriodCountry	1	
dailyWorkPeriodRegion	1	
vehicleOdometerValue	3	
...		
VuSpecificConditionData		Datos sobre condiciones específicas registrados durante el día cuyos datos se transfieren. Si la sección está vacía, tan solo se envía noOfSpecificConditionRecords = 0
noOfSpecificConditionRecords	2	
...	(5)	
SpecificConditionRecord		
EntryTime	4	
specificConditionType	1	
...		
Signature	128	Firma RSA de todos los datos, desde TimeReal hasta el último byte del último registro de una condición específica

2.2.6.3. *Respuesta positiva a la petición de transferencia de datos sobre incidentes y fallos*

DDP_031 El campo de datos del mensaje "Respuesta positiva a la petición de transferencia de datos sobre incidentes y fallos" contiene los datos siguientes en este orden, con el SID 76 Hex, el TREP 03 Hex y el método adecuado de división y recuento de submensajes:

Elemento de datos	Longitud (Bytes)	Observaciones
VuFaultData		Todos los fallos almacenados o en curso en la VU. Si la sección está vacía, tan solo se envía noOfVuFaults = 0
NoOfVuFaults	1	
...	(82)	
VuFaultRecord: FaultType	1	
VuFaultRecord: FaultRecordPurpose	1	
VuFaultRecord: FaultBeginTime	4	
VuFaultRecord: FaultEndTime	4	
VuFaultRecord: CardNumberDriverSlotBegin	18	
VuFaultRecord: cardNumberCodriverSlotBegin	18	
VuFaultRecord: CardNumberDriverSlotEnd	18	
VuFaultRecord: CardNumberCodriverSlotEnd	18	
...		
VuEventData		Todos los incidentes (excepto los de exceso de velocidad) almacenados o en curso en la VU. Si la sección está vacía, tan solo se envía noOfVuEvents = 0
NoOfVuEvents	1	
...	(83)	
VuEventRecord: EventType	1	
VuEventRecord: EventRecordPurpose	1	
VuEventRecord: EventBeginTime	4	
VuEventRecord: EventEndTime	4	
VuEventRecord: CardNumberDriverSlotBegin	18	
VuEventRecord: cardNumberCodriverSlotBegin	18	
VuEventRecord: CardNumberDriverSlotEnd	18	
VuEventRecord: CardNumberCodriverSlotEnd	18	
VuEventRecord: SimilarEventsNumber	1	
...		
VuOverSpeedingControlData		Datos relativos al último control del exceso de velocidad (si no hay datos se indica un valor por defecto)
LastOverspeedControlTime	4	
FirstOverspeedSince	4	
NumberOfOverspeedSince	1	
VuOverSpeedingEventData		Todos los incidentes de exceso de velocidad almacenados en la VU. Si la sección está vacía, tan solo se envía noOfVuOverSpeedingEvents = 0
NoOfVuOverSpeedingEvents	1	
...	(31)	
VuOverSpeedingEventRecord: EventType	1	
VuOverSpeedingEventRecord: EventRecordPurpose	1	
VuOverSpeedingEventRecord: EventBeginTime	4	
VuOverSpeedingEventRecord: EventEndTime	4	
VuOverSpeedingEventRecord: MaxSpeedValue	1	
VuOverSpeedingEventRecord: AverageSpeedValue	1	
VuOverSpeedingEventRecord: CardNumberDriverSlotBegin	18	
VuOverSpeedingEventRecord: SimilarEventsNumber	1	
...		
VuTimeAdjustmentData		Todos los ajustes de hora almacenados en la VU (fuera del marco de un calibrado completo). Si la sección está vacía, tan solo se envía noOfVuTimeAdjRecords = 0
NoOfVuTimeAdjRecords	1	
...	(98)	
VuTimeAdjustmentRecord: OldTimeValue	4	
VuTimeAdjustmentRecord: NewTimeValue	4	
VuTimeAdjustmentRecord: WorkshopName	36	
VuTimeAdjustmentRecord: WorkshopAddress	36	
VuTimeAdjustmentRecord: WorkshopCardNumber	18	
...		
Signature	128	Firma RSA de todos los datos, desde noOfVuFaults hasta el último byte del último time adjustment record

2.2.6.4. *Respuesta positiva a la petición de transferencia de datos pormenorizados sobre la velocidad*

DDP_032 El campo de datos del mensaje "Respuesta positiva a la petición de transferencia de datos pormenorizados sobre la velocidad" contiene los datos siguientes en este orden, con el SID 76 Hex, el TREP 04 Hex y el método adecuado de división y recuento de submensajes:

Elemento de datos	Longitud (Bytes)	Observaciones
VuDetailedSpeedData		Todos los datos pormenorizados almacenados en la VU y relativos a la velocidad del vehículo (un bloque de datos por cada minuto que haya estado el vehículo en movimiento) 60 valores de velocidad por cada minuto (un valor por segundo)
NoOfSpeedBlocks	2	
...		
VuDeatailedSpeedBlock		
SpeedBlockBeginDate	4	
speedsPerSecond	60	
...		
Signature	128	Firma RSA de todos los datos, desde noOfSpeedBlocks hasta el último byte del último bloque con datos de velocidad

2.2.6.5. *Respuesta positiva a la petición de transferencia de datos técnicos*

DDP_033 El campo de datos del mensaje "Respuesta positiva a la petición de transferencia de datos técnicos" contiene los datos siguientes en este orden, con el SID 76 Hex, el TREP 05 Hex y el método adecuado de división y recuento de submensajes:

Elemento de datos	Longitud (Bytes)	Observaciones
VuIdentification		
vuManufacturerName	36	
vuManufacturerAddress	36	
vuPartNumber	16	
vuSerialNumber	8	
vuSoftwareIdentification		
vuSoftwareVersion	4	
vuSoftInstallationDate	4	
vuManufacturingDate	4	
vuApprovalNumber	8	
SensorPaired		
sensorSerialNumber	8	
sensorApprovalNumber	8	
sensorPairingDateFirst	4	
VuCalibrationData		Todos los registros de calibrado almacenados en la VU
noOfVuCalibrationRecords	1	
...	(164)	
VuCalibrationRecord		
calibrationPurpose	1	
workshopName	36	
workshopAddress	36	
workshopCardNumber	18	
workshopCardExpiryDate	4	
vehicleIdentificationNumber	17	
vehicleRegistrationIdentification		
vehicleRegistrationNation	1	
vehicleRegistrationNumber	14	
wVehicleCharacteristicConstant	2	
kConstantOfRecordingEquipment	2	
lTyreCircumference	2	
tyreSize	15	
authorisedSpeed	1	
oldOdometerValue	3	
newOdometerValue	3	
oldTimeValue	4	
newTimeValue	4	
nextCalibrationDate	4	
...		
Signature	128	Firma RSA de todos los datos, desde vuManufacturerName hasta el último byte del último VuCalibrationRecord

2.3. **Almacenamiento de un archivo en un ESM**

DDP_034 Si una sesión de transferencia ha incluido una transferencia de datos de la VU, el IDE deberá almacenar en un único archivo físico todos los datos recibidos de la VU durante dicha sesión de transferencia dentro de los mensajes de respuesta positiva a la solicitud de transferencia. Los datos almacenados excluyen las cabeceras de mensajes, los contadores de submensajes, los submensajes vacíos y las sumas de control, pero incluyen el SID y el TREP (del primer submensaje exclusivamente si es que hay varios submensajes).

3. PROTOCOLO DE TRANSFERENCIA DE LOS DATOS ALMACENADOS EN TARJETAS DE TACÓGRAFO

3.1. **Ámbito de aplicación**

El presente apartado describe cómo se transfieren directamente a un IDE los datos almacenados en una tarjeta. El IDE no forma parte del entorno seguro, por tanto no se lleva a cabo una autentificación entre la tarjeta y el IDE.

3.2. **Definiciones**

Sesión de transferencia: Cada vez que se transfieren los datos de la ICC. Esta sesión comprende el procedimiento completo desde el reinicio de la ICC por parte de un IFD hasta la desactivación de la ICC (extracción de la tarjeta o siguiente reinicio).

Archivo de datos firmado: Un archivo de la ICC. El archivo se transfiere al IFD en forma de texto. En la ICC, el archivo se somete a una comprobación aleatoria y se firma, y la firma se transfiere al IFD.

3.3. **Transferencia de los datos de la tarjeta**

DDP_035 La transferencia de los datos de una tarjeta de tacógrafo consta de los pasos siguientes:

— Transferencia de la información común de la tarjeta almacenada en los archivos EF `ICC` y `IC`. Esta información es opcional y no se protege con una firma digital.

— Transferencia de los archivos EF `Card_Certificate` y `CA_Certificate`. Esta información no se protege con una firma digital.

  Es obligatorio transferir estos archivos para cada sesión de transferencia.

— Transferencia del resto de archivos EF con datos de aplicación (dentro del archivo DF `Tachograph`) excepto EF `Card_Download`. Esta información se protege con una firma digital.

  — Es obligatorio transferir al menos los archivos EF `Application_Identification` e `ID` para cada sesión de transferencia.

  — Cuando se transfieran los datos de una tarjeta del conductor, también es obligatorio transferir los siguientes archivos EF:

    — `Events_Data`,

    — `Faults_Data`,

    — `Driver_Activity_Data`,

    — `Vehicles_Used`,

    — `Places`,

    — `Control_Activity_Data`,

    — `Specific_Conditions`.

— Cuando se transfieran los datos de una tarjeta del conductor, se actualizará la fecha `LastCard_Download` en el archivo EF `Card_Download`.

— Cuando se transfieran los datos de una tarjeta del centro de ensayo, habrá que reiniciar el contador de calibrado en el archivo `Card_Download`.

3.3.1. ***Secuencia de inicialización***

DDP_036 El IDE deberá iniciar la secuencia de la manera siguiente:

Tarjeta	Dirección	IDE/IFD	Significado/Observaciones
	⇦	Reinicio de hardware	
ATR	⇨		

Opcionalmente se puede utilizar PPS para cambiar a una velocidad en baudios más alta, siempre y cuando la admita la ICC.

3.3.2. ***Secuencia para archivos de datos no firmados***

DDP_037 A continuación se muestra la secuencia para transferir los archivos EF `ICC`, `IC`, `Card_Certificate` y `CA_Certificate`:

Tarjeta	Dirección	IDE/IFD	Significado/Observaciones
	⇦	SELECT FILE	Selección de archivo utilizando su identificador
OK	⇨		
	⇦	READ BINARY	Si el archivo contiene más datos de los que caben en la memoria temporal del lector o de la tarjeta, habrá que repetir el comando hasta que se haya leído el archivo completo
Datos del archivo OK	⇨	Almacenar datos en un ESM	Según el apartado 3.4 Formato de almacenamiento de datos

Nota: antes de seleccionar el `Card_Certificate`, es preciso seleccionar la aplicación de tacógrafo (selección por AID).

3.3.3. ***Secuencia para archivos de datos firmados***

DDP_038 La secuencia siguiente debe utilizarse para cada uno de los archivos siguientes que debe transferirse junto con su firma:

Tarjeta	Dir	IDE/IFD	Significado/Observaciones
	⇦	SELECT FILE	
OK	⇨		
	⇦	PERFORM HASH OF FILE	Calcula el valor de comprobación aleatoria con los datos contenidos en el archivo seleccionado, utilizando el algoritmo de comprobación aleatoria especificado en el apéndice 11. Éste no es un comando ISO.
Realizar una comprobación aleatoria del archivo y almacenar temporalmente el valor obtenido			
OK	⇨		
	⇦	READ BINARY	Si el archivo contiene más datos de los que caben en la memoria temporal del lector o de la tarjeta, habrá que repetir el comando hasta que se haya leído el archivo completo
Datos del archivo OK	⇨	Almacenar los datos recibidos en un ESM	Según el apartado to 3.4 Formato de almacenamiento de datos
	⇦	PSO: COMPUTE DIGITAL SIGNATURE	
Realizar operación de seguridad. Calcular firma digital' utilizando el valor de comprobación aleatoria almacenado temporalmente			
Firma OK	⇨	Añadir datos a los datos previamente almacenados en el ESM	Según el apartado 3.4 Formato de almacenamiento de datos

3.3.4. ***Secuencia para reiniciar el contador del calibrado***

DDP_039 A continuación se muestra la secuencia para reiniciar el contador `NoOfCalibrationsSinceDownload` en el EF `Card_Download`, incluido en una tarjeta del centro de ensayo:

Tarjeta	Dir	IDE/IFD	Significado/Observaciones
	⇦	SELECT FILE EF `Card_Download`	Selección de archivo utilizando su identificador
OK	⇨		
	⇦	UPDATE BINARY `NoOfCalibrationsSinceDownload` = '00 00'	
reinicia el número de transferencia de la tarjeta			
OK	⇨		

3.4. **Formato de almacenamiento de datos**

3.4.1. ***Introducción***

DDP_040 Los datos transferidos deben almacenarse de acuerdo con las condiciones siguientes:

— Los datos almacenados deben ser transparentes. Es decir, durante el almacenamiento es preciso respetar el orden de los bytes que se transfieren de la tarjeta, así como el orden de los bits contenidos en cada byte.

— Todos los archivos de la tarjeta cuyos datos se transfieren en una sesión se almacenan en un archivo dentro del ESM.

3.4.2. ***Formato de archivo***

DDP_041 El formato de archivo es una concatenación de varios objetos TLV.

DDP_042 La etiqueta de un EF consiste en el FID más la terminación "00".

DDP_043 La etiqueta de la firma de un EF consiste en el FID del archivo más la terminación "01".

DDP_044 La longitud es un valor de dos bytes. Este valor define el número de bytes en el campo de valor. El valor "FF FF" en el campo de longitud se reserva para uso futuro.

DDP_045 Si un archivo no se transfiere, no deberá almacenarse ninguna información relacionada con dicho archivo (ni la etiqueta ni la longitud cero).

DDP_046 Inmediatamente después del objeto TLV que contiene los datos del archivo, habrá que almacenar una firma como el siguiente objeto TLV.

Definición	Significado	Longitud
FID (2 bytes) || "00"	Etiqueta para EF (FID)	3 bytes
FID (2 bytes) || "01"	Etiqueta para firma de EF (FID)	3 bytes
xx xx	Longitud del campo de valor	2 bytes

Ejemplo de datos en un archivo transferido y almacenado en un ESM:

Etiqueta	Longitud	Valor
`00 02 00`	`00 11`	Datos del archivo `ICC`
`C1 00 00`	`00 C2`	Datos del archivo EF `Card_Certificate`
		…
`05 05 00`	`0A 2E`	Datos del archivo EF `Vehicles_Used`
`05 05 01`	`00 80`	Firma del archivo `Vehicles_Used`

4. TRANSFERENCIA DE LOS DATOS DE UNA TARJETA DE TACÓGRAFO A TRAVÉS DE UNA UNIDAD INTRAVEHICULAR

DDP_047 La VU debe permitir la transferencia del contenido de una tarjeta de conductor insertada en un IDE conectado.

DDP_048 El IDE deberá enviar a la VU el mensaje "Petición de transferencia de datos de la tarjeta" para iniciar este modo (véase el punto 9).

DDP_049 A continuación, la VU deberá transferir todos los datos de la tarjeta, archivo por archivo, de acuerdo con el protocolo de transferencia descrito en el punto 3, para luego enviar al IDE todos los datos recibidos de la tarjeta. Estos datos se envían con el formato adecuado de archivo TLV (véase el apartado 3.4.2) y encapsulados en un mensaje de "Respuesta positiva a la petición de transferencia de datos".

DDP_050 El IDE deberá recuperar los datos contenidos en el mensaje de "Respuesta positiva a la petición de transferencia de datos" (separando todas las cabeceras, SIDs, TREPs, contadores de submensajes y sumas de control) y almacenarlos en un único archivo físico, tal y como se especifica en el punto 2.3.

DDP_051 A continuación, según proceda, la VU actualizará el archivo `ControlActivityData` o el `Card_Download` de la tarjeta del conductor.

Apéndice 8

PROTOCOLO DE CALIBRADO

ÍNDICE

1. INTRODUCCIÓN

El presente apéndice define el modo en que se intercambian datos entre una unidad intravehicular y un verificador a través de la línea K que forma parte de la interfaz de calibrado descrita en el apéndice 6. Asimismo, en el presente apéndice se explica el control de la línea de señal de entrada/salida en el conector de calibrado.

El establecimiento de las comunicaciones con una línea K se describe en el apartado 4 "Servicios de comunicación".

Este apéndice utiliza la idea de "sesiones de diagnóstico" para determinar el alcance del control de línea K bajo condiciones diversas. La sesión por defecto es la "StandardDiagnosticSession" en la cual todos los datos se pueden leer desde una unidad intravehicular pero no es posible escribir ningún dato en una unidad intravehicular.

La selección de la sesión de diagnóstico se explica en el apartado 5 "Servicios de administración".

CPR_001 La "ECUProgrammingSessions" permite la introducción de datos en la unidad intravehicular. Si se introducen datos de calibrado (requisitos 097 y 098), la unidad intravehicular deberá estar además en el modo de funcionamiento CALIBRADO.

La transferencia de datos a través de la línea K se describe en el apartado 6 "Servicios de transmisión de datos". Los formatos de los datos transferidos se detallan en el apartado 8 "Formatos dataRecords".

CPR_002 La "ECUAdjustementSession" permite seleccionar el modo I/O de la línea de señal I/O de calibrado a través de la interfaz de la línea K. El procedimiento de control de la línea de señal I/O de calibrado se describe en el apartado 7 "Control de los impulsos de prueba — Unidad funcional para control de entrada/salida".

CPR_003 En todo el documento, nos referiremos a la dirección del verificador como 'tt'. A pesar de que puedan existir direcciones preferentes para los verificadores, la VU deberá responder correctamente a cualquier dirección de verificador. La dirección física de la VU es 0xEE.

2. TÉRMINOS, DEFINICIONES Y REFERENCIAS

Todos los protocolos, mensajes y códigos de error se rigen principalmente por el proyecto actual de norma ISO 14229-1 (Vehículos de carretera. Sistemas de diagnóstico. Parte 1: Servicios de diagnóstico, versión de 6 de febrero de 2001).

La codificación de bytes y los valores hexadecimales se utilizan para los identificadores de servicios, las peticiones y respuestas de servicio, y los parámetros normalizados.

El término "verificador" se refiere al equipo empleado para introducir datos de programación/calibrado en la VU.

Los términos "cliente" y "servidor" se emplean de acuerdo con lo dispuesto en la norma ISO14230 y se refieren al verificador y a la VU, respectivamente.

Referencias:

ISO 14230-2: Vehículos de carretera — Sistemas de diagnóstico — Protocolo Keyword 2000 — Parte 2: Nivel de enlace de datos. Primera edición: 1999. Vehículos de carretera — Sistemas de diagnóstico.

3. VISIÓN GENERAL DE LOS SERVICIOS

3.1. **Servicios disponibles**

La tabla siguiente ofrece una visión general de los servicios que estarán disponibles en el aparato de control y que se definen en el presente documento.

CPR_004 La tabla indica los servicios que están disponibles en una sesión de diagnóstico activada.

— La 1ª columna especifica los servicios que están disponibles.

— La 2ª columna incluye el número de apartado del presente apéndice donde se ofrece mas información sobre el servicio que corresponda.

— La 3ª columna asigna los valores de identificador de servicio (Sid) para los mensajes de petición.

— La 4ª columna especifica los servicios de la "StandardDiagnosticSession" (SD) que deben aplicarse en cada VU.

— La 5ª columna especifica los servicios de la "ECUAdjustmentSession" (ECUAS) que deben aplicarse para poder controlar la línea de señal I/O en el conector de calibrado de la VU, situado en el panel frontal.

— La 6ª columna especifica los servicios de la "ECUProgrammingSession" (ECUPS) que deben aplicarse para poder programar los parámetros en la VU.

Tabla 1

Tabla resumen con los valores de los identificadores de servicios

			Sesiones de diagnóstico		
Nombre del servicio de diagnóstico	Nº de apartado	Valor SId petición	SD	ECUAS	ECUPS
StartCommunication	4.1	81	■	■	■
StopCommunication	4.2	82	■		
Testerpresent	4.3	3E	■	■	■
StartDiagnosticSession	5.1	10	■	■	■
SecurityAccess	5.2	27	■	■	■
ReadDataByIdentifier	6.1	22	■	■	■
WriteDataByIdentifier	6.2	2E			■
InputOutputControlByIdentifier	7.1	2F		■	

■ Este símbolo indica que el servicio es obligatorio en esa sesión de diagnóstico.
La ausencia de símbolo indica que el servicio no se admite en esa sesión de diagnóstico.

3.2. **Códigos de respuesta**

Se definen los códigos de respuesta para cada servicio.

4. SERVICIOS DE COMUNICACIÓN

Estos servicios son necesarios para establecer y mantener la comunicación, y no aparecen en el nivel de aplicación. Los servicios disponibles se especifican en la tabla siguiente:

Tabla 2

Servicios de comunicación

Nombre del servicio	Descripción
StartCommunication	El cliente solicita el comienzo de una sesión de comunicación con uno o varios servidores
StopCommunication	El cliente solicita el término de la sesión de comunicación actual
TesterPresent	El cliente indica al servidor que todavía está presente

CPR_005 El servicio StartCommunication sirve para comenzar una comunicación. A fin de utilizar un servicio, es preciso inicializar la comunicación y que los parámetros de comunicación sean adecuados para el modo deseado.

4.1. **Servicio StartCommunication**

CPR_006 Nada más recibir una indicación primitiva StartCommunication, la VU deberá comprobar si el enlace de comunicación solicitado se puede inicializar en las condiciones que haya en ese momento. Las condiciones válidas para la inicialización de un enlace de comunicación se describen en la norma ISO 14230-2.

CPR_007 A continuación, la VU hace todo lo necesario para inicializar el enlace de comunicación y enviar una primitiva de respuesta StartCommunication con los parámetros de respuesta positiva seleccionados.

CPR_008 Si una VU que ya está inicializada (y ha entrado en una sesión de diagnóstico) recibe una nueva petición StartCommunication Request (por ejemplo, debido a la recuperación de un error en el verificador), la petición será aceptada y la VU se reinicializará.

CPR_009 Si el enlace de comunicación no se puede inicializar por algún motivo, la VU deberá seguir funcionando del modo que lo estaba haciendo justo antes del intento de inicialización de dicho enlace de comunicación.

CPR_010 Es preciso asignar una dirección física al mensaje StartCommunication Request.

CPR_011 La inicialización de la VU para los servicios se efectúa a través de un método de "inicialización rápida".

— Antes de cualquier actividad hay un tiempo de inactividad del bus.

— A continuación el verificador envía una pauta de inicialización.

— Toda la información necesaria para establecer la comunicación está contenida en la respuesta de la VU.

CPR_012 Una vez concluida la inicialización:

— Todos los parámetros de comunicación se configuran con los valores definidos en la tabla 4 de acuerdo con los bytes clave.

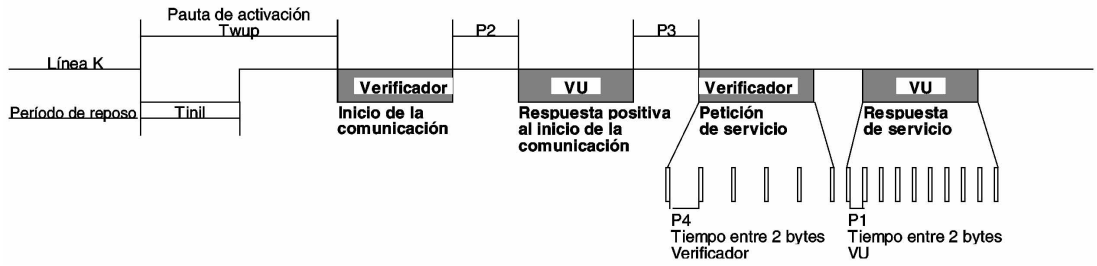
— La VU está esperando la primera petición del verificador.

— La VU se encuentra en el modo de diagnóstico por defecto, es decir, StandardDiagnosticSession.

— La línea de señal I/O de calibrado se encuentra en el estado por defecto, es decir, desactivada.

CPR_014 La velocidad de datos en la línea K será de 10400 baudios.

CPR_016 El verificador comienza la inicialización rápida transmitiendo una pauta de activación (Wup) por la línea K. La pauta comienza después del período de reposo de la línea K con un tiempo Tinil breve. El verificador transmite el primer bit del servicio StartCommunication después de un tiempo Twup que sigue al primer flanco descendente.



CPR_017 Los valores de sincronización para la inicialización rápida y las comunicaciones en general se describen con todo detalle en las tablas siguientes. Existen diferentes posibilidades para el tiempo de reposo (Trep):

— Primera transmisión después de conectar la alimentación, Trep = 300 ms.

— Después de haber terminado un servicio StopCommunication, Trep = P3 mín.

— Después de haberse interrumpido la comunicación por exceso del tiempo límite P3 máx, Trep = 0.

Tabla 3

Valores de sincronización para inicialización rápida

Parámetro		Valor mín.	Valor máx.
Tinil	25 ± 1 ms	24 ms	26 ms
Twup	50 ± 1 ms	49 ms	51 ms

Tabla 4

Valores de sincronización de la comunicación

Parámetro de sincronización	Descripción del parámetro	Valores límite inferior (ms)	Valores límite superior (ms)
		mín.	máx.
P1	Tiempo entre 2 bytes para respuesta de la VU	0	20
P2	Tiempo transcurrido entre la petición del verificador y la respuesta de la VU o entre dos respuestas de la VU	25	250
P3	Tiempo transcurrido desde el final de las respuestas de la VU hasta el comienzo de la nueva petición del verificador	55	5000
P4	Tiempo entre 2 bytes para petición del verificador	5	20

CPR_018 En las tablas siguientes se describe con detalle el formato de mensaje para inicialización rápida.

Tabla 5

Mensaje StartCommunication Request (petición de inicio de la comunicación)

Nº de byte	Nombre del parámetro	Valor hex	Término nemónico
#1	Byte de formato — asignación de dirección física	81	FMT
#2	Byte de dirección de destino	EE	TGT
#3	Byte de dirección de origen	tt	SRC
#4	StartCommunication Request Service	81	SCR
#5	Suma de control	00-FF	CS

Tabla 6

Mensaje StartCommunication Positive Response (respuesta positiva a la petición de inicio de la comunicación)

Nº de byte	Nombre del parámetro	Valor hex	Término nemónico
#1	Byte de formato — asignación de dirección física	80	FMT
#2	Byte de dirección de destino	tt	TGT
#3	Byte de dirección de origen	EE	SRC
#4	Byte de longitud adicional	03	LEN
#5	StartCommunication Positive Response Service Id	C1	SCRPR
#6	Byte clave 1	EA	KB1
#7	Byte clave 2	8F	KB2
#8	Suma de control	00-FF	CS

CPR_019 No hay respuesta negativa al mensaje StartCommunication Request. Si no hay un mensaje de respuesta positiva que transmitir, entonces la VU no se inicializa, no transmite ninguna información y continúa en el modo normal de funcionamiento.

4.2. **Servicio StopCommunication**

4.2.1. ***Descripción del mensaje***

Este servicio del nivel de comunicación sirve para poner fin a una sesión de comunicación.

CPR_020 Nada más recibir una indicación primitiva StopCommunication, la VU deberá comprobar si las condiciones que haya en ese momento permiten poner término a la comunicación. En caso afirmativo, la VU hará todo lo necesario para terminar la comunicación.

CPR_021 Si es posible poner fin a la comunicación, antes de que ésta termine la VU deberá emitir una primitiva de respuesta StopCommunication con los parámetros de respuesta positiva seleccionados.

CPR_022 Si por algún motivo no es posible poner fin a la comunicación, la VU deberá emitir una primitiva de respuesta StopCommunication con el parámetro de respuesta negativa seleccionado.

CPR_023 Si la VU detecta que se ha sobrepasado el tiempo límite P3máx, la comunicación deberá terminar sin que se emita una primitiva de respuesta.

4.2.2. ***Formato del mensaje***

CPR_024 En las tablas siguientes se describe con detalle los formatos de mensaje para las primitivas StopCommunication.

Tabla 7

Mensaje StopCommunication Request (petición de interrupción de la comunicación)

Nº de byte	Nombre del parámetro	Valor hex	Término nemónico
#1	Byte de formato — asignación de dirección física	80	FMT
#2	Byte de dirección de destino	EE	TGT
#3	Byte de dirección de origen	tt	SRC
#4	Byte de longitud adicional	01	LEN
#5	StopCommunication Request Service Id	82	SPR
#6	Suma de control	00-FF	CS

Tabla 8

Mensaje StopCommunication Positive Response (respuesta positiva a la petición de interrupción de la comunicación)

Nº de byte	Nombre del parámetro	Valor hex	Término nemónico
#1	Byte de formato — asignación de dirección física	80	FMT
#2	Byte de dirección de destino	tt	TGT
#3	Byte de dirección de origen	EE	SRC
#4	Byte de longitud adicional	01	LEN
#5	StopCommunication Positive Response Service	C2	SPRPR
#6	Suma de control	00-FF	CS

Tabla 9

Mensaje StopCommunication Negative Response (respuesta negativa a la petición de interrupción de la comunicación)

Nº de byte	Nombre del parámetro	Valor hex	Término nemónico
#1	Byte de formato — asignación de dirección física	80	FMT
#2	Byte de dirección de destino	tt	TGT
#3	Byte de dirección de origen	EE	SRC
#4	Byte de longitud adicional	03	LEN
#5	negative Response Service Id	7F	NR
#6	StopCommunication Request Service Identification	82	SPR
#7	responseCode = generalReject	10	RC_GR
#8	Suma de control	00-FF	CS

4.2.3. ***Definición de parámetros***

Este servicio no precisa definición de parámetros.

4.3. **Servicio TesterPresent**

4.3.1. ***Descripción del mensaje***

El servicio TesterPresent lo utiliza el verificador para indicar al servidor que sigue presente, con el fin de evitar que éste retorne automáticamente al funcionamiento normal y, posiblemente, interrumpa la comunicación. Este servicio, que se envía periódicamente, mantiene activa la comunicación / sesión de diagnóstico reinicializando el temporizador P3 cada vez que se recibe una petición de este servicio.

4.3.2. ***Formato del mensaje***

CPR_079 En las tablas siguientes se describen con detalle los formatos de mensaje para las primitivas TesterPresent.

Tabla 10

Mensaje TesterPresent Request (petición de presencia de verificador)

Nº de byte	Nombre del parámetro	Valor hex	Término nemónico
#1	Byte de formato — asignación de dirección física	80	FMT
#2	Byte de dirección de destino	EE	TGT
#3	Byte de dirección de origen	tt	SRC
#4	Byte de longitud adicional	02	LEN
#5	TesterPresent Request Service Id	3E	TP
#6	Sub Function = responseRequired = [sí	01	RESPREQ_Y
	no]	02	RESPREQ_NO
#7	Suma de control	00-FF	CS

CPR_080 Si se pone a "sí" el parámetro responseRequired, el servidor responderá con el mensaje de respuesta positiva siguiente. Si se pone a "no", el servidor no enviará respuesta.

Tabla 11

Mensaje TesterPresent Positive Response (respuesta positiva a la presencia de verificador)

Nº de byte	Nombre del parámetro	Valor hex	Término nemónico
#1	Byte de formato — asignación de dirección física	80	FMT
#2	Byte de dirección de destino	tt	TGT
#3	Byte de dirección de origen	EE	SRC
#4	Byte de longitud adicional	01	LEN
#5	TesterPresent Positive Response Service Id	7E	TPPR
#6	Suma de control	00-FF	CS

CPR_081 El servicio soportará los siguientes códigos de respuesta negativa:

Tabla 12

Mensaje TesterPresent Negative Response (respuesta negativa a la presencia de verificador)

Nº de byte	Nombre del parámetro	Valor hex	Término nemónico
#1	Byte de formato — asignación de dirección física	80	FMT
#2	Byte de dirección de destino	tt	TGT
#3	Byte de dirección de origen	EE	SRC
#4	Byte de longitud adicional	03	LEN
#5	negative Response Service Id	7F	NR
#6	TesterPresent Request Service Identification	3E	TP
#7	responseCode = [SubFunctionNotSupported-InvalidFormat	12	RC_SFNS_IF
	incorrectMessageLength]	13	RC_IML
#8	Suma de control	00-FF	CS

5. SERVICIOS DE ADMINISTRACIÓN

Los servicios disponibles se describen con detalle en la tabla siguiente:

Tabla 13

Servicios de administración

Nombre del servicio	Descripción
StartDiagnosticSession	El cliente solicita el comienzo de una sesión de diagnóstico con una VU
SecurityAccess	El cliente solicita acceso a las funciones restringidas a usuarios autorizados

5.1. **Servicio StartDiagnosticSession**

5.1.1. ***Descripción del mensaje***

CPR_025 El servicio StartDiagnosticSession sirve para activar diferentes sesiones de diagnóstico en el servidor. Una sesión de diagnóstico activa un conjunto específico de servicios de acuerdo con la Tabla 17. Una sesión puede activar servicios específicos de un fabricante de vehículos que no forman parte del presente documento. Las reglas de aplicación deberán cumplir los siguientes requisitos.

— Habrá siempre exactamente una sesión de diagnóstico activa en la VU.

— La VU iniciará siempre la StandardDiagnosticSession al encendido. Si no se inicia ninguna otra sesión de diagnóstico, se estará ejecutando la StandardDiagnosticSession mientras la VU esté encendida.

— Si el verificador solicita una sesión de diagnóstico que se está ejecutando ya, la VU enviará un mensaje de respuesta positiva.

— Cuando el verificador solicite una nueva sesión de diagnóstico, la VU enviará primero un mensaje de respuesta positiva StartDiagnosticSession antes de que la nueva sesión se active en la VU. Si la VU no puede iniciar la nueva sesión de diagnóstico solicitada, responderá con un mensaje de respuesta negativa StartDiagnosticSession, y proseguirá la sesión ya activa.

CPR_026 Sólo se iniciará una sesión de diagnóstico si se ha establecido comunicación entre el cliente y la VU.

CPR_027 Los parámetros de sincronización definidos en la Tabla 4 deben estar activados tras comenzar la sesión de diagnóstico (StartDiagnosticSession). El parámetro diagnosticSession estará configurado a “StandardDiagnosticSession” (sesión normal) en el mensaje de petición si previamente estaba activada otra sesión de diagnóstico.

5.1.2. ***Formato del mensaje***

CPR_028 En las tablas siguientes se describe con detalle los formatos de mensaje para las primitivas StartDiagnosticSession.

Tabla 14

Mensaje StartDiagnosticSession Request (petición de inicio de la sesión de diagnóstico)

Nº de byte	Nombre del parámetro	Valor hex	Término nemónico
#1	Byte de formato — asignación de dirección física	80	FMT
#2	Byte de dirección de destino	EE	TGT
#3	Byte de dirección de origen	tt	SRC
#4	Byte de longitud adicional	02	LEN
#5	StartDiagnosticSession Request Service Id	10	STDS
#6	diagnosticSession = [un valor de la Tabla 17]	xx	DS_…
#7	Suma de control	00-FF	CS

Tabla 15

Mensaje StartDiagnosticSession Positive Response (respuesta positiva a la petición de inicio de la sesión de diagnóstico)

Nº de byte	Nombre del parámetro	Valor hex	Término nemónico
#1	Byte de formato — asignación de dirección física	80	FMT
#2	Byte de dirección de destino	tt	TGT
#3	Byte de dirección de origen	EE	SRC
#4	Byte de longitud adicional	02	LEN
#5	StartDiagnosticSession Positive Response Service Id	50	STDSPR
#6	diagnosticSession = [el mismo valor que en el byte nº 6 de la Tabla 14]	xx	DS_…
#7	Suma de control	00-FF	CS

Tabla 16

Mensaje StartDiagnosticSession Negative Response (respuesta negativa a la petición de inicio de la sesión de diagnóstico)

Nº de byte	Nombre del parámetro	Valor hex	Término nemónico
#1	Byte de formato — asignación de dirección física	80	FMT
#2	Byte de dirección de destino	tt	TGT
#3	Byte de dirección de origen	EE	SRC
#4	Byte de longitud adicional	03	LEN
#5	Negative Response Service Id	7F	NR
#6	StartDiagnosticSession Request Service Id	10	STDS
#7	ResponseCode = [subFunctionNotSupported ([a])	12	RC_SFNS
	incorrectMessageLength ([b])	13	RC_IML
	conditionsNotCorrect ([c])]	22	RC_CNC
#8	Suma de control	00-FF	CS

([a]) el valor introducido en el byte nº 6 del mensaje de petición es inadmisible; es decir, no figura en la Tabla 17.
([b]) la longitud del mensaje no es correcta.
([c]) no se satisfacen los criterios de la petición StartDiagnosticSession.

5.1.3. ***Definición de parámetros***

CPR_029 El servicio StartDiagnosticSession utiliza el parámetro diagnosticSession (DS_) para seleccionar el comportamiento específico del servidor o servidores. En el presente documento se especifican las siguientes sesiones de diagnóstico:

Tabla 17

Definición de valores de la sesión de diagnóstico

Hex	Descripción	Término nemónico
81	StandardDiagnosticSession (sesión de diagnóstico normal) Esta sesión de diagnóstico activa todos los servicios especificados en la Tabla 1, columna 4 "SD". Dichos servicios permiten la lectura de datos de un servidor (VU). Esta sesión de diagnóstico se activa después de haber finalizado con éxito la inicialización entre el cliente (verificador) y el servidor (VU). Es posible que otras sesiones de diagnóstico especificadas en este apartado sobrescriban esta sesión de diagnóstico.	SD
85	ECUProgrammingSession (sesión de programación ECUPS) Esta sesión de diagnóstico activa todos los servicios especificados en la Tabla 1, columna 6 "ECUPS". Dichos servicios admiten la programación de memoria de un servidor (VU). Es posible que otras sesiones de diagnóstico especificadas en este apartado sobrescriban esta sesión de diagnóstico.	ECUPS
87	ECUAdjustmentSession (sesión de ajuste ECUA) Esta sesión de diagnóstico activa todos los servicios especificados en la columna 5 "AS" de la Tabla 1, columna 5 "ECUAS". Dichos servicios admiten el control de entrada/salida de un servidor (VU). Es posible que otras sesiones de diagnóstico especificadas en este apartado sobrescriban esta sesión de diagnóstico.	ECUAS

5.2. **Servicio SecurityAccess**

No es posible escribir datos de calibrado ni acceder a la línea de entrada/salida de calibrado a menos que la VU se encuentre en el modo CALIBRADO. Para poder acceder al modo CALIBRADO es preciso insertar una tarjeta de centro de ensayo válida y además introducir el PIN adecuado en la VU.

El servicio SecurityAccess es un medio para introducir el PIN y para indicar al verificador si la VU se encuentra o no en el modo CALIBRADO.

El PIN también se puede introducir por otros métodos.

5.2.1. ***Descripción del mensaje***

El servicio SecurityAccess se compone de un mensaje SecurityAccess "requestSeed", seguido eventualmente de un mensaje SecurityAccess "sendKey". El servicio SecurityAccess debe utilizarse después del servicio StartDiagnosticSession.

CPR_033 El verificador deberá utilizar el mensaje SecurityAccess "requestSeed" para comprobar si la unidad intravehicular está preparada para aceptar un PIN.

CPR_034 Si la unidad intravehicular ya se encuentra en el modo CALIBRADO, deberá contestar a la petición enviando una "simiente" (seed) de 0x0000, utilizando para ello el servicio SecurityAccess Positive Response.

CPR_035 Si la unidad intravehicular está preparada para aceptar un PIN para la verificación por parte de una tarjeta de centro de ensayo, deberá contestar a la petición enviando una "simiente" (seed) mayor que 0x0000, utilizando para ello el servicio SecurityAccess Positive Response.

CPR_036 Si la unidad intravehicular no está preparada para aceptar un PIN del verificador, ya sea porque la tarjeta del centro de ensayo que se ha insertado no es válida, porque no se ha insertado una tarjeta del centro de ensayo, o porque la unidad intravehicular espera el PIN de otro método, deberá contestar a la petición con una respuesta negativa, con un código de respuesta configurado a conditionsNotCorrectOrRequestSequenceError.

CPR_037 A continuación, el verificador utilizará en su caso el mensaje SecurityAccess "sendKey" para enviar un PIN a la unidad intravehicular. A fin de dar tiempo suficiente para el proceso de autenticación de la tarjeta, la VU utilizará el código de respuesta negativa requestCorrectlyReceived-ResponsePending para ampliar el tiempo de respuesta. Sin embargo, el tiempo de respuesta máximo no excederá de 5 minutos. En cuanto quede completado el servicio solicitado, la VU enviará un mensaje de respuesta positiva o un mensaje de respuesta negativa con un código de respuesta distinto de éste. La VU podrá repetir el código de respuesta negativa requestCorrectlyReceived-ResponsePending hasta que quede completado el servicio solicitado y se envíe el mensaje de respuesta final.

CPR_038 La unidad intravehicular deberá contestar a esta petición utilizando el servicio SecurityAccess Positive Response, exclusivamente cuando se encuentre en el modo de CALIBRADO.

CPR_039 En los casos siguientes, la unidad intravehicular deberá contestar a esta petición con una respuesta negativa, con un código de respuesta configurado a:

— subFunctionNotSupported: Formato del parámetro de subfunción no válido (accessType),

— conditionsNotCorrectOrRequestSequenceError: La unidad intravehicular no está lista para aceptar una entrada PIN,

— invalidKey: El PIN no es válido y no se ha sobrepasado el número de intentos de verificación del PIN,

— exceedNumberOfAttempts: El PIN no es válido y se ha sobrepasado el número de intentos de verificación del PIN,

— generalReject: El PIN es correcto pero ha fallado la autentificación mutua con la tarjeta del centro de ensayo.

5.2.2. ***Formato del mensaje — SecurityAccess — requestSeed***

CPR_040 En las tablas siguientes se describe con detalle los formatos de mensaje para las primitivas SecurityAccess "requestSeed".

Tabla 18

Mensaje SecurityAccess Request- requestSeed (petición de simiente)

Nº de byte	Nombre del parámetro	Valor hex	Término nemónico
#1	Byte de formato — asignación de dirección física	80	FMT
#2	Byte de dirección de destino	EE	TGT
#3	Byte de dirección de origen	tt	SRC
#4	Byte de longitud adicional	02	LEN
#5	SecurityAccess Request Service Id	27	SA
#6	accessType — requestSeed	7D	AT_RSD
#7	Suma de control	00-FF	CS

Tabla 19

Mensaje SecurityAccess — requestSeed Positive Response (respuesta positiva a la petición de simiente)

Nº de byte	Nombre del parámetro	Valor hex	Término nemónico
#1	Byte de formato — asignación de dirección física	80	FMT
#2	Byte de dirección de destino	tt	TGT
#3	Byte de dirección de origen	EE	SRC
#4	Byte de longitud adicional	04	LEN
#5	SecurityAccess Positive Response Service Id	67	SAPR
#6	accessType — requestSeed	7D	AT_RSD
#7	Seed High	00-FF	SEEDH
#8	Seed Low	00-FF	SEEDL
#9	Suma de control	00-FF	CS

Tabla 20

Mensaje SecurityAccess Negative Response (respuesta negativa)

Nº de byte	Nombre del parámetro	Valor hex	Término nemónico
#1	Byte de formato — asignación de dirección física	80	FMT
#2	Byte de dirección de destino	tt	TGT
#3	Byte de dirección de origen	EE	SRC
#4	Byte de longitud adicional	03	LEN
#5	NegativeResponse Service Id	7F	NR
#6	SecurityAccess Request Service Id	27	SA
#7	responseCode = [conditionsNotCorrectOrRequestSequenceError incorrectMessageLength]	22 13	RC_CNC RC_IML
#8	Suma de control	00-FF	CS

5.2.3. ***Formato del mensaje — SecurityAccess — sendKey***

CPR_041 En las tablas siguientes se describe con detalle los formatos de mensaje para las primitivas SecurityAccess — sendKey.

Tabla 21

Mensaje SecurityAccess Request — sendKey (envío de clave)

Nº de byte	Nombre del parámetro	Valor hex	Término nemónico
#1	Byte de formato — asignación de dirección física	80	FMT
#2	Byte de dirección de destino	EE	TGT
#3	Byte de dirección de origen	tt	SRC
#4	Byte de longitud adicional	m+2	LEN
#5	SecurityAccess Request Service Id	27	SA
#6	accessType — sendKey	7E	AT_SK
#7 a #m+6	Clave #1 (alto) … Clave #m (bajo, m debe ser como mínimo 4 y como máximo 8)	xx … xx	KEY
#m+7	Suma de control	00-FF	CS

Tabla 22

Mensaje SecurityAccess — sendKey Positive Response (respuesta positiva)

Nº de byte	Nombre del parámetro	Valor hex	Término nemónico
#1	Byte de formato — asignación de dirección física	80	FMT
#2	Byte de dirección de destino	tt	TGT
#3	Byte de dirección de origen	EE	SRC
#4	Byte de longitud adicional	02	LEN
#5	SecurityAccess Positive Response Service Id	67	SAPR
#6	accessType — sendKey	7E	AT_SK
#7	Suma de control	00-FF	CS

Tabla 23

Mensaje SecurityAccess Negative Response (respuesta negativa)

Nº de byte	Nombre del parámetro	Valor hex	Término nemónico
#1	Byte de formato — asignación de dirección física	80	FMT
#2	Byte de dirección de destino	tt	TGT
#3	Byte de dirección de origen	EE	SRC
#4	Byte de longitud adicional	03	LEN
#5	NegativeResponse Service Id	7F	NR
#6	SecurityAccess Request Service Id	27	SA
#7	ResponseCode = [generalReject	10	RC_GR
	subFunctionNotSupported	12	RC_SFNS
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
	invalidKey	35	RC_IK
	exceededNumberOfAttempts	36	RC_ENA
	requestCorrectlyReceived-ResponsePending]	78	RC_RCR_RP
#8	Suma de control	00-FF	CS

6. SERVICIOS DE TRANSMISIÓN DE DATOS

En la tabla siguiente se describen con detalle los servicios disponibles:

Tabla 24

Servicios de transmisión de datos

Nombre del servicio	Descripción
ReadDataByIdentifier	El cliente solicita la transmisión del valor actual de un registro con acceso mediante recordDataIdentifier
WriteDataByIdentifier	El cliente solicita la escritura de un registro al que se acceda mediante recordDataIdentifier

6.1. **Servicio ReadDataByIdentifier**

6.1.1. ***Descripción del mensaje***

CPR_050 El servicio ReadDataByIdentifier lo utiliza el cliente para solicitar valores de registros de datos procedentes de un servidor e identificados mediante un recordDataIdentifier. Es responsabilidad del fabricante de la VU cumplir las condiciones del servidor al llevar a cabo este servicio.

6.1.2. ***Formato del mensaje***

CPR_051 En las tablas siguientes se describe con detalle los formatos de mensaje para las primitivas ReadDataByIdentifier.

Tabla 25

Mensaje ReadDataByIdentifier Request (petición del servicio)

Nº de byte	Nombre del parámetro	Valor hex	Término nemónico
#1	Byte de formato — asignación de dirección física	80	FMT
#2	Byte de dirección de destino	EE	TGT
#3	Byte de dirección de origen	tt	SRC
#4	Byte de longitud adicional	03	LEN
#5	ReadDataByIdentifier Request Service Id	22	RDBI
#6 bis #7	recordDataIdentifier = [un valor de la Tabla 28]	xxxx	RDI_…
#8	Suma de control	00-FF	CS

Tabla 26

Mensaje ReadDataByIdentifier Positive Response (respuesta positiva a la petición de servicio)

Nº de byte	Nombre del parámetro	Valor hex	Término nemónico
#1	Byte de formato — asignación de dirección física	80	FMT
#2	Byte de dirección de destino	tt	TGT
#3	Byte de dirección de origen	EE	SRC
#4	Byte de longitud adicional	m+3	LEN
#5	ReadDataByIdentifier Positive Response Service Id	62	RDBIPR
#6 y #7	recordDataIdentifier = [mismo valor que los bytes #6 y #7 Tabla 25]	xxxx	RDI_…
#8 a #m+7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Suma de control	00-FF	CS

Tabla 27

Mensaje ReadDataByIdentifier Negative Response (respuesta negativa a la petición de servicio)

Nº de byte	Nombre del parámetro	Valor hex	Término nemónico
#1	Byte de formato — asignación de dirección física	80	FMT
#2	Byte de dirección de destino	tt	TGT
#3	Byte de dirección de origen	EE	SRC
#4	Byte de longitud adicional	03	LEN
#5	Negative Response Service Id	7F	NR
#6	ReadDataByIdentifier Request Service Id	22	RDBI
#7	ResponseCode = [requestOutOfRange incorrectMessageLength conditionsNotCorrect]	31 13 22	RC_ROOR RC_IML RC_CNC
#8	Suma de control	00-FF	CS

6.1.3. ***Definición de parámetros***

CPR_052 El parámetro recordDataIdentifier (RDI_) incluido en el mensaje ReadDataByIdentifier Request identifica un registro de datos.

CPR_053 La tabla siguiente muestra los valores recordDataIdentifier definidos en el presente documento.

La tabla recordDataIdentifier tiene cuatro columnas y múltiples filas.

— La 1ª columna (Hex) incluye el valor hexadecimal asignado al recordDataIdentifier especificado en la 3ª columna.

— La 2ª columna (Elemento de datos) especifica el elemento de datos, según el apéndice 1, en el que se basa el recordDataIdentifier (a veces es necesario transcodificar).

— La 3ª columna (Descripción) especifica el correspondiente nombre recordDataIdentifier.

— La 4ª columna (Término nemónico) especifica el término nemónico de este recordDataIdentifier.

Tabla 28

Definición de los valores de recordDataIdentifier (identificador de datos de registros)

Hex	Elemento de datos	Nombre recordDataIdentifier (véase formato en el punto 8.2)	Término nemónico
F90B	CurrentDateTime	TimeDate	RDI_TD
F912	HighResOdometer	HighResolutionTotalVehicleDistance	RDI_HRTVD
F918	K-ConstantOfRecordingEquipment	Kfactor	RDI_KF
F91C	L-TyreCircumference	LfactorTyreCircumference	RDI_LF
F91D	W-VehicleCharacteristicConstant	WvehicleCharacteristicFactor	RDI_WVCF
F921	TyreSize	TyreSize	RDI_TS
F922	nextCalibrationDate	NextCalibrationDate	RDI_NCD
F92C	SpeedAuthorised	SpeedAuthorised	RDI_SA
F97D	vehicleRegistrationNation	RegisteringMemberState	RDI_RMS
F97E	VehicleRegistrationNumber	VehicleRegistrationNumber	RDI_VRN
F190	VehicleIdentificationNumber	VIN	RDI_VIN

CPR_054 El mensaje ReadDataByIdentifier Positive Response utiliza el parámetro dataRecord (DREC_) para facilitar al cliente (verificador) el valor del registro de datos identificado por el recordDataIdentifier. Los formatos de datos se especifican en la sección 8. Pueden implementarse dataRecords opcionales de usuario adicionales, que incluyan datos específicos de la VU, tanto internos como de entrada y salida, pero no se definen en el presente documento.

6.2. **Servicio WriteDataByIdentifier**

6.2.1. ***Descripción del mensaje***

CPR_056 El cliente utiliza el servicio WriteDataByIdentifier para escribir valores de registros de datos en un servidor. Los datos se identifican con un recordDataIdentifier. El fabricante de la VU es el responsable de que se cumplan las condiciones del servidor cuando se utilice este servicio. Para actualizar los parámetros relacionados en la Tabla 28, la VU debe estar en el modo CALIBRADO.

6.2.2. ***Formato del mensaje***

CPR_057 En las tablas siguientes se describe con detalle los formatos de mensaje para las primitivas WriteDataByIdentifier.

Tabla 29

Mensaje WriteDataByIdentifier Request (petición del servicio)

Nº de byte	Nombre del parámetro	Valor hex	Término nemónico
#1	Byte de formato — asignación de dirección física	80	FMT
#2	Byte de dirección de destino	EE	TGT
#3	Byte de dirección de origen	tt	SRC
#4	Byte de longitud adicional	m+3	LEN
#5	WriteDataByIdentifier Request Service Id	2E	WDBI
#6 a #7	recordDataIdentifier = [un valor de la Tabla 28]	xxxx	RDI_…
#8 a #m+7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Suma de control	00-FF	CS

Tabla 30

Mensaje WriteDataByIdentifier Positive Response (respuesta positiva a la petición de servicio)

Nº de byte	Nombre del parámetro	Valor hex	Término nemónico
#1	Byte de formato — asignación de dirección física	80	FMT
#2	Byte de dirección de destino	tt	TGT
#3	Byte de dirección de origen	EE	SRC
#4	Byte de longitud adicional	03	LEN
#5	WriteDataByIdentifier Positive Response Service Id	6E	WDBIPR
#6 a #7	recordDataIdentifier = [mismo valor que bytes #6 y #7 Tabla 29	xxxx	RDI_…
#8	Suma de control	00-FF	CS

Tabla 31

Mensaje WriteDataByIdentifier Negative Response (respuesta negativa a la petición de servicio)

Nº de byte	Nombre del parámetro	Valor hex	Término nemónico
#1	Byte de formato — asignación de dirección física	80	FMT
#2	Byte de dirección de destino	tt	TGT
#3	Byte de dirección de origen	EE	SRC
#4	Byte de longitud adicional	03	LEN
#5	NegativeResponse Service Id	7F	NR
#6	WriteDataByIdentifier Request Service Id	2E	WDBI
#7	ResponseCode = [requestOutOfRange	31	RC_ROOR
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect]	22	RC_CNC
#8	Suma de control	00-FF	CS

6.2.3. ***Definición de parámetros***

El parámetro recordDataIdentifier (RDI_) se define en la Tabla 28.

El parámetro dataRecord (DREC_) lo utiliza el mensaje de petición WriteDataByIdentifier para facilitar al servidor (VU) los valores de registros de datos identificados por el recordDataIdentifier. Los formatos de datos se especifican en la sección 8.

7. CONTROL DE LOS IMPULSOS DE PRUEBA — UNIDAD FUNCIONAL PARA CONTROL DE ENTRADA/SALIDA

Los servicios disponibles se describen con detalle en la tabla siguiente:

Tabla 32

Unidad funcional para control de entrada/salida

Nombre del servicio	Descripción
InputOutputControlByIdentifier	El cliente solicita el control de una entrada/salida específica del servidor

7.1. **Servicio InputOutputControlByIdentifier**

7.1.1. ***Descripción del mensaje***

Existe una conexión, a través del conector frontal, que permite controlar o efectuar un seguimiento de los impulsos de prueba utilizando un verificador adecuado.

CPR_058 Esta línea de señal I/O de calibrado se puede configurar con el comando de la línea K empleando el servicio InputOutputControlByIdentifier para seleccionar la función de entrada o salida que se precise para la línea. Los estados de la línea disponibles son:

— desactivado,

— speedSignalInput, donde se utiliza la línea de señal I/O de calibrado para introducir una señal de velocidad (señal de prueba) que sustituye la señal de velocidad del sensor de movimiento,

— realTimeSpeedSignalOutputSensor, donde se utiliza la línea de señal I/O de calibrado para sacar la señal de velocidad del sensor de movimiento,

— RTCOutput, donde se utiliza la línea de señal I/O de calibrado para sacar la señal del reloj de TUC.

CPR_059 Para configurar el estado de la línea, la unidad intravehicular tiene que haber entrado en una sesión de ajuste y debe estar en el modo de CALIBRADO. Al salir de la sesión de ajuste o del modo de CALIBRADO, la unidad intravehicular debe cerciorarse de que la línea de señal I/O vuelve al estado "desactivado" (por defecto).

CPR_060 Si se reciben impulsos de velocidad por la línea de entrada de la VU para señales de velocidad en tiempo real, y la línea de señal I/O de calibrado está configurada para transmitir entradas, entonces dicha línea de señal I/O deberá configurarse para transmitir salidas o deberá volver al estado de desactivación.

CPR_061 Se seguirá el orden siguiente:

— establecer comunicación mediante el servicio StartCommunication,

— entrar en una sesión de ajuste mediante el servicio StartDiagnosticSession y estar en el modo de CALIBRADO (el orden de estas dos operaciones no es importante),

— cambiar el estado de la salida mediante el servicio InputOutputControlBylIdentifier.

7.1.2. ***Formato del mensaje***

CPR_062 En las tablas siguientes se describe con detalle los formatos de mensaje para las primitivas InputOutputControlByIdentifier.

Tabla 33

Mensaje InputOutputControlByIdentifier Request (petición del servicio)

Nº de byte	Nombre del parámetro	Valor hex	Término nemónico
#1	Byte de formato — asignación de dirección física	80	FMT
#2	Byte de dirección de destino	EE	TGT
#3	Byte de dirección de origen	tt	SRC
#4	Byte de longitud adicional	xx	LEN
#5	InputOutputControlByIdentifier Request Sid	2F	IOCBI
#6 y #7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 o #8 a #9	ControlOptionRecord = [		COR_…
	inputOutputControlParameter — un valor de la Tabla 36	xx	IOCP_…
	controlState — un valor de la Tabla 37 (véase nota)]	xx	CS_…
#9 o #10	Suma de control	00-FF	CS

Nota: El parámetro controlState sólo está presente en algunos casos (véase el punto 7.1.3).

Tabla 34

Mensaje InputOutputControlByIdentifier Positive Response (respuesta positiva a la petición de servicio)

Nº de byte	Nombre del parámetro	Valor hex	Término nemónico
#1	Byte de formato — asignación de dirección física	80	FMT
#2	Byte de dirección de destino	tt	TGT
#3	Byte de dirección de origen	EE	SRC
#4	Byte de longitud adicional	xx	LEN
#5	inputOutputControlByIdentifier Positive Response SId	6F	IOCBIPR
#6 y #7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 o #8 a #9	controlStatusRecord = [		CSR_
	inputOutputControlParameter (mismo valor que byte #8 Tabla 33)	xx	IOCP_…
	controlState (mismo valor que byte #9 Tabla 33)] (si es aplicable)	xx	CS_…
#9 o #10	Suma de control	00-FF	CS

Tabla 35

Mensaje InputOutputControlByIdentifier Negative Response (respuesta negativa a la petición de servicio)

Nº de byte	Nombre del parámetro	Valor hex	Término nemónico
#1	Byte de formato — asignación de dirección física	80	FMT
#2	Byte de dirección de destino	tt	TGT
#3	Byte de dirección de origen	EE	SRC
#4	Byte de longitud adicional	03	LEN
#5	negativeResponse Service Id	7F	NR
#6	inputOutputControlByIdentifier Request SId	2F	IOCBI
#7	responseCode = [		
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect	22	RC_CNC
	requestOutOfRange	31	RC_ROOR
	deviceControlLimitsExceeded]	7A	RC_DCLE
#8	Suma de control	00-FF	CS

7.1.3. ***Definición de parámetros***

CPR_064 El parámetro inputOutputControlParameter (IOCP_) se define en la tabla siguiente.

Tabla 36

Definición de los valores de inputOutputControlParameter

Hex	Descripción	Término nemónico
01	ReturnControlToECU Este valor deberá indicar al servidor (VU) que el verificador ya no tiene control sobre la línea de señal I/O de calibrado	RCTECU
01	ResetToDefault Este valor deberá indicar al servidor (VU) su obligación de reiniciar la señal de I/O de calibrado al estado que le corresponde por defecto	RTD
03	ShortTermAdjustment Este valor deberá indicar al servidor (VU) su obligación de ajustar la línea de señal de I/O de calibrado al valor incluido en el parámetro controlState	STA

CPR_065 El parámetro controlState, definido en la tabla siguiente, sólo está presente cuando el parámetro inputOutputControlParameter se ha configurado a ShortTermAdjustment.

Tabla 37

Definición de los valores de controlState

Modo	Valor hex	Descripción
Desactivado	00	Línea I/O desactivada (estado por defecto)
Activado	01	Línea I/O de calibrado activada como speedSignalInput
Activado	02	Línea I/O de calibrado activada como realTimeSpeedSignalOutputSensor
Activado	03	Línea I/O de calibrado activada como RTCOutput

8. FORMATOS DE DATARECORDS

En la presente sección se detallan:

— las reglas generales que se aplicarán a los intervalos de los parámetros transmitidos por la unidad intravehicular al verificador,

— los formatos que se utilizarán en los datos transferidos a través de los servicios de transmisión de datos descritos en la sección 6.

CPR_067 La VU admitirá todos los parámetros identificados.

CPR_068 Los datos transmitidos por la VU al verificador en respuesta a un mensaje de petición serán del tipo medido (es decir, el valor actual del parámetro solicitado medido u observado por el VU).

8.1. **Intervalos de los parámetros transmitidos**

CPR_069 En la Tabla 38 se definen los intervalos utilizados para determinar la validez de un parámetro transmitido.

CPR_070 Los valores del intervalo “indicador de error” constituyen un medio para que la unidad intravehicular indique inmediatamente que no dispone en ese momento de datos paramétricos válidos por causa de algún tipo de error en el equipo de grabación.

CPR_071 Los valores del intervalo “no disponible” constituyen un medio para que la unidad intravehicular transmita un mensaje que contiene un parámetro que no está disponible o no está admitido en ese módulo. Los valores del intervalo “no solicitado” constituyen un medio para que un dispositivo transmita un mensaje de comando e identifique para qué parámetros no se espera respuesta del dispositivo receptor.

CPR_072 Si el fallo de un componente impide la transmisión de datos válidos para un parámetro, deberá utilizarse en lugar de dichos datos el indicador de error descrito en la Tabla 38. Sin embargo, si los datos medidos o calculados adquieren un valor que es válido, pero se sale del intervalo definido para el parámetro, no se utilizará el indicador de error. Se transmitirán los datos utilizando el valor mínimo o máximo del parámetro según proceda.

Tabla 38

Intervalos dataRecords

Nombre del intervalo	1 byte (valor hex)	2 bytes (valor hex)	4 bytes (valor hex)	ASCII
Señal válida	00 a FA	0000 a FAFF	00000000 a FAFFFFFF	1 a 254
Indicador específico del parámetro	FB	FB00 a FBFF	FB000000 a FBFFFFFF	ninguno
Reservado para futuros bits de indicador	FC a FD	FC00 a FDFF	FC000000 a FDFFFFFF	ninguno
Indicador de error	FE	FE00 a FEFF	FE000000 a FEFFFFFF	0
No disponible o no solicitado	FF	FF00 a FFFF	FF000000 a FFFFFFFF	FF

CPR_073 Para los parámetros codificados en ASCII, el carácter ASCII "*" está reservado como delimitador.

8.2. **Formatos dataRecords**

De la Tabla 39 a la Tabla 42 se detallan los formatos que se usarán a través de los servicios ReadDataByIdentifier y WriteDataByIdentifier.

CPR_074 En la Tabla 39 se ofrece la longitud, resolución e intervalo operativo para cada parámetro identificado por su recordDataIdentifier:

Tabla 39

Formato de dataRecords

Nombre del parámetro	Longitud de dato (bytes)	Resolución	Intervalo operativo
TimeDate	8	Véanse detalles en la Tabla 40	
HighResolutionTotalVehicleDistance	4	avance 5 m/bit, inicio 0 m	0 a + 21 055 406 km
Kfactor	2	avance 0,001 pulsos/m/bit, inicio 0	0 a 64,255 pulsos/m
LfactorTyreCircumference	2	avance 0,125 10^{-3} m/bit, inicio 0	0 a 8 031 m
WvehicleCharacteristicFactor	2	avance 0,001 pulsos/m/bit, inicio 0	0 a 64,255 pulsos/m
TyreSize	15	ASCII	ASCII
NextCalibrationDate	3	Véanse detalles en la Tabla 41	
SpeedAuthorised	2	avance 1/256 km/h/bit, inicio 0	0 a 250 996 km/h
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	Véanse detalles en la Tabla 42	
VIN	17	ASCII	ASCII

CPR_075 En la Tabla 40 se detallan los formatos de los distintos bytes del parámetro TimeDate:

Tabla 40

Formato detallado de TimeDate (valor recordDataIdentifier # F00B)

Byte	Definición del parámetro	Resolución	Intervalo operativo
1	Segundos	avance 0,25 s/bit, inicio 0 s	0 a 59,75 s
2	Minutos	avance 1 min/bit, inicio 0 min	0 a 59 min
3	Horas	avance 1 h/bit, inicio 0 h	0 a 23 h
4	Meses	avance 1mes/bit, inicio 0 mes	1 a 12 meses
5	Días	avance 0,25 día/bit, inicio 0 día (véase Nota de la Tabla 41)	0,25 a 31,75 días
6	Año	avance 1 año/bit, inicio +1985 (véase Nota de la Tabla 41)	1985 a 2235
7	Local Minute Offset	avance 1 min/bit, inicio – 125 min	– 59 a 59 min
8	Local Hour Offset	avance 1 h/bit, inicio – 125 h	– 23 a + 23 h

CPR_076 En la Tabla 41 se detallan los formatos de los distintos bytes del parámetro NextCalibrationDate.

Tabla 41

Formato detallado de NextCalibrationDate (valor recordDataIdentifier # F022)

Byte	Definición del parámetro	Resolución	Intervalo operativo
1	Mes	avance 1 mes/bit, 0 mes	1 a 12 meses
2	Día	avance 0,25 día/bit, 0 día (véase Nota)	0,25 a 31,75 días
3	Año	avance 1 año/bit, inicio +1985 (véase Nota)	1985 a 2235

Nota relativa al uso del parámetro "Día":
1. Un valor de 0 para la fecha es nulo. Los valores 1, 2, 3 y 4 se utilizan para identificar el primer día del mes; 5, 6, 7 y 8 para el segundo; etc.
2. Este parámetro no influye el parámetro de horas ni lo modifica.

Nota relativa al uso del parámetro "Año":
Un valor de 0 para el año identifica el año 1985; un valor de 1, el año 1986; etc.

CPR_078 En la Tabla 42 se detallan los formatos de los distintos bytes del parámetro VehicleRegistrationNumber:

Tabla 42

Formato detallado de VehicleRegistrationNumber (valor recordDataIdentifier # F07E)

Byte	Definición del parámetro	Resolución	Intervalo operativo
1	Página de código (según se define en el apéndice 1)	ASCII	01 a 0A
2 a 14	Número de registro del vehículo (según se define en el apéndice 1)	ASCII	ASCII

Apéndice 9

HOMOLOGACIÓN DE MODELO RELACIÓN DE PRUEBAS MÍNIMAS EXIGIDAS

ÍNDICE

1. INTRODUCCIÓN

1.1. **Homologación**

La homologación CEE de un aparato de control (o componente) o de una tarjeta de tacógrafo se basa en:

— una certificación de seguridad, realizada por una autoridad ITSEC, para acreditar el cumplimiento de un objetivo de seguridad conforme al apéndice 10 del presente anexo,

— una certificación funcional, realizada por una autoridad de un Estado miembro, para certificar que el elemento sujeto a verificación cumple los requisitos del presente anexo en cuanto a las funciones que desempeña, la exactitud de medición y las características medioambientales,

— una certificación de interoperabilidad, realizada por un organismo competente, para garantizar que el aparato de control (o la tarjeta de tacógrafo) puede interoperar sin restricciones con los modelos necesarios de tarjeta de tacógrafo (o aparato de control) (véase el capítulo VIII del presente anexo).

En el presente apéndice se especifican las pruebas mínimas que debe realizar la autoridad del Estado miembro durante los ensayos funcionales, y las pruebas mínimas que debe realizar el organismo competente durante los ensayos de interoperabilidad, aunque no se determina el tipo de pruebas ni los procedimientos a seguir durante las mismas.

El presente apéndice no se ocupa de los aspectos relativos a la certificación de seguridad. Si durante la evaluación de seguridad y el proceso de certificación se llevan a cabo algunas de las pruebas exigidas para la homologación, no habrá que repetirlas posteriormente. En ese caso, tan solo se comprobarán los resultados de dichas pruebas de seguridad. A título informativo, en el presente apéndice hemos marcado con un asterisco ("*") las condiciones que es preciso verificar (y también las condiciones estrechamente asociadas con pruebas que deban realizarse) durante la certificación de seguridad.

El presente apéndice trata por separado la homologación del sensor de movimiento y la homologación de la unidad intravehicular, al tratarse de componentes del aparato de control. La interoperabilidad entre todos los modelos de sensor de movimiento y todos los modelos de unidad intravehicular no es una condición necesaria, de manera que la homologación de un sensor de movimiento sólo podrá concederse en combinación con la homologación de una unidad intravehicular, y viceversa.

1.2. **Referencias**

En el presente apéndice se utilizan las referencias siguientes:

IEC 68-2-1	Verificación medioambiental — Parte 2: Pruebas — Pruebas A: Frío. 1990 + Modificación 2: 1994.
IEC 68-2-2	Verificación medioambiental — Parte 2: Pruebas — Pruebas B: Calor seco. 1974 + Modificación 2: 1994.
IEC 68-2-6	Procedimientos básicos de verificación medioambiental — Métodos de ensayo — Prueba Fc y orientaciones: Vibración (sinusoidal). 6ª edición: 1985.
IEC 68-2-14	Procedimientos básicos de verificación medioambiental — Métodos de ensayo — Prueba N: Cambio de temperatura. Modificación 1: 1986.
IEC 68-2-27	Procedimientos básicos de verificación medioambiental — Métodos de ensayo —Prueba Ea y orientaciones: Choque. Edición 3: 1987.
IEC 68-2-30	Procedimientos básicos de verificación medioambiental — Métodos de ensayo — Prueba Db y orientaciones: Calor húmedo, cíclico (ciclo de 12 + 12 horas). Modificación 1: 1985.
IEC 68-2-35	Procedimientos básicos de verificación medioambiental — Métodos de ensayo — Prueba Fda: Banda ancha de vibración aleatoria — Reproducibilidad alta. Modificación 1: 1983.
IEC 529	Niveles de protección ofrecidos por cubiertas (códigos IP). Edición 2: 1989.
IEC 61000-4-2	Compatibilidad electromagnética (EMC) — Técnicas de ensayo y medición — Prueba de inmunidad a descargas electrostáticas: 1995/Modificación 1: 1998.
ISO 7637-1	Vehículos de carretera — Perturbaciones eléctricas por conducción y acoplamiento — Parte 1: Turismos y vehículos comerciales ligeros con una tensión de alimentación nominal de 12 V — Conducción eléctrica transitoria por líneas de alimentación exclusivamente. Edición 2: 1990.

ISO 7637-2 Vehículos de carretera — Perturbaciones eléctricas por conducción y acoplamiento — Parte 2: Vehículos comerciales con una tensión de alimentación nominal de 24 V — Conducción eléctrica transitoria por líneas de alimentación exclusivamente. Primera edición: 1990.

ISO 7637-3 Vehículos de carretera — Perturbaciones eléctricas por conducción y acoplamiento — Parte 3: Vehículos con una tensión de alimentación de 12 V o 24 V — Transmisión eléctrica transitoria mediante acoplamiento capacitivo e inductivo por líneas que no sean de alimentación. Primera edición: 1995 + Cor 1: 1995.

ISO/IEC 7816-1 Tarjetas de identificación — Tarjetas de circuito(s) integrado(s) con contactos — Parte 1: Características físicas. Primera edición: 1998.

ISO/IEC 7816-2 Tecnología de la información — Tarjetas de identificación — Tarjetas de circuito(s) integrado(s) con contactos — Parte 2: Dimensiones y ubicación de los contactos. Primera edición: 1999.

ISO/IEC 7816-3 Tecnología de la información — Tarjetas de identificación — Tarjetas de circuito(s) integrado(s) con contactos — Parte 3: Señales electrónicas y protocolo de transmisión. Edición 2: 1997.

ISO/IEC 10373 Tarjetas de identificación — Métodos de ensayo. Primera edición: 1993.

2. PRUEBAS FUNCIONALES DE LA UNIDAD INTRAVEHICULAR

Nº	Prueba	Descripción	Condiciones asociadas
1.	**Examen administrativo**		
1.1.	Documentación	Corrección de la documentación	
1.2.	Resultados de la prueba del fabricante	Resultados de la prueba realizada por el fabricante durante la integración. Demostraciones sobre papel	070, 071, 073
2.	**Inspección visual**		
2.1.	Cumplimiento de lo dispuesto en la documentación		
2.2.	Identificación/inscripciones		168, 169
2.3.	Materiales		163 a 167
2.4	Precintos		251
2.5.	Interfaces externas		
3.	**Pruebas funcionales**		
3.1.	Funciones disponibles		002, 004, 244
3.2.	Modos de funcionamiento		006*, 007*, 008*, 009*, 106, 107
3.3.	Funciones y derechos de acceso a los datos		010*, 011*, 240, 246, 247
3.4.	Inserción y extracción de las tarjetas de supervisión		013, 014, 015*, 016*, 106
3.5.	Medición de la velocidad y la distancia		017 a 026
3.6.	Medición de la hora (ensayo realizado a 20 °C)		027 a 032
3.7.	Supervisión de las actividades del conductor		033 a 043, 106
3.8.	Supervisión del régimen de conducción		044, 045, 106
3.9.	Entradas manuales		046 a 050b
3.10.	Gestión de los bloqueos introducidos por las empresas		051 a 055
3.11.	Supervisión de las actividades de control		056, 057
3.12.	Detección de incidentes o fallos		059 a 069, 106

Nº	Prueba	Descripción	Condiciones asociadas
3.13.	Datos de identificación del aparato		075*, 076*, 079
3.14.	Datos de inserción y extracción de la tarjeta del conductor		081* a 083*
3.15.	Datos sobre la actividad del conductor		084* a 086*
3.16.	Datos sobre lugares		087* a 089*
3.17.	Datos del cuentakilómetros		090* a 092*
3.18.	Datos pormenorizados sobre la velocidad		093*
3.19.	Datos sobre incidentes		094*, 095
3.20.	Datos sobre fallos		096*
3.21.	Datos de calibrado		097*, 098*
3.22.	Datos de ajuste de la hora		100*, 101*
3.23.	Datos sobre actividades de control		102*, 103*
3.24.	Datos sobre los bloqueos introducidos por las empresas		104*
3.25.	Datos sobre actividades de transferencia		105*
3.26.	Datos sobre condiciones específicas		105a*, 105b*
3.27.	Registro y almacenamiento de datos en tarjetas de tacógrafo		108, 109*, 109a*, 110*, 111, 112
3.28.	Visualización		072, 106, 113 a 128, PIC_001, DIS_001
3.29.	Impresión		072, 106, 129 a 138, PIC_001, PRT_001 a PRT_012
3.30.	Advertencias		106, 139 a 148, PIC_001
3.31.	Transferencia de datos a medios externos		072, 106, 149 a 151
3.32.	Envío de datos a dispositivos externos adicionales		152, 153
3.33.	Calibrado		154*, 155*, 156*, 245
3.34.	Ajuste de la hora		157*, 158*
3.35.	No interferencia con funciones adicionales		003, 269

Nº	Prueba	Descripción	Condiciones asociadas
4.	**Pruebas ambientales**		
4.1.	Temperatura	Verificar el correcto funcionamiento mediante: — IEC 68-2-1, prueba Ad, con una duración de 72 horas a la temperatura más baja (- 20 °C), 1 hora funcionando, 1 hora parado — IEC 68-2-2, prueba Bd, con una duración de 72 horas a la temperatura más alta (+ 70 °C), 1 hora funcionando, 1 hora parado Ciclos de temperatura: verificar que la unidad intravehicular es capaz de soportar cambios rápidos en la temperatura ambiente. Verificación mediante IEC 68-2-14, prueba Na de 20 ciclos, en cada uno de los cuales se pasa de la temperatura más baja (- 20 °C) a la temperatura más alta (+ 70 °C), con un tiempo de permanencia de 2 horas en cada extremo de temperatura Es posible llevar a cabo un conjunto reducido de pruebas (entre las que se definen en la sección 3 de esta tabla) a la temperatura más baja, a la temperatura más alta y durante los ciclos de temperatura	159
4.2.	Humedad	Verificar que la unidad intravehicular es capaz de soportar una prueba de calor húmedo por ciclos. Verificación mediante IEC 68-2-30, prueba Db, seis ciclos de 24 horas, con una variación de temperatura de + 25 °C a + 55 °C en cada caso y una humedad relativa del 97 % a + 25 °C y del 93 % a + 55 °C	160
4.3.	Vibraciones	1. Vibraciones sinusoidales: verificar que la unidad intravehicular es capaz de soportar vibraciones sinusoidales con las características siguientes: desplazamiento constante entre 5 y 11 Hz: pico de 10 mm aceleración constante entre 11 y 300 Hz: 5 g Esta exigencia se verifica mediante la norma IEC 68-2-6, prueba Fc, con una duración mínima de 3 x 12 horas (12 horas por cada eje) 2. Vibraciones aleatorias: verificar que la unidad intravehicular es capaz de soportar vibraciones aleatorias con las características siguientes: frecuencia 5-150 Hz, nivel 0,02 g^2/Hz Esta exigencia se verifica mediante la norma IEC 68-2-35, prueba Ffda, con una duración mínima de 3 x 12 horas (12 horas por cada eje), 1 hora funcionando, 1 hora parado Las dos pruebas arriba descritas se llevan a cabo con dos muestras diferentes del tipo de equipo que se someta a prueba	163
4.4.	Protección frente a la penetración de agua y cuerpos extraños	Verificar que el índice de protección de la unidad intravehicular con arreglo a la norma IEC 529 es al menos IP 40, si se monta en condiciones de funcionamiento en un vehículo	164, 165
4.5.	Protección frente a sobretensiones	Verificar que la unidad intravehicular es capaz de soportar un suministro eléctrico de: versiones de 24 V: 34 V a + 40 °C 1 hora versiones de 12 V: 17 V a + 40 °C 1 hora	161
4.6.	Protección frente a la inversión de la polaridad	Verificar que la unidad intravehicular es capaz de soportar una inversión de su fuente de alimentación	161

Nº	Prueba	Descripción	Condiciones asociadas
4.7.	Protección frente a cortocircuitos	Verificar que las señales de entrada y de salida están protegidas frente a cortocircuitos con respecto a la fuente de alimentación y a la masa	161
5.	**Pruebas de compatibilidad electromagnética**		
5.1.	Emisiones radiadas y susceptibilidad	Cumplimiento de la Directiva 95/54/CEE	162
5.2.	Descargas electrostáticas	Cumplimiento de la norma IEC 61000-4-2, ± 2 kV (nivel 1)	162
5.3.	Susceptibilidad transitoria conducida en la fuente de alimentación	En las versiones de 24 V: cumplimiento de la norma ISO 7637-2 impulso 1a: Vs = - 100 V, Ri = 10 ohmios impulso 2: Vs = + 100 V, Ri = 10 ohmios impulso 3a: Vs = - 100 V, Ri = 50 ohmios impulso 3b: Vs = + 100 V, Ri = 50 ohmios impulso 4: Vs = - 16 V Va = - 12 V, t6=100 ms impulso 5: Vs = + 120 V, Ri = 2,2 ohmios, td = 250 ms En las versiones de 12 V: cumplimiento de la norma ISO 7637-1 impulso 1: Vs = - 100 V, Ri = 10 ohmios impulso 2: Vs = + 100 V, Ri = 10 ohmios impulso 3a: Vs = - 100 V, Ri = 50 ohmios impulso 3b: Vs = + 100 V, Ri = 50 ohmios impulso 4: Vs = - 6 V, Va = - 5 V, t6 = 15 ms impulso 5: Vs = + 65 V, Ri = 3 ohmios, td = 100 ms El impulso 5 deberá verificarse exclusivamente en las unidades intravehiculares concebidas para ser instaladas en vehículos que no dispongan de protección común externa contra volcado de la carga	162

3. PRUEBAS FUNCIONALES DEL SENSOR DE MOVIMIENTO

Nº	Prueba	Descripción	Condiciones asociadas
1.	**Examen administrativo**		
1.1.	Documentación	Corrección de la documentación	
2.	**Inspección visual**		
2.1.	Cumplimiento de lo dispuesto en la documentación		
2.2.	Identificación/inscripciones		169, 170
2.3.	Materiales		163 a 167
2.4.	Precintos		251
3.	**Pruebas funcionales**		
3.1.	Datos de identificación del sensor		077*
3.2.	Acoplamiento del sensor de movimiento y la unidad intravehicular		099*, 155
3.3.	Detección de movimiento		
	Precisión de la medición del movimiento		022 a 026

Nº	Prueba	Descripción	Condiciones asociadas
4.	**Pruebas ambientales**		
4.1.	Temperatura de funcionamiento	Verificar el correcto funcionamiento (tal y como se define en la prueba nº 3.3) en el intervalo de temperaturas [— 40 °C; + 135 °C] mediante: — IEC 68-2-1 prueba Ad, con una duración de 96 horas a la temperatura más baja $To_{mín}$ — IEC 68-2-2 prueba Bd, con una duración de 96 horas a la temperatura más alta $To_{máx}$	159
4.2.	Ciclos de temperatura	Verificar el correcto funcionamiento (tal y como se define en la prueba nº 3.3) mediante IEC 68-2-14, prueba Na de 20 ciclos, en cada uno de los cuales se pasa de la temperatura más baja (– 40 °C) a la temperatura más alta (+ 135 °C), con un tiempo de permanencia de 2 horas en cada extremo de temperatura Es posible llevar a cabo un conjunto reducido de pruebas (entre las que se definen en la prueba 3.3) a la temperatura más baja, a la temperatura más alta y durante los ciclos de temperatura	159
4.3.	Ciclos de humedad	Verificar el correcto funcionamiento (tal y como se define en la prueba nº 3.3) mediante IEC 68-2-30, prueba Db, seis ciclos de 24 horas, con una variación de temperatura de + 25 °C a + 55 °C en cada caso y una humedad relativa del 97 % a + 25 °C y del 93 % a + 55 °C	160
4.4.	Vibraciones	Verificar el correcto funcionamiento (tal y como se define en la prueba nº 3.3) mediante IEC 68-2-6, prueba Fc, con una duración de 100 ciclos de frecuencia: desplazamiento constante entre 10 y 57 Hz: pico de 1,5 mm Aceleración constante entre 57 y 500 Hz: 20 g	163
4.5.	Choque mecánico	Verificar el correcto funcionamiento (tal y como se define en la prueba nº 3.3) mediante IEC 68-2-27, prueba Ea, 3 choques en ambas direcciones de los 3 ejes perpendiculares	163
4.6.	Protección frente a la penetración de agua y cuerpos extraños	Verificar que el índice de protección del sensor de movimiento con arreglo a la norma IEC 529 es al menos IP 64, si se monta en condiciones de funcionamiento en un vehículo	165
4.7.	Protección frente a la inversión de la polaridad	Verificar que el sensor de movimiento es capaz de soportar una inversión de su fuente de alimentación	161
4.8.	Protección frente a cortocircuitos	Verificar que las señales de entrada y de salida están protegidas frente a cortocircuitos a la fuente de alimentación y a masa	161
5.	**Compatibilidad electromagnética**		
5.1.	Emisiones radiadas y susceptibilidad	Verificar el cumplimiento de la Directiva 95/54/CE	162
5.2.	Descargas electrostáticas	Cumplimiento de la norma IEC 61000-4-2, ± 2 kV (nivel 1)	162
5.3.	Susceptibilidad transitoria conducida en las líneas de datos	Cumplimiento de la norma ISO 7637-3 (nivel III)	162

4. PRUEBAS FUNCIONALES DE LAS TARJETAS DE TACÓGRAFO

Nº	Prueba	Descripción	Condiciones asociadas
1.	**Examen administrativo**		
1.1.	Documentación	Corrección de la documentación	
2.	**Inspección visual**		
2.1.		Cerciorarse de que todas las características de protección y datos visibles están bien impresos en la tarjeta y se ajustan a la normativa	171 a 181
3.	**Pruebas físicas**		
3.1.	Comprobar las dimensiones de la tarjeta y la ubicación de los contactos		184 ISO/IEC 7816-1 ISO/IEC 7816-2
4.	**Pruebas de protocolos**		
4.1.	ATR	Comprobar si el ATR es conforme	ISO/IEC 7816-3 TCS 304, 307, 308
4.2.	T=0	Comprobar si el protocolo T=0 es conforme	ISO/IEC 7816-3 TCS 302, 303, 305
4.3.	PTS	Comprobar si el comando PTS es conforme. Para ello, ajustar T=1 partiendo de T=0	ISO/IEC 7816-3 TCS 309 a 311
4.4.	T=1	Comprobar si el protocolo T=1 es conforme	ISO/IEC 7816-3 TCS 303, / 306
5.	**Estructura de la tarjeta**		
5.1.		Comprobar si la estructura de archivos de la tarjeta es conforme. Para ello, verificar la presencia de los archivos obligatorios en la tarjeta y sus condiciones de acceso	TCS 312 TCS 400*, 401, 402, 403*, 404, 405*, 406, 407, 408*, 409, 410*, 411, 412, 413*, 414, 415*, 416, 417, 418*, 419
6.	**Pruebas funcionales**		
6.1.	Proceso normal	Comprobar al menos una vez cada uno de los usos permitidos de cada comando (por ejemplo, comprobar el comando UPDATE BINARY con CLA = '00' CLA = '0C' y con diferentes parámetros P1, P2 y Lc). Comprobar que las operaciones se han llevado a cabo en la tarjeta (por ejemplo, leyendo el archivo donde se ha ejecutado el comando)	TCS 313 bis TCS 379
6.2.	Mensajes de error	Comprobar al menos una vez cada uno de los mensajes de error (especificados en el apéndice 2) para cada comando. Comprobar al menos una vez cada uno de los errores genéricos (excepto los errores de integridad '6400' verificados durante la certificación de seguridad)	
7.	**Pruebas ambientales**		
7.1.		Cerciorarse de que las tarjetas funcionan de acuerdo con las condiciones límite definidas con arreglo a la norma ISO/IEC 10373	185 a 188 ISO/IEC 7816-1

5. PRUEBAS DE INTEROPERABILIDAD

Nº	Prueba	Descripción
1.	Autentificación mutua	Comprobar que la autentificación mutua entre la unidad intravehicular y la tarjeta de tacógrafo funciona normalmente
2.	Pruebas de lectura/escritura	Ejecutar un escenario de actividad típico en la unidad intravehicular. Dicho escenario deberá adaptarse al tipo de tarjeta que se esté verificando y deberá incluir pruebas de escritura en tantos EFs como sea posible en la tarjeta Verificar mediante una transferencia de la tarjeta que todos los registros correspondientes se han realizado correctamente Verificar mediante una impresión diaria de los datos de la tarjeta que todos los registros correspondientes se pueden leer correctamente

Apéndice 10

OBJETIVOS GENÉRICOS DE SEGURIDAD

En el presente apéndice se especifica el contenido mínimo que deben tener los objetivos de seguridad del sensor de movimiento, de la unidad intravehicular y de las tarjetas de tacógrafo.

A fin de establecer los objetivos de seguridad que posteriormente habrán de certificar, los fabricantes deberán refinar y completar los documentos según sea necesario, sin modificar ni borrar las especificaciones existentes sobre amenazas, objetivos, medios procedimentales y funciones de aplicación de la seguridad.

ÍNDICE

Objetivo genérico de seguridad del sensor de movimiento

Objetivo genérico de seguridad de la unidad intravehicular

Objetivo genérico de seguridad de la tarjeta de tacógrafo

OBJETIVO GENÉRICO DE SEGURIDAD DEL SENSOR DE MOVIMIENTO

1. **Introducción**

El presente documento contiene una descripción del sensor de movimiento, de las amenazas que deberá ser capaz de neutralizar y de los objetivos de seguridad que debe lograr. En las páginas siguientes se especifican las funciones necesarias para la aplicación de la seguridad, así como la resistencia mínima que deben tener los mecanismos de seguridad y el nivel de certeza exigido para las tareas de desarrollo y evaluación.

Las condiciones que se citan en el presente documento son las especificadas en el cuerpo del anexo I B. Para mayor claridad de lectura, en ocasiones las condiciones de los objetivos de seguridad son una repetición de las condiciones mencionadas en el anexo I B. En caso de ambigüedad entre una condición de un objetivo de seguridad y la condición del anexo I B que se toma como referencia, prevalecerá esta última.

Las condiciones del anexo I B que no se mencionan en los objetivos de seguridad, tampoco dan lugar a funciones de aplicación de la seguridad.

Hemos asignado etiquetas individuales a las diferentes especificaciones sobre amenazas, objetivos, medios procedimentales y funciones SEF, con el fin de garantizar el seguimiento hasta los documentos de desarrollo y evaluación.

2. **Abreviaturas, definiciones y referencias**

2.1. ***Abreviaturas***

ROM	Read Only Memory (memoria de solo lectura)
SEF	Security Enforcing Function (función de aplicación de la seguridad)
PO	Target Of Evaluation (objetivo de evaluación)
FE	Vehicle Unit (unidad intravehicular)

2.2. ***Definiciones***

Tacógrafo digital	Aparato de control
Entidad	Un dispositivo conectado al sensor de movimiento
Datos de movimiento	Los datos que se intercambian con la VU, representativos de la velocidad y la distancia recorrida
Piezas separadas físicamente	Componentes físicos del sensor de movimiento que están distribuidos en el vehículo en oposición a otros componentes físicos alojados en el interior de la carcasa del sensor de movimiento
Datos de seguridad	Los datos específicos que se precisan como apoyo para las funciones de aplicación de la seguridad (por ejemplo, claves criptográficas)
Sistema	Equipos, personas u organizaciones relacionados de algún modo con el aparato de control
Usuario	Un usuario humano del sensor de movimiento (excepto en la expresión “datos de usuario”)
Datos de usuario	Cualquier tipo de datos que registre o almacene el sensor de movimiento, exceptuando los datos de movimiento o de seguridad

2.3. ***Referencias***

ITSEC Criterios de evaluación de la seguridad de la tecnología de la información, 1991.

3. **Características generales del producto**

3.1. ***Descripción y método de uso del sensor de movimiento***

El sensor de movimiento se ha concebido para ser instalado en vehículos de transporte por carretera, y tiene por misión facilitar a la VU datos de movimiento seguros, representativos de la velocidad y la distancia recorrida por el vehículo.

El sensor de movimiento está conectado mediante una interfaz mecánica a una parte móvil cuyo movimiento puede ser representativo de la velocidad o la distancia recorrida por el vehículo. El sensor se puede colocar en la caja de cambios o en cualquier otra parte del vehículo.

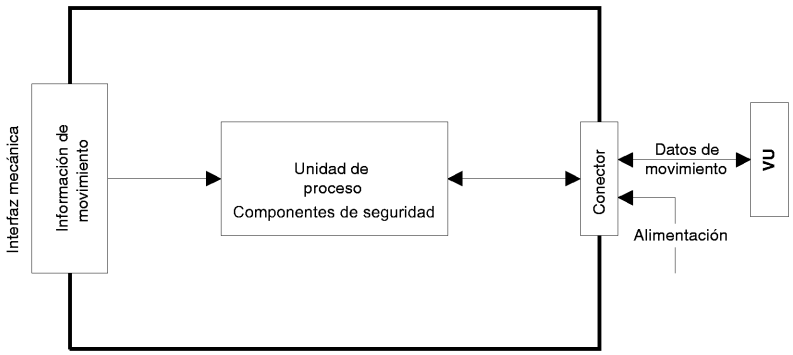
En el modo operativo, el sensor de movimiento está conectado a una VU.

También puede conectarse a equipos específicos con fines de gestión (a discreción del fabricante)

La figura siguiente muestra un sensor de movimiento típico:

Figura 1

Sensor de movimiento típico

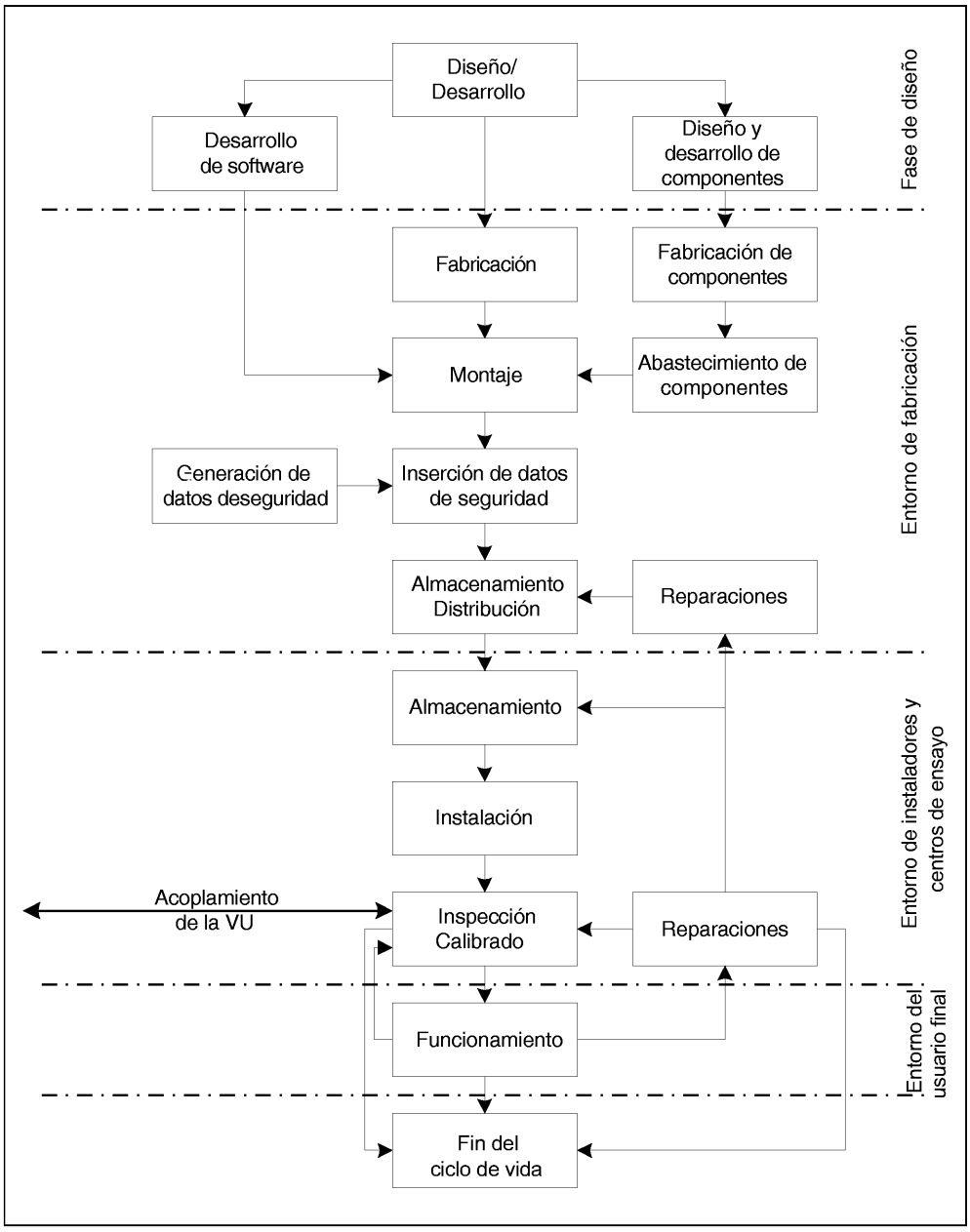


3.2. ***Ciclo de vida del sensor de movimiento***

La figura siguiente muestra el ciclo de vida típico de un sensor de movimiento:

Figura 2

Ciclo de vida típico del sensor de movimiento



3.3. ***Amenazas***

En este apartado se describen las amenazas que podría tener que afrontar el sensor de movimiento.

3.3.1. *Amenazas para las políticas de control de accesos*

A.Acceso Los usuarios podrían tratar de acceder a funciones que les están prohibidas

3.3.2. *Amenazas relacionadas con el diseño*

A.Fallos	Un posible fallo del hardware, del software o de los procedimientos de comunicación podría llevar al sensor de movimiento a una situación imprevista que comprometiera su seguridad
A.Pruebas	El empleo de modos de prueba no invalidados o el aprovechamiento de influencias no legítimas podrían comprometer la seguridad del sensor de movimiento
A.Diseño	Los usuarios podrían tratar de averiguar de forma ilícita los pormenores de diseño, ya sea a través del material del fabricante (mediante robo, soborno, etc.) o por métodos de ingeniería inversa

3.3.3. *Amenazas orientadas al funcionamiento*

A.Medio_ambiente	Los usuarios podrían comprometer la seguridad del sensor de movimiento mediante ataques de carácter medioambiental (térmicos, electromagnéticos, ópticos, químicos, mecánicos, etc.)
A.Hardware	Los usuarios podrían tratar de modificar el hardware del sensor de movimiento
A.Origen_mecánico	Los usuarios podrían tratar de manipular la entrada del sensor de movimiento (por ejemplo, desenroscándola de la caja de cambios, etc.)
A.Datos_de_movimiento	Los usuarios podrían tratar de modificar los datos de movimiento del vehículo (adición, modificación, borrado, repetición de la señal)
A.Suministro_eléctrico	Los usuarios podrían tratar de anular los objetivos de seguridad del sensor de movimiento modificando (cortando, reduciendo, incrementando) su suministro eléctrico
A.Datos_de_seguridad	Los usuarios podrían tratar de obtener de forma ilícita los datos de seguridad durante la generación o el transporte o el almacenamiento de dichos datos en el equipo
A.Software	Los usuarios podrían tratar de modificar el software del sensor de movimiento
A.Datos_almacenados	Los usuarios podrían tratar de modificar los datos almacenados (datos de seguridad o datos de usuario)

3.4. ***Objetivos de seguridad***

El principal objetivo de seguridad del sistema del tacógrafo digital es el siguiente:

O.Principal	Los datos que vayan a comprobar las autoridades de control deben estar disponibles y reflejar íntegramente y con precisión las actividades de los conductores y vehículos bajo control, tanto en lo que respecta a los períodos de conducción, trabajo, disponibilidad y descanso, como en lo que respecta a la velocidad del vehículo

Este objetivo de seguridad global exige el cumplimiento del objetivo de seguridad del sensor de movimiento:

O.Principal_sensor	Los datos transmitidos por el sensor de movimiento deben estar a disposición de la VU, para que ésta pueda determinar íntegramente y con precisión el movimiento del vehículo en lo que respecta a la velocidad y la distancia recorrida

3.5. ***Objetivos de seguridad informática***

A continuación se relacionan los objetivos de seguridad informática específicos del sensor de movimiento, que contribuyen a la consecución de su principal objetivo de seguridad:

O.Acceso	El sensor de movimiento debe controlar el acceso de las entidades conectadas a las funciones y a los datos
O.Auditoría	El sensor de movimiento debe investigar los intentos de violación de su seguridad y debe realizar un seguimiento de los mismos para localizar las entidades responsables
O.Autentificación	El sensor de movimiento debe autentificar las entidades conectadas

O.Procesamiento	El sensor de movimiento debe garantizar que las entradas se procesan correctamente para obtener datos de movimiento precisos
O.Fiabilidad	El sensor de movimiento debe ofrecer un servicio fiable
O.Intercambio_seguro	El sensor de movimiento debe garantizar la seguridad en los intercambios de datos con la VU

3.6. ***Medios físicos, de personal o procedimentales***

En este apartado se describen los requisitos físicos, de personal o procedimentales que contribuyen a la seguridad del sensor de movimiento.

3.6.1. *Diseño del equipo*

M.Desarrollo	Los técnicos encargados de desarrollar el sensor de movimiento deben garantizar que la asignación de responsabilidades durante la fase de desarrollo se lleva a cabo de manera que se mantenga la seguridad TI
M.Fabricación	Los fabricantes del sensor de movimiento deben garantizar que la asignación de responsabilidades durante la fase de fabricación se lleva a cabo de manera que se mantenga la seguridad TI, y que durante todo el proceso de fabricación el sensor de movimiento está protegido frente a ataques físicos que pudieran comprometer la seguridad TI

3.6.2. *Entrega del equipo*

M.Entrega	Los fabricantes del sensor de movimiento, los fabricantes del vehículo y los instaladores o centros de ensayo deben garantizar que la manipulación del sensor de movimiento se lleva a cabo de manera que se mantenga la seguridad TI

3.6.3. *Generación y abastecimiento de datos de seguridad*

M.Generación_datos_seg	Los algoritmos de generación de datos de seguridad sólo serán accesibles a personas autorizadas y de confianza
M.Transporte_datos_seg	Los datos de seguridad se generarán, transportarán e introducirán en el sensor de movimiento de forma que se preserve su confidencialidad e integridad

3.6.4. *Instalación, calibrado e inspección del aparato de control*

M.Centros_homologados	La instalación, calibrado y reparación del aparato de control se encomendará exclusivamente a instaladores o centros de ensayo homologados y de confianza
M.Interfaz_mecánica	Es obligatorio disponer de medios para detectar la manipulación física de la interfaz mecánica (por ejemplo, precintos)
M.Inspecciones_periódicas	El aparato de control debe someterse a inspecciones y calibrados periódicos

3.6.5. *Control del cumplimiento de la ley*

M.Controles	Es preciso comprobar el cumplimiento de la ley mediante controles periódicos y aleatorios que incluyan auditorías de seguridad

3.6.6. *Actualizaciones del software*

M.Actualizaciones_software	Las nuevas versiones de software del sensor de movimiento no se aplicarán hasta después de haber recibido el certificado de seguridad

4. **Funciones de aplicación de la seguridad**

4.1. ***Identificación y autentificación***

UIA_101 El sensor de movimiento deberá ser capaz de establecer, para cada interacción, la identidad de cualquier entidad a la que esté conectado.

UIA_102 La identidad de una entidad conectada constará de:

— un grupo de entidad:

— VU,

— dispositivo de gestión,

— otros,

una identificación de entidad (VU exclusivamente).

UIA_103 La identificación de entidad de una VU conectada constará del número de homologación y del número de serie de dicha VU.

UIA_104 El sensor de movimiento deberá ser capaz de autentificar cualquier VU o dispositivo de gestión al que esté conectado:

— en el momento de producirse la conexión de la entidad,

— al recuperarse el suministro eléctrico

UIA_105 El sensor de movimiento deberá ser capaz de reautentificar periódicamente la VU a la que está conectado.

UIA_106 El sensor de movimiento deberá ser capaz de detectar e impedir el uso de datos de autentificación que se hayan copiado y reproducido.

UIA_107 Tras haberse detectado varios intentos consecutivos de autentificación con resultados negativos (número de intentos a discreción del fabricante y no superior a 20), la función SEF deberá:

— generar un registro de auditoría del incidente,

— enviar una advertencia a la entidad,

— seguir exportando datos de movimiento en un modo no seguro.

4.2. ***Control de accesos***

Los controles de accesos garantizan que sólo las personas autorizadas pueden leer, crear o modificar la información del TOE.

4.2.1. *Política de control de accesos*

ACC_101 El sensor de movimiento deberá controlar los derechos de acceso a las funciones y a los datos.

4.2.2. *Derechos de acceso a los datos*

ACC_102 El sensor de movimiento deberá garantizar que los datos de identificación del sensor de movimiento sólo pueden escribirse una vez (condición 078).

ACC_103 Los datos de usuario que acepte o almacene el sensor de movimiento deberán proceder exclusivamente de entidades autentificadas.

ACC_104 El sensor de movimiento deberá aplicar un sistema adecuado que regule los derechos de acceso a la lectura y la escritura de datos de seguridad.

4.2.3. *Estructura de archivos y condiciones de acceso*

ACC_105 La estructura de los archivos de la aplicación y de los archivos de datos, así como las condiciones de acceso, deberán crearse durante el proceso de fabricación y posteriormente no se podrán modificar ni borrar.

4.3. ***Responsabilidad***

ACT_101 El sensor de movimiento deberá almacenar en su memoria sus propios datos de identificación (condición 077).

ACT_102 El sensor de movimiento deberá almacenar en su memoria los datos de instalación (condición 099).

ACT_103 El sensor de movimiento deberá ser capaz de enviar los datos de control a entidades autentificadas cuando éstas lo soliciten.

4.4. ***Auditoría***

AUD_101 El sensor de movimiento deberá generar registros de auditoría para los incidentes que afecten a su seguridad.

AUD_102 Los incidentes que afectan a la seguridad del sensor de movimiento son los siguientes:

— intentos de violación de la seguridad:

  — fallo de autentificación,

  — error en la integridad de los datos almacenados,

  — error en una transferencia interna de datos,

  — apertura no autorizada de la carcasa,

  — sabotaje del hardware,

— fallo del sensor.

AUD_103 Los registros de auditoría deberán incluir los datos siguientes:

— fecha y hora del incidente,

— tipo de incidente,

— identidad de la entidad conectada.

Cuando estos datos no estén disponibles, se mostrará por defecto una indicación adecuada (a discreción del fabricante).

AUD_104 El sensor de movimiento deberá enviar los registros de auditoría a la VU en el mismo momento de su generación, y también podrá guardarlos en su memoria.

AUD_105 Si el sensor de movimiento guarda los registros de auditoría, deberá garantizar que permanecen almacenados 20 de dichos registros, con independencia de si se agota la capacidad de la memoria. Si una entidad autentificada lo solicita, el sensor de movimiento deberá ser capaz de enviarle los registros de auditoría almacenados.

4.5. ***Precisión***

4.5.1. *Política de control del flujo de información*

ACR_101 El sensor de movimiento deberá garantizar que los datos de movimiento sólo se pueden procesar y extraer de la entrada mecánica.

4.5.2. *Transferencias internas de datos*

Las condiciones descritas en este apartado se aplican exclusivamente si el sensor de movimiento utiliza piezas separadas físicamente.

ACR_102 Si se transfieren datos entre piezas del sensor de movimiento que se encuentren separadas físicamente, dichos datos deberán estar protegidos de posibles modificaciones.

ACR_103 Si se detecta un error durante una transferencia interna, la transmisión deberá repetirse y la función SEF deberá generar un registro de auditoría del incidente.

4.5.3. *Integridad de los datos almacenados*

ACR_104 El sensor de movimiento deberá comprobar la existencia de errores de integridad en los datos de usuario que almacena en su memoria.

ACR_105 Si se detecta un error de integridad en los datos de usuario almacenados, la función SEF deberá generar un registro de auditoría.

4.6. ***Fiabilidad de servicio***

4.6.1 *Pruebas*

RLB_101 Todos los comandos, acciones o puntos de prueba específicos para las necesidades de ensayo propias de la fase de fabricación deberán ser desactivados o eliminados antes de que termine dicha fase, y no se podrán restablecer para su empleo posterior.

RLB_102 El sensor de movimiento deberá efectuar comprobaciones automáticas en el momento de la puesta en marcha y durante el funcionamiento normal, a fin de verificar su correcto funcionamiento. Las comprobaciones automáticas del sensor de movimiento deberán incluir una verificación de la integridad de los datos de seguridad y una verificación de la integridad del código ejecutable almacenado (si no se encuentra en una memoria ROM).

RLB_103 Si se detecta un fallo interno durante una comprobación automática, la función SEF deberá generar un registro de auditoría (fallo del sensor).

4.6.2. *Software*

RLB_104 Debe ser imposible analizar o depurar sobre el terreno el software del sensor de movimiento.

RLB_105 No deberán aceptarse como código ejecutable las entradas procedentes de fuentes externas.

4.6.3. *Protección física*

RLB_106 Si el sensor de movimiento se diseña de manera que pueda abrirse, deberá detectar la apertura de la carcasa, incluso sin alimentación eléctrica externa (durante un mínimo de 6 meses). En tal caso, la función SEF deberá generar un registro de auditoría del incidente. (Es admisible que el registro de auditoría se genere y se almacene después de haberse reconectado el suministro eléctrico).

Si el sensor de movimiento no puede abrirse, deberá estar diseñado de manera que los intentos de manipulación física puedan detectarse con facilidad (por ejemplo, mediante inspección ocular).

RLB_107 El sensor de movimiento deberá detectar determinados actos (a discreción del fabricante) de sabotaje del hardware.

RLB_108 En el caso arriba descrito, la función SEF deberá generar un registro de auditoría y el sensor de movimiento deberá: (*a discreción del fabricante).*

4.6.4. *Interrupciones del suministro eléctrico*

RLB_109 El sensor de movimiento mantendrá las condiciones de seguridad durante las interrupciones u oscilaciones del suministro eléctrico.

4.6.5. *Condiciones de reinicio*

RLB_110 En caso de interrupción del suministro eléctrico, o si se detiene una transacción antes de que concluya, o si se da cualquier otra condición de reinicio, el sensor de movimiento deberá reiniciarse limpiamente.

4.6.6. *Disponibilidad de los datos*

RLB_111 El sensor de movimiento deberá garantizar que se obtiene acceso a los recursos cuando es necesario y que dichos recursos no se solicitan ni se retienen de forma innecesaria.

4.6.7. *Múltiples aplicaciones*

RLB_112 Si el sensor de movimiento ofrece otras aplicaciones aparte de la de tacógrafo, todas ellas deberán estar separadas entre sí por medios físicos o lógicos. Dichas aplicaciones no deberán compartir datos de seguridad, y sólo podrá haber una tarea activa en un momento dado.

4.7. ***Intercambio de datos***

DEX_101 Los datos de movimiento que el sensor de movimiento exporte a la VU deberán ir acompañados de los atributos de seguridad asociados, de manera que la VU sea capaz de verificar su integridad y autenticidad.

4.8. ***Apoyo criptográfico***

Los requisitos del presente apartado se aplican exclusivamente cuando es necesario, en función de los mecanismos de seguridad empleados y según las soluciones del fabricante.

CSP_101 En todas las operaciones criptográficas que lleve a cabo el sensor de movimiento se emplearán un algoritmo y un tamaño de clave específicos.

CSP_102 Si el sensor de movimiento genera claves criptográficas, deberá ser con arreglo a algoritmos específicos de generación de claves y tamaños de clave específicos.

CSP_103 Si el sensor de movimiento distribuye claves criptográficas, deberá ser con arreglo a métodos específicos de distribución de claves.

CSP_104 Si el sensor de movimiento accede a claves criptográficas, deberá ser con arreglo a métodos específicos de acceso a claves criptográficas.

CSP_105 Si el sensor de movimiento destruye claves criptográficas, deberá ser con arreglo a métodos específicos de destrucción de claves criptográficas.

5. **Definición de mecanismos de seguridad**

Los mecanismos de seguridad que desempeñan las funciones de aplicación de la seguridad del sensor de movimiento los define el fabricante del sensor de movimiento.

6. **Resistencia mínima de los mecanismos de seguridad**

La resistencia mínima de los mecanismos de seguridad del sensor de movimiento es Alta, tal y como se define en el documento de referencia ITSEC.

7. **Nivel de certeza**

El nivel de certeza que se toma como objetivo para el sensor de movimiento es el nivel E3, tal y como se define en el documento de referencia ITSEC.

8. **Fundamento lógico**

Las matrices siguientes aportan un fundamento lógico para las funciones SEF, al mostrar:

— qué amenazas contrarresta cada SEF o cada medio,

— qué objetivos de seguridad TI cumple cada SEF.

	Amenazas											Objetivos TI					
	A.Acceso	A.Fallos	A.Pruebas	A.Diseño	A.Medio ambiente	A.Hardware	A.Origen mecánico	A.Datos de movimiento	A.Suministro eléctrico	A.Datos de seguridad	A.Software	A.Datos almacenados	A.Acceso	A.Identificación	A.Fallos	A.Pruebas	A.Diseño	A.Parámetros de calibrado
Medios físicos, de personal o procedimentales																		
Desarrollo		x	x	x														
Fabricación			x	x														
Entrega						x					x	x						
Generación de datos de seguridad										x								
Transporte de datos de seguridad										x								
Centros de ensayo homologados							x											
Interfaz mecánica							x											
Inspecciones periódicas						x	x		x		x							
Controles del cumplimiento de la ley					x	x	x		x	x	x							
Actualizaciones del software											x							
Funciones de aplicación de la seguridad																		
Identificación y autentificación																		
UIA_101 Identificación de entidades	x							x					x		x			x
UIA_102 Identidad de entidades	x												x		x			
UIA_103 Identidad de la VU														x				
UIA_104 Autentificación de entidades	x							x					x		x			x
UIA_105 Reautentificación	x							x					x		x			x
UIA_106 Autentificación infalsificable	x							x					x		x			
UIA_107 Fallo de autentificación								x						x			x	
Control de accesos																		
ACC_101 Política de control de accesos	x									x		x	x					
ACC_102 Identificación del sensor de movimiento												x	x					

	Amenazas												Objetivos TI					
	A.Acceso	A.Fallos	A.Pruebas	A.Diseño	A.Medio ambiente	A.Hardware	A.Origen mecánico	A.Datos de movimiento	A.Suministro eléctrico	A.Datos de seguridad	A.Software	A.Datos almacenados	A.Acceso	A.Identificación	A.Fallos	A.Pruebas	A.Diseño	A.Parámetros de calibrado
ACC_103 Datos de usuario												x	x					
ACC_104 Datos de seguridad										x		x	x					
ACC_105 Estructura de archivos y condiciones de acceso	x									x		x	x					
Responsabilidad																		
ACT_101 Datos de identificación del sensor de movimiento														x				
ACT_102 Datos de acoplamiento														x				
ACT_103 Datos de control														x				
Auditoría																		
AUD_101 Registros de auditoría														x				
AUD_102 Lista de incidentes de auditoría	x				x	x						x		x				
AUD_103 Datos de auditoría														x				
AUD_104 Herramientas de auditoría														x				
AUD_105 Almacenamiento de registros de auditoría														x				
Precisión																		
ACR_101 Política de control del flujo de información								x								x	x	
ACR_102 Transferencias internas																x	x	
ACR_103 Transferencias internas														x				
ACR_104 Integridad de los datos almacenados												x					x	
ACR_105 Integridad de los datos almacenados												x		x				
Fiabilidad																		
RLB_101 Pruebas de fabricación			x	x													x	
RLB_102 Comprobaciones automáticas		x				x			x		x						x	
RLB_103 Comprobaciones automáticas						x			x		x			x				
RLB_104 Análisis de software				x							x						x	
RLB_105 Entradas del software											x					x	x	
RLB_106 Apertura de la carcasa				x	x	x				x	x	x					x	
RLB_107 Sabotaje del hardware						x											x	
RLB_108 Sabotaje del hardware						x								x				
RLB_109 Interrupciones del suministro eléctrico									x								x	
RLB_110 Reinicio		x															x	
RLB_111 Disponibilidad de los datos																x	x	
RLB_112 Múltiples aplicaciones																	x	
Intercambio de datos																		
DEX_101 Exportación de datos de movimiento seguros								x										x
Apoyo criptográfico																		
CSP_101 Algoritmos																	x	x
CSP_102 Generación de claves																	x	x
CSP_103 Distribución de claves																	x	x
CSP_104 Acceso a claves																	x	x
CSP_105 Destrucción de claves																	x	x

OBJETIVO GENÉRICO DE SEGURIDAD DE LA UNIDAD INTRAVEHICULAR

1. **Introducción**

El presente documento contiene una descripción de la unidad intravehicular, de las amenazas que deberá ser capaz de neutralizar y de los objetivos de seguridad que debe lograr. En las páginas siguientes se especifican las funciones necesarias para la aplicación de la seguridad, así como la resistencia mínima que deben tener los mecanismos de seguridad y el nivel de certeza exigido para las tareas de desarrollo y evaluación.

Las condiciones que se citan en el presente documento son las especificadas en el cuerpo del anexo I B. Para mayor claridad de lectura, en ocasiones las condiciones de los objetivos de seguridad son una repetición de las condiciones mencionadas en el anexo I B. En caso de ambigüedad entre una condición de un objetivo de seguridad y la condición del anexo I B que se toma como referencia, prevalecerá ésta última.

Las condiciones del anexo I B que no se mencionan en los objetivos de seguridad, tampoco dan lugar a funciones de aplicación de la seguridad.

Hemos asignado etiquetas individuales a las diferentes especificaciones sobre amenazas, objetivos, medios procedimentales y funciones SEF, con el fin de garantizar el seguimiento hasta los documentos de desarrollo y evaluación.

2. **Abreviaturas, definiciones y referencias**

2.1. ***Abreviaturas***

PIN	Personal Identification Number (número de identificación personal)
ROM	Read Only Memory (memoria de solo lectura)
SEF	Security Enforcing Function (función de aplicación de la seguridad)
TOE	Target Of Evaluation (objetivo de evaluación)
VU	Vehicle Unit (unidad intravehicular)

2.2. ***Definiciones***

Tacógrafo digital	Aparato de control
Datos de movimiento	Los datos que se intercambian con el sensor de movimiento, representativos de la velocidad y la distancia recorrida
Piezas separadas físicamente	Componentes físicos de la VU que están distribuidos en el vehículo en oposición a otros componentes físicos alojados en el interior de la carcasa de la VU
Datos de seguridad	Los datos específicos que se precisan como apoyo para las funciones de aplicación de la seguridad (por ejemplo, claves criptográficas)
Sistema	Equipos, personas u organizaciones relacionados de algún modo con el aparato de control
Usuario	Por usuarios se entenderá el usuario humano del equipo. Los usuarios normales de la VU incluyen a los conductores, controladores, centros de ensayo y empresas
Datos de usuario	Cualquier tipo de datos que registre o almacene la VU del modo descrito en el capítulo III.12., exceptuando los datos de seguridad

2.3. ***Referencias***

ITSEC Criterios para evaluación de la seguridad de la tecnología de la información, 1991

3. **Características generales del producto**

3.1. ***Descripción y método de uso de la unidad intravehicular***

La VU se ha concebido para ser instalada en vehículos de transporte por carretera, y tiene por misión registrar, almacenar, mostrar en pantalla, imprimir y enviar datos relacionados con las actividades del conductor.

La VU está conectada a un sensor de movimiento con el que intercambia datos de movimiento del vehículo.

Los usuarios se identifican a la VU por medio de tarjetas de tacógrafo.

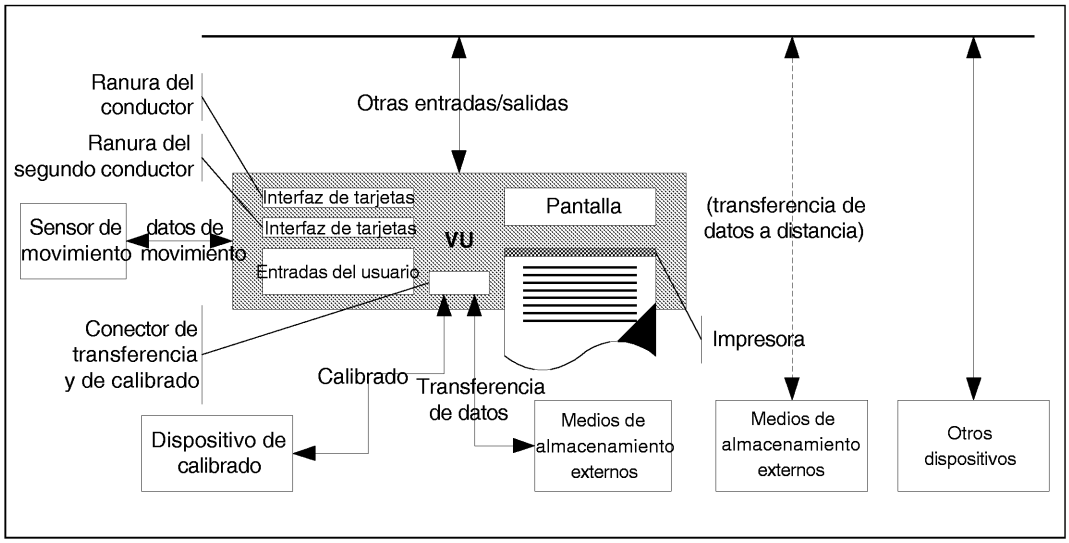
La VU registra y almacena en su memoria los datos correspondientes a las actividades de los usuarios, y también registra dichas actividades en tarjetas de tacógrafo.

La VU envía datos a la pantalla, a la impresora y a dispositivos externos.

La figura siguiente muestra el entorno operativo de la unidad intravehicular instalada:

Figura 2

Entorno operativo de la VU



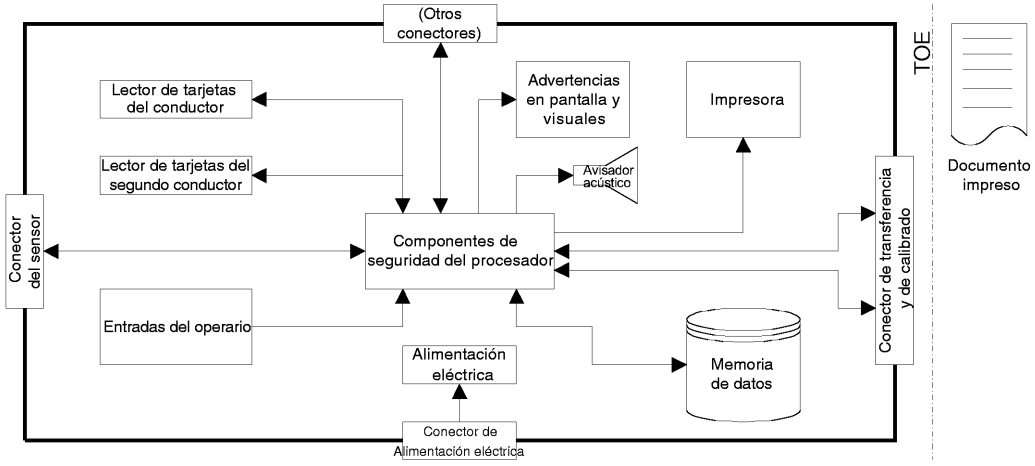
Las características generales, funciones y modos de funcionamiento de la VU se describen en el capítulo II del anexo I B.

Las condiciones funcionales de la VU se especifican en el capítulo III del anexo I B.

La figura siguiente muestra una VU típica:

Figura 3

VU típica (…) opcional



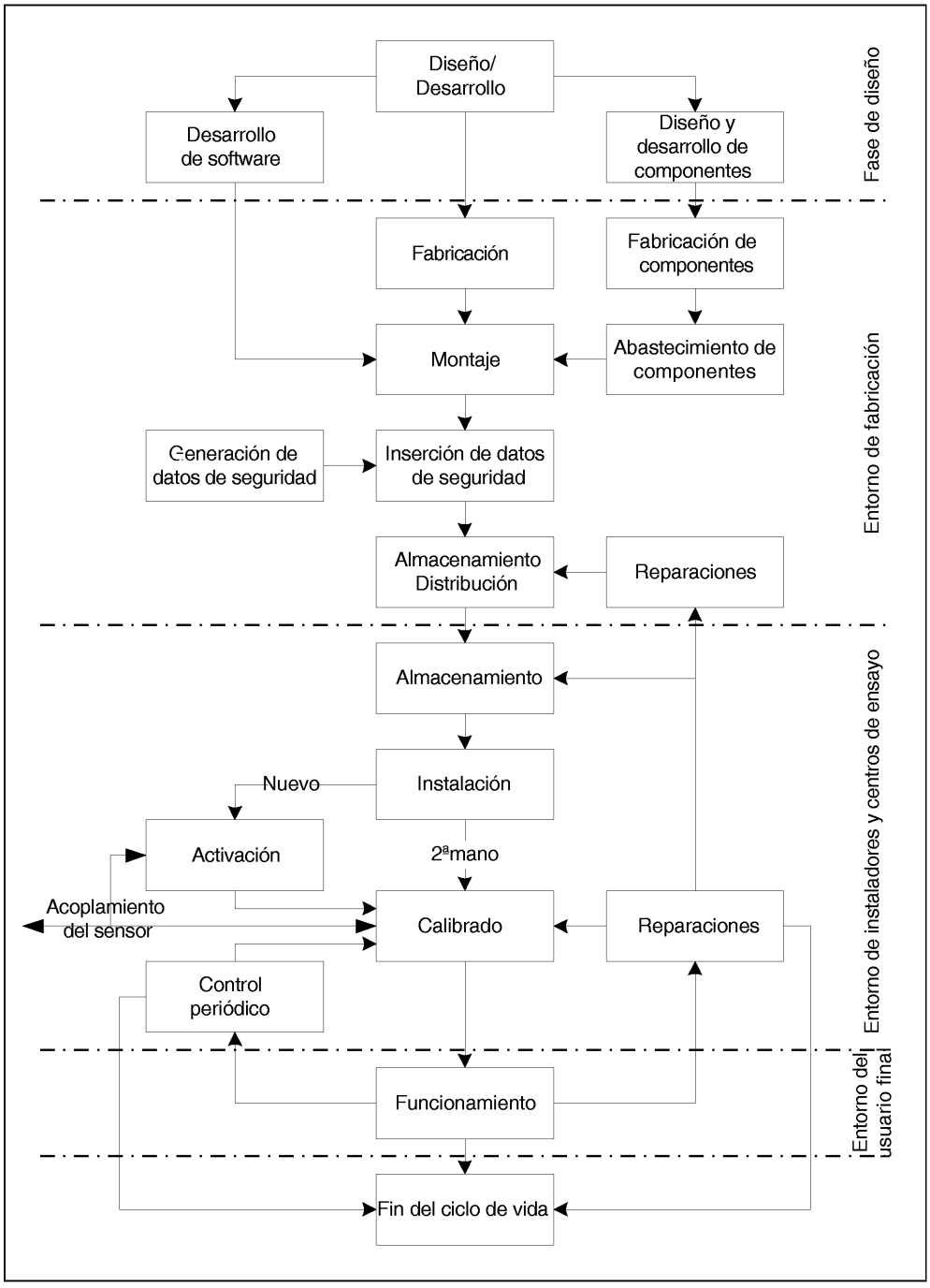
Es preciso señalar que, aunque el mecanismo de la impresora forma parte del TOE, no ocurre lo mismo con el documento impreso resultante.

3.2. ***Ciclo de vida de la unidad intravehicular***

La figura siguiente muestra el ciclo de vida típico de la VU:

Figura 4

Ciclo de vida típico de la VU



3.3. ***Amenazas***

En este apartado se describen las amenazas que podría tener que afrontar la VU.

3.3.1. *Amenazas a las políticas de identificación y de control de accesos*

A.Acceso	Los usuarios podrían tratar de acceder a funciones que les están prohibidas (por ejemplo, un conductor que intente acceder a la función de calibrado)
A.Identificación	Los usuarios podrían tratar de utilizar varias identificaciones o ninguna

3.3.2. *Amenazas relacionadas con el diseño*

A.Fallos	Un posible fallo del hardware, del software o de los procedimientos de comunicación podría llevar a la VU a una situación imprevista que comprometiera su seguridad
A.Pruebas	El empleo de modos de prueba no invalidados o el aprovechamiento de influencias no legítimas podrían comprometer la seguridad de la VU
A.Diseño	Los usuarios podrían tratar de averiguar de forma ilícita los pormenores de diseño, ya sea a través del material del fabricante (mediante robo, soborno, etc.) o por métodos de ingeniería inversa

3.3.3. *Amenazas orientadas al funcionamiento*

A.Parámetros_calibrado	Los usuarios podrían tratar de descalibrar el equipo (modificando los datos de calibrado o a través de flaquezas organizativas)
A.Intercambio_datos_tarjeta	Los usuarios podrían tratar de modificar datos mientras se intercambian entre la VU y las tarjetas de tacógrafo (adición, modificación, borrado, repetición de la señal)
A.Reloj	Los usuarios podrían tratar de modificar el reloj interno
A.Medio_ambiente	Los usuarios podrían comprometer la seguridad de la VU mediante ataques de carácter medioambiental (térmicos, electromagnéticos, ópticos, químicos, mecánicos, etc.)
A.Dispositivos_falsos	Los usuarios podrían tratar de conectar dispositivos falsos (sensor de movimiento, tarjetas inteligentes) a la VU
A.Hardware	Los usuarios podrían tratar de modificar el hardware de la VU
A.Datos_de_movimiento	Los usuarios podrían tratar de modificar los datos de movimiento del vehículo (adición, modificación, borrado, repetición de la señal)
A.No_activado	Los usuarios podrían utilizar un equipo no activado
A.Salida_de_datos	Los usuarios podrían tratar de modificar la salida de datos (impresión, visualización o transferencia)
A.Suministro_eléctrico	Los usuarios podrían tratar de anular los objetivos de seguridad de la VU modificando (cortando, reduciendo, incrementando) su suministro eléctrico
A.Datos_de_seguridad	Los usuarios podrían tratar de obtener de forma ilícita los datos de seguridad durante la generación o el transporte o el almacenamiento de dichos datos en el equipo
A.Software	Los usuarios podrían tratar de modificar el software de la VU
A.Datos_almacenados	Los usuarios podrían tratar de modificar los datos almacenados (datos de seguridad o datos de usuario)

3.4. ***Objetivos de seguridad***

El sistema del tacógrafo digital tiene un objetivo de seguridad primordial:

O.Principal	Los datos que vayan a comprobar las autoridades de control deben estar disponibles y reflejar íntegramente y con precisión las actividades de los conductores y vehículos bajo control, tanto en lo que respecta a los períodos de conducción, trabajo, disponibilidad y descanso, como en lo que respecta a la velocidad del vehículo

Este objetivo de seguridad global exige el cumplimiento de los objetivos de seguridad de la VU:

O.Principal_VU	Los datos que se vayan a medir y registrar y que luego vayan a comprobar las autoridades de control deben estar disponibles y reflejar con precisión las actividades de los conductores y vehículos bajo control, tanto en lo que respecta a los períodos de conducción, trabajo, disponibilidad y descanso, como en lo que respecta a la velocidad del vehículo
O.Exportación_VU	La VU debe ser capaz de exportar datos a medios de almacenamiento externos de manera que se pueda verificar su integridad y autenticidad

3.5. ***Objetivos de seguridad en cuanto a tecnología de la información***

A continuación se relacionan los objetivos de seguridad TI específicos de la VU, que contribuyen a la consecución de sus objetivos de seguridad principales:

O.Acceso	La VU debe controlar el acceso de los usuarios a las funciones y a los datos
O.Responsabilidad	La VU debe recopilar datos de control exactos
O.Auditoría	La VU debe investigar los intentos de violar la seguridad del sistema y debe realizar un seguimiento de los mismos para localizar a los usuarios responsables
O.Autentificación	La VU debería autentificar a los usuarios y a las entidades conectadas (cuando es preciso establecer una vía de confianza entre entidades)
O.Integridad	La VU debe mantener la integridad de los datos almacenados
O.Salida	La VU debe garantizar que la salida de datos refleja con precisión los datos medidos o almacenados
O.Procesamiento	La VU debe garantizar que las entradas se procesan correctamente para obtener datos de usuario precisos
O.Fiabilidad	La VU debe ofrecer un servicio fiable
O.Intercambio_seguro	La VU debe garantizar la seguridad en los intercambios de datos con el sensor de movimiento y con las tarjetas de tacógrafo

3.6. ***Medios físicos, de personal o procedimentales***

El presente apartado describe los requisitos físicos, de personal o procedimentales que contribuyen a la seguridad de la VU.

3.6.1. *Diseño del equipo*

M.Desarrollo	Los técnicos encargados de desarrollar la VU deben garantizar que la asignación de responsabilidades durante la fase de desarrollo se lleva a cabo de manera que se mantenga la seguridad TI
M.Fabricación	Los fabricantes de la VU deben garantizar que la asignación de responsabilidades durante la fase de fabricación se lleva a cabo de manera que se mantenga la seguridad TI, y que durante todo el proceso de fabricación la VU está protegida frente a ataques físicos que pudieran comprometer la seguridad TI

3.6.2. *Entrega y activación del equipo*

M.Entrega	Los fabricantes de la VU, los fabricantes del vehículo y los instaladores o centros de ensayo deben garantizar que la manipulación de VUs no activadas se lleva a cabo de manera que se mantenga la seguridad de dichas VUs
M.Activación	Los fabricantes del vehículo y los instaladores o centros de ensayo deben activar la VU después de haberla instalado, antes de que el vehículo abandone la nave donde se llevó a cabo la instalación

3.6.3. *Generación y abastecimiento de datos de seguridad*

M.Generación_datos_seg	Los algoritmos de generación de datos de seguridad sólo serán accesibles a personas autorizadas y de confianza
M.Transporte_datos_seg	Los datos de seguridad se generarán, transportarán e introducirán en la VU de forma que se preserve su confidencialidad e integridad

3.6.4. *Entrega de tarjetas*

M.Disponibilidad_tarjeta	Las tarjetas de tacógrafo deben estar disponibles y entregarse exclusivamente a personas autorizadas
M.Una_tarjeta_conductor	Los conductores deben estar en posesión de **una** sola tarjeta de conductor válida en un momento dado
M.Posibilidad_seguimiento	Debe ser posible localizar las tarjetas entregadas (listas blancas, listas negras), y es preciso utilizar listas negras durante las auditorías de seguridad

3.6.5. *Instalación, calibrado e inspección del aparato de control*

M.Centros_homologados	La instalación, calibrado y reparación del aparato de control se encomendará exclusivamente a instaladores o centros de ensayo homologados y de confianza
M.Inspecciones_periódicas	El aparato de control debe someterse a inspecciones y calibrados periódicos
M.Calibrado_correcto	Los parámetros del vehículo que los instaladores y centros de ensayo homologados introduzcan en el aparato de control durante el calibrado deben ser los adecuados

3.6.6. *Funcionamiento del equipo*

M.Actuación_correcta_conductores	Los conductores deben cumplir las reglas y actuar de forma responsable (por ejemplo, utilizar sus propias tarjetas, seleccionar debidamente su actividad si se trata de una actividad seleccionada manualmente, etc.)

3.6.7. *Control del cumplimiento de la ley*

M.Controles	Es preciso comprobar el cumplimiento de la ley mediante controles periódicos y aleatorios que incluyan auditorías de seguridad

3.6.8. *Actualizaciones del software*

M.Actualizaciones_software	Las nuevas versiones de software de la VU no se aplicarán hasta después de haber recibido el certificado de seguridad

4. **Funciones de aplicación de la seguridad**

4.1. ***Identificación y autentificación***

4.1.1. *Identificación y autentificación del sensor de movimiento*

UIA_201 La VU deberá ser capaz de establecer, para cada interacción, la identidad del sensor de movimiento al que esté conectada.

UIA_202 La identidad del sensor de movimiento constará del número de homologación y el número de serie del sensor.

UIA_203 La VU deberá autentificar el sensor de movimiento al que está conectada:

— en el momento de producirse la conexión del sensor de movimiento,

— cada vez que se calibre el aparato de control,

— al recuperarse el suministro eléctrico.

La autentificación será mutua y la activará la VU.

UIA_204 La VU deberá reidentificar y reautentificar periódicamente (frecuencia a discreción del fabricante y superior a una vez cada hora) el sensor de movimiento al que está conectada, y garantizar que no se ha cambiado el sensor identificado durante el último calibrado del aparato de control.

UIA_205 La VU deberá ser capaz de detectar e impedir el uso de datos de autentificación que se hayan copiado y reproducido.

UIA_206 Tras haberse detectado varios intentos consecutivos de autentificación con resultados negativos (*número de intentos a discreción del fabricante, y no superior a 20*), o tras haberse detectado que la identidad del sensor de movimiento ha cambiado sin contar con la debida autorización (es decir, no durante un calibrado del aparato de control), la función SEF deberá:

— generar un registro de auditoría del incidente,

— enviar una advertencia al usuario,

— seguir aceptando y utilizando los datos de movimiento no seguros que envíe el sensor de movimiento.

4.1.2. *Identificación y autentificación del usuario*

UIA_207 La VU deberá realizar un seguimiento permanente y selectivo de la identidad de dos usuarios, para lo cual supervisará las tarjetas de tacógrafo que se inserten en las dos ranuras del aparato (la del conductor y la del segundo conductor).

UIA_208 La identidad del usuario constará de:

— un grupo de usuario:

  — CONDUCTOR (tarjeta de conductor),

  — CONTROLADOR (tarjeta de control),

  — CENTRO DE ENSAYO (tarjeta del centro de ensayo),

  — EMPRESA (tarjeta de empresa),

  — INDETERMINADO (no hay tarjeta insertada),

— una identificación de usuario, compuesta de:

  — el código del Estado miembro que expide la tarjeta y el número de tarjeta,

  — INDETERMINADO si se desconoce el grupo de usuario.

Las identidades indeterminadas pueden conocerse de forma implícita o explícita.

UIA_209 La VU deberá autentificar a sus usuarios en el momento de insertar la tarjeta.

UIA_210 La VU deberá reautentificar a sus usuarios:

— al recuperarse el suministro eléctrico,

— periódicamente o al ocurrir determinados incidentes (frecuencia a discreción del fabricante y superior a una vez por día).

UIA_211 La autentificación deberá consistir en una comprobación de que la tarjeta insertada es una tarjeta de tacógrafo válida y posee datos de seguridad que sólo el sistema podría distribuir. La autentificación será mutua y la activará la VU.

UIA_212 Además de las condiciones anteriores, habrá que autentificar a los centros de ensayo mediante una verificación del número PIN. Los números PIN deberán tener una longitud mínima de 4 caracteres.

Nota: Si el número PIN se transfiere a la VU desde un equipo externo situado en la proximidad de la VU, no será necesario proteger la confidencialidad del número PIN durante la transferencia.

UIA_213 La VU deberá ser capaz de detectar e impedir el uso de datos de autentificación que se hayan copiado y reproducido.

UIA_214 Tras haberse detectado 5 intentos consecutivos de autentificación con resultados negativos, la función SEF deberá:

— generar un registro de auditoría del incidente,

— enviar una advertencia al usuario,

— inferir que el usuario es INDETERMINADO y que la tarjeta no es válida (definición z), y cumplir la condición 007.

4.1.3. *Identificación y autentificación de una empresa conectada a distancia*

La posibilidad de conexión a distancia de una compañía es opcional. Por consiguiente, el presente apartado se aplica exclusivamente en el caso de haberse incluido esta característica.

UIA_215 En cada interacción con una empresa conectada a distancia, la VU deberá ser capaz de establecer la entidad de dicha empresa.

UIA_216 La identidad de la empresa conectada a distancia constará del código del Estado miembro que haya expedido su tarjeta de empresa y el número de dicha tarjeta de empresa.

UIA_217 La VU deberá autentificar la empresa conectada a distancia antes de autorizar la exportación de datos hacia ella.

UIA_218 La autentificación deberá consistir en una comprobación de que la empresa posee una tarjeta válida y que ésta guarda datos de seguridad que sólo el sistema podría distribuir.

UIA_219 La VU deberá ser capaz de detectar e impedir el uso de datos de autentificación que se hayan copiado y reproducido.

UIA_220 Tras haberse detectado 5 intentos consecutivos de autentificación con resultados negativos, la VU deberá:

— enviar una advertencia a la empresa conectada a distancia.

4.1.4. *Identificación y autentificación del dispositivo de gestión*

Los fabricantes de la VU pueden prever la instalación de dispositivos dedicados con funciones adicionales de gestión de la VU (por ejemplo, actualización del software, recarga de datos de seguridad, etc.). Por consiguiente, el presente apartado se aplica exclusivamente en el caso de haberse incluido esta característica.

UIA_221 En cada interacción con un dispositivo de gestión, la VU deberá ser capaz de establecer la identidad de dicho dispositivo.

UIA_222 Antes de permitir otras interacciones, la VU deberá autentificar el dispositivo de gestión.

UIA_223 La VU deberá ser capaz de detectar e impedir el uso de datos de autentificación que se hayan copiado y reproducido.

4.2. ***Control de accesos***

Los controles de accesos garantizan que sólo las personas autorizadas pueden leer, crear o modificar la información del TOE.

Es preciso señalar que los datos de usuario que registra la VU, a pesar de presentar aspectos de privacidad o sensibilidad comercial, no poseen un carácter confidencial. Así pues, la condición funcional relativa a los derechos de acceso a la lectura de datos (condición 011) no da lugar a una función de aplicación de la seguridad.

4.2.1. *Política de control de accesos*

ACC_201 La VU deberá gestionar y comprobar los derechos de control de acceso a las funciones y a los datos.

4.2.2. *Derechos de acceso a las funciones*

ACC_202 La VU deberá aplicar las reglas de selección del modo de funcionamiento (condiciones 006 a 009).

ACC_203 La VU deberá utilizar el modo de funcionamiento para aplicar las reglas de control del acceso a las funciones (condición 010).

4.2.3. *Derechos de acceso a los datos*

ACC_204 La VU deberá aplicar las reglas de acceso a la operación de escritura de los datos de identificación de la VU (condición 076).

ACC_205 La VU deberá aplicar las reglas de acceso a la operación de escritura de los datos de identificación del sensor de movimiento acoplado (condiciones 079 y 155).

ACC_206 Una vez activada, la VU deberá garantizar que sólo en el modo de calibrado es posible introducir los datos de calibrado en la VU y almacenarlos en su memoria (condiciones 154 y 156).

ACC_207 Una vez activada, la VU deberá aplicar las reglas de acceso a las operaciones de escritura y borrado de los datos de calibrado (condición 097).

ACC_208 Una vez activada, la VU deberá garantizar que sólo en el modo de calibrado es posible introducir los datos de ajuste de la hora en la VU y almacenarlos en su memoria (esta condición no se aplica a los pequeños ajustes que permiten las condiciones 157 y 158).

ACC_209 Una vez activada, la VU deberá aplicar las reglas de acceso a las operaciones de escritura y borrado de los datos de ajuste de la hora (condición 100).

ACC_210 La VU deberá aplicar un sistema adecuado que regule los derechos de acceso a la lectura y la escritura de datos de seguridad (condición 080).

4.2.4. *Estructura de archivos y condiciones de acceso*

ACC_211 La estructura de los archivos de la aplicación y de los archivos de datos, así como las condiciones de acceso, deberán crearse durante el proceso de fabricación y posteriormente no se podrán modificar ni borrar.

4.3. ***Responsabilidad***

ACT_201 La VU deberá garantizar que los conductores son responsables de sus actividades (condiciones 081, 084, 087, 105a, 105b, 109 y 109a).

ACT_202 La VU deberá guardar datos de identificación permanentes (condición 075).

ACT_203 La VU deberá garantizar que los centros de ensayo son responsables de sus actividades (condiciones 098, 101 y 109).

ACT_204 La VU deberá garantizar que los controladores son responsables de sus actividades (condiciones 102, 103 y 109).

ACT_205 La VU deberá registrar los datos del cuentakilómetros (condición 090) y datos pormenorizados sobre la velocidad (condición 093).

ACT_206 La VU deberá garantizar que los datos de usuario mencionados en las condiciones 081 a 093 y 102 a 105b, inclusive, no se modificarán después de haberse registrado, excepto cuando pasen a ser los datos más antiguos y deban ser sustituidos por otros nuevos.

ACT_207 La VU deberá garantizar que no modificará los datos ya almacenados en una tarjeta de tacógrafo (condiciones 109 y 109a), salvo para sustituir los datos más antiguos por otros nuevos (condición 110) o en el caso descrito en la nota del apartado 2.1 del apéndice 1.

4.4. ***Auditoría***

Las funciones de auditoría se precisan exclusivamente para los incidentes que puedan indicar una manipulación o un intento de violación de la seguridad. Dichas funciones no son necesarias para el ejercicio normal de los derechos, aunque tengan que ver con la seguridad.

AUD_201 La VU deberá registrar los incidentes que afecten a su seguridad y los datos asociados (condiciones 094, 096 y 109).

AUD_202 Los incidentes que afectan a la seguridad de la VU son los siguientes:

— Intentos de violación de la seguridad:

  — fallo de autentificación del sensor de movimiento,

  — fallo de autentificación de la tarjeta de tacógrafo,

  — cambio no autorizado del sensor de movimiento,

  — error de integridad en la entrada de los datos de la tarjeta,

  — error de integridad en los datos de usuario almacenados,

  — error en una transferencia interna de datos,

  — apertura no autorizada de la carcasa,

  — sabotaje del hardware,

— Error al cerrar la última sesión de la tarjeta,

— Error en los datos de movimiento,

— Interrupción del suministro eléctrico,

— Fallo interno de la VU.

AUD_203 La VU deberá aplicar las reglas de almacenamiento de registros de auditoría (condiciones 094 y 096).

AUD_204 La VU deberá almacenar en su memoria los registros de auditoría generados por el sensor de movimiento.

AUD_205 Deberá ser posible imprimir, visualizar y transferir registros de auditoría.

4.5. ***Reutilización de objetos***

REU_201 La VU deberá garantizar que los objetos de almacenamiento temporal se pueden reutilizar sin que ello suponga un flujo inadmisible de información.

4.6. ***Precisión***

4.6.1. *Política de control del flujo de información*

ACR_201 La VU deberá garantizar que los datos de usuario relacionados con las condiciones 081, 084, 087, 090, 093, 102, 104, 105, 105a y 109 proceden de las fuentes apropiadas, que son:

— datos de movimiento del vehículo,

— reloj en tiempo real de la VU,

— parámetros de calibrado del aparato de control,

— tarjetas de tacógrafo,

— datos introducidos por el usuario.

ACR_201a La VU deberá garantizar que los datos de usuario que se introduzcan con arreglo a la condición 109a se referirán exclusivamente al período transcurrido desde la última vez que se extrajera la tarjeta hasta la inserción actual (condición 050a).

4.6.2. *Transferencias internas de datos*

Las condiciones descritas en este apartado se aplican exclusivamente si la VU utiliza piezas separadas físicamente.

ACR_202 Si se transfieren datos entre piezas de la VU que se encuentren separadas físicamente, dichos datos deberán estar protegidos frente a posibles modificaciones.

ACR_203 Si se detecta un error durante una transferencia interna, la transmisión deberá repetirse y la función SEF deberá generar un registro de auditoría del incidente.

4.6.3. *Integridad de los datos almacenados*

ACR_204 La VU deberá comprobar la existencia de errores de integridad en los datos de usuario que almacena en su memoria.

ACR_205 Si se detecta un error de integridad en los datos de usuario almacenados, la función SEF deberá generar un registro de auditoría.

4.7. ***Fiabilidad de servicio***

4.7.1. *Pruebas*

RLB_201 Todos los comandos, acciones o puntos de prueba específicos para las necesidades de ensayo propias de la fase de fabricación de la VU deberán ser desactivados o eliminados antes de que se active la VU, y no se podrán restablecer para su empleo posterior.

RLB_202 La VU deberá efectuar comprobaciones automáticas en el momento de la puesta en marcha y durante el funcionamiento normal, a fin de verificar su correcto funcionamiento. Las comprobaciones automáticas de la VU deberán incluir una verificación de la integridad de los datos de seguridad y una verificación de la integridad del código ejecutable almacenado (si no se encuentra en una memoria ROM).

RLB_203 Si se detecta un fallo interno durante una comprobación automática, la función SEF deberá:

— generar un registro de auditoría (excepto en el modo de calibrado) (fallo interno de la VU),

— preservar la integridad de los datos almacenados.

4.7.2. *Software*

RLB_204 Una vez activada la VU, debe ser imposible analizar o depurar el software sobre el terreno.

RLB_205 No deberán aceptarse como código ejecutable las entradas procedentes de fuentes externas.

4.7.3. *Protección física*

RLB_206 Si la VU se diseña de manera que pueda abrirse, deberá detectar la apertura de la carcasa, excepto en el modo de calibrado, incluso sin alimentación eléctrica externa (durante un mínimo de 6 meses). En tal caso, la función SEF deberá generar un registro de auditoría (es admisible que el registro de auditoría se genere y se almacene después de haberse reconectado el suministro eléctrico).

Si la VU no puede abrirse, deberá estar diseñada de manera que los intentos de manipulación física puedan detectarse con facilidad (por ejemplo, mediante inspección ocular).

RLB_207 Una vez activada, la VU deberá detectar determinados actos (a discreción del fabricante) de sabotaje del hardware.

RLB_208 En el caso arriba descrito, la función SEF deberá generar un registro de auditoría y la VU deberá: (a discreción del fabricante).

4.7.4. *Interrupciones del suministro eléctrico*

RLB_209 La VU deberá detectar las desviaciones que se produzcan con respecto a los valores especificados para el suministro eléctrico, incluido un posible corte.

RLB_210 En el caso arriba descrito, la función SEF deberá:

— generar un registro de auditoría (excepto en el modo de calibrado),

— preservar el estado de seguridad de la VU,

— mantener las funciones de seguridad relacionadas con los componentes o procesos que sigan operativos,

— preservar la integridad de los datos almacenados.

4.7.5. *Condiciones de reinicio*

RLB_211 En caso de interrupción del suministro eléctrico, o si se detiene una transacción antes de que concluya, o si se da cualquier otra condición de reinicio, la VU deberá reiniciarse limpiamente.

4.7.6. *Disponibilidad de los datos*

RLB_212 La VU deberá garantizar que se obtiene acceso a los recursos cuando es necesario y que dichos recursos no se solicitan ni se retienen de forma innecesaria.

RLB_213 La VU debe garantizar que las tarjetas no pueden liberarse antes de haber guardado en ellas los datos pertinentes (condiciones 015 y 016).

RLB_214 En el caso arriba descrito, la función SEF deberá generar un registro de auditoría del incidente.

4.7.7. *Múltiples aplicaciones*

RLB_215 Si la VU ofrece otras aplicaciones aparte de la de tacógrafo, todas ellas deberán estar separadas entre sí por medios físicos o lógicos. Dichas aplicaciones no deberán compartir datos de seguridad, y sólo podrá haber una tarea activa en un momento dado.

4.8. ***Intercambio de datos***

Este apartado se refiere al intercambio de datos entre la VU y los dispositivos conectados.

4.8.1. *Intercambio de datos con el sensor de movimiento*

DEX_201 La VU deberá verificar la integridad y autenticidad de los datos de movimiento importados del sensor de movimiento.

DEX_202 Si se detecta un error de integridad o de autenticidad en los datos de movimiento, la función SEF deberá:

— generar un registro de auditoría,

— seguir utilizando los datos importados.

4.8.2. *Intercambio de datos con tarjetas de tacógrafo*

DEX_203 La VU deberá verificar la integridad y la autenticidad de los datos importados de tarjetas de tacógrafo.

DEX_204 Si se detecta un error de integridad o de autenticidad en los datos de una tarjeta, la VU deberá:

— generar un registro de auditoría,

— abstenerse de utilizar los datos.

DEX_205 Los datos que la VU exporte a las tarjetas de tacógrafo inteligentes deberán ir acompañados de los atributos de seguridad asociados, de manera que la tarjeta pueda verificar su integridad y autenticidad.

4.8.3. *Intercambio de datos con medios de almacenamiento externos (función de transferencia)*

DEX_206 La VU deberá generar una evidencia de origen para los datos transferidos a medios externos.

DEX_207 La VU deberá ofrecer al destinatario la posibilidad de verificar la evidencia de origen de los datos transferidos.

DEX_208 Los datos que la VU transfiera a los medios de almacenamiento externos deberán ir acompañados de los atributos de seguridad asociados, de modo que pueda verificarse la integridad y autenticidad de los datos transferidos.

4.9. ***Apoyo criptográfico***

Las condiciones del presente apartado se aplican exclusivamente cuando es necesario, en función de los mecanismos de seguridad empleados y según las soluciones del fabricante.

CSP_201 En todas las operaciones criptográficas que lleve a cabo la VU se empleará un algoritmo y un tamaño de clave específicos.

CSP_202 Si la VU genera claves criptográficas, deberá ser con arreglo a algoritmos específicos de generación de claves y tamaños de clave específicos.

CSP_203 Si la VU distribuye claves criptográficas, deberá ser con arreglo a métodos específicos de distribución de claves.

CSP_204 Si la VU accede a claves criptográficas, deberá ser con arreglo a métodos específicos de acceso a claves criptográficas.

CSP_205 Si la VU destruye claves criptográficas, deberá ser con arreglo a métodos específicos de destrucción de claves criptográficas.

5. **Definición de mecanismos de seguridad**

Los mecanismos de seguridad necesarios se especifican en el apéndice 11.

El resto de mecanismos de seguridad los definen los fabricantes.

6. **Resistencia mínima de los mecanismos de seguridad**

La resistencia mínima de los mecanismos de seguridad de la unidad intravehicular es Alta, tal y como se define en el documento de referencia ITSEC.

7. **Nivel de certeza**

El nivel de certeza que se toma como objetivo para la unidad intravehicular es el nivel E3, tal y como se define en el documento de referencia ITSEC.

8. **Fundamento lógico**

Las matrices siguientes aportan un fundamento lógico para las funciones SEF, al mostrar:

— qué amenazas contrarresta cada SEF o cada medio,

— qué objetivos de seguridad TI cumple cada SEF.

	Amenazas																		Objetivos TI								
	A.Acceso	A.Identificación	A.Fallos	A.Pruebas	A.Diseño	A.Parámetros de calibrado	A.Intercambio datos tarjeta	A.Reloj	A.Medio ambiente	A.Dispositivos falsos	A.Hardware	A.Datos de movimiento	A.No activado	A.Salida de datos	A.Suministro eléctrico		A.Datos de seguridad	A.Software	A.Datos almacenados	O.Acceso	O.Responsabilidad	O.Auditoría	O.Autentificación	O.Integridad	O.Salida	O.Procesamiento	O.Fiabilidad	O.Intercambio seguro
Medios físicos, de personal o procedimentales																												
Desarrollo			x	x	x																							
Fabricación				x	x																							
Entrega													x															
Activación	x												x															
Generación de datos de seguridad																	x											
Transporte de datos de seguridad																	x											
Disponibilidad de la tarjeta		x																										
Una tarjeta de conductor		x																										
Pos. de seguimiento de la tarjeta		x																										
Centros de ensayo homologados						x		x																				
Inspecciones y calibrados periódicos						x		x				x	x			x												
Actuación correcta de los centros de ensayo						x		x																				
Actuación correcta de los conductores		x																										
Controles del cumplimiento de la ley		x				x		x	x		x		x		x			x	x									
Actualización del software																			x									
Funciones de aplicación de la seguridad																												
Identificación y autentificación																												
UIA_201 Identificación del sensor										x		x											x					x
UIA_202 Identidad del sensor										x		x											x					x
UIA_203 Autentificación del sensor										x		x											x					x
UIA_204 Reidentificación y reautentificación del sensor										x		x											x					x
UIA_205 Autentificación infalsificable										x		x											x					
UIA_206 Fallo de autentificación										x		x										x					x	
UIA_207 Identificación de los usuarios	x	x								x									x			x					x
UIA_208 Identidad del usuario	x	x								x									x			x					x
UIA_209 Autentificación del usuario	x	x								x									x			x					x
UIA_210 Reautentificación del usuario	x	x								x									x			x					x
UIA_211 Medios de autentificación	x	x								x									x			x					
UIA_212 Comprobaciones PIN	x	x				x		x											x			x					
UIA_213 Autentificación infalsificable	x	x								x									x			x					

	Amenazas																				Objetivos TI									
	A.Acceso	A.Identificación	A.Fallos	A.Pruebas	A.Diseño	A.Parámetros de calibrado	A.Intercambio datos tarjeta	A.Reloj	A.Medio ambiente	A.Dispositivos falsos	A.Hardware	A.Datos de movimiento	A.No activado	A.Salida de datos	A.Suministro eléctrico		A.Datos de seguridad	A.Software	A.Datos almacenados	O.Acceso	O.Responsabilidad	O.Auditoría	O.Autentificación	O.Integridad	O.Salida	O.Procesamiento	O.Fiabilidad	O.Intercambio seguro
UIA_214 Fallo de autentificación	x	x								x												x							
UIA_215 Identificación del usuario a distancia	x	x																		x			x						x
UIA_216 Identidad del usuario a distancia	x	x																		x			x						
UIA_217 Autentificación del usuario a distancia	x	x																		x			x						x
UIA_218 Medios de autentificación	x	x																		x			x						
UIA_219 Autentificación infalsificable	x	x																		x			x						
UIA_220 Fallo de autentificación	x	x																											
UIA_221 Identificación del dispositivo de gestión	x	x																		x			x						
UIA_222 Autentificación del dispositivo de gestión	x	x																		x			x						
UIA_223 Autentificación infalsificable	x	x																		x			x						
Control de accesos																													
ACC_201 Política de control de accesos	x					x		x									x		x	x									
ACC_202 Derechos de acceso a las funciones	x					x		x												x									
ACC_203 Derechos de acceso a las funciones	x					x		x												x									
ACC_204 ID de la VU																			x	x									
ACC_205 ID del sensor conectado										x									x	x									
ACC_206 Datos de calibrado	x					x													x	x									
ACC_207 Datos de calibrado						x													x	x									
ACC_208 Datos de ajuste de la hora								x											x	x									
ACC_209 Datos de ajuste de la hora								x											x	x									
ACC_210 Datos de seguridad																	x		x	x									
ACC_211 Estructura de archivos y condiciones de acceso	x					x											x		x	x									
Responsabilidad																													
ACT_201 Resp. conductores																					x								
ACT_202 Datos ID de la VU																					x	x							
ACT_203 Resp. centros de ensayo																					x								
ACT_204 Resp. controladores																					x								
ACT_205 Resp. movimiento de vehículos																					x								
ACT_206 Modificación de los datos de control																			x					x			x		
ACT_207 Modificación de los datos de control																			x					x			x		

	Amenazas																		Objetivos TI							
	A.Acceso	A.Identificación	A.Fallos	A.Pruebas	A.Diseño	A.Parámetros de calibrado	A.Intercambio datos tarjeta	A.Reloj	A.Medio ambiente	A.Dispositivos falsos	A.Hardware	A.Datos de movimiento	A.No activado	A.Salida de datos	A.Suministro eléctrico		A.Datos de seguridad	A.Software	A.Datos almacenados	O.Acceso	O.Responsabilidad	O.Auditoría	O.Autentificación	O.Integridad	O.Salida	O.Procesamiento	O.Fiabilidad	O.Intercambio seguro
Auditoría																												
AUD_201 Registros de auditoría																						x						
AUD_202 Lista de incidentes de auditoría	x						x				x	x		x	x				x			x						
AUD_203 Reglas de almacenamiento de registros de auditoría																						x						
AUD_204 Registros de auditoría del sensor																						x						
AUD_205 Herramientas de auditoría																						x						
Reutilización																												
REU_201 Reutilización																	x									x	x	
Precisión																												
ACR_201 Política de control del flujo de información						x			x		x															x	x	
ACR_202 Transferencias internas														x											x	x	x	
ACR_203 Transferencias internas														x								x						
ACR_204 Integridad de los datos almacenados																			x					x			x	
ACR_205 Integridad de los datos almacenados																			x			x						
Fiabilidad																												
RLB_201 Pruebas de fabricación				x	x																						x	
RLB_202 Comprobaciones automáticas			x								x				x			x									x	
RLB_203 Comprobaciones automáticas											x				x			x				x						
RLB_204 Análisis de software					x													x									x	
RLB_205 Entradas del software																		x							x	x	x	
RLB_206 Apertura de la carcasa					x				x		x			x			x	x	x						x		x	
RLB_207 Sabotaje del hardware											x																x	
RLB_208 Sabotaje del hardware											x											x						
RLB_209 Interrupciones del suministro eléctrico															x												x	
RLB_210 Interrupciones del suministro eléctrico															x							x						
RLB_211 Reinicio			x																								x	
RLB_212 Disponibilidad de los datos																										x	x	
RLB_213 Liberación de la tarjeta																											x	
RLB_214 Error al cerrar la sesión de la tarjeta																							x					
RLB_215 Múltiples aplicaciones																											x	
Intercambio de datos																												
DEX_201 Importación de datos de movimiento seguros												x																x
DEX_202 Importación de datos de movimiento seguro												x							x									
DEX_203 Importación de datos de tarjeta seguros							x																					x

	Amenazas																			Objetivos TI								
	A.Acceso	A.Identificación	A.Fallos	A.Pruebas	A.Diseño	A.Parámetros de calibrado	A.Intercambio datos tarjeta	A.Reloj	A.Medio ambiente	A.Dispositivos falsos	A.Hardware	A.Datos de movimiento	A.No activado	A.Salida de datos	A.Suministro eléctrico		A.Datos de seguridad	A.Software	A.Datos almacenados	O.Acceso	O.Responsabilidad	O.Auditoría	O.Autentificación	O.Integridad	O.Salida	O.Procesamiento	O.Fiabilidad	O.Intercambio seguro
DEX_204 Importación de datos de tarjeta seguros							x															x						
DEX_205 Exportación de datos seguros a tarjetas							x																					x
DEX_206 Evidencia de origen																								x	x			
DEX_207 Evidencia de origen																								x	x			
DEX_208 Exportación segura a medios externos																								x	x			
Apoyo criptográfico																												
CSP_201 Algoritmos																											x	x
CSP_202 Generacióndeclaves																											x	x
CSP_203 Distribución de claves																											x	x
CSP_204 Acceso a claves																											x	x
CSP_205 Destrucción de claves																											x	x

OBJETIVO GENÉRICO DE SEGURIDAD DE LA TARJETA DE TACÓGRAFO

1. **Introducción**

El presente documento contiene una descripción de la tarjeta de tacógrafo, de las amenazas que deberá ser capaz de neutralizar y de los objetivos de seguridad que debe lograr. En las páginas siguientes se especifican las funciones necesarias para la aplicación de la seguridad, así como la resistencia mínima que deben tener los mecanismos de seguridad y el nivel de certeza exigido para las tareas de desarrollo y evaluación.

Las condiciones que se citan en el presente documento son las especificadas en el cuerpo del anexo I B. Para mayor claridad de lectura, en ocasiones las condiciones de los objetivos de seguridad son una repetición de las condiciones mencionadas en el anexo I B. En caso de ambigüedad entre una condición de un objetivo de seguridad y la condición del anexo I B que se toma como referencia, prevalecerá ésta última.

Las condiciones del anexo I B que no se mencionan en los objetivos de seguridad, tampoco dan lugar a funciones de aplicación de la seguridad.

Una tarjeta de tacógrafo es una tarjeta inteligente normalizada que incorpora una aplicación de tacógrafo dedicada y debe cumplir una serie de requisitos de seguridad actualizados, tanto funcionales como de certeza, aplicables a este tipo de tarjetas. Por consiguiente, este objetivo de seguridad incluye tan solo las condiciones de seguridad adicionales que necesita la aplicación de tacógrafo.

Hemos asignado etiquetas individuales a las diferentes especificaciones sobre amenazas, objetivos, medios procedimentales y funciones SEF, con el fin de garantizar el seguimiento hasta los documentos de desarrollo y evaluación.

2. **Abreviaturas, definiciones y referencias**

2.1. ***Abreviaturas***

CI	Circuito Integrado (componente electrónico diseñado para realizar funciones de proceso o de memoria),
OS	Operating system (sistema operativo),
PIN	Personal Identification Number (número de identificación personal),
ROM	Read Only Memory (memoria de solo lectura),
SFP	Security Functions Policy (política de funciones de seguridad),
TOE	Target of Evaluation (objetivo de evaluación),
TSF	TOE Security Function (función de seguridad TOE),
VU	Vehicle Unit (unidad intravehicular).

2.2. ***Definiciones***

Tacógrafo digital	Aparato de control
Datos sensibles	Datos que se almacenan en la tarjeta de tacógrafo y que es preciso proteger para evitar una modificación no autorizada o bien una pérdida de integridad o confidencialidad (cuando proceda para los datos de seguridad). Los datos sensibles incluyen los datos de seguridad y los datos de usuario
Datos de seguridad	Los datos específicos que se precisan como apoyo para las funciones de aplicación de la seguridad (por ejemplo, claves criptográficas)
Sistema	Equipos, personas u organizaciones relacionados de algún modo con el aparato de control
Usuario	Una entidad (usuario humano o entidad TI externa) ajena al TOE que interactúa con el TOE (excepto en la expresión “datos de usuario”)

Datos de usuario	Datos sensibles almacenados en la tarjeta de tacógrafo, distintos de los datos de seguridad. Los datos de usuario incluyen los datos de identificación y los datos de actividad
Datos de identificación	Los datos de identificación incluyen los datos de identificación de la tarjeta y los datos de identificación del titular
Datos de identificación de la tarjeta	Datos de usuario relativos a la identificación de la tarjeta, tal y como se define en las condiciones 190, 191, 192, 194, 215, 231 y 235
Datos de identificación del titular	Datos de usuario relativos a la identificación del titular, tal y como se define en las condiciones 195, 196, 216, 232 y 236
Datos de actividad	Los datos de actividad incluyen los datos sobre las actividades del titular, los datos sobre incidentes y fallos y los datos sobre actividades de control
Datos de actividades del titular	Datos de usuario relativos a las actividades que realiza el titular, tal y como se definen en las condiciones 197, 199, 202, 212, 212a, 217, 219, 221, 226, 227, 229, 230a, 233 y 237
Datos de incidentes y fallos	Datos de usuario relativos a incidentes o fallos, tal y como se definen en las condiciones 204, 205, 207, 208 y 223
Datos de actividades de control	Datos de usuario relativos a controles del cumplimiento de la ley, tal y como se definen en las condiciones 210 y 225

2.3. ***Referencias***

ITSEC	Criterios de evaluación de la seguridad de la tecnología de la información, 1991
IC PP	Smartcard Integrated Circuit Protection Profile (perfil de protección del circuito integrado de una tarjeta inteligente) — Versión 2.0 — Septiembre 1998. Registrado en el organismo de certificación francés con el número PP/9806
ES PP	Smart Card Integrated Circuit With Embedded Software Protection Profile (perfil de proteccion del circuito integrado de una tarjeta inteligente con software integrado) — Versión 2.0 — Junio 99. Registrado en el organismo de certificación francés con el número PP/9911

3. **Características generales del producto**

3.1. ***Descripción y método de uso de la tarjeta de tacógrafo***

Una tarjeta de tacógrafo es una tarjeta inteligente, tal y como se describe en los documentos IC PP y ES PP, que incorpora una aplicación diseñada para uso con el aparato de control.

Las funciones básicas de la tarjeta de tacógrafo son:

— almacenar los datos de identificación de la tarjeta y los datos de identificación del titular. La unidad intravehicular emplea dichos datos para identificar al titular de la tarjeta, para poner a su disposición los derechos de acceso a los datos y las funciones que le correspondan, y para garantizar que es responsable de sus actividades,

— almacenar datos sobre las actividades del titular, datos sobre incidentes y fallos y datos sobre actividades de control, siempre en relación con el titular de la tarjeta.

Por consiguiente, la tarjeta de tacógrafo se concibe para ser utilizada por un dispositivo de interfaz integrado en la unidad intravehicular, aunque también se puede utilizar con cualquier lector de tarjetas (por ejemplo, de un ordenador personal) que tenga pleno acceso a la lectura de los datos de usuario.

Durante la fase final de uso del ciclo de vida de la tarjeta de tacógrafo (fase 7 del ciclo de vida descrito en el documento ES PP), las unidades intravehiculares sólo pueden escribir datos de usuario en la tarjeta.

Las condiciones funcionales de una tarjeta de tacógrafo se especifican en el cuerpo del anexo I B y en el apéndice 2.

3.2. ***Ciclo de vida de la tarjeta de tacógrafo***

El ciclo de vida de la tarjeta de tacógrafo se ajusta al ciclo de vida de una tarjeta inteligente, descrito en el documento ES PP.

3.3. ***Amenazas***

Además de las amenazas de carácter general que se relacionan en los documentos ES PP e IC PP, la tarjeta de tacógrafo quizá tenga que afrontar las amenazas siguientes:

3.3.1. *Objetivos finales*

El objetivo final de un atacante será la modificación de los datos de usuario almacenados en el TOE.

A.Datos_identificación	La modificación de los datos de identificación que almacena el TOE (por ejemplo, el tipo de tarjeta, la fecha de caducidad de la tarjeta o los datos de identificación del titular) permitiría un uso fraudulento del TOE y constituiría una seria amenaza al objetivo global de seguridad del sistema.
A.Datos_actividad	La modificación de los datos de actividad almacenados en el TOE constituiría una amenaza para la seguridad del TOE.
A.Intercambio_datos	La modificación de los datos de actividad (adición, borrado, modificación) durante la importación o la exportación constituiría una amenaza para la seguridad del TOE.

3.3.2. *Vías de ataque*

Existen varias maneras de atacar los datos que contiene el TOE:

— intentar averiguar de forma ilícita las características de diseño del hardware y el software del TOE, y especialmente sus funciones o datos de seguridad. Una manera de obtener un conocimiento ilícito serían los ataques al material del diseñador o del fabricante (robo, soborno, etc.) o el examen directo del TOE (pruebas físicas, análisis de inferencias, etc.),

— aprovecharse de los puntos débiles en el diseño o la realización del TOE (explotar los errores de hardware y de software, los fallos de transmisión y los errores inducidos por el estrés ambiental; explotar los puntos débiles de funciones de seguridad como los procedimientos de autentificación, el control de acceso a los datos, las operaciones criptográficas, etc.),

— modificar el TOE o sus funciones de seguridad mediante ataques físicos, eléctricos o lógicos o una combinación de los tres.

3.4. ***Objetivos de seguridad***

El sistema del tacógrafo digital tiene un objetivo de seguridad primordial:

O.Principal	Los datos que vayan a comprobar las autoridades de control deben estar disponibles y reflejar íntegramente y con precisión las actividades de los conductores y vehículos bajo control, tanto en lo que respecta a los períodos de conducción, trabajo, disponibilidad y descanso, como en lo que respecta a la velocidad del vehículo.

Este objetivo de seguridad global exige el cumplimiento de los objetivos de seguridad principales del TOE:

O.Datos_Identificación_tarjeta	El TOE debe preservar los datos de identificación de la tarjeta y los datos de identificación del titular que se almacenan durante el proceso de personalización de la tarjeta.
O.Almacenamiento_actividad_tarjeta	El TOE debe preservar los datos de usuario que almacenan en la tarjeta las unidades intravehiculares.

3.5. ***Objetivos de seguridad en cuanto a tecnología de la información***

Además de los objetivos generales de seguridad de las tarjetas inteligentes, enumerados en los documentos ES PP e IC PP, a continuación se relacionan los objetivos de seguridad TI específicos del TOE que contribuyen a la consecución de los objetivos de seguridad principales durante la fase final de uso del ciclo de vida:

O.Acceso_datos	El TOE debe limitar los derechos de acceso a la escritura de datos de usuario, y concederlos exclusivamente a unidades intravehiculares autentificadas.
O.Comunicaciones_seguras	El TOE debe ser capaz de aplicar protocolos y procedimientos de comunicación seguros entre la tarjeta y el dispositivo de interfaz cuando lo exija la aplicación.

3.6. ***Medios físicos, de personal o procedimentales***

Los requisitos físicos, de personal o procedimentales que contribuyen a la seguridad del TOE se relacionan en los documentos ES PP e IC PP (capítulos sobre los objetivos de seguridad del entorno).

4. **Funciones de aplicación de la seguridad**

En este apartado se definen algunas de las operaciones permitidas, como la asignación o selección del documento ES PP, y se exponen nuevas condiciones funcionales SEF.

4.1. ***Cumplimiento de los perfiles de protección***

CPP_301 El TOE deberá cumplir lo dispuesto en el documento IC PP.

CPP_302 El TOE deberá cumplir lo dispuesto en el documento ES PP, con las especificaciones que se exponen más adelante.

4.2. ***Identificación y autentificación del usuario***

La tarjeta debe identificar la entidad en la que está insertada, y debe saber si se trata o no de una unidad intravehicular autentificada. La tarjeta puede exportar cualquier tipo de datos de usuario con independencia de la entidad a la que esté conectada, excepto la tarjeta de control que tan solo puede exportar datos de identificación del titular a unidades intravehiculares autentificadas (mostrando su nombre en la pantalla o en los documentos impresos, de manera que el controlador pueda saber con total seguridad que la unidad intravehicular no es falsa).

4.2.1. *Identificación del usuario*

Asignación (FIA_UID.1.1) *Lista de acciones con mediación de la función TSF*: ninguna.

Asignación (FIA_ATD.1.1) *Lista de atributos de seguridad*:

— USER_GROUP: VEHICLE_UNIT, NON_VEHICLE_UNIT,

— USER_ID: Número de matriculación del vehículo (VRN) y código del Estado miembro que lo matricula (USER_ID se conoce exclusivamente si USER_GROUP = VEHICLE_UNIT).

4.2.2. *Autentificación del usuario*

Asignación (FIA_UAU.1.1) *Lista de acciones con mediación de la función TSF*:

— tarjeta de conductor y tarjeta del centro de ensayo: exportar datos de usuario con atributos de seguridad (función de transferencia de los datos de la tarjeta),

— tarjeta de control: exportar datos de usuario sin atributos de seguridad, salvo los datos de identificación del titular.

UIA_301 La autentificación de una unidad intravehicular deberá consistir en una comprobación de que dicha unidad posee datos de seguridad que sólo el sistema podría distribuir.

Selección (FIA_UAU.3.1 y FIA_UAU.3.2): impedir.

Asignación (FIA_UAU.4.1) *Mecanismo(s) de autentificación identificado(s)*: cualquier mecanismo de autentificación.

UIA_302 La tarjeta del centro de ensayo deberá ofrecer otro mecanismo de autentificación, consistente en la verificación de un código PIN (este mecanismo se ha ideado para que la unidad intravehicular pueda cerciorarse de la identidad del titular de la tarjeta, no para proteger el contenido de la tarjeta del centro de ensayo).

4.2.3. *Fallos de autentificación*

Las asignaciones siguientes describen la reacción de la tarjeta en cada fallo de autentificación del usuario.

Asignación (FIA_AFL.1.1) *Número*: 1, *lista de incidentes de autentificación*: autentificación de un dispositivo de interfaz para tarjetas.

Asignación (FIA_AFL.1.2) *Lista de acciones*:

— enviar una advertencia a la entidad conectada,

— suponer que el usuario es una NON_VEHICLE_UNIT.

Las asignaciones siguientes describen la reacción de la tarjeta en caso de fallo del mecanismo adicional de autentificación exigido en el epígrafe UIA_302.

Asignación (FIA_AFL.1.1) *Número*: 5, *lista de incidentes de autentificación*: verificaciones del código PIN (tarjeta del centro de ensayo).

Asignación (FIA_AFL.1.2) *Lista de acciones*:

— enviar una advertencia a la entidad conectada,

— bloquear el procedimiento de verificación del PIN, de manera que todo intento posterior de verificación fracase,

— ser capaz de indicar a los usuarios subsiguientes el motivo del bloqueo.

4.3. ***Control de accesos***

4.3.1. *Política de control de accesos*

Durante la fase final de uso de su ciclo de vida, la tarjeta de tacógrafo es objeto de una política de funciones de seguridad (SFP) sobre control de accesos, denominada AC_SFP.

Asignación (FDP_ACC.2.1) *SFP de control de accesos*: AC_SFP.

4.3.2. *Funciones de control de accesos*

Asignación (FDP_ACF.1.1) *SFP de control de accesos*: AC_SFP.

Asignación (FDP_ACF.1.1) *Grupo de atributos de seguridad que se ha designado*: USER_GROUP.

Asignación (FDP_ACF.1.2) *Reglas de acceso entre sujetos y objetos controlados, con operaciones controladas sobre objetos controlados*:

— GENERAL_READ: Los datos de usuario figuran en el TOE y los puede leer cualquier usuario. La única excepción son los datos de identificación del titular, que se encuentran en las tarjetas de control y sólo los puede leer la VEHICLE_UNIT.

— IDENTIF_WRITE: Los datos de identificación sólo se pueden escribir una vez y antes de que termine la fase 6 del ciclo de vida de la tarjeta. Los usuarios no están autorizados para escribir ni modificar los datos de identificación durante la fase final de uso del ciclo de vida de la tarjeta.

— ACTIVITY_WRITE: La VEHICLE_UNIT es la única que puede escribir los datos de actividad en el TOE.

— SOFT_UPGRADE: Ninguno de los usuarios puede actualizar el software del TOE.

— FILE_STRUCTURE: La estructura de los archivos y las condiciones de acceso deberán crearse antes de que termine la fase 6 del ciclo de vida del TOE, y posteriormente no podrán ser modificados ni borrados por ningún usuario.

4.4. ***Responsabilidad***

ACT_301 El TOE deberá guardar datos de identificación permanentes.

ACT_302 Deberá existir una indicación de la fecha y la hora en que se haya producido la personalización del TOE. Dicha indicación permanecerá inalterable.

4.5. ***Auditoría***

El TOE debe realizar un seguimiento de los incidentes que indiquen una violación potencial de su seguridad.

Asignación (FAU_SAA.1.2) *Subconjunto de incidentes auditables definidos*:

— fallo de autentificación del titular de la tarjeta (5 verificaciones consecutivas del PIN con resultados negativos),

— error de comprobación automática,

— error en la integridad de los datos almacenados,

— error de integridad en la entrada de los datos de actividad.

4.6. ***Precisión***

4.6.1. *Integridad de los datos almacenados*

Asignación (FDP_SDI.2.2) *Acciones que es preciso adoptar*: enviar una advertencia a la entidad conectada,

4.6.2. *Autentificación de los datos básicos*

Asignación (FDP_DAU.1.1) *Lista de objetos o tipos de información*: Datos de actividad.

Asignación (FDP_DAU.1.2) *Lista de sujetos*: Cualquiera.

4.7. ***Fiabilidad de servicio***

4.7.1. *Pruebas*

Selección (FPT_TST.1.1): en el momento de la puesta en marcha, periódicamente durante el funcionamiento normal.

Nota: en el momento de la puesta en marcha significa antes de que se ejecute el código (y no necesariamente durante el procedimiento Answer To Reset).

RLB_301 Las comprobaciones automáticas del TOE deberán incluir la verificación de integridad de los códigos de software que no estén almacenados en la memoria ROM.

RLB_302 Si se detecta un error de comprobación automática, la función TSF deberá enviar una advertencia a la entidad conectada.

RLB_303 Una vez haya terminado la verificación del OS, todos los comandos y las acciones con fines específicos de verificación deberán ser desactivados o eliminados. No deberá ser posible anular dichos controles y recuperarlos para el uso. Durante un estado del ciclo de vida, jamás se accederá a un comando asociado exclusivamente a otro estado.

4.7.2. *Software*

RLB_304 Debe ser imposible analizar, depurar o modificar sobre el terreno el software del TOE.

RLB_305 No deberán aceptarse como código ejecutable las entradas procedentes de fuentes externas.

4.7.3. *Suministro eléctrico*

RLB_306 El TOE mantendrá las condiciones de seguridad durante las interrupciones u oscilaciones del suministro eléctrico.

4.7.4. *Condiciones de reinicio*

RLB_307 Si se corta el suministro eléctrico (o se producen oscilaciones en el suministro) del TOE, o si se detiene una transacción antes de que concluya, o si se da cualquier otra condición de reinicio, el TOE deberá reiniciarse limpiamente.

4.8. ***Intercambio de datos***

4.8.1. *Intercambio de datos con una unidad intravehicular*

DEX_301 El TOE deberá verificar la integridad y autenticidad de los datos importados de una unidad intravehicular.

DEX_302 Si se detecta un error de integridad en los datos importados, el TOE deberá:

— enviar una advertencia a la entidad que envía los datos,

— abstenerse de utilizar los datos.

DEX_303 Los datos de usuario que el TOE exporte a la unidad intravehicular deberán ir acompañados de los atributos de seguridad asociados, de manera que la unidad intravehicular pueda verificar la integridad y autenticidad de los datos recibidos.

4.8.2. *Exportación de datos a medios externos, distintos de una unidad intravehicular (función de transferencia)*

DEX_304 El TOE deberá ser capaz de generar una evidencia de origen para los datos transferidos a medios externos.

DEX_305 El TOE deberá ofrecer al destinatario la posibilidad de verificar la evidencia de origen de los datos transferidos.

DEX_306 El TOE deberá ser capaz de adjuntar los atributos de seguridad asociados a los datos que transfiera a medios de almacenamiento externos, de manera que se pueda verificar la integridad de los datos transferidos.

4.9. ***Apoyo criptográfico***

CSP_301 Si la función TSF genera claves criptográficas, deberá ser con arreglo a algoritmos específicos de generación de claves y tamaños de clave específicos. Las claves de las sesiones criptográficas que se generen podrán utilizarse un determinado número de veces (a discreción del fabricante y no superior a 240).

CSP_302 Si la función TSF distribuye claves criptográficas, deberá ser con arreglo a los métodos especificados de distribución de claves criptográficas.

5. **Definición de mecanismos de seguridad**

Los mecanismos de seguridad necesarios se especifican en el apéndice 11.

El resto de mecanismos de seguridad los define el fabricante del TOE.

6. **Resistencia mínima declarada de los mecanismos**
La resistencia mínima de los mecanismos de seguridad de la tarjeta de tacógrafo es Alta, tal y como se define en el documento de referencia ITSEC.

7. **Nivel de certeza**
El nivel de certeza que se toma como objetivo para la tarjeta de tacógrafo es el nivel E3, tal y como se define en el documento de referencia ITSEC.

8. **Fundamento lógico**
Las matrices siguientes aportan un fundamento lógico para las funciones SEF adicionales, al mostrar:

— qué amenazas contrarresta cada SEF,

— qué objetivos de seguridad TI cumple cada SEF.

	Amenazas											Objetivos TI								
	A.CLON*	A.DIS_ES2	A.T_ES	A.T_CMD	A.MOD_SOFT*	A.MOD_LOAD	A.MOD_EXE	A.MOD_SHARE	A.Datos ident.	A.Datos de actividad	A.Intercambio de datos	O.TAMPER_ES	O.CLON*	O.OPERATE*	O.FLAW*	O.DIS_MECHANISM2	O.DIS_MEMORY*	O.MOD_MEMORY*	O.Acceso a los datos	O.Comunicaciones seguras
UIA_301 Medios de autentificación																			x	
UIA_302 Verificaciones del PIN																			x	
ACT_301 Datos de identificación																				
ACT_302 Fecha de personalización																				
RLB_301 Integridad del software												x		x						
RLB_302 Comprobaciones automáticas												x		x						
RLB_303 Pruebas de fabricación					x	x						x		x						
RLB_304 Análisis de software					x		x	x				x		x						
RLB_305 Entradas del software					x	x		x				x		x						
RLB_306 Suministro eléctrico									x	x		x		x						
RLB_307 Reinicio												x		x						
DEX_301 Importación de datos seguros											x									x
DEX_302 Importación de datos seguros											x									x
DEX_303 Exportación de datos seguros a la VU											x									x
DEX_304 Evidencia de origen											x									x
DEX_305 Evidencia de origen											x									x
DEX_306 Exportación segura a medios externos											x									x
CSP_301 Generación de claves												x								x
CSP_302 Distribución de claves												x								x

Apéndice 11

MECANISMOS DE SEGURIDAD COMUNES

ÍNDICE

1. GENERALIDADES

En el presente apéndice se especifican los mecanismos de seguridad que garantizan:

— la autentificación mutua entre las VU y las tarjetas de tacógrafo, incluido el acuerdo sobre la clave de la sesión,

— la confidencialidad, integridad y autentificación de los datos transferidos entre las VU y las tarjetas de tacógrafo,

— la integridad y autentificación de datos transferidos de las VU a medios de almacenamiento externos,

— la integridad y autentificación de datos transferidos de las tarjetas de tacógrafo a medios de almacenamiento externos.

1.1. **Referencias**

En el presente apéndice aparecen las siguientes referencias:

SHA-1	National Institute of Standards and Technology (NIST). Publicación FIPS 180-1: Norma sobre códigos de comprobación seguros. Abril 1995
PKCS1	Laboratorios RSA. PKCS # 1: Norma de cifrado RSA. Versión 2.0. Octubre 1998
TDES	National Institute of Standards and Technology (NIST). Publicación FIPS 46-3: Norma de cifrado de datos. Borrador 1999
TDES-OP	ANSI X9.52, Modos de funcionamiento del algoritmo triple de encriptación de datos. 1998
ISO/IEC 7816-4	Tecnología de la información — Tarjetas de identificación — Tarjetas de circuito(s) integrado(s) con contactos — Parte 4: Comandos interindustriales para intercambio. Primera edición: 1995 + Modificación 1: 1997
ISO/IEC 7816-6	Tecnología de la información — Tarjetas de identificación — Tarjetas de circuito(s) integrado(s) con contactos — Parte 6: Elementos de datos interindustriales. Primera edición: 1996 + Cor 1: 1998
ISO/IEC 7816-8	Tecnología de la información — Tarjetas de identificación — Tarjetas de circuito(s) integrado(s) con contactos — Parte 8: Comandos interindustriales relacionados con la seguridad. Primera edición 1999
ISO/IEC 9796-2	Tecnología de la información — Técnicas de seguridad — Esquemas de firma digital con recuperación de mensaje — Parte 2: Mecanismos que emplean una función de comprobación aleatoria. Primera edición: 1997
ISO/IEC 9798-3	Tecnología de la información — Técnicas de seguridad — Mecanismos de autentificación de entidades — Parte 3: Autentificación de entidades mediante un algoritmo de clave pública. Segunda edición 1998
ISO 16844-3	Vehículos de carretera-Sistemas de tacógrafo — Parte 3: Interfaz del sensor de movimiento

1.2. **Notaciones y términos abreviados**

En el presente apéndice se emplean las siguientes notaciones y términos abreviados:

(K_a, K_b, K_c)	Un conjunto de claves que utiliza el algoritmo triple de encriptación de datos,
CA	Certification authority (autoridad de certificación),
CAR	Certification authority reference (referencia a la autoridad de certificación),
CC	Cryptographic checksum (suma de control criptográfica),
CG	Criptograma,
CH	Command header (cabecera de comando),
CHA	Certificate holder authorisation (autorización del titular del certificado),
CHR	Certificate holder reference (referencia al titular del certificado),
D()	Descifrado con DES,
DE	Data element (elemento de datos),
DO	Data object (objeto de datos),
d	Clave privada RSA, exponente privado,
e	Clave pública RSA, exponente público,
E()	Cifrado con DES,
EQT	Equipment (equipo),
Hash()	Valor de comprobación aleatoria, una salida de *Hash*,
Hash	Función de comprobación aleatoria,
KID	Key identifier (identificador de clave),
Km	Clave TDES. Clave maestra definida en ISO 16844-3,
Km_{vu}	Clave TDES insertada en las unidades de vehículos,
Km_{wc}	Clave TDES insertada en las tarjetas de los centros de ensayo,
m	Representante de mensaje, un número entero entre 0 y *n*-1,
n	Claves RSA, módulo,
PB	Padding bytes (bytes de relleno),
PI	Padding indicator byte (byte indicador de relleno, se utiliza en un criptograma para confidencialidad DO),
PV	Plain value (valor plano),
s	Representante de la firma, un número entero entre 0 y *n*-1,
SSC	Send sequence counter (contador de la secuencia de envío),
SM	Secure messaging (mensajería segura),
TCBC	Modo de funcionamiento por cifrado progresivo TDEA,
TDEA	Algoritmo triple de encriptación de datos,
TLV	Tag length value (valor de longitud de la etiqueta),
VU	Vehicle unit (unidad intravehicular),
X.C	Certificado del usuario X, expedido por una autoridad de certificación,
X.CA	Una autoridad de certificación del usuario X,
$X.CA.PK_oX.C$	La operación de abrir un certificado para extraer una clave pública. Se trata de un operador infijo, cuyo operando izquierdo es la clave pública de una autoridad de certificación, y cuyo operando derecho es el certificado expedido por dicha autoridad. El resultado es la clave pública del usuario X cuyo certificado es el operando derecho,

X.PK	Clave pública RSA de un usuario X,
X.PK[I]	Cifrado RSA de cierta información I, utilizando la clave pública del usuario X,
X.SK	Clave privada RSA de un usuario X,
X.SK[I]	Cifrado RSA de cierta información I, utilizando la clave privada del usuario X,
'xx'	Un valor hexadecimal,
||	Operador de concatenación.

2. SISTEMAS Y ALGORITMOS CRIPTOGRÁFICOS

2.1. **Sistemas criptográficos**

CSM_001 Las unidades intravehiculares y las tarjetas de tacógrafo deberán emplear un sistema criptográfico RSA clásico de clave pública para ofrecer los siguientes mecanismos de seguridad:

— autentificación entre unidades intravehiculares y tarjetas,

— transporte de claves de sesión triple DES entre las unidades intravehiculares y las tarjetas de tacógrafo,

— firma digital de los datos transferidos desde unidades intravehiculares o tarjetas de tacógrafo a medios externos.

CSM_002 Las unidades intravehiculares y las tarjetas de tacógrafo deberán emplear un sistema criptográfico simétrico triple DES para ofrecer un mecanismo que garantice la integridad de los datos durante los intercambios de datos de usuario entre las unidades intravehiculares y las tarjetas de tacógrafo, y para ofrecer, cuando proceda, la confidencialidad en los intercambios de datos entre las unidades intravehiculares y las tarjetas de tacógrafo.

2.2. **Algoritmos criptográficos**

2.2.1. ***Algoritmo RSA***

CSM_003 El algoritmo RSA se define íntegramente con las relaciones siguientes:

$$X.SK[m] = s = m^d \bmod n$$

$$X.PK[s] = m = s^e \bmod n$$

En el documento de referencia PKCS1 figura una descripción más completa de la función RSA.

El exponente público e será, para los cálculos RSA, distinto de 2 en todas las claves RSA generadas.

2.2.2. ***Algoritmo de comprobación aleatoria***

CSM_004 Los mecanismos de firma digital deberán emplear el algoritmo SHA-1 de comprobación aleatoria, que se define en el documento de referencia SHA-1.

2.2.3. ***Algoritmo de encriptación de datos***

CSM_005 En el modo de funcionamiento por cifrado progresivo deberán emplearse algoritmos con base DES.

3. CLAVES Y CERTIFICADOS

3.1. **Generación y distribución de claves**

3.1.1. ***Generación y distribución de claves RSA***

CSM_006 Las claves RSA deberán generarse en tres niveles jerárquicos funcionales:

— nivel europeo,

— nivel de Estado miembro,

— nivel de equipo.

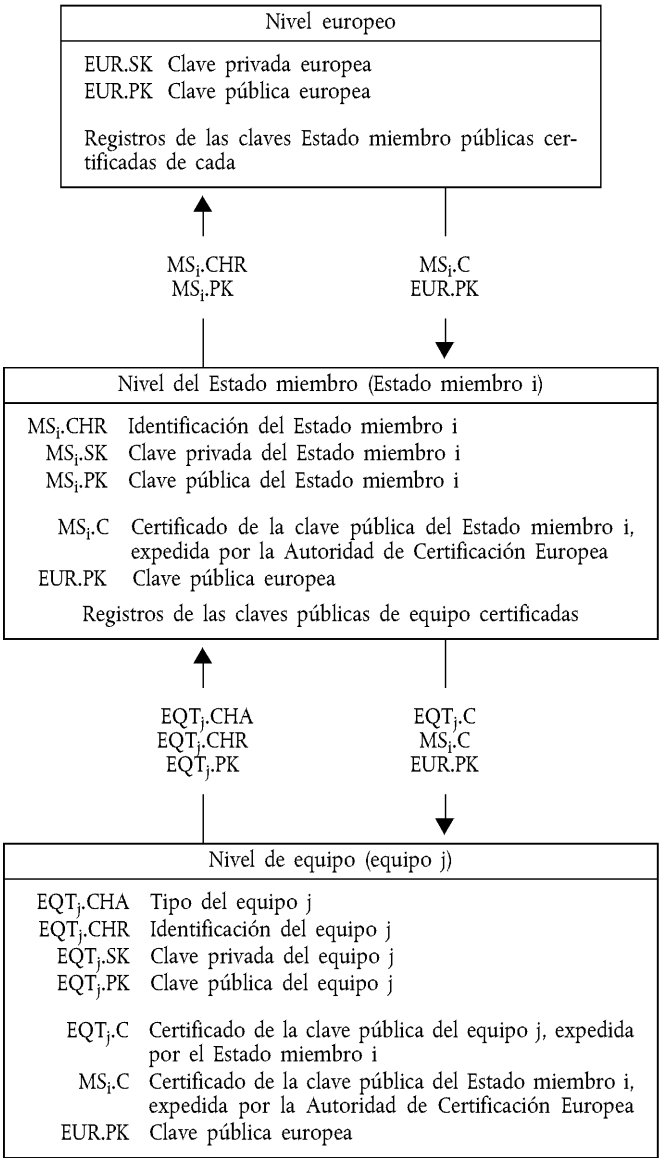
CSM_007 En el nivel europeo deberá generarse un único par de claves europeas (EUR.SK y EUR.PK). La clave privada europea deberá emplearse para certificar las claves públicas de los Estados miembros. Se conservarán registros de todas las claves certificadas. Todas estas tareas se realizarán bajo la gestión de una autoridad de certificación europea, y bajo la autoridad y la responsabilidad de la Comisión Europea.

CSM_008 En el nivel de los Estados miembros, deberá generarse un par de claves de Estado miembro (MS.SK y MS.PK). La autoridad de certificación europea se encargará de certificar las claves públicas de los Estados miembros. La clave privada del Estado miembro deberá emplearse para certificar las claves públicas que vayan a introducirse en el equipo (unidad intravehicular o tarjeta de tacógrafo). Se conservarán registros de todas las claves públicas certificadas, junto con la identificación del equipo para el que están destinadas. Todas estas tareas se realizarán bajo la gestión de una autoridad de certificación del Estado miembro que corresponda. Un Estado miembro podrá cambiar periódicamente su par de claves.

CSM_009 En el nivel de equipo, deberá generarse e introducirse en cada equipo un único par de claves (EQT.SK y EQT.PK). Una autoridad de certificación del Estado miembro se encargará de certificar las claves públicas del equipo. Todas estas tareas podrán realizarse bajo la gestión de los fabricantes de los equipos, los personalizadores de los equipos o las autoridades de los Estados miembros. Este par de claves se emplea para los servicios de autentificación, firma digital y cifrado.

CSM_010 Es preciso mantener la confidencialidad de las claves privadas durante su generación, transporte (en su caso) y almacenamiento.

El gráfico siguiente resume el flujo de datos en este proceso:



3.1.2. ***Claves de prueba RSA***

CSM_011 Con el fin de verificar los equipos (inclusive pruebas de interoperabilidad), la autoridad de certificación europea deberá generar otro par de claves de prueba europeas y al menos dos pares de claves de prueba de Estado miembro, cuyas claves públicas deberán certificarse con la clave privada de prueba europea. Los fabricantes deberán introducir, en el equipo que se someta a las pruebas de homologación, las claves de prueba certificadas por una de estas claves de prueba de Estado miembro.

3.1.3. ***Claves del sensor de movimiento***

La confidencialidad de las tres claves TDES descritas a continuación se mantendrá adecuadamente durante la generación, el transporte (si lo hay) y el almacenamiento.

A fin de admitir equipo de grabación conforme con la norma ISO 16844, la autoridad de certificación europea y las autoridades de certificación de los Estados miembros garantizarán, además, lo siguiente:

CSM_036 La autoridad de certificación europea generará Km_{VU} y Km_{WC}, dos claves Triple DES independientes y únicas, y generará Km como:

$$Km = Km_{VU} \text{ XOR } Km_{WC}$$

La autoridad de certificación europea remitirá estas claves, con arreglo a procedimientos de seguridad adecuados, a las autoridades de certificación de los Estados miembros cuando éstas lo soliciten.

CSM_037 Las autoridades de certificación europeas:

— utilizarán Km para cifrar los datos del sensor de movimiento solicitados por los fabricantes del sensor de movimiento (los datos que deben cifrarse con Km se definen en ISO 16844-3),

— remitirán Km_{VU} a los fabricantes de la unidad del vehículo, con arreglo a procedimientos de seguridad adecuados, para su inserción en las unidades del vehículo,

— se encargarán de que Km_{WC} se inserte en todas las tarjetas de centros de ensayo (`SensorInstallationSecData` en el archivo elemental `Sensor_Installation_Data` durante la personalización de la tarjeta.

3.1.4. ***Generación y distribución de claves de sesión T-DES***

CSM_012 Las unidades intravehiculares y las tarjetas de tacógrafo deberán, como parte del proceso de autentificación mutua, generar e intercambiar los datos necesarios para elaborar una clave común de sesión triple DES. La confidencialidad de este intercambio de datos deberá estar protegida por un mecanismo criptográfico RSA.

CSM_013 Esta clave deberá emplearse en todas las operaciones criptográficas subsiguientes que utilicen mensajería segura. Su validez expirará al término de cada sesión (al extraer o reiniciar la tarjeta) o después de 240 usos (un uso de la clave = un comando que se envíe a la tarjeta y utilice mensajería segura, y la respuesta asociada).

3.2. **Claves**

CSM_014 Las claves RSA (con independencia de su nivel) deberán tener las longitudes siguientes: módulo *n* 1024 bits, exponente público *e* 64 bits máximo, exponente privado *d* 1024 bits.

CSM_015 Las claves triple DES deberán tener la forma (K_a, K_b, K_a), donde K_a y K_b son claves independientes con una longitud de 64 bits. No se configurarán bits para la detección de errores de paridad.

3.3. **Certificados**

CSM_016 Los certificados de clave pública RSA deberán ser "no autodescriptivos" y "verificables con tarjeta" (ref.: ISO/IEC 7816-8).

3.3.1. ***Contenido de los certificados***

CSM_017 Los certificados de clave pública RSA incluyen los datos siguientes en este orden:

Dato	Formato	Bytes	Observaciones
CPI	Nº ENTERO	1	Identificador de perfil del certificado ('01' para esta versión)
CAR	CADENA DE OCTETOS	8	Referencia a la autoridad de certificación
CHA	CADENA DE OCTETOS	7	Autorización del titular del certificado
EOV	Fecha	4	Fin de la validez del certificado. Este dato es opcional y se rellena con las letras 'FF' si no se utiliza
CHR	CADENA DE OCTETOS	8	Referencia al titular del certificado
n	CADENA DE OCTETOS	128	Clave pública (módulo)
e	CADENA DE OCTETOS	8	Clave pública (exponente público)
		164	

Notas:

1. El "Identificador de perfil del certificado" (CPI) define la estructura exacta de un certificado de autentificación. Se puede utilizar como un identificador interno del equipo en una lista de cabeceras que describa la concatenación de elementos de datos en el certificado.

   A continuación se muestra la lista de cabeceras asociada al contenido de este certificado:

'4D'	'16'	'5F 29'	'01'	'42'	'08'	'5F 4B'	'07'	'5F 24'	'04'	'5F 20'	'08'	'7F 49'	'05'	'81'	'81 80'	'82'	'08'
Etiqueta de lista de cabeceras ampliada	Longitud de la lista de cabeceras	Etiqueta CPI	Longitud CPI	Etiqueta CAR	Longitud CAR	Etiqueta CHA	Longitud CHA	Etiqueta EOV	Longitud EOV	Etiqueta CHR	Longitud CHR	Etiqueta de clave pública (construida)	Longitud de los DOs subsiguientes	Etiqueta del módulo	Longitud del módulo	Etiqueta del exponente público	Longitud del exponente público

2. La "referencia a la autoridad de certificación" (CAR) sirve para identificar a la CA que expide el certificado, de manera que el elemento de datos se puede utilizar simultáneamente como un identificador de la clave de la autoridad, para señalar la clave pública de la autoridad de certificación (la codificación se explica más adelante, cuando se habla del identificador de clave).

3. La "autorización del titular del certificado" (CHA) sirve para identificar los derechos que posee el titular del certificado. Consta del identificador de la aplicación de tacógrafo y del tipo de equipo a que se refiere el certificado (con arreglo al elemento de datos *EquipmentType*, "00" para un Estado miembro).

4. La "referencia al titular del certificado" (CHR) sirve para identificar de forma inequívoca al titular del certificado, de manera que el elemento de datos se puede utilizar simultáneamente como un identificador de clave de sujeto para señalar la clave pública del titular del certificado.

5. Los identificadores de clave permiten identificar de forma inequívoca al titular del certificado y a las autoridades de certificación. Los identificadores de clave se codifican de la manera siguiente:

   5.1. Equipo (VU o tarjeta):

Dato	Núm. de serie del equipo	Fecha	Tipo	Fabricante
Long.	4 bytes	2 bytes	1 byte	1 byte
Valor	Número entero	Codificación BCD mm aa	Específico del fabricante	Código del fabricante

En el caso de una VU, el fabricante, cuando solicita un certificado, puede o no conocer la identificación del equipo en el que se introducirán las claves.

En el primer caso, el fabricante enviará la identificación del equipo, junto con la clave pública, a la autoridad de certificación de su Estado miembro. El certificado que ésta expida contendrá la identificación del equipo. El fabricante debe cerciorarse de que las claves y el certificado se introducen en el equipo que corresponde. El identificador de clave tiene la forma arriba descrita.

En caso contrario, el fabricante debe identificar de forma inequívoca cada solicitud de certificado y enviar dicha identificación, junto con la clave pública, a la autoridad de certificación de su Estado miembro. El certificado que ésta expida contendrá la identificación de la solicitud. Una vez se haya instalado la clave en el equipo, el fabricante, por su parte, debe comunicar a la autoridad de su Estado miembro la asignación de la clave al equipo (es decir, la identificación de la solicitud del certificado, la identificación del equipo). El identificador de clave posee la forma siguiente:

Dato	Nº serie solicitud de certificado	Fecha	Tipo	Fabricante
Long.	4 bytes	2 bytes	1 byte	1 byte
Valor	Codificación BCD	Codificación BCD mm aa	'FF'	Código del fabricante

5.2. Autoridad de certificación:

Dato	Identificación de la autoridad	Nº serie de la clave	Información adicional	Identificador
Long.	4 bytes	1 byte	2 bytes	1 byte
Valor	1 byte código numérico de la nación 3 bytes código alfanumérico de la nación	Número entero	Codificación adicional (específica de la CA) 'FF FF' si no se utiliza	'01'

El número de serie de la clave sirve para distinguir las diferentes claves de un Estado miembro en caso de que se cambie la clave.

6. Los responsables de verificar los certificados deberán saber de forma implícita que la clave pública certificada es una clave RSA relevante para los servicios de autentificación, verificación de la firma digital y cifrado para confidencialidad (el certificado no contiene ningún Identificador de Objeto que lo especifique).

3.3.2. ***Certificados expedidos***

CSM_018 El certificado expedido es una firma digital con recuperación parcial del contenido del certificado, según la norma ISO/IEC 9796-2, y se le añade una "referencia a la autoridad de certificación".

$$X.C = X.CA.SK['6A' \,||\, C_r \,||\, Hash(Cc) \,||\, 'BC'] \,||\, C_n \,||\, X.CAR$$

Con el contenido del certificado $= Cc = \underset{106\ bytes}{C_r} \,||\, \underset{58\ bytes}{C_n}$

Notas:

1. Este certificado tiene una longitud de 206 bytes.

2. La referencia CAR, oculta por la firma, también se añade, de manera que es posible seleccionar la clave pública de la autoridad de certificación para verificar el certificado.

3. El responsable de verificar el certificado deberá conocer de forma implícita el algoritmo empleado por la autoridad de certificación para firmar el certificado.

4. A continuación se muestra la lista de cabeceras asociada a este certificado expedido:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
Etiqueta del certificado CV (Construida)	Long. de los DOs subsiguientes	Etiqueta de firma	Long. de la firma	Etiqueta de resto	Long. del resto	Etiqueta CAR	Longitud CAR

3.3.3. ***Verificación y apertura del certificado***

La verificación y apertura del certificado consiste en verificar la firma con arreglo a la norma ISO/IEC 9796-2, recuperar el contenido del certificado y la clave pública: X.PK = X.CA.PK$_o$X.C, y verificar la validez del certificado.

CSM_019 Este proceso consta de las siguientes etapas:

Verificación de la firma y recuperación del contenido:

— conocido el X.C, recuperar la firma, C_n' y CAR′: X.C = Firma (128 Bytes) || C_n' (58 Bytes) || CAR' (8 Bytes)

— conocida la referencia CAR′, seleccionar la clave pública de la autoridad de certificación (si no se ha hecho antes por otros medios),

— abrir la firma con la clave pública de la CA: Sr′ = X.CA.PK [Firma],

— comprobar que Sr′ comienza con 6A′ y termina con BC′

— calcular Cr′ y H′ a partir de: Sr' = '6A' || C_r' (106 Bytes) || H' (20 Bytes) || 'BC'

— recuperar el contenido C′ del certificado = C_r' || C_n',

— comprobar que *Hash*(C′) = H′

Si estas comprobaciones arrojan un resultado positivo, el certificado es genuino y su contenido es C′.

Una vez conocido el contenido C′, verificación de la validez:

— si procede, comprobar el final de la fecha de validez,

Una vez conocido el contenido C′, recuperación y almacenamiento de la clave pública, el identificador de clave, la autorización del titular del certificado y el fin de la validez del certificado:

— X.PK = *n* || *e*

— X.KID = CHR

— X.CHA = CHA

— X.EOV = EOV

4. MECANISMO DE AUTENTIFICACIÓN MUTUA

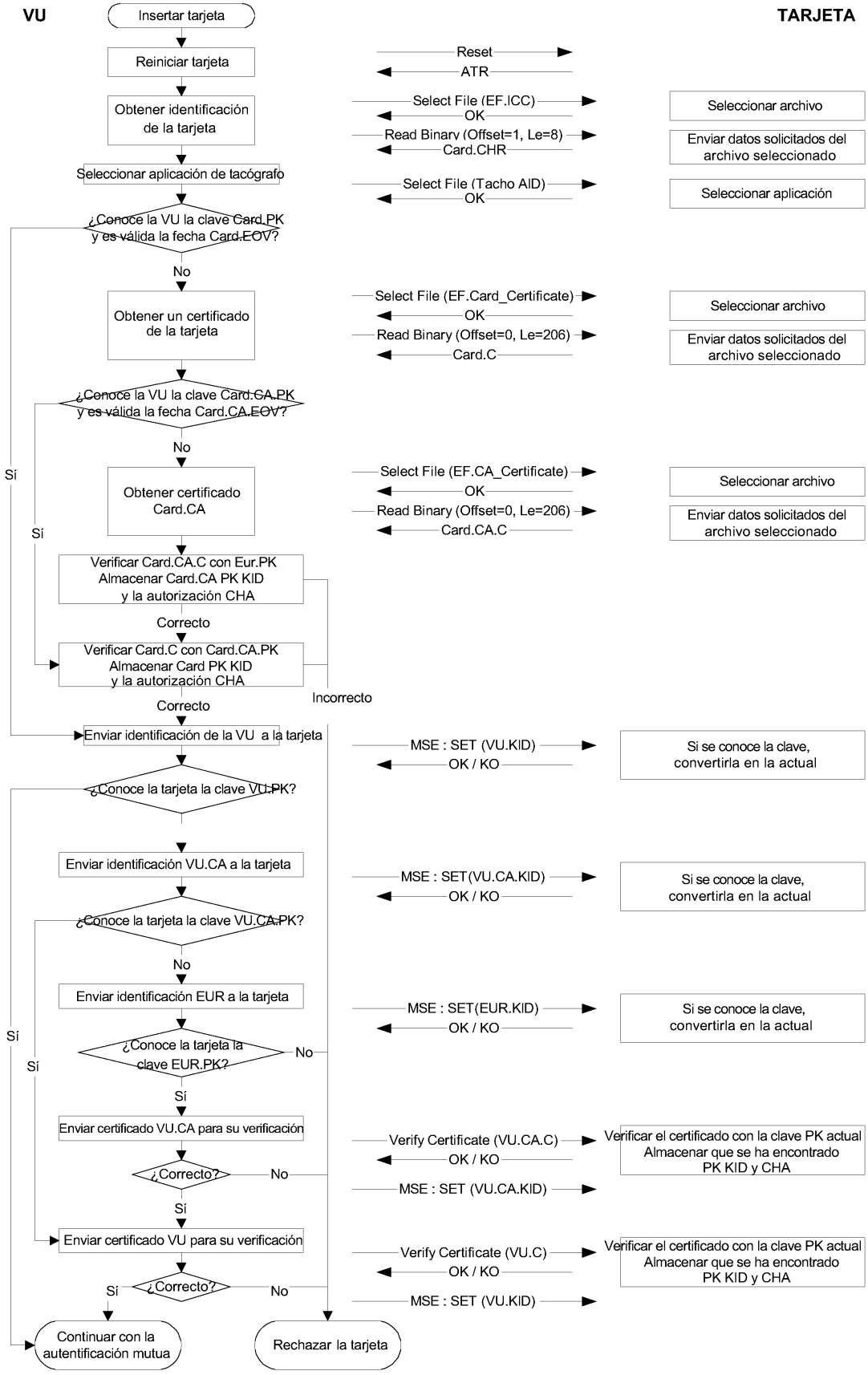
La autentificación mutua entre tarjetas y VUs se basa en el siguiente principio:

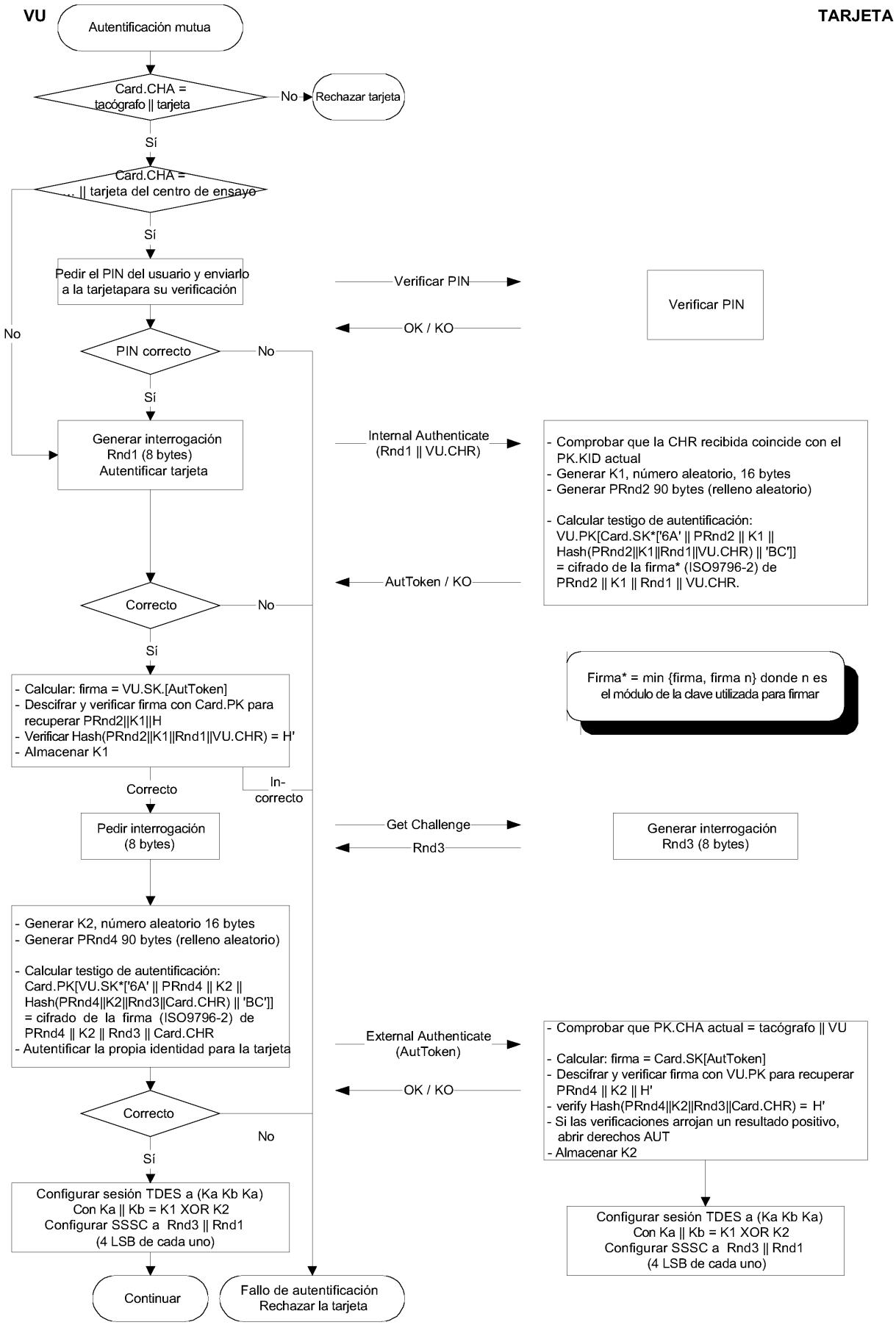
Cada parte deberá demostrar a la otra que está en posesión de un par de claves válido cuya clave pública ha sido certificada por la autoridad de certificación de un Estado miembro, y que dicha autoridad ha sido certificada por la autoridad de certificación europea.

La demostración se lleva a cabo firmando con la clave privada un número aleatorio enviado por la otra parte, quien debe recuperar dicho número cuando verifique esta firma.

El mecanismo lo activa la VU al insertar la tarjeta. Comienza con el intercambio de certificados y la apertura de claves públicas, y termina con la creación de una clave de sesión.

CSM_020 Deberá utilizarse el protocolo siguiente (las flechas indican los comandos y datos que se intercambian [véase el apéndice 2)]:




VU
TARJETA
Autentificación mutua
Card.CHA = tacógrafo || tarjeta
No
Rechazar tarjeta
Sí
Card.CHA = ... || tarjeta del centro de ensayo
Sí
Pedir el PIN del usuario y enviarlo a la tarjetapara su verificación
Verificar PIN
Verificar PIN
OK / KO
No
PIN correcto
No
Sí
Generar interrogación Rnd1 (8 bytes) Autentificar tarjeta
Internal Authenticate (Rnd1 || VU.CHR)
- Comprobar que la CHR recibida coincide con el PK.KID actual
- Generar K1, número aleatorio, 16 bytes
- Generar PRnd2 90 bytes (relleno aleatorio)
- Calcular testigo de autentificación: VU.PK[Card.SK*['6A' || PRnd2 || K1 || Hash(PRnd2||K1||Rnd1||VU.CHR) || 'BC']] = cifrado de la firma* (ISO9796-2) de PRnd2 || K1 || Rnd1 || VU.CHR.
AutToken / KO
Correcto
No
Sí
Firma* = min {firma, firma n} donde n es el módulo de la clave utilizada para firmar
- Calcular: firma = VU.SK.[AutToken]
- Descifrar y verificar firma con Card.PK para recuperar PRnd2||K1||H
- Verificar Hash(PRnd2||K1||Rnd1||VU.CHR) = H'
- Almacenar K1
Correcto
In-correcto
Pedir interrogación (8 bytes)
Get Challenge
Rnd3
Generar interrogación Rnd3 (8 bytes)
- Generar K2, número aleatorio 16 bytes
- Generar PRnd4 90 bytes (relleno aleatorio)
- Calcular testigo de autentificación: Card.PK[VU.SK*['6A' || PRnd4 || K2 || Hash(PRnd4||K2||Rnd3||Card.CHR) || 'BC']] = cifrado de la firma (ISO9796-2) de PRnd4 || K2 || Rnd3 || Card.CHR
- Autentificar la propia identidad para la tarjeta
External Authenticate (AutToken)
- Comprobar que PK.CHA actual = tacógrafo || VU
- Calcular: firma = Card.SK[AutToken]
- Descifrar y verificar firma con VU.PK para recuperar PRnd4 || K2 || H'
- verify Hash(PRnd4||K2||Rnd3||Card.CHR) = H'
- Si las verificaciones arrojan un resultado positivo, abrir derechos AUT
- Almacenar K2
OK / KO
Correcto
No
Sí
Configurar sesión TDES a (Ka Kb Ka) Con Ka || Kb = K1 XOR K2 Configurar SSSC a Rnd3 || Rnd1 (4 LSB de cada uno)
Configurar sesión TDES a (Ka Kb Ka) Con Ka || Kb = K1 XOR K2 Configurar SSSC a Rnd3 || Rnd1 (4 LSB de cada uno)
Continuar
Fallo de autentificación Rechazar la tarjeta

5. MECANISMOS DE CONFIDENCIALIDAD, INTEGRIDAD Y AUTENTIFICACIÓN EN LAS TRANSFERENCIAS DE DATOS ENTRE LA VU Y LAS TARJETAS

5.1. **Mensajería segura**

CSM_021 La integridad de las transferencias de datos entre la VU y las tarjetas estará protegida por un sistema de mensajería segura, de conformidad con los documentos de referencia ISO/IEC 7816-4 e ISO/IEC 7816-8.

CSM_022 Cuando haya que proteger los datos durante la transferencia, se añadirá un objeto de datos consistente en una suma de control criptográfica a los objetos de datos que se envíen en el comando o la respuesta. El receptor deberá verificar dicha suma de control criptográfica.

CSM_023 La suma de control criptográfica de los datos enviados en un comando deberá integrar la cabecera del comando y todos los objetos de datos que se envíen (= > CLA = '0C', y todos los objetos de datos deberán estar englobados en etiquetas donde b1 = 1).

CSM_024 Los bytes correspondientes a la información de estado en la respuesta deberán estar protegidos por una suma de control criptográfica cuando dicha respuesta no contenga un campo de datos.

CSM_025 Las sumas de control criptográficas deberán tener una longitud de 4 bytes.

Así pues, la estructura de comandos y respuestas cuando se utiliza un sistema de mensajería segura es así:

Los DOs empleados son un conjunto parcial de los DOs de mensajería segura que se describen en la norma ISO/IEC 7816-4:

Etiqueta	Mnemónico	Significado
'81'	T_{PV}	Dato de valor plano no codificado en BER-TLV (con la protección de la suma CC)
'97'	T_{LE}	Valor de Le en el comando no seguro (con la protección de la suma CC)
'99'	T_{SW}	Información de estado (con la protección de la suma CC)
'8E'	T_{CC}	Suma de control criptográfica
'87'	$T_{PI\ CG}$	Byte indicador de relleno || Criptograma (Valor plano no codificado en BER-TLV)

Dado un par de respuestas para un comando no seguro:

Cabecera del comando	Cuerpo del comando
CLA INS P1 P2	[campo L_c] [campo de datos] [campo L_e]
cuatro bytes	L bytes, designados B_1 a B_L

Cuerpo de la respuesta	Cola de la respuesta
[Campo de datos]	SW1 SW2
L_r bytes de datos	Dos bytes

El correspondiente par de respuestas para el comando seguro es:

Comando seguro:

Cabecera del comando (CH)	Cuerpo del comando										
CLA INS P1 P2	[Nuevo campo L_c]	[Nuevo campo de datos]									[Nuevo campo L_e]
'OC'	Longitud del nuevo campo de datos	T_{PV}	L_{PV}	PV	T_{LE}	L_{LE}	L_e	T_{CC}	L_{CC}	CC	'00'
		'81'	L_c	Campo de datos	'97'	'01'	L_e	'8E'	'04'	CC	

Datos que habrá que integrar en la suma de control = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB

PB = Bytes de relleno (80 .. 00) con arreglo a las normas ISO-IEC 7816-4 y ISO 9797, método 2.

Los DOs PV y LE sólo están presentes cuando existen datos correspondientes en el comando no seguro.

Respuesta segura:

1. Caso en que el campo de datos de la respuesta no está vacío y no es necesario protegerlo para garantizar la confidencialidad:

Cuerpo de la respuesta						Cola de la respuesta
[Nuevo campo de datos]						nuevo SW1 SW2
T_{PV}	L_{PV}	PV	T_{CC}	L_{CC}	CC	
'81'	L_r	Campo de datos	'8E'	'04'	CC	

Datos que habrá que integrar en la suma de control = T_{PV} || L_{PV} || PV || PB

2. Caso en que el campo de datos de la respuesta no está vacío y debe ser protegido para garantizar la confidencialidad:

Cuerpo de la respuesta						Cola de la respuesta
[Nuevo campo de datos]						nuevo SW1 SW2
$T_{PI\ CG}$	$L_{PI\ CG}$	PI CG	T_{CC}	L_{CC}	CC	
'87'		PI || CG	'8E'	'04'	CC	

Datos que deberá llevar el CG: datos no codificados en BER-TLV y bytes de relleno.

Datos que habrá que integrar en la suma de control = $T_{PI\ CG}$ || $L_{PI\ CG}$ || PI CG || PB

3. Caso en que el campo de datos de la respuesta está vacío:

Cuerpo de la respuesta						Cola de la respuesta
[Nuevo campo de datos]						nuevo SW1 SW2
T_{SW}	L_{SW}	SW	T_{CC}	L_{CC}	CC	
'99'	'02'	nuevo SW1 SW2	'8E'	'04'	CC	

Datos que habrá que integrar en la suma de control = T_{SW} || L_{SW} || SW || PB

5.2. **Tratamiento de los errores de mensajería segura**

CSM_026 Si la tarjeta de tacógrafo detecta un error SM mientras está interpretando un comando, los bytes de estado tendrán que ser devueltos sin SM. De acuerdo con la norma ISO/IEC 7816-4, se definen los siguientes bytes de estado para indicar errores SM:

'66 88' Ha fallado la verificación de la suma de control criptográfica,

'69 87' Faltan los objetos de datos SM que se esperaban,

'69 88' Objetos de datos SM incorrectos.

CSM_027 Si la tarjeta de tacógrafo devuelve bytes de estado sin DOs SM o con un DO SM erróneo, la VU tendrá que interrumpir la sesión.

5.3. **Algoritmo para calcular sumas de control criptográficas**

CSM_028 Las sumas de control criptográficas se construyen utilizando MACs según ANSI X9.19, con DES:

— etapa inicial: el bloque de control inicial y0 es E(Ka, SSC),

— etapa secuencial: los bloques de control y1, .. , yn se calculan utilizando Ka,

— etapa final: la suma de control criptográfica se calcula a partir del último bloque de control yn de la manera siguiente: E(Ka, D(Kb, yn)),

donde E() significa cifrado con DES, y D() significa descifrado con DES.

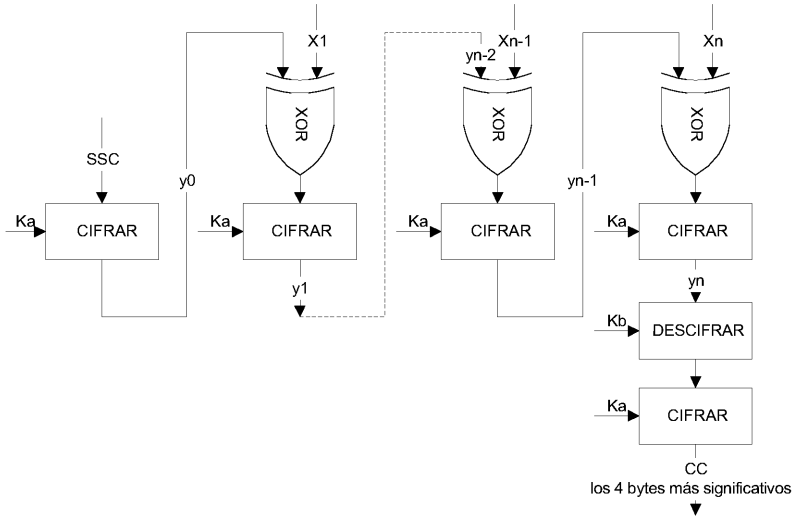
Se transfieren los cuatro bytes más significativos de la suma de control criptográfica.

CSM_029 El contador de la secuencia de envío (SSC) deberá iniciarse durante el procedimiento de acuerdo de la clave:

SSC inicial: Rnd3 (los 4 bytes menos significativos) || Rnd1 (los 4 bytes menos significativos).

CSM_030 El contador de la secuencia de envío deberá incrementarse en una unidad cada vez antes de que se calcule el MAC (es decir, el SSC para el primer comando es el SSC inicial + 1, el SSC para la primera respuesta es el SSC inicial - 2).

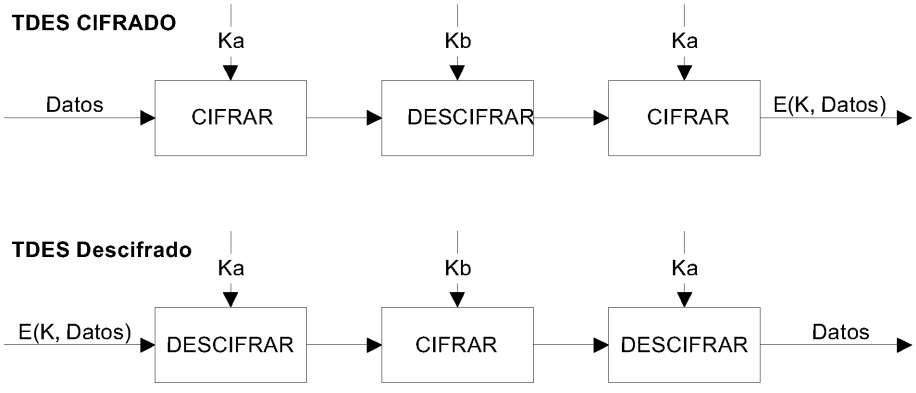
El gráfico siguiente muestra el método de cálculo del MAC:



5.4. **Algoritmo para calcular criptogramas con los que mantener la confidencialidad de los DOs**

CSM_031 Los criptogramas se calculan utilizando el algoritmo TDEA en el modo de funcionamiento TCBC, de acuerdo con los documentos de referencia TDES y TDES-OP y con el vector nulo como bloque de valor inicial.

El gráfico siguiente muestra la aplicación de claves en TDES:



6. MECANISMOS DE FIRMA DIGITAL PARA LA TRANSFERENCIA DE DATOS

CSM_032 El equipo dedicado inteligente (IDE) almacena en un archivo físico los datos recibidos de un equipo (VU o tarjeta) durante una sesión de transferencia. Dicho archivo debe contener los certificados MS_i.C y EQT.C. El archivo contiene además firmas digitales de bloques de datos, tal y como se especifica en el apéndice 7, apartado Protocolos de transferencia de datos.

CSM_033 Las firmas digitales de los datos transferidos deberán utilizar un esquema de firma digital con apéndice, de manera que los datos transferidos puedan leerse sin necesidad de descifrarlos, si se desea.

6.1. **Generación de firmas**

CSM_034 La generación de firmas de datos por parte del equipo deberá seguir el esquema de firma con apéndice que se define en el documento de referencia PKCS1 con la función de comprobación aleatoria SHA-1:

Firma = EQT.SK['00' || '01' || *PS* || '00' || DER(SHA-1(datos))]

PSCadena de octetos de relleno con un valor 'FF' tal que la longitud sea 128.

DER(SHA-1(M)) es la codificación de la identificación del algoritmo para la función de comprobación aleatoria y el valor de comprobación aleatoria, con el fin de obtener un valor ASN.1 del tipo *DigestInfo* (reglas de codificación distinguidas):

'30'||'21'||'30'||'09'||'06'||'05'||'2B'||'0E'||'03'||'02'||'1A'||'05'||'00'||'04'||'14'||Valor de comprobación aleatoria.

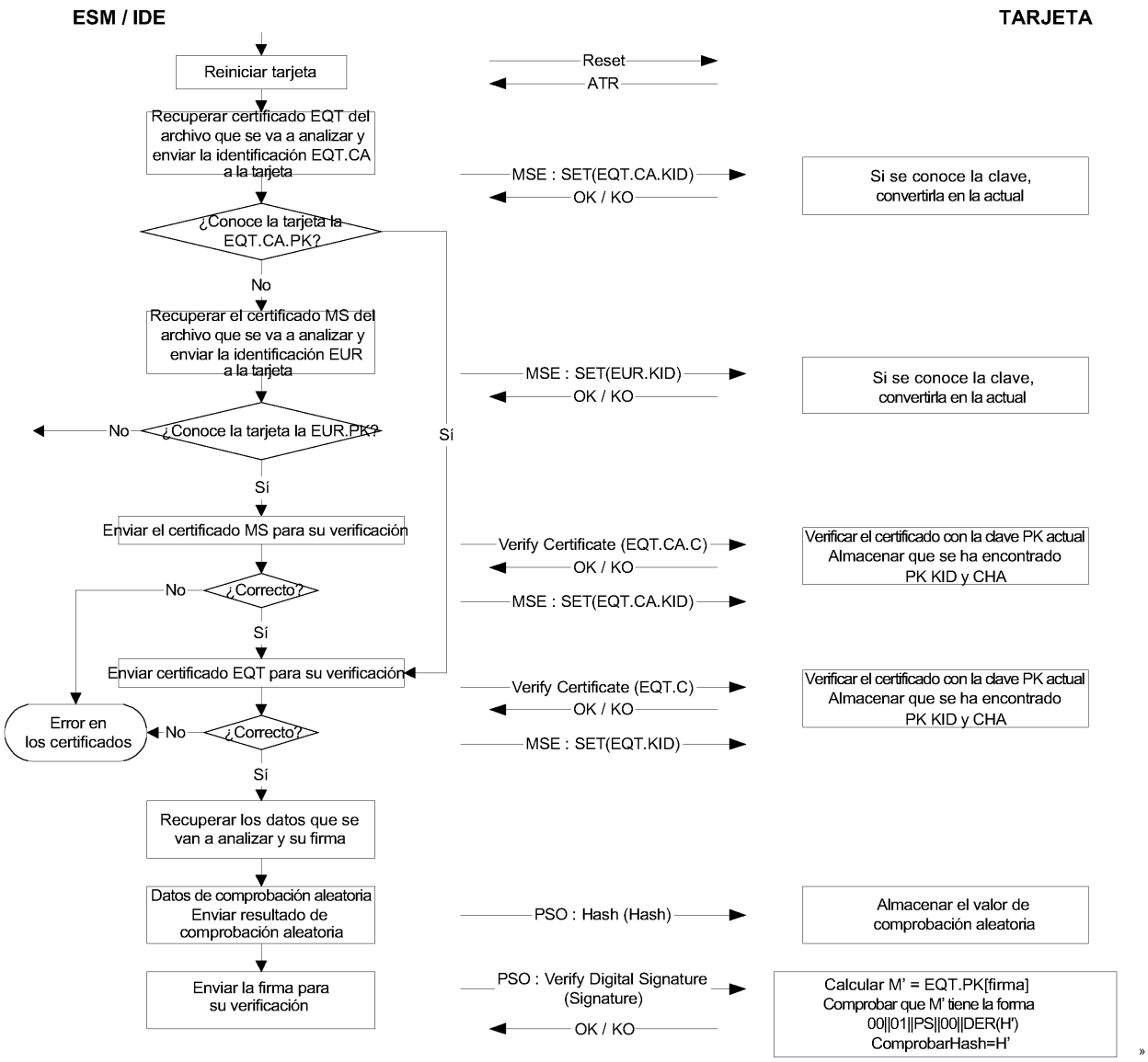
6.2. **Verificación de firmas**

CSM_035 La verificación de la firma en los datos transferidos se ajustará al esquema de firma con apéndice que se define en el documento de referencia PKCS1 con la función de comprobación aleatoria SHA-1.

El responsable de verificación debe conocer independientemente (y confiar en) la clave pública europea EUR.PK.

La tabla siguiente muestra el protocolo que una IDE que incorpore una tarjeta de control puede seguir para verificar la integridad de los datos transferidos y almacenados en el ESM (medio de almacenamiento externo). La tarjeta de control sirve para descifrar las firmas digitales. En este caso, puede que esta función no esté implementada en la IDE.

Las siglas EQT se refieren al equipo que ha transferido y firmado los datos que han de analizarse.


ESM / IDE
TARJETA
Reiniciar tarjeta
Reset
ATR
Recuperar certificado EQT del archivo que se va a analizar y enviar la identificación EQT.CA a la tarjeta
MSE : SET(EQT.CA.KID)
OK / KO
Si se conoce la clave, convertirla en la actual
¿Conoce la tarjeta la EQT.CA.PK?
No
Sí
Recuperar el certificado MS del archivo que se va a analizar y enviar la identificación EUR a la tarjeta
MSE : SET(EUR.KID)
OK / KO
Si se conoce la clave, convertirla en la actual
No
¿Conoce la tarjeta la EUR.PK?
Sí
Enviar el certificado MS para su verificación
Verify Certificate (EQT.CA.C)
OK / KO
Verificar el certificado con la clave PK actual
Almacenar que se ha encontrado PK KID y CHA
No
¿Correcto?
MSE : SET(EQT.CA.KID)
Sí
Enviar certificado EQT para su verificación
Verify Certificate (EQT.C)
OK / KO
Verificar el certificado con la clave PK actual
Almacenar que se ha encontrado PK KID y CHA
Error en los certificados
No
¿Correcto?
MSE : SET(EQT.KID)
Sí
Recuperar los datos que se van a analizar y su firma
Datos de comprobación aleatoria
Enviar resultado de comprobación aleatoria
PSO : Hash (Hash)
Almacenar el valor de comprobación aleatoria
Enviar la firma para su verificación
PSO : Verify Digital Signature (Signature)
OK / KO
Calcular M' = EQT.PK[firma]
Comprobar que M' tiene la forma 00||01||PS||00||DER(H')
ComprobarHash=H'

»