II

(Actos no legislativos)

REGLAMENTOS

REGLAMENTO DE EJECUCIÓN (UE) 2018/502 DE LA COMISIÓN

de 28 de febrero de 2018

por el que se modifica el Reglamento de Ejecución (UE) 2016/799 que establece los requisitos para la construcción, ensayo, instalación, funcionamiento y reparación de los tacógrafos y de sus componentes

(Texto pertinente a efectos del EEE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) n.º 165/2014 del Parlamento Europeo y del Consejo, de 4 de febrero de 2014, relativo a los tacógrafos en el transporte por carretera ([1]), y en particular su artículo 11 y su artículo 12, apartado 7,

Considerando lo siguiente:

(1) El Reglamento (UE) n.º 165/2014 introdujo los tacógrafos inteligentes —tacógrafos digitales de segunda generación—, que incluyen una conexión con el dispositivo GNSS (sistema mundial de radionavegación por satélite), un dispositivo de comunicación a efectos de teledetección temprana y una interfaz opcional con sistemas de transporte inteligentes.

(2) Los requisitos técnicos para la construcción, ensayo, instalación, funcionamiento y reparación de los tacógrafos y de sus componentes se establecen en el Reglamento de Ejecución (UE) 2016/799 de la Comisión ([2]).

(3) De conformidad con los artículos 8, 9 y 10 del Reglamento (UE) n.º 165/2014, a partir del 15 de junio de 2019 los tacógrafos instalados en vehículos matriculados por primera vez deben ser tacógrafos inteligentes. Debe, por tanto, modificarse el Reglamento de Ejecución (UE) 2016/799 de modo que las provisiones técnicas establecidas en él se apliquen a partir de esa fecha.

(4) A fin de cumplir lo dispuesto en el artículo 8 del Reglamento (UE) n.º 165/2014, que establece que la posición del vehículo debe registrarse cada tres horas de tiempo de conducción acumulado, el Reglamento de Ejecución (UE) 2016/799 debe modificarse de modo que posibilite que la información sobre la posición del vehículo se almacene con una frecuencia de tres horas, utilizando un sistema de medición que no pueda reinicializarse, y que se evite así una confusión con la noción de «tiempo de conducción continua», que es un parámetro con una función diferente.

(5) La unidad instalada en el vehículo puede consistir en una sola unidad o en varias unidades repartidas por el vehículo. Los dispositivos GNSS y DSRC (comunicaciones especializadas de corto alcance) pueden, por tanto, ser tanto internos como externos con respecto al cuerpo principal de la unidad instalada en el vehículo. Si son externos, debe ser posible que ambos dispositivos y el cuerpo principal de la unidad instalada en el vehículo sean homologados como componentes, con el fin de adaptar el proceso de homologación de los tacógrafos inteligentes a las necesidades del mercado.

(6) Las normas sobre el almacenamiento de incidentes de conflicto temporal y ajustes de la hora deben modificarse, a fin de distinguir entre los ajustes de hora automáticos, que se producen a raíz de un posible intento de manipulación o de un fallo en el funcionamiento del tacógrafo, y los ajustes debidos a otras razones, como su mantenimiento.

(7) Los identificadores de datos deben poder distinguir entre los datos transferidos desde un tacógrafo inteligente y los transferidos desde un tacógrafo de una generación anterior.

([1]) DO L 60 de 28.2.2014, p. 1.

([2]) Reglamento de Ejecución (UE) 2016/799 de la Comisión, de 18 de marzo de 2016, por el que se ejecuta el Reglamento (UE) n.º 165/2014 del Parlamento Europeo y del Consejo, que establece los requisitos para la construcción, ensayo, instalación, funcionamiento y reparación de los tacógrafos y de sus componentes (DO L 139 de 26.5.2016, p. 1).

(8) El período de validez de la tarjeta de empresa debe ampliarse de dos a cinco años, para igualarlo con el período de validez de la tarjeta de conductor.

(9) Debe definirse mejor la descripción de determinados fallos e incidentes, la validación de la introducción de los lugares donde comienzan o terminan los períodos de trabajo diarios y la utilización del consentimiento del conductor en la interfaz con sistemas de transporte inteligentes (ITS), por lo que respecta a los datos transmitidos por la unidad instalada en el vehículo a través de la red del vehículo, así como otros aspectos técnicos.

(10) Para garantizar que la certificación de los precintos del tacógrafo esté actualizada, estos han de adaptarse a la nueva norma sobre la seguridad de los precintos mecánicos utilizados en los tacógrafos.

(11) El presente Reglamento afecta a la construcción, ensayo, instalación y funcionamiento de sistemas que constan también de equipos radioeléctricos, regulados por la Directiva 2014/53/UE del Parlamento Europeo y del Consejo ([1]). Dicha Directiva regula la comercialización y puesta en servicio de equipos eléctricos y electrónicos que utilizan ondas radioeléctricas a fines de radiocomunicación o radiodeterminación a nivel horizontal, por lo que se refiere, en particular, a la seguridad eléctrica, la compatibilidad con otros sistemas, el acceso al espectro radioeléctrico, el acceso a servicios de emergencia o cualquier otra disposición delegada. A fin de garantizar el uso eficiente del espectro radioeléctrico, evitar interferencias radioeléctricas perjudiciales, garantizar la seguridad y la compatibilidad electromagnética de los equipos radioeléctricos y respetar cualquier otro requisito delegado, el presente Reglamento se entenderá sin perjuicio de las disposiciones de esa Directiva.

(12) Procede, por tanto, modificar el Reglamento de Ejecución (UE) 2016/799 en consecuencia.

(13) Las medidas previstas en el presente Reglamento se ajustan al dictamen del Comité a que se refiere el artículo 42, apartado 3, del Reglamento (UE) n.º 165/2014.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

El Reglamento de Ejecución (UE) 2016/799 queda modificado como se indica a continuación:

1) El artículo 1 se modifica como sigue:

a) los apartados 2 y 3 se sustituyen por el texto siguiente:

«2. La construcción, ensayo, instalación, inspección, funcionamiento y reparación de los tacógrafos inteligentes y sus componentes deberán cumplir los requisitos técnicos establecidos en el anexo IC del presente Reglamento.

3. Los tacógrafos distintos de los tacógrafos inteligentes seguirán teniendo que cumplir, en lo que se refiere a las condiciones de construcción, ensayo, instalación, inspección, funcionamiento y reparación, los requisitos establecidos en el anexo I del Reglamento (UE) n.º 165/2014 o en el anexo IB del Reglamento (CEE) n.º 3821/85 del Consejo (*), según proceda.

(*) Reglamento (CEE) n.º 3821/85 del Consejo, de 20 de diciembre de 1985, relativo al aparato de control en el sector de los transportes por carretera (DO L 370 de 31.12.1985, p. 8).»;

b) se añade el apartado 5 siguiente:

«5. El presente Reglamento se entenderá sin perjuicio de la Directiva 2014/53/UE del Parlamento Europeo y del Consejo (*).

(*) Directiva 2014/53/UE del Parlamento Europeo y del Consejo, de 16 de abril de 2014, relativa a la armonización de las legislaciones de los Estados miembros sobre la comercialización de equipos radioeléctricos, y por la que se deroga la Directiva 1999/5/CE (DO L 153 de 22.5.2014, p. 62).».

2) El artículo 2 se modifica como sigue:

a) la definición 3 se sustituye por el texto siguiente:

«3) "expediente del fabricante": la documentación completa, en formato electrónico o en papel, que contiene toda la información facilitada por el fabricante o su agente a la autoridad de homologación a efectos de la homologación de un tacógrafo o de uno de sus componentes, incluidos los certificados a que se refiere el artículo 12, apartado 3, del Reglamento (UE) n.º 165/2014, los resultados de los ensayos definidos en el anexo IC del presente Reglamento, así como dibujos, fotografías y demás documentos pertinentes;»;

([1]) Directiva 2014/53/UE del Parlamento Europeo y del Consejo, de 16 de abril de 2014, relativa a la armonización de las legislaciones de los Estados miembros sobre la comercialización de equipos radioeléctricos, y por la que se deroga la Directiva 1999/5/CE (DO L 153 de 22.5.2014, p. 62).

b) la definición 7 se sustituye por el texto siguiente:

«7) "tacógrafo inteligente" o "tacógrafo de segunda generación": un tacógrafo digital que cumple lo dispuesto en los artículos 8, 9 y 10 del Reglamento (UE) n.º 165/2014, así como en el anexo IC del presente Reglamento;»;

c) la definición 8 se sustituye por el texto siguiente:

«8) "componente del tacógrafo": cualquiera de los elementos siguientes: la unidad instalada en el vehículo, el sensor de movimiento, la tarjeta de tacógrafo, la hoja de registro, el dispositivo GNSS externo y el dispositivo externo de teledetección temprana;»;

d) se añade la definición 10 siguiente:

«10) "unidad instalada en el vehículo": el tacógrafo, excepto el sensor de movimiento y los cables que conectan dicho sensor.

Puede consistir en una sola unidad o en varias unidades repartidas por el vehículo, e incluye una unidad de procesamiento, una memoria de datos, una función de medición de la hora, dos dispositivos de interfaz de tarjeta inteligente para el conductor y el segundo conductor, una impresora, una pantalla, conectores y dispositivos para que el usuario introduzca datos, un receptor GNSS y un dispositivo de comunicación a distancia.

La unidad instalada en el vehículo puede estar compuesta de los siguientes componentes sujetos a homologación:

— la unidad instalada en el vehículo, como componente único (con un receptor GNSS y un dispositivo de comunicación a distancia incluidos),

— el cuerpo principal de la unidad instalada en el vehículo (con un dispositivo de comunicación a distancia incluido) y un dispositivo GNSS externo,

— el cuerpo principal de la unidad instalada en el vehículo (con un receptor GNSS incluido) y un dispositivo de comunicación a distancia externo,

— el cuerpo principal de la unidad instalada en el vehículo, un dispositivo GNSS externo y un dispositivo de comunicación a distancia externo.

Si la unidad instalada en el vehículo se compone de varias unidades repartidas por el vehículo, el cuerpo principal es la unidad que contenga la unidad de procesamiento, la memoria de datos y la función de medición de la hora.

"unidad instalada en el vehículo (VU)" se utiliza tanto para "unidad instalada en el vehículo" como para "cuerpo principal de la unidad instalada en el vehículo".».

3) En el artículo 6, el párrafo tercero se sustituye por el texto siguiente:

«Sin embargo, el anexo IC será aplicable a partir del 15 de junio de 2019, a excepción del apéndice 16, que será aplicable a partir del 2 de marzo de 2016.».

4) El anexo IC se modifica de conformidad con el anexo I del presente Reglamento.

5) El anexo II se modifica de conformidad con el anexo II del presente Reglamento.

Artículo 2

Entrada en vigor

El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

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

Hecho en Bruselas, el 28 de febrero de 2018.

Por la Comisión

El Presidente

Jean-Claude JUNCKER

ANEXO I

El anexo IC del Reglamento (UE) 2016/799 se modifica como sigue:

1) El índice queda modificado como sigue:

a) el apartado 3.12.5 se sustituye por el texto siguiente:

«3.12.5 Lugares y posiciones donde comienzan o terminan los períodos de trabajo diarios y/o donde se alcanzan las tres horas de tiempo de conducción acumulado»;

b) el apartado 4.5.3.2.16 se sustituye por el texto siguiente:

«4.5.3.2.16 Datos sobre lugares en tres horas de conducción acumuladas»;

c) el apartado 4.5.4.2.14 se sustituye por el texto siguiente:

«4.5.4.2.14 Datos sobre lugares en tres horas de conducción acumuladas»;

d) el apartado 6.2 se sustituye por el texto siguiente:

«6.2 Verificación de componentes nuevos o reparados».

2) El apartado 1 se modifica como sigue:

a) la definición ll) se sustituye por el texto siguiente:

«ll) Dispositivo de comunicación a distancia o dispositivo de teledetección temprana:

Equipo de la unidad instalada en el vehículo que se utiliza para realizar controles de carretera selectivos.»;

b) la definición tt) se sustituye por el texto siguiente:

«tt) ajuste de la hora:

Ajuste de la hora actual; este ajuste puede realizarse de manera automática a intervalos regulares, utilizando como referencia la hora que proporciona el receptor GNSS, o efectuarse durante el calibrado.»;

c) el primer guion de la definición yy) se sustituye por el texto siguiente:

«— se instala y utiliza exclusivamente en vehículos de las categorías M1 y N1 (según se definen en el anexo II de la Directiva 2007/46/CE del Parlamento Europeo y del Consejo (*), en su versión modificada más reciente);»;

d) se añade una nueva definición fff):

«fff) tiempo de conducción acumulado:

Valor que representa el número total de minutos de conducción acumulados de un vehículo determinado.

El valor del tiempo de conducción acumulado es un recuento sin sincronizar de todos los minutos considerados como actividad de CONDUCCIÓN por la función de supervisión de las actividades de conducción del aparato de control, y solo se utiliza para poner en marcha el registro de la posición del vehículo, cada vez que se alcanza un múltiplo de tres horas de conducción acumuladas. La acumulación se inicia cuando se activa el aparato de control. No se ve afectada por ninguna otra condición, como "Fuera de ámbito" o "Trayecto en transbordador/tren".

El tiempo de conducción acumulado es un valor que no está destinado a mostrarse en pantalla, imprimirse ni transferirse.».

3) En el apartado 2.3, el último guion del punto 13 se sustituye por el texto siguiente:

«— el período de validez operativa normal de las unidades instaladas en vehículos es de quince años a partir de la fecha efectiva de los certificados de dichas unidades, pero podrán utilizarse durante tres meses adicionales solo para la transferencia de datos.».

4) En el apartado 2.4, el párrafo primero se sustituye por el texto siguiente:

«La seguridad del sistema tiene por objeto proteger la memoria de datos, de manera que se evite el acceso a la misma de 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 instalada en el vehículo, de los datos intercambiados entre el aparato de control y las tarjetas de tacógrafo y de los datos intercambiados entre la unidad instalada en el vehículo y el dispositivo GNSS externo, de existir este, se protege la confidencialidad, integridad y autenticidad de los datos intercambiados a través de la comunicación de teledetección temprana con fines de control y se verifica la integridad y autenticidad de los datos transferidos.».

5) En el apartado 3.2, el segundo guion del punto 27 se sustituye por el texto siguiente:

«— las posiciones en que el tiempo de conducción acumulado llega a un múltiplo de tres horas;».

6) En el apartado 3.4, el punto 49 se sustituye por el texto siguiente:

«49) Si el primer cambio de actividad a PAUSA/DESCANSO o DISPONIBILIDAD tiene lugar antes de que hayan transcurrido 120 segundos tras 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).».

7) En el apartado 3.6.1, el punto 59 se sustituye por el texto siguiente:

«59) El conductor deberá introducir entonces el lugar en que se encuentra actualmente el vehículo, que se considerará una entrada temporal.

Si se cumplen las siguientes condiciones, se valida la entrada temporal efectuada en la última extracción de la tarjeta (es decir, ya no se sobrescribirá):

— introducción de un lugar donde comienza el período de trabajo diario actual durante la introducción manual de conformidad con el requisito 61;

— la siguiente introducción de un lugar donde comienza el período de trabajo diario actual, si el titular de la tarjeta no introduce el lugar donde comienza o finalizó el período de trabajo durante la introducción manual de conformidad con el requisito 61.

Si se cumplen las siguientes condiciones, se sobrescribe la entrada temporal efectuada en la última extracción de la tarjeta y se valida el nuevo valor:

— la siguiente introducción de un lugar donde finaliza el período de trabajo diario actual, si el titular de la tarjeta no introduce el lugar donde comienza o finalizó el período de trabajo durante la introducción manual de conformidad con el requisito 61.».

8) En el apartado 3.6.2, los guiones sexto y séptimo se sustituyen por el texto siguiente:

«— un lugar en que haya terminado un período de trabajo diario precedente, asociado a la hora pertinente (sobrescribiendo y validando así la entrada realizada con motivo de la última extracción de la tarjeta), o

— un lugar en que comienza el período de trabajo diario actual, asociado a la hora pertinente (validando así una entrada temporal realizada con motivo de la última extracción de la tarjeta).».

9) El apartado 3.9.15 se sustituye por el texto siguiente:

«3.9.15 Incidente "Conflicto temporal"

86) Este incidente se produce cuando, **fuera del modo de calibrado**, la VU detecta una discrepancia de más de un minuto entre la hora de la función de medición de la hora de la unidad instalada en el vehículo y la hora procedente del receptor GNSS. Este incidente se registra junto con el valor del reloj interno de la unidad instalada en el vehículo y va acompañado de un ajuste de la hora automático. Después de haberse producido un incidente de conflicto temporal, la VU no generará más incidentes del mismo tipo durante las doce horas siguientes. Este incidente no se producirá cuando no hubiera una señal GNSS válida detectable por el receptor GNSS en los últimos treinta días o más.».

10) En el apartado 3.9.17 se añade el siguiente guion:

«— fallo de la interfaz ITS (si procede).».

11) El apartado 3.10 se modifica como sigue:

i) el texto que precede al cuadro del punto 89 se sustituye por el siguiente:

(no afecta a la versión española)

ii) en el cuadro, se añade la fila siguiente:

«Interfaz ITS (opcional)	Funcionamiento correcto»	

12) En el apartado 3.12, el segundo guion se sustituye por el texto siguiente:

«— El número medio de posiciones por día se define como al menos 6 posiciones en las que comienza el período de trabajo diario, 6 posiciones en las que el tiempo de conducción acumulado del conductor llega a un múltiplo de tres horas, y 6 posiciones en las que termina el período de trabajo diario, por lo que "365 días" incluyen al menos 6570 posiciones.».

13) El apartado 3.12.5 se modifica como sigue:

a) el título y el apartado 108 se sustituyen por el texto siguiente:

«3.12.5 Lugares y posiciones donde comienzan o terminan los períodos de trabajo diarios y/o donde se alcanzan las tres horas de tiempo de conducción acumulado

108) El aparato de control deberá registrar y almacenar en su memoria de datos:

— los lugares y las posiciones en que el conductor y/o el segundo conductor comienzan su período de trabajo diario;

— las posiciones en que el tiempo de conducción acumulado llega a un múltiplo de tres horas;

— los lugares y las posiciones en que el conductor y/o el segundo conductor finalizan su período de trabajo diario.»;

b) el cuarto guion del punto 110 se sustituye por el texto siguiente:

«— el tipo de entrada (comienzo, final o tres horas de tiempo de conducción acumulado),»;

c) el punto 111 se sustituye por el texto siguiente:

«111) La memoria de datos deberá ser capaz de mantener almacenados durante al menos 365 días los lugares y posiciones en que comienzan o finalizan los períodos de trabajo diarios y/o se alcanzan las tres horas de tiempo de conducción acumulado.».

14) En el apartado 3.12.7, el punto 116 se sustituye por el texto siguiente:

(no afecta a la versión española)

15) En el apartado 3.12.8, el cuadro queda modificado como sigue:

a) se inserta el siguiente elemento entre los elementos «Ausencia de información sobre la posición procedente del receptor GNSS» y «Error en datos de movimiento»:

«Error de comunicación con el dispositivo GNSS externo	— el incidente de mayor duración ocurrido cada uno de los últimos diez días, — los cinco incidentes de mayor duración ocurridos en los últimos 365 días.	— fecha y hora de comienzo del incidente, — fecha y hora de finalización del incidente, — tipo de tarjeta(s), número, Estado miembro emisor y generación de cualquier tarjeta insertada al comenzar o al terminar el incidente, — número de incidentes similares ocurridos ese día.»

b) el elemento «Conflicto temporal» se sustituye por el texto siguiente:

«Conflicto temporal	— el incidente más grave ocurrido cada uno de los últimos diez días (es decir, los que presentan mayor diferencia entre la fecha y hora del aparato de control y la fecha y hora del GNSS), — los cinco incidentes más graves ocurridos en los últimos 365 días,	— fecha y hora del aparato de control, — fecha y hora del GNSS, — tipo de tarjeta(s), número, Estado miembro emisor y generación de cualquier tarjeta insertada al comenzar o al terminar el incidente, — número de incidentes similares ocurridos ese día.»

16) En el apartado 3.20, el punto 200 se sustituye por el texto siguiente:

«200) El aparato de control podrá ir también equipado de interfaces normalizadas que permitan que un aparato externo utilice en modo operativo o de calibrado los datos registrados o producidos por el tacógrafo.

En el apéndice 13 se especifica y normaliza una interfaz ITS opcional. Podrán coexistir otras interfaces de la unidad instalada en el vehículo, siempre que se cumplan plenamente los requisitos del apéndice 13 en términos de lista mínima de datos, seguridad y consentimiento del conductor.

El consentimiento del conductor no se aplica a los datos transmitidos por el aparato de control a la red del vehículo. En caso de que los datos personales inyectados en la red del vehículo sean luego procesados fuera de dicha red, es responsabilidad del fabricante del vehículo que el tratamiento de datos personales sea conforme con el Reglamento (UE) 2016/679 (“Reglamento general de protección de datos”).

El consentimiento del conductor tampoco se aplica a los datos del tacógrafo transferidos a una empresa a distancia (requisito 193), dado que este caso está sujeto al derecho de acceso de las tarjetas de empresa.

Se aplicarán los siguientes requisitos a los datos de ITS facilitados a través de esa interfaz:

— estos datos constituirán una selección de los datos existentes a partir del diccionario de datos del tacógrafo (apéndice 1),

— un subconjunto de esta selección de datos se identificará como "datos personales",

— el subconjunto de "datos personales" solo estará disponible si está habilitado el consentimiento verificable del conductor, aceptando que sus datos personales puedan abandonar la red del vehículo,

— en cualquier momento, podrá habilitarse o inhabilitarse el consentimiento del conductor a través de comandos del menú, siempre que esté insertada la tarjeta de conductor,

— la selección y el subconjunto de datos se emitirán a través del protocolo inalámbrico Bluetooth en el radio de la cabina del vehículo, con una frecuencia de refresco de un minuto,

— el emparejamiento del dispositivo exterior con la interfaz ITS estará protegido por un PIN aleatorio y dedicado de al menos cuatro dígitos, registrado y disponible a través de la pantalla de cada unidad instalada en el vehículo,

— en ninguna circunstancia podrá la presencia de la interfaz ITS perturbar ni alterar el correcto funcionamiento y la seguridad de la unidad instalada en el vehículo.

También se podrán enviar otros datos, además de la selección de datos existentes, que se considera la lista mínima, siempre que no se puedan considerar datos personales.

El aparato de control deberá ser capaz de comunicar el estado del consentimiento del conductor a otras plataformas de la red del vehículo.

Cuando el encendido del vehículo esté activado (ON), estos datos se enviarán de manera permanente.».

17) En el apartado 3.23, el punto 211 se sustituye por el texto siguiente:

«211) La hora del reloj interno de la VU se reajustará automáticamente cada doce horas. Cuando este reajuste no sea posible porque no se disponga de señal GNSS, se fijará la hora tan pronto como la VU pueda acceder a una hora válida facilitada por el receptor GNSS, según las condiciones de encendido del vehículo. La referencia temporal para la fijación automática de la hora del reloj interno de la VU se derivará del receptor GNSS.».

18) En el apartado 3.26, los puntos 225 y 226 se sustituyen por el texto siguiente:

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

— nombre y dirección del fabricante,

— número de pieza del fabricante y año de fabricación,

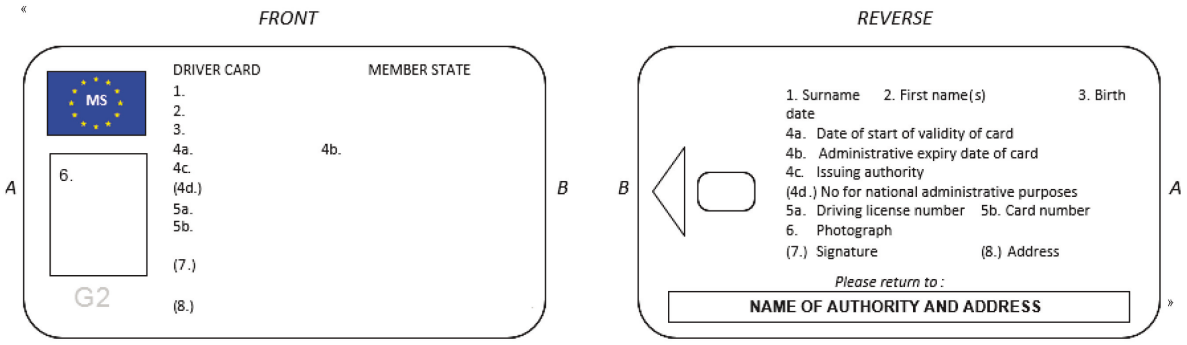
— número de serie,

— marca de homologación.

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

19) En el apartado 4.1, el dibujo correspondiente al anverso y el reverso de la tarjeta de conductor se sustituye por el siguiente:

«



»

20) En el apartado 4.5.3.1.8, el primer guion del punto 263 se sustituye por el texto siguiente:

«— fallo de la tarjeta (cuando esa tarjeta sea el tema del fallo),».

21) En el apartado 4.5.3.2.8, el primer guion del punto 288 se sustituye por el texto siguiente:

«— fallo de la tarjeta (cuando esa tarjeta sea el tema del fallo),».

22) El apartado 4.5.3.2.16 se sustituye por el texto siguiente:

«4.5.3.2.16 Datos sobre lugares en tres horas de conducción acumuladas

305) La tarjeta de conductor deberá ser capaz de almacenar los siguientes datos relativos a la posición del vehículo cuando el tiempo de conducción acumulado alcance un múltiplo de tres horas:

— fecha y hora en las que el tiempo de conducción acumulado llega a un múltiplo de tres horas,

— posición del vehículo,

— la exactitud del GNSS, fecha y hora en que se haya determinado la posición,

— la lectura del cuentakilómetros del vehículo.

306) La tarjeta de conductor deberá ser capaz de almacenar al menos 252 de estos registros.».

23) El apartado 4.5.4.2.14 se sustituye por el texto siguiente:

«4.5.4.2.14 Datos sobre lugares en tres horas de conducción acumuladas

353) La tarjeta de taller deberá ser capaz de almacenar los siguientes datos relativos a la posición del vehículo cuando el tiempo de conducción acumulado alcance un múltiplo de tres horas:

— fecha y hora en las que el tiempo de conducción acumulado llega a un múltiplo de tres horas,

— posición del vehículo,

— la exactitud del GNSS, fecha y hora en que se haya determinado la posición,

— la lectura del cuentakilómetros del vehículo.

354) La tarjeta de taller deberá ser capaz de almacenar al menos dieciocho de estos registros.».

24) En el apartado 5.2, el punto 396 se sustituye por el texto siguiente:

«396) En la placa deberán figurar, como mínimo, los datos siguientes:

— nombre y domicilio o nombre comercial del instalador o taller 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 del informe del coeficiente característico del vehículo y de la medida de la circunferencia efectiva de los neumáticos de las ruedas,

— número de identificación del vehículo (VIN),

— presencia (o no) de un dispositivo GNSS externo,

— número de serie del dispositivo GNSS externo, en su caso,

— número de serie del dispositivo de comunicación a distancia, de existir este,

— número de serie de todos los precintos existentes,

— parte del vehículo en la que, en su caso, está instalado el adaptador,

— parte del vehículo en la que está instalado el sensor de movimiento, si no está conectado a la caja de cambios o si no se utiliza un adaptador,

— descripción del color del cable entre el adaptador y la parte del vehículo que proporciona sus impulsos de entrada,

— número de serie del sensor de movimiento integrado del adaptador.».

25) El apartado 5.3 se modifica como sigue:

a) se inserta un nuevo punto 398 *bis* tras el punto 398:

«398 *bis*) Los precintos antes mencionados deberán certificarse de conformidad con la norma EN 16882:2016.»;

b) en el punto 401, el párrafo segundo se sustituye por el texto siguiente:

«Este número de identificación único se define del siguiente modo: MMNNNNNNNN mediante marcado que no se pueda retirar, siendo MM un identificador único del fabricante (registro en base de datos gestionada por la CE) y NNNNNNNN un identificador alfanumérico del precinto, único en el dominio del fabricante.»;

c) el punto 403 se sustituye por el texto siguiente:

«403) Los fabricantes de los precintos quedarán registrados en una base de datos específica cuando obtengan un modelo de precinto certificado de conformidad con la norma EN 16882:2016 y harán públicos sus identificadores de precintos a través de un procedimiento que establecerá la Comisión Europea.»;

d) el punto 404 se sustituye por el texto siguiente:

«404) Los talleres autorizados y los fabricantes de vehículos utilizarán únicamente, en el marco del Reglamento (UE) n.º 165/2014, precintos certificados de conformidad con la norma EN 16882:2016 procedentes de los fabricantes de precintos recogidos en la base de datos mencionada anteriormente.».

26) El apartado 6.2 se sustituye por el texto siguiente:

«6.2 Verificación de componentes nuevos o reparados

407) 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 apartados 3.2.1, 3.2.2, 3.2.3 y 3.3.».

27) En el apartado 6.3, el punto 408 se sustituye por el texto siguiente:

«408) En el momento de su instalación en un vehículo, la instalación en su conjunto (incluido el aparato de control) deberá ajustarse a las disposiciones sobre tolerancias máximas establecidas en los capítulos 3.2.1, 3.2.2, 3.2.3 y 3.3. El conjunto de la instalación deberá precintarse de conformidad con el capítulo 5.3 e incluirá un calibrado.».

28) El apartado 8.1 queda modificado como sigue:

a) el texto anterior al punto 425 se sustituye por el texto siguiente:

«A efectos del presente capítulo, por "aparato de control" se entenderá el "aparato de control o sus componentes". No será preciso homologar el cable o cables que conectan el sensor de movimiento a la VU, el dispositivo GNSS externo a la VU o el dispositivo de comunicación a distancia externo a la VU. El papel que utilice el aparato de control se considerará un componente de dicho aparato.

Todo fabricante podrá solicitar la homologación de los componentes de su aparato de control con cualquier otro tipo de componentes de aparato de control, siempre que cada componente cumpla los requisitos del presente anexo. De manera alternativa, los fabricantes podrán también solicitar la homologación del aparato de control.

Tal como se describe en la definición 10 del artículo 2 del presente Reglamento, existen diferentes variedades de unidades de vehículo según el montaje de sus componentes. Sea cual sea el montaje de los componentes de la unidad instalada en el vehículo, la antena exterior y, en su caso, el separador de antena conectado al receptor GNSS o al dispositivo de comunicación a distancia no forman parte de la homologación de la unidad instalada en el vehículo.

No obstante, los fabricantes que hayan obtenido la homologación del aparato de control mantendrán una lista pública de las antenas y los separadores compatibles con cada unidad instalada en el vehículo, dispositivo GNSS externo y dispositivo de comunicación a distancia externo homologados.»;

b) el punto 427 se sustituye por el texto siguiente:

«427) Las autoridades de homologación de los Estados miembros no concederán el certificado de homologación mientras no estén en posesión de:

— un certificado de seguridad (si se solicita en el presente anexo),

— un certificado funcional, y

— un certificado de interoperabilidad (si se solicita en el presente anexo)

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

29) El apéndice 1 se modifica como sigue:

a) el índice queda modificado como sigue:

i) el apartado 2.63 se sustituye por el texto siguiente:

«2.63. Reservado para usos futuros»;

ii) el apartado 2.78 se sustituye por el texto siguiente:

«2.78. GNSSAccumulatedDriving»;

iii) el apartado 2.79 se sustituye por el texto siguiente:

«2.79. GNSSAccumulatedDrivingRecord»;

iv) el apartado 2.111 se sustituye por el texto siguiente:

«2.111. NoOfGNSSADRecords»;

v) el apartado 2.160 se sustituye por el texto siguiente:

«2.160. Reservado para usos futuros»;

vi) el apartado 2.203 se sustituye por el texto siguiente:

«2.203. VuGNSSADRecord»;

vii) el apartado 2.204 se sustituye por el texto siguiente:

«2.204. VuGNSSADRecordArray»;

viii) el apartado 2.230 se sustituye por el texto siguiente:

«2.230. Reservado para usos futuros»;

ix) el apartado 2.231 se sustituye por el texto siguiente:

«2.231. Reservado para usos futuros»;

b) en el apartado 2 se añadirá el texto siguiente antes del apartado 2.1:

«En el caso de los tipos de datos de la tarjeta utilizados para las aplicaciones de la generación 1 y la generación 2, el tamaño especificado en el presente apéndice es el correspondiente a la aplicación de generación 2. Se da por supuesto que el lector conoce el tamaño de la aplicación de generación 1. Los números de requisito del anexo IC correspondientes a estos tipos de datos incluyen tanto las aplicaciones de generación 1 como las de generación 2.»;

c) el apartado 2.19 se sustituye por el texto siguiente:

«2.19. **CardEventData**

Generación 1:

Información almacenada en una tarjeta de conductor o de taller relativa a los incidentes asociados al titular de la tarjeta (anexo IC, requisitos 260 y 318).

```
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).

Generación 2:

Información almacenada en una tarjeta de conductor o de taller relativa a los incidentes asociados al titular de la tarjeta (anexo IC, requisitos 285 y 341).

```
CardEventData ::= SEQUENCE SIZE(11) 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).»;

d) el apartado 2.30 se sustituye por el texto siguiente:

«2.30. **CardRenewalIndex**

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

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

Asignación de valor: (véase el capítulo 7 del presente anexo).

"0" Primera expedición.

Orden de incremento: "0, …, 9, A, …, Z"»;

e) en el apartado 2.61, el texto que aparece después del encabezamiento «Generación 2» se sustituye por el texto siguiente:

```
«DriverCardApplicationIdentification ::= SEQUENCE {
typeOfTachographCardId          EquipmentType,
cardStructureVersion            CardStructureVersion,
noOfEventsPerType               NoOfEventsPerType,
noOfFaultsPerType               NoOfFaultsPerType,
activityStructureLength         CardActivityLengthRange,
noOfCardVehicleRecords          NoOfCardVehicleRecords,
noOfCardPlaceRecords            NoOfCardPlaceRecords,
noOfGNSSADRecords               NoOfGNSSADRecords,
noOfSpecificConditionRecords    NoOfSpecificConditionRecords
noOfCardVehicleUnitRecords      NoOfCardVehicleUnitRecords
}
```

Además de los de la generación 1, se utilizan los siguientes elementos de datos:

noOfGNSSCDRecords es el número de registros GNSS de conducción acumulada que puede almacenar la tarjeta.

noOfSpecificConditionRecords es el número de registros de condiciones específicas que puede almacenar la tarjeta.

noOfCardVehicleUnitRecords es el número de registros sobre unidades instaladas en vehículos que puede almacenar la tarjeta.»;

f) el apartado 2.63 se sustituye por el texto siguiente:

«2.63. **Reservado para usos futuros**»;

g) en el apartado 2.67, el texto que aparece después del encabezamiento «Generación 2» se sustituye por el texto siguiente:

«se utilizan los mismos valores que en la generación 1, con los siguientes añadidos:

```
--GNSS Facility                 (8),
--Remote Communication Module   (9),
--ITS interface module          (10),
--Plaque                        (11),--may be used in SealRecord
--M1/N1 Adapter                 (12),--may be used in SealRecord
--European Root CA (ERCA)       (13),
--Member State CA (MSCA)        (14),
--External GNSS connection      (15),--may be used in SealRecord
--Unused                        (16),--used in SealDataVu
--Driver Card (Sign)            (17),--only to be used in the CHA
                                field of a signing certificate
--Workshop Card (Sign)          (18), --only to be used in the CHA
                                field of a signing certificate
--Vehicle Unit (Sign)           (19), --only to be used in the CHA
                                field of a signing certificate
--RFU                           (20..255)
```

Nota 1: Pueden utilizarse en SealRecord, si procede, los valores de generación 2 de la placa, el adaptador y la conexión del GNSS externo, así como los valores de generación 1 de la unidad instalada en el vehículo y el sensor de movimiento.

Nota 2: En el campo CardHolderAuthorisation (CHA) de un certificado de generación 2, los valores 1, 2 y 6 deben interpretarse en el sentido de que indican un certificado para la autenticación mutua del tipo de equipo respectivo. Para indicar el certificado respectivo para crear una firma digital, deben utilizarse los valores 17, 18 o 19.»;

h) en el apartado 2.70, el texto que aparece después del encabezamiento «Generación 2» se sustituye por el texto siguiente:

«Generación 2:

'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	Conflicto de movimiento del vehículo,
'0B'H	Conflicto temporal (entre el GNSS y el reloj interno de la VU),
'0C'H	Error de comunicación con el dispositivo de comunicación a distancia,
'0D'H	Ausencia de información sobre la posición procedente del receptor GNSS,
'0E'H	Error de comunicación con el dispositivo GNSS externo,
'0F'H	RFU,
'1x'H	Intentos de violación de la seguridad relacionados con la VU,
'10'H	No hay más información,
'11'H	Fallo de autenticación del sensor de movimiento,
'12'H	Fallo de autenticación 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	Detección de manipulación de GNSS,
'1A'H	Fallo de autenticación del dispositivo GNSS externo,
'1B'H	Certificado del dispositivo GNSS externo expirado,
'1C'H to '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 autenticación,
'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 to '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	Receptor GNSS interno,
'37'H	Dispositivo GNSS externo,
'38'H	Dispositivo de comunicación a distancia,
'39'H	Interfaz ITS,
'3A'H to '3F'H	RFU,
'4x'H	Fallos de las tarjetas,
'40'H	No hay más información,
'41'H to '4F'H	RFU,
'50'H to '7F'H	RFU,
'80'H to 'FF'H	específicos del fabricante.»;

i) el apartado 2.71 se sustituye por el texto siguiente:

«2.71. **ExtendedSealIdentifier**

Generación 2:

El identificador de precinto ampliado identifica de manera única un precinto (anexo IC, requisito 401).

```
ExtendedSealIdentifier ::= SEQUENCE{
   manufacturerCode                OCTET STRING (SIZE(2)),
   sealIdentifier                  OCTET STRING (SIZE(8))
}
```

manufacturerCode es un código del fabricante del precinto.

sealIdentifier es un identificador del precinto que es exclusivo para el fabricante.»;

j) los apartados 2.78 y 2.79 se sustituyen por el texto siguiente:

«2.78. **GNSSAccumulatedDriving**

Generación 2:

Información almacenada en una tarjeta de conductor o de taller y relativa a la posición GNSS del vehículo si el tiempo de conducción acumulado alcanza un múltiplo de tres horas (anexo IC, requisitos 306 y 354).

```
GNSSAccumulatedDriving := SEQUENCE {
   gnssADPointerNewestRecord       INTEGER(0..NoOfGNSSADRecords -1),
   gnssAccumulatedDrivingRecords   SET SIZE(NoOfGNSSADRecords) OF
                                   GNSSAccumulatedDrivingRecord
}
```

gnssADPointerNewestRecord es el índice del último registro actualizado de conducción acumulado del GNSS.

Asignación de valor es el número correspondiente al numerador del registro de conducción acumulado del GNSS. Al primer registro de la estructura se le asigna el número '0'.

gnssAccumulatedDrivingRecords es el conjunto de registros que contienen la fecha y hora en que la conducción acumulada alcanza un múltiplo de tres horas e información sobre la posición del vehículo.

2.79. **GNSSAccumulatedDrivingRecord**

Generación 2:

Información almacenada en una tarjeta de conductor o de taller y relativa a la posición GNSS del vehículo si el tiempo de conducción acumulado alcanza un múltiplo de tres horas (anexo IC, requisitos 305 y 353).

```
GNSSAccumulatedDrivingRecord ::= SEQUENCE {
  timeStamp                    TimeReal,
  gnssPlaceRecord              GNSSPlaceRecord,
  vehicleOdometerValue         OdometerShort
}
```

timeStamp es la fecha y la hora en las que el tiempo de conducción acumulado llega a un múltiplo de tres horas.

gnssPlaceRecord contiene información relacionada con la posición del vehículo.

vehicleOdometerValue es la lectura del cuentakilómetros en el momento en que el tiempo de conducción acumulado llega a un múltiplo de tres horas.»;

k) el apartado 2.86 se sustituye por el texto siguiente:

«2.86. **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 instalada en el vehículo, de una tarjeta de tacógrafo o de un dispositivo GNSS externo.

La segunda opción sirve para hacer referencia a la clave pública de una VU (en los casos en que el número de serie de dicha VU 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.»;

l) el apartado 2.92 se sustituye por el texto siguiente:

«2.92. **MAC**

Generación 2:

Una suma de control criptográfica de 8, 12 o 16 bytes de longitud correspondiente a los conjuntos de cifrado que se especifican en el apéndice 11.

```
MAC ::= CHOICE {
   Mac8                 OCTET STRING (SIZE(8)),
   Mac12                OCTET STRING (SIZE(12)),
   Mac16                OCTET STRING (SIZE(16)),
}»;
```

m) el apartado 2.111 se sustituye por el texto siguiente:

«2.111. **NoOfGNSSADRecords**

Generación 2:

Número de registros GNSS de conducción acumulada que puede almacenar una tarjeta.

$$\mathrm{NoOfGNSSADRecords ::= INTEGER\ (0..2^{16}-1)}$$

Asignación de valor: véase el apéndice 2.»;

n) en el apartado 2.120, la asignación de valor '16H' se sustituye por lo siguiente:

«'16'H VuGNSSADRecord »;

o) el apartado 2.160 se sustituye por el texto siguiente:

«2.160. **Reservado para usos futuros**»;

p) el apartado 2.162 se sustituye por el texto siguiente:

«2.162. **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, UTC.

```
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, UTC.

La fecha/hora máxima posible es en el año 2106.»;

q) el apartado 2.179 se sustituye por el texto siguiente:

«2.179. **VuCardRecord**

Generación 2:

Información almacenada en una unidad instalada en el vehículo y relativa a una tarjeta de tacógrafo utilizada (anexo IC, requisito 132).

```
VuCardRecord ::= SEQUENCE {
cardNumberAndGenerationInformation      FullCardNumberAndGeneration,
cardExtendedSerialNumber                ExtendedSerialNumber,
cardStructureVersion                    CardStructureVersion,
cardNumber                              CardNumber
}
```

cardNumberAndGenerationInformation es el número de tarjeta completo y la generación de la tarjeta utilizada (tipo de datos 2.74).

cardExtendedSerialNumber según se lee del archivo EF_ICC del MF de la tarjeta.

cardStructureVersion según se lee del archivo EF_Application_Identification del DF_Tachograph_G2.

cardNumber según se lee del archivo EF_Identification del DF_Tachograph_G2.»;

r) los apartados 2.203 y 2.204 se sustituyen por el texto siguiente:

«2.203. **VuGNSSADRecord**

Generación 2:

Información almacenada en una unidad instalada en el vehículo y relativa a la posición GNSS del vehículo si el tiempo de conducción acumulado alcanza un múltiplo de tres horas (anexo IC, requisitos 108 y 110).

```
VuGNSSADRecord ::= SEQUENCE {
   timeStamp                        TimeReal,
   cardNumberAndGenDriverSlot       FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlot     FullCardNumberAndGeneration,
   gnssPlaceRecord                  GNSSPlaceRecord,
   vehicleOdometerValue             OdometerShort
}
```

timeStamp es la fecha y la hora en las que el tiempo de conducción acumulado llega a un múltiplo de tres horas.

cardNumberAndGenDriverSlot identifica la tarjeta, incluida su generación, que está insertada en la ranura del conductor.

cardNumberAndGenCodriverSlot identifica la tarjeta, incluida su generación, que está insertada en la ranura del segundo conductor.

gnssPlaceRecord contiene información relacionada con la posición del vehículo.

vehicleOdometerValue es la lectura del cuentakilómetros en el momento en que el tiempo de conducción acumulado llega a un múltiplo de tres horas.

2.204. **VuGNSSADRecordArray**

Generación 2:

Información almacenada en una unidad instalada en el vehículo y relativa a la posición GNSS del vehículo si el tiempo de conducción acumulado alcanza un múltiplo de tres horas (anexo IC, requisitos 108 y 110).

```
VuGNSSADRecordArray ::= SEQUENCE {
   recordType                    RecordType,
   recordSize                    INTEGER(1..65535),
   noOfRecords                   INTEGER(0..65535),
   records                       SET SIZE(noOfRecords) OF VuGNSSADRecord
}
```

recordType denota el tipo de registro (VuGNSSADRecord).

Asignación de valor: véase RecordType

recordSize es el tamaño de VuGNSSADRecord en bytes.

noOfRecords es el número de registros que hay en el conjunto.

records es un conjunto de registros GNSS sobre conducción acumulada.»;

s) los apartados 2.230 y 2.231 se sustituyen por el texto siguiente:

«2.230. Reservado para usos futuros

2.231. Reservado para usos futuros»;

t) en el apartado 2.234, el texto que aparece después del encabezamiento «Generación 2» se sustituye por el texto siguiente:

```
«WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords,
   noOfCalibrationRecords              NoOfCalibrationRecords,
   noOfGNSSADRecords                   NoOfGNSSADRecords,
   noOfSpecificConditionRecords        NoOfSpecificConditionRecords,
   noOfCardVehicleUnitRecords          NoOfCardVehicleUnitRecords
}
```

Además de los de la generación 1, se utilizan los siguientes elementos de datos:

noOfGNSSADRecords es el número de registros GNSS de conducción acumulada que puede almacenar la tarjeta.

noOfSpecificConditionRecords es el número de registros de condiciones específicas que puede almacenar la tarjeta.

noOfCardVehicleUnitRecords es el número de registros sobre unidades instaladas en vehículos que puede almacenar la tarjeta.».

30) El apéndice 2 se modifica como sigue:

a) en el apartado 1.1 se añaden las siguientes abreviaciones:

«CHA Autorización del titular del certificado

DO Objeto de datos»;

b) el apartado 3.3 se modifica como sigue:

i) el punto TCS_24 se sustituye por el texto siguiente:

«TCS_24 Estas condiciones de seguridad pueden enlazarse de los modos siguientes:

AND: deben cumplirse todas las condiciones de seguridad;

OR: debe cumplirse al menos una condición de seguridad.

Las normas de acceso para el sistema de archivos, es decir, los comandos SELECT, READ BINARY y UPDATE BINARY, se especifican en el apartado 4. Las normas de acceso para el resto de los comandos se especifican en las tablas siguientes. El término 'no aplicable' se utiliza si no existe ningún requisito para admitir el comando. En este caso, el comando puede ser o no ser admitido, pero la condición de acceso es "fuera de ámbito".»;

ii) en el punto TCS_25, el cuadro se sustituye por el siguiente:

«Comando	Tarjeta de conductor	Tarjeta de taller	Tarjeta de control	Tarjeta de empresa
External Authenticate				
— Para autenticación de generación 1	ALW	ALW	ALW	ALW
— Para autenticación de generación 2	ALW	PWD	ALW	ALW
Internal Authenticate	ALW	PWD	ALW	ALW
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	No aplicable	No aplicable	No aplicable	No aplicable
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	No aplicable	No aplicable
PSO: Hash	No aplicable	No aplicable	ALW	No aplicable

Comando	Tarjeta de conductor	Tarjeta de taller	Tarjeta de control	Tarjeta de empresa
PERFORM HASH of FILE	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	No aplicable	No aplicable
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	No aplicable	No aplicable	ALW	No aplicable
Verify	No aplicable	ALW	No aplicable	No aplicable»

iii) en el apartado TCS_26, el cuadro se sustituye por el siguiente:

«Comando	Tarjeta de conductor	Tarjeta de taller	Tarjeta de control	Tarjeta de empresa
External Authenticate				
— Para autenticación de generación 1	No aplicable	No aplicable	No aplicable	No aplicable
— Para autenticación de generación 2	ALW	PWD	ALW	ALW
Internal Authenticate	No aplicable	No aplicable	No aplicable	No aplicable
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	No aplicable	ALW	ALW	No aplicable
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	No aplicable	No aplicable
PSO: Hash	No aplicable	No aplicable	ALW	No aplicable
PERFORM HASH of FILE	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	No aplicable	No aplicable
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	No aplicable	No aplicable	ALW	No aplicable
Verify	No aplicable	ALW	No aplicable	No aplicable»

iv) en el apartado TCS_27, el cuadro se sustituye por el siguiente:

«Comando	Tarjeta de conductor	Tarjeta de taller	Tarjeta de control	Tarjeta de empresa
External Authenticate				
— Para la autenticación de generación 1	No aplicable	No aplicable	No aplicable	No aplicable
— Para la autenticación de generación 2	ALW	PWD	ALW	ALW
Internal Authenticate	No aplicable	No aplicable	No aplicable	No aplicable
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	No aplicable	No aplicable	No aplicable	No aplicable
PSO: Compute Digital Signature	No aplicable	No aplicable	No aplicable	No aplicable
PSO: Hash	No aplicable	No aplicable	No aplicable	No aplicable
PERFORM HASH of FILE	No aplicable	No aplicable	No aplicable	No aplicable
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	No aplicable	No aplicable	No aplicable	No aplicable
Verify	No aplicable	ALW	No aplicable	No aplicable»

c) en el apartado 3.4, el punto TCS_29 se sustituye por el texto siguiente:

«TCS_29 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	00	Ha fallado la autenticación (Advertencia).
63	CX	CHV (PIN) incorrecto. “X” indica el contador de intentos restantes.

SW1	SW2	Significado
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 autenticación externa), o bien firma incorrecta (durante la verificación de la firma).
67	00	Longitud incorrecta (Lc o Le incorrecta).
68	83	Último comando de la cadena esperado.
69	00	Comando prohibido (no hay respuesta disponible en T=0).
69	82	Estado de seguridad no satisfecho.
69	83	Método de autenticación 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	80	Parámetros incorrectos en el campo de datos.
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).
6C	XX	Longitud incorrecta, SW2 indica la longitud exacta. No se devuelve un campo de datos.
6D	00	Código de instrucción no admitido o no válido.
6E	00	Clase no admitida.
6F	00	— Otros errores de comprobación

Pueden devolverse otras palabras de estado como las definidas en la norma ISO/CEI 7816-4, si su comportamiento no se menciona explícitamente en el presente apéndice.

Por ejemplo, existe la opción de devolver las siguientes palabras de estado:

6881: Canal lógico no admitido

6882: Mensajería segura no admitida.»;

d) en el apartado 3.5.1.1, el último guion del punto TCS_38 se sustituye por el texto siguiente:

«— 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 "**6500**".»;

e) en el apartado 3.5.1.2, el último guion del punto TCS_41 se sustituye por el texto siguiente:

«— 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 "**6500**".»;

f) en el apartado 3.5.2.1, el sexto guion del punto TCS_43 se sustituye por el texto siguiente:

«— 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**".»;

g) el apartado 3.5.2.1.1 se modifica como sigue:

i) en el punto TCS_45, el cuadro se sustituye por el siguiente:

«Byte	Longitud	Valor	Descripción
#1	1	"81h"	T_{PV}: Etiqueta para datos del valor plano
#2	L	"NNh" o "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	"99h"	Etiqueta para el estado de procesado (SW1-SW2) – opcional para mensajería segura de generación 1
#(3+L+NN)	1	"02h"	Longitud del estado de procesado – opcional para mensajería segura de generación 1
#(4+L+NN) - #(5+L+NN)	2	"XX XXh"	Estado de procesado de la respuesta APDU sin proteger – opcional para mensajería segura de generación 1
#(6+L+NN)	1	"8Eh"	TCC: Etiqueta para suma de control criptográfica
#(7+L+NN)	1	"XXh"	LCC: Longitud de la siguiente suma de control criptográfica "04h" para mensajería segura de generación 1 (véase la parte A del apéndice 11) "08h", "0Ch" o "10h" dependiendo de la longitud de la clave AES para mensajería segura de generación 2 (véase la parte B del apéndice 11)

Byte	Longitud	Valor	Descripción
#(8+L+NN)-#(7+M+L+NN)	M	"XX..XXh"	Suma de control criptográfica
SW	2	"XXXXh"	Palabras de estado (SW1,SW2)»

ii) en el punto TCS_46, el cuadro se sustituye por el siguiente:

«Byte	Longitud	Valor	Descripción
#1	1	"87h"	$T_{PI\ CG}$: Etiqueta para datos cifrados (criptograma)
#2	L	"MMh" o "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 LPI CG > 127 bytes
#(2+L)-#(1+L+MM)	MM	"01XX..XXh"	Datos cifrados: Indicador de relleno y criptograma
#(2+L+MM)	1	"99h"	Etiqueta para el estado de procesado (SW1-SW2) – opcional para mensajería segura de generación 1
#(3+L+MM)	1	"02h"	Longitud del estado de procesado – opcional para mensajería segura de generación 1
#(4+L+MM) - #(5+L+MM)	2	"XX XXh"	Estado de procesado de la respuesta APDU sin proteger – opcional para mensajería segura de generación 1
#(6+L+MM)	1	"8Eh"	TCC: Etiqueta para suma de control criptográfica
#(7+L+MM)	1	"XXh"	LCC: Longitud de la siguiente suma de control criptográfica "04h" para mensajería segura de generación 1 (véase la parte A del apéndice 11) "08h", "0Ch" o "10h" dependiendo de la longitud de la clave AES para mensajería segura de generación 2 (véase la parte B del apéndice 11)
#(8+L+MM)- #(7+N+L+MM)	N	"XX..XXh"	Suma de control criptográfica
SW	2	"XXXXh"	Palabras de estado (SW1,SW2)»

h) en el apartado 3.5.2.2, el sexto guion del punto TCS_50 se sustituye por el texto siguiente:

«— 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**".»;

i) en el apartado 3.5.2.3, el punto TCS_52 queda modificado como sigue:

i) la última fila del cuadro se sustituye por el texto siguiente:

«Le	1	"XXh"	Según se especifica en la norma ISO/CEI 7816-4»

ii) se añade la siguiente frase:

«En T=0, la tarjeta asume el valor Le = "00h" si no se aplica mensajería segura.

En T=1, se contesta con el estado de procesado "6700" si Le ="01h".»;

j) en el apartado 3.5.2.3, el sexto guion del punto TCS_53 se sustituye por el texto siguiente:

«— 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**".»;

k) en el apartado 3.5.3.2, el sexto guion del punto TCS_63 se sustituye por el texto siguiente:

«— 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**".»;

l) en el apartado 3.5.5, el punto TCS_72 se sustituye por el texto siguiente:

«TCS_72 El IFD debe añadir bytes "FFh" para rellenar por la derecha el PIN que introduzca el usuario y debe codificarse en ASCII, hasta llegar a una longitud de 8 bytes; véase también el tipo de datos WorkshopCardPIN en el apéndice 1.»;

m) en el apartado 3.5.8, el punto TCS_95 se sustituye por el texto siguiente:

«TCS_95 Si el comando INTERNAL AUTHENTICATE se ejecuta correctamente, la clave de la sesión actual de generación 1, si la hay, se borra y deja de estar disponible. Para disponer de una nueva clave de sesión de generación 1, es preciso que se ejecute correctamente el comando EXTERNAL AUTHENTICATE para el mecanismo de autenticación de generación 1.

Nota: Para las claves de sesión de generación 2, véase el apéndice 11, CSM_193 y CSM_195. Si se establecen claves de sesión de generación 2 y la tarjeta de tacógrafo recibe el comando APDU plano INTERNAL AUTHENTICATE, aborta la sesión de mensajería segura de generación 2 y destruye las claves de sesión de generación 2.»;

n) en el apartado 3.5.9, el punto TCS_97 se sustituye por el texto siguiente:

«TCS_97 La variante del comando para la autenticación mutua de la tarjeta de la VU de segunda generación puede ejecutarse en el MF, DF tacógrafo y DF tacógrafo_G2; véase también TCS_34. Si el comando EXTERNAL AUTHENTICATE de generación 2 se ejecuta correctamente, la clave de la sesión actual de generación 1, si la hay, se borra y deja de estar disponible.

Nota: Para las claves de sesión de generación 2, véase el apéndice 11, CSM_193 y CSM_195. Si se establecen claves de sesión de generación 2 y la tarjeta de tacógrafo recibe el comando APDU plano EXTERNAL AUTHENTICATE, aborta la sesión de mensajería segura de generación 2 y destruye las claves de sesión de generación 2.»;

o) en el apartado 3.5.10, se añade la siguiente fila al cuadro del punto TCS_101:

«5 + L + 1	1	"00h"	Según se especifica en la norma ISO/CEI 7816-4»

p) en el apartado 3.5.11.2.3, se añaden los siguientes párrafos en el punto TCS_114:

«— Si el currentAuthenticatedTime de la tarjeta es posterior a la fecha de caducidad de la clave pública seleccionada, se contesta con el estado de procesado **"6A88"**.

Nota: En el caso del comando MSE: SET AT para la autenticación de la VU, la clave referenciada es una clave pública VU_MA. La tarjeta establecerá la clave pública VU_MA para su uso, si dispone de ella en su memoria, que coincida con la referencia al titular del certificado (CHR) que figura en el campo de datos del comando (la tarjeta puede identificar las claves públicas VU_MA mediante el campo CHA del certificado). La tarjeta devolverá el estado «6A 88» a este comando solo en el caso de que no esté disponible en la unidad instalada en el vehículo la clave pública VU_Sign o ninguna otra clave pública. Véase la definición del campo CHA en el apéndice 11, y la del tipo de dato equipmentType en el apéndice 1.

Igualmente, en caso de que se envíe a una tarjeta de control un comando MSE: SET DST que haga referencia a un EQT (por ejemplo, una VU o una tarjeta), de conformidad con CSM_234 la clave referenciada es siempre una clave EQT_Sign que debe utilizarse para la verificación de una firma digital. Con arreglo a la figura 13 del apéndice 11, la tarjeta de control siempre habrá almacenado la clave pública EQT_Sign pertinente. En algunos casos, la tarjeta de control podrá haber almacenado la correspondiente clave pública EQT_MA. La tarjeta de control establecerá siempre la clave pública EQT_Sign para su uso cuando reciba un comando MSE: SET DST.»;

q) el apartado 3.5.13 se modifica como sigue:

i) el punto TCS_121 se sustituye por el texto siguiente:

«TCS_121 El valor de comprobación aleatoria del archivo temporalmente almacenado deberá borrarse si se calcula un nuevo valor de comprobación aleatoria del archivo por medio del comando PERFORM HASH of FILE, si se selecciona un DF y si se reinicia la tarjeta del tacógrafo.»;

ii) el punto TCS_123 se sustituye por el texto siguiente:

«TCS_123 La aplicación de tacógrafo de generación 2 deberá admitir el algoritmo SHA-2 (SHA-256, SHA-384 o SHA-512), especificado en la serie de cifrado del apéndice 11, parte B, para la clave de firma de tarjeta Card_Sign.»;

iii) el cuadro del punto TCS_124 se sustituye por el siguiente:

«Byte	Longi-tud	Valor	Descripción
CLA	1	"80h"	CLA
INS	1	"2Ah"	Realizar operación de seguridad
P1	1	"90h"	Etiqueta: Hash
P2	1	"00h"	Algoritmo conocido implícitamente Para la aplicación de tacógrafo de generación 1: SHA-1 Para la aplicación de tacógrafo de generación 2: algoritmo SHA-2 (SHA-256, SHA-384 o SHA-512), definido en la serie de cifrado del apéndice 11, parte B, para la clave de firma de tarjeta Card_Sign»

r) el apartado 3.5.14 se modifica como sigue:

el texto que aparece después del encabezamiento y hasta el punto TCS_126 se sustituye por el siguiente:

«Este comando sirve para calcular la firma digital de un código de comprobación aleatoria calculado previamente (véase PERFORM HASH of FILE, §3.5.13).

Solo la tarjeta de conductor y la tarjeta de taller deben admitir este comando en el DF tacógrafo y el DF tacógrafo_G2.

Otros tipos de tarjetas de tacógrafo pueden o no incorporar este comando. En el caso de la aplicación de tacógrafo de generación 2, solo la tarjeta de conductor y la tarjeta de taller tienen una clave de firma de generación 2, otras tarjetas no pueden ejecutar el comando correctamente y terminan con un código de error adecuado.

El comando puede o no estar accesible en el MF. Si el comando no está accesible en el MF, deberá terminar con un código de error apropiado.

Este comando cumple con lo dispuesto en la norma ISO/CEI 7816-8. Este comando tiene un uso restringido en relación con dicha norma.»;

s) el apartado 3.5.15 se modifica como sigue:

i) el cuadro del punto TCS_133 se sustituye por el siguiente:

«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 DO relevantes para verificación
Lc	1	"XXh"	Longitud Lc del campo de datos subsiguiente
#6	1	"9Eh"	Etiqueta para firma digital
#7 o #7-#8	L	"NNh" o "81 NNh"	Longitud de la firma digital (L es 2 bytes si la firma digital es más larga que 127 bytes): 128 bytes codificados conforme a la parte A del apéndice 11 para una aplicación de tacógrafo de generación 1. Dependiendo de la curva seleccionada para la aplicación de tacógrafo de generación 2 (véase la parte B del apéndice 11)
#(7+L)-#(6+L+NN)	NN	"XX..XXh"	Contenido de la firma digital»

ii) se añade el siguiente guion al punto TCS_134:

«— Si la clave pública seleccionada (utilizada para verificar la firma digital) tiene un CHA.LSB (CertificateHolderAuthorisation.equipmentType) que no es apropiado para la verificación de firmas digitales según el apéndice 11, se contesta con el estado de procesado "**6985**".»;

t) el apartado 3.5.16 se modifica como sigue:

i) en el cuadro del punto TCS_138 se añade la fila siguiente:

«5 + L + 1	1	“00h”	Según se especifica en la norma ISO/CEI 7816-4»

ii) se añade el siguiente guion al punto TCS_139:

«— “**6985**” indica que el sello de tiempo de 4 bytes que aparece en el campo de datos del comando es anterior a cardValidityBegin o posterior a cardExpiryDate.»;

u) el apartado 4.2.2 se modifica como sigue:

i) en la estructura de datos del punto TCS_154, las líneas desde DF Tachograph G2 hasta EF CardMA_Certificate y desde EF GNSS_Places hasta el final de este punto se sustituyen por el texto siguiente:

«

File / Data element	No of Records	Size (bytes) Min	Max	Default Values
DF Tachograph_G2		*20268*	*40316*	
EF Application_Identification		*17*	*17*	
DriverCardApplicationIdentification		*17*	*17*	
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		2	2	{00 00}
noOfGNSSADRecords		2	2	{00 00}
noOfSpecificConditionRecords		2	2	{00 00}
noOfCardVehicleUnitRecords		2	2	{00 00}
EF CardMA_Certificate		*204*	*341*	

...

EF GNSS_Places		*4538*	*6050*	
GNSSContinuousDriving		*4538*	*6050*	
gnssADPointerNewestRecord		2	2	{00 00}
gnssAccumulatedDrivingRecords		4536	6048	
GNSSContinuousDrivingRecord	n_8	*18*	*18*	
timeStamp		4	4	{00..00}
gnssPlaceRecord		14	14	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
vehicleOdometerValue		3	3	{00..00}

»;

ii) en el punto TCS_155, en el cuadro, el elemento NoOfGNSSCDRecords se sustituye por el siguiente:

«n_8	NoOfGNSSADRecords	252	336»

v) en el apartado 4.3.1, el texto correspondiente a la abreviación SC4 en el punto TCS_156 se sustituye por el texto siguiente:

«**SC4** Para el comando READ BINARY con byte INS par:

(SM-C-MAC-G1 Y SM-R-ENC-MAC-G1) O

(SM-C-MAC-G2 Y SM-R-ENC-MAC-G2)

Para el comando READ BINARY con byte INS impar (si se admite): NEV»;

w) el apartado 4.3.2 se modifica como sigue:

i) en la estructura de datos del punto TCS_162, las líneas desde DF Tachograph G2 hasta EF CardMA_Certificate, desde EF Calibration hasta extendedSealIdentifier y desde EF GNSS_Places hasta vehicleOdometerValue se sustituyen por el texto siguiente:

«

File / Data element	No of Records	Size (bytes) Min	Max	Default Values
DF Tachograph_G2	*1878*		*49787*	
EF Application_Identification	*19*		*19*	
WorkshopCardApplicationIdentificatio	*19*		*19*	
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	2		2	{00 00}
noOfCalibrationRecords	2		2	{00 00}
noOfGNSSADRecords	2		2	{00 00}
noOfSpecificConditionRecords	2		2	{00 00}
noOfCardVehicleUnitRecords	2		2	{00 00}
EF CardMA_Certificate	*204*		*341*	
...				
EF Calibration		*15668*	*45394*	
WorkshopCardCalibrationData		*15668*	*45394*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		2	2	{00}
calibrationRecords		*15664*	*45390*	
WorkshopCardCalibrationRecord	n_5	*178*	*178*	
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}
sensorGNSSSerialNumber		8	8	{00..00}
rcmSerialNumber		8	8	{00..00}
vuAbility		1	1	{00}
sealDataCard		56	56	
noOfSealRecords		1	1	{00}
SealRecords		55	55	
SealRecord	5	11	11	
equipmentType		1	1	{00}
extendedSealIdentifier		10	10	{00..00}

...

EF GNSS_Places		*326*	*434*	
└GNSSContinuousDriving		*326*	*434*	
├gnssADPointerNewestRecord		2	2	{00 00}
└gnssAccumulatedDrivingRecords		324	432	
└GNSSContinuousDrivingRecord	n_8	*18*	*18*	
├timeStamp		4	4	{00..00}
└gnssPlaceRecord		14	14	
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
├geoCoordinates		6	6	{00..00}
vehicleOdometerValue		3	3	{00..00}

»

ii) el elemento NoOfGNSSCDRecords del cuadro del punto TCS_163 se sustituye por lo siguiente:

«n_8	NoOfGNSSADRecords	18	24»

31) En el apéndice 3, el apartado 2 queda modificado como sigue:

a) se inserta la línea siguiente después de la línea con los pictogramas «Lugar donde comienza el período de trabajo diario» y «Lugar donde termina el período de trabajo diario»:

« Posición tras un tiempo de conducción acumulado de tres horas»;

b) la combinación de pictogramas «ajuste de la hora (por el taller)» se sustituye por la siguiente:

« Conflicto temporal o ajuste de la hora (por el taller)»;

c) las siguientes combinaciones de pictogramas se añaden a la lista de incidentes:

«  Ausencia de información de posición del receptor GNSS o Error de comunicación con el dispositivo GNSS externo;

 Error de comunicación con el dispositivo de comunicación a distancia».

32) El apéndice 4 se modifica como sigue:

a) el apartado 2 se modifica como sigue:

i) el bloque número 11.4 se sustituye por lo siguiente:

«11.4 *Introducción de los lugares donde comienzan o terminan los períodos de trabajo diarios*

pi = pictograma del lugar de comienzo/ finalización, hora, país y región	pihh:mm Cou Reg
longitud de la posición registrada	lon ±DDD°MM.M'
latitud de la posición registrada	lat ± DD°MM.M'
sello de tiempo del momento en que se haya determinado la posición	hh:mm
Cuentakilómetros	x xxx xxx **km**»

ii) el bloque número 11.5 se sustituye por lo siguiente:

«11.5. *Posiciones tras un tiempo de conducción acumulado de tres horas* pi = posición tras un tiempo de conducción acumulado de tres horas hora longitud de la posición registrada latitud de la posición registrada sello de tiempo del momento en que se haya determinado la posición Cuentakilómetros		pihh:mm lon ± DDD°MM.M' lat ± DD°MM.M ' hh:mm x xxx xxx **km**»

b) en el apartado 3.1, la posición 11.5 del formato de impresión diaria se sustituye por lo siguiente:

«11.5	Posiciones tras un tiempo de conducción acumulado de tres horas, en orden cronológico»

c) en el apartado 3.2, el formato de impresión diaria se sustituye por lo 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 + GEN)
4	Identificación del vehículo (vehículo del que se obtiene el documento impreso)
5	Identificación de la VU (VU cuya impresión se obtiene + GEN)
6	Último calibrado de la VU actual
7	Último control realizado en este tacógrafo
9	Delimitador de las actividades del conductor
10	Delimitador de la ranura del conductor (ranura 1)
10a	Condición «Fuera de ámbito» al comienzo de este día
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)
10a	Condición «Fuera de ámbito» al comienzo de este día
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	Síntesis de los intervalos sin tarjeta en la ranura del conductor
11.4	Lugares introducidos en orden cronológico
11.5	Posiciones tras un tiempo de conducción acumulado de tres horas, en orden cronológico
11.7	Totalidad de actividades
11.2	Resumen de los intervalos sin tarjeta en la ranura del segundo conductor
11.4	Lugares introducidos en orden cronológico
11.5	Posiciones tras un tiempo de conducción acumulado de tres horas, en orden cronológico

11.8	Totalidad de actividades
11.3	Resumen de actividades por el conductor, incluidas ambas ranuras
11.4	Lugares introducidos por este conductor en orden cronológico
11.5	Posiciones tras un tiempo de conducción acumulado de tres horas, en orden cronológico
11.9	Totalidad de actividades relativas al conductor actual
13.1	Delimitador de incidentes/fallos
13.4	Registro de incidentes/fallos (últimos cinco incidentes o fallos almacenados o en curso en la VU)
22.1	Lugar de control
22.2	Firma del controlador
22.3	Hora de comienzo (espacio reservado a un conductor sin una tarjeta para indicar
22.4	Hora de finalización qué períodos le atañen o corresponden)
22.5	Firma del conductor»

d) en el apartado 3.7, el punto PRT_014 se sustituye por el texto siguiente:

(no afecta a la versión española)

33) El apéndice 7 se modifica como sigue:

a) el apartado 1.1 se sustituye por el texto siguiente:

«1.1. **Ámbito de aplicación**

Se pueden transferir datos a un ESM:

— desde una unidad instalada en el vehículo (VU), 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); y

— desde una tarjeta de tacógrafo y a través de una unidad instalada en el vehículo, 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.

Los datos transferidos desde una VU se firman utilizando los mecanismos de seguridad comunes del apéndice 11, parte B (Sistema de tacógrafo de segunda generación), excepto cuando la supervisión del conductor la realiza una autoridad de control de un país no perteneciente a la UE utilizando una tarjeta de control de primera generación, en cuyo caso los datos se firman mediante los mecanismos de seguridad comunes del apéndice 11, parte A (Sistema de tacógrafo de primera generación), tal y como se establece en el requisito MIG_015 del apéndice 15 (Migración).

En el presente apéndice se especifican, por lo tanto, dos tipos de transferencias de datos desde la VU:

— Transferencia de datos desde la VU de generación 2, con la estructura de datos de segunda generación, firmada utilizando los mecanismos de seguridad comunes del apéndice 11, parte B,

— Transferencia de datos desde la VU de generación 1, con la estructura de datos de primera generación, firmada utilizando los mecanismos de seguridad comunes del apéndice 11, parte A.

Igualmente, existen dos tipos de transferencias de datos desde tarjetas de conductor de segunda generación insertadas en una VU, como se especifica en los apartados 3 y 4 del presente apéndice.»;

b) el apartado 2.2.2 se modifica como sigue:

i) el cuadro se sustituye por el siguiente:

«Estructura del mensaje	Máx. 4 bytes Cabecera				Máx. 255 bytes Datos			1 byte Suma de control
IDE -> **<- VU**	FMT	TGT	SRC	LEN	SID	DS_ / TRTP	DATA	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		EA, 8F	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 (fase 1)								
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	EE
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		00,00,00,00-,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								
Visión general	80	EE	F0	02	36	01 o 21		97
Actividades	80	EE	F0	06	36	02 o 22	Fecha	CS
Incidentes y fallos	80	EE	F0	02	36	03 o 23		99
Datos pormenorizados sobre la velocidad	80	EE	F0	02	36	04 o 24		9A
Datos técnicos	80	EE	F0	02	36	05 o 25		9B
Transferencia de los datos de la tarjeta	80	EE	F0	02	36	06	Ranura	CS

Estructura del mensaje	Máx. 4 bytes Cabecera				Máx. 255 bytes Datos			1 byte Suma de control
IDE -> **<- VU**	FMT	TGT	SRC	LEN	SID	DS_ / TRTP	DATA	CS
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								
Denegación general	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
Envío no aceptado	80	F0	EE	03	7F	SId pet.	50	CS
Falta respuesta	80	F0	EE	03	7F	SId pet.	78	CS
Datos no disponibles	80	F0	EE	03	7F	SId pet.	FA	CS»

ii) se añaden los siguientes guiones a las notas que aparecen después del cuadro:

«— Para las peticiones de transferencia de datos desde VU de segunda generación, se utilizan los TRTP 21 a 25; para las peticiones de transferencia de datos desde VU de primera generación, se utilizan los TRTP 01 a 05, que la VU aceptará solo en el marco de la supervisión del conductor realizada por una autoridad de control de un país no perteneciente a la UE, utilizando una tarjeta de control de primera generación.

— Los TRTP 11 a 19 y 31 a 39 se reservan para peticiones de transferencia específicas de los fabricantes.»;

c) el apartado 2.2.2.9 se modifica como sigue:

i) el punto DDP_011 se sustituye por el texto siguiente:

«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 seis tipos de transferencias de datos: Para la transferencia de datos desde la VU se pueden utilizar dos valores de TRTP distintos para cada tipo de transferencia:

Tipo de transferencia de datos	Valor del TRTP para la transferencia de datos desde la VU de primera generación	Valor del TRTP para la transferencia de datos desde la VU de segunda generación
Visión general	01	21
Actividades de una fecha específica	02	22
Incidentes y fallos	03	23
Datos pormenorizados sobre la velocidad	04	24
Datos técnicos	05	25

Tipo de transferencia de datos	Valor del TRTP
Transferencia de los datos de la tarjeta	06»

ii) el punto DDP_054 se sustituye por el texto siguiente:

«DDP_054 Es obligatorio que el IDE solicite la transferencia de datos resumen (TRTP 01 o 21) durante una sesión de transferencia, ya que solo así se asegura que los certificados de la VU se registran en el archivo transferido (y se permite la verificación de la firma digital).

En el segundo caso (TRTP 02 o 22), el mensaje de petición de transferencia de datos incluye la indicación del día natural (en formato `TimeReal`) cuyos datos se van a transferir.»;

d) en el apartado 2.2.2.10, el punto DDP_055 se sustituye por el texto siguiente:

«DDP_055 En el primer caso (TREP 01 o 21), 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; e

— inspecciones anteriores.»;

e) en el apartado 2.2.2.16, el último guion del punto DDP_018 se sustituye por el texto siguiente:

«— 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, o se solicita una transferencia de datos desde una VU de primera generación fuera del marco de la supervisión del conductor realizada por una autoridad de control de un país no perteneciente a la UE).»;

f) el apartado 2.2.6.1 se modifica como sigue:

i) El primer párrafo del punto DDP_029 se sustituye por el texto siguiente:

«El campo de datos del mensaje Positive Response Transfer Data Overview (respuesta positiva a la petición de transferencia de datos resumen) contiene los datos siguientes en este orden, con el SId 76 Hex, el TREP 01 o 21 Hex y el método adecuado de división y recuento de submensajes:»;

ii) el encabezamiento «Estructura de datos de primera generación» se sustituye por el texto siguiente:

«Estructura de datos de primera generación (TREP 01 Hex)»;

iii) el encabezamiento «Estructura de datos de segunda generación» se sustituye por el texto siguiente:

«Estructura de datos de segunda generación (TREP 21 Hex)»;

g) el apartado 2.2.6.2 se modifica como sigue:

i) El primer párrafo del punto DDP_030 se sustituye por el texto siguiente:

«El campo de datos del mensaje Positive Response Transfer Data Activities (respuesta positiva a la petición de transferencia de datos sobre actividades) contiene los datos siguientes en este orden, con el SId 76 Hex, el TREP 02 o 22 Hex y el método adecuado de división y recuento de submensajes:»;

ii) el encabezamiento «Estructura de datos de primera generación» se sustituye por el texto siguiente:

«Estructura de datos de primera generación (TREP 02 Hex)»;

iii) el encabezamiento «Estructura de datos de segunda generación» se sustituye por el texto siguiente:

«Estructura de datos de segunda generación (TREP 22 Hex)»;

iv) el elemento VuGNSSCDRecordArray que aparece bajo el encabezamiento «Estructura de datos de segunda generación (TREP 22 Hex)» se sustituye por el texto siguiente:

«VuGNSSADRecordArray	Posiciones GNSS del vehículo si el número de horas de conducción acumulada del vehículo alcanza un múltiplo de tres. Si esta sección está vacía, se envía una cabecera de conjunto con el mensaje “noOfRecords=0”.»

h) el apartado 2.2.6.3 se modifica como sigue:

i) el primer párrafo del punto DDP_031 se sustituye por el texto siguiente:

«El campo de datos del mensaje Positive Response Transfer Data Events and Faults (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 o 23 Hex y el método adecuado de división y recuento de submensajes:»;

ii) el encabezamiento «Estructura de datos de primera generación» se sustituye por el texto siguiente:

«Estructura de datos de primera generación (TREP 03 Hex)»;

iii) el encabezamiento «Estructura de datos de segunda generación» se sustituye por el texto siguiente:

«Estructura de datos de segunda generación (TREP 23 Hex)»;

iv) se suprime el elemento VuTimeAdjustmentGNSSRecordArray que aparece bajo el encabezamiento «Estructura de datos de segunda generación (TREP 23 Hex)»;

i) el apartado 2.2.6.4 se modifica como sigue:

i) el primer párrafo del punto DDP_032 se sustituye por el texto siguiente:

«El campo de datos del mensaje Positive Response Transfer Data Detailed Speed (respuesta positiva a la petición de transferencia de datos detallados sobre la velocidad) contiene los datos siguientes en este orden, con el SId 76 Hex, el TREP 04 o 24 Hex y el método adecuado de división y recuento de submensajes:»;

ii) el encabezamiento «Estructura de datos de primera generación» se sustituye por el texto siguiente:

«Estructura de datos de primera generación (TREP 04)»;

iii) el encabezamiento «Estructura de datos de segunda generación» se sustituye por el texto siguiente:

«Estructura de datos de segunda generación (TREP 24)»;

j) el apartado 2.2.6.5 se modifica como sigue:

i) el primer párrafo del punto DDP_033 se sustituye por el texto siguiente:

«El campo de datos del mensaje Positive Response Transfer Data Technical Data (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 o 25 Hex y el método adecuado de división y recuento de submensajes:»;

ii) el encabezamiento «Estructura de datos de primera generación» se sustituye por el texto siguiente:

«Estructura de datos de primera generación (TREP 05)»;

iii) el encabezamiento «Estructura de datos de segunda generación» se sustituye por el texto siguiente:

«Estructura de datos de segunda generación (TREP 25)»;

k) en el apartado 3.3, el punto DDP_035 se sustituye por el texto siguiente:

«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` e `IC`. Esta información es opcional y no se protege con una firma digital.

— (para las tarjetas de tacógrafo de primera y segunda generación) Transferencia de los archivos EF dentro del archivo `Tachograph DF`:

— 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 los archivos EF con datos de aplicación (dentro del archivo `Tachograph DF`) excepto el EF `Card_Download`. Esta información se protege con una firma digital, utilizando los mecanismos de seguridad comunes del apéndice 11, parte A.

— Es obligatorio transferir al menos los archivos EF `Application_Identification` e `Identification` para cada sesión de transferencia.

— Cuando se transfieran los datos de una tarjeta de conductor, también es obligatorio transferir los siguientes archivos EF:

— `Events_Data`,

— `Faults_Data`,

— Driver_Activity_Data,

— Vehicles_Used,

— Places,

— Control_Activity_Data,

— Specific_Conditions,

— (solo para las tarjetas de tacógrafo de segunda generación) Excepto cuando la transferencia de una tarjeta de conductor insertada en una VU se realiza durante una supervisión del conductor por parte de una autoridad de control de un país no perteneciente a la UE, utilizando una tarjeta de control de primera generación, transferir los archivos EF dentro del archivo Tachograph_G2 DF:

— Transferir los archivos EF CardSignCertificate, CA_Certificate y Link_Certificate, si existen. 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 Tachograph_G2 DF) excepto el EF Card_Download. Esta información se protege con una firma digital, utilizando los mecanismos de seguridad comunes del apéndice 11, parte B.

— Es obligatorio transferir al menos los archivos EF Application_Identification e Identification para cada sesión de transferencia.

— Cuando se transfieran los datos de una tarjeta de conductor, también es obligatorio transferir los siguientes archivos EF:

— Events_Data,

— Faults_Data,

— Driver_Activity_Data,

— Vehicles_Used,

— Places,

— Control_Activity_Data,

— Specific_Conditions,

— VehicleUnits_Used,

— GNSS Places.

— Cuando se transfieran los datos de una tarjeta de conductor, se actualizará la fecha de LastCardDownload en el archivo EF Card_Download, en los DF Tachograph y, si procede, Tachograph_G2 .

— Cuando se transfieran los datos de una tarjeta de taller, habrá que reiniciar el contador de calibrado en el archivo EF Card_Download en los DF Tachograph y, si procede, Tachograph_G2 .

— Cuando se transfieran los datos de una tarjeta de taller, no se transferirá el `Sensor_Installation_Data` en los DF `Tachograph` y, si procede, `Tachograph_G2` .»;

l) en el apartado 3.3.2, el primer párrafo del punto DDP_037 se sustituye por el texto siguiente:

«A continuación se muestra la secuencia para transferir los archivos EF ICC, IC, Card_Certificate (o CardSign-Certificate para DF tacógrafo_G2), CA_Certificate y Link_Certificate (solo para DF tacógrafo_G2):»;

m) en el apartado 3.3.3, se sustituye el cuadro por el siguiente:

«Tarjeta	Dir	IDE/IFD	Significado/Observaciones
	⇦	**Select File (seleccionar archivo)**	
OK	⇨		
	⇦	**Perform Hash of File (realizar comprobación aleatoria de archivo)**	— 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, parte A o B. Este no es un comando ISO.
Realizar una comprobación aleatoria del archivo y almacenar temporalmente el valor obtenido			
OK	⇨		
	⇦	**Read Binary (leer archivo binario)**	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.
File Data (datos del archivo) **OK**	⇨	Almacenar los datos recibidos en un ESM	según lo previsto en el apartado **3.4** Data storage format
	⇦	**PSO: Compute Digital Signature (calcular firma digital)**	
Realizar la operación de seguridad “calcular firma digital” utilizando el valor de comprobación aleatoria almacenado temporalmente			
Signature (firma) **OK**	⇨	Añadir datos a los datos previamente almacenados en el ESM	según lo previsto en el apartado **3.4** Data storage format»

n) en el apartado 3.4.2, el punto DDP_046 se sustituye por el texto siguiente:

«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) en el DF Tachograph o para la información común de la tarjeta	3 bytes
FID (2 bytes) || 01	Etiqueta para firma de EF (FID) en el DF Tachograph	3 bytes
FID (2 bytes) || 02	Etiqueta para firma de EF (FID) en el DF Tachograph_G2	3 bytes
FID (2 bytes) || 03	Etiqueta para firma de EF (FID) en el DF Tachograph_G2	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 EF ICC
C1 00 00	00 C2	Datos del archivo EF Card_Certificate
		…
05 05 00	0A 2E	Datos del archivo EF Vehicles_Used (en el DF Tachograph)
05 05 01	00 80	Firma del archivo EF Vehicles_Used (en el DF Tachograph)
05 05 02	0A 2E	Datos del archivo EF Vehicles_Used (en el DF Tachograph_G2)
05 05 03	xx xx	Firma del archivo EF Vehicles_Used (en el DF Tachograph_G2)»

o) en el apartado 4, el punto DDP_049 se sustituye por el texto siguiente:

«DDP_049 Tarjetas de conductor de primera generación: Los datos se transferirán utilizando el protocolo de transferencia de datos de primera generación, y los datos transferidos deberán tener el mismo formato que los datos transferidos desde una unidad instalada en el vehículo de primera generación.

Tarjetas de conductor de segunda generación: la VU deberá transferir todos los datos de la tarjeta, archivo por archivo, de acuerdo con el protocolo de transferencia descrito en el apartado 3, para luego enviar al IDE todos los datos recibidos de la tarjeta. Estos datos se enviarán con el formato adecuado de archivo TLV (véase el apartado 3.4.2) y encapsulados en un mensaje Positive Response Transfer Data (respuesta positiva a la petición de transferencia de datos).».

34) En el apartado 2 del apéndice 8, el texto que aparece después del encabezamiento «Referencias» se sustituye por el texto siguiente:

«ISO 14230-2: Vehículos de carretera — Sistemas de diagnóstico — Protocolo Keyword 2000 — Parte 2: Nivel de enlace de datos.

Primera edición: 1999.».

35) El apéndice 9 se modifica como sigue:

a) en el índice, el apartado 6 se sustituye por lo siguiente:

«6. PRUEBAS DEL DISPOSITIVO DE COMUNICACIÓN A DISTANCIA EXTERNO»;

b) en el apartado 1.1, el primer guion se sustituye por el texto siguiente:

«— una **certificación de seguridad** basada en criterios comunes especificados para acreditar el cumplimiento de un objetivo de seguridad conforme al apéndice 10 del presente anexo;»;

c) en el apartado 2, el cuadro de las pruebas funcionales de la unidad instalada en el vehículo se sustituye por el siguiente:

«N.º	Prueba	Descripción	Condiciones correspondientes
1	**Examen administrativo**		
1.1	Documentación	Corrección de la documentación	
1.2	Resultados de las pruebas del fabricante	Resultados de la prueba realizada por el fabricante durante la integración. Demostraciones sobre papel.	88, 89, 91
2	**Inspección visual**		
2.1	Cumplimiento de lo dispuesto en la documentación		
2.2	Identificación/inscripciones		224 a 226
2.3	Materiales		219 a 223
2.4	Precintos		398, 401 a 405
2.5	Interfaces externas		
3	**Pruebas funcionales**		
3.1	Funciones disponibles		02, 03, 04, 05, 07, 382
3.2	Modos de funcionamiento		09 a 11*, 134, 135
3.3	Funciones y derechos de acceso a los datos		12*, 13*, 382, 383, 386 a 389
3.4	Inserción y extracción de las tarjetas de supervisión		15, 16, 17, 18, 19*, 20*, 134
3.5	Medición de la velocidad y la distancia		21 a 31
3.6	Medición de la hora (ensayo realizado a 20 °C)		38 a 43
3.7	Supervisión de las actividades del conductor		44 a 53, 134
3.8	Supervisión del régimen de conducción		54, 55, 134
3.9	Entradas manuales		56 a 62
3.10	Gestión de los bloqueos introducidos por las empresas		63 a 68
3.11	Supervisión de las actividades de control		69, 70
3.12	Detección de incidentes o fallos		71 a 88, 134

N.º	Prueba	Descripción	Condiciones correspondientes
3.13	Datos de identificación del aparato		93*, 94*, 97, 100
3.14	Datos de inserción y extracción de la tarjeta del conductor		102* a 104*
3.15	Datos sobre la actividad del conductor		105* a 107*
3.16	Datos sobre lugares y posiciones		108* a 112*
3.17	Datos del cuentakilómetros		113* a 115*
3.18	Datos pormenorizados sobre la velocidad		116*
3.19	Datos sobre incidentes		117*
3.20	Datos sobre fallos		118*
3.21	Datos de calibrado		119* a 121*
3.22	Datos de ajuste de la hora		124*, 125*
3.23	Datos sobre actividades de control		126*, 127*
3.24	Datos sobre los bloqueos introducidos por las empresas		128*
3.25	Datos sobre actividades de transferencia		129*
3.26	Datos sobre condiciones específicas		130*, 131*
3.27	Registro y almacenamiento de datos en tarjetas de tacógrafo		136, 137, 138*, 139*, 141*, 142, 143 144, 145, 146*, 147*, 148*, 149, 150
3.28	Visualización		90, 134, 151 a 168, PIC_001, DIS_001
3.29	Impresión		90, 134 169 a 181, PIC_001, PRT_001 a PRT_014
3.30	Advertencias		134, 182 a 191, PIC_001
3.31	Transferencia de datos a medios externos		90, 134, 192 a 196
3.32	Comunicación remota para pruebas en carretera específicas		197 a 199
3.33	Envío de datos a dispositivos externos adicionales		200, 201
3.34	Calibrado		202 a 206*, 383, 384, 386 a 391
3.35	Verificación del calibrado en carretera		207 a 209
3.36	Ajuste de la hora		210 a 212*
3.37	No interferencia con funciones adicionales		06, 425

N.º	Prueba	Descripción	Condiciones correspondientes
3.38	Interfaz del sensor de movimiento		02, 122
3.39	Dispositivo GNSS externo		03, 123
3.40	Comprobar si la VU detecta, registra y almacena el o los incidentes o fallos descritos por el fabricante de la VU cuando un sensor de movimiento acoplado reaccione a los campos magnéticos perturbando la detección de movimiento del vehículo.		217
3.41	Serie de cifrado y parámetros de dominio estandarizados		CSM_48, CSM_50
4.	**Pruebas ambientales**		
4.1	Temperatura	Verificar la funcionalidad mediante: Prueba en virtud de la ISO 16750-4, apartado 5.1.1.2: prueba de funcionamiento a temperatura baja (72 h a – 20 °C). Esta prueba se refiere a la IEC 60068-2-1: Verificación medioambiental – Parte 2-1: Pruebas – Prueba A: Frío Prueba en virtud de la ISO 16750-4: apartado 5.1.2.2: prueba de funcionamiento a temperatura alta (72 h a 70 °C). Esta prueba se refiere a la IEC 60068-2-2: Procedimientos básicos de verificación medioambiental; Parte 2: pruebas; Prueba B: Calor seco. Prueba en virtud de la ISO 16750-4, apartado 5.3.2: cambio rápido de temperatura con una duración de transición específica (– 20 °C/70 °C, 20 ciclos, tiempo: 2 horas en cada temperatura). Es posible llevar a cabo un conjunto reducido de pruebas (de 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.	213
4.2	Humedad	Verificar que la unidad instalada en el vehículo puede soportar una humedad cíclica (prueba de calor) mediante la norma IEC 60068-2-30, 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.	214
4.3	Mecánica	1. Vibraciones sinusoidales: verificar que la unidad instalada en el vehículo es capaz de soportar vibraciones sinusoidales de las siguientes características: desplazamiento constante entre 5 y 11 Hz: pico de 10 mm; y aceleración constante entre 11 y 300 Hz: 5 g. Esta exigencia se verifica mediante la norma IEC 60068-2-6, prueba Fc, con una duración mínima de 3 × 12 horas (12 horas por cada eje). La ISO 16750-3 no requiere una prueba de vibración sinusoidal para dispositivos situados en el puesto de conducción del vehículo desacoplado.	219

N.º	Prueba	Descripción	Condiciones correspondientes
		2. Vibraciones aleatorias: Prueba en virtud de la ISO 16750-3, apartado 4.1.2.8: prueba VIII: vehículo comercial, puesto de conducción del vehículo desacoplado. Prueba de vibraciones aleatorias, 10-2 000 Hz, RMS vertical 21,3 m/s^2, RMS longitudinal 11,8 m/s^2, RMS lateral 13,1 m/s^2, 3 ejes, 32 horas por eje, incluido un ciclo de temperatura – 20 - + 70 °C. Esta prueba se refiere a la IEC 60068-2-64: Verificación medioambiental – Parte 2-64: Pruebas – Prueba Fh: Vibración, aleatorio de banda ancha y orientación. 3. Choques: choque mecánico con semionda sinusoidal de 3 g de conformidad con la ISO 16750. Las pruebas arriba descritas se llevan a cabo con muestras diferentes del tipo de equipo que se someta a prueba.	
4.4	Protección frente a la penetración de agua y cuerpos extraños	Prueba en virtud de la ISO 20653: Vehículos de carretera – Niveles de protección (código IP) – Protección del equipo eléctrico frente a objetos extraños, al agua y al acceso (sin cambio en los parámetros); valor mínimo IP 40.	220, 221
4.5	Protección frente a sobretensiones	Verificar que la unidad instalada en el vehículo es capaz de soportar un suministro eléctrico de: versiones de 24 V: 34 V a + 40 °C 1 hora; y versiones de 12 V: 17 V a + 40 °C 1 hora.(ISO 16750-2)	216
4.6	Protección frente a la inversión de la polaridad	Verificar que la unidad instalada en el vehículo es capaz de soportar una inversión de su fuente de alimentación. (ISO 16750-2)	216
4.7	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. (ISO 16750-2)	216
5	**Pruebas de compatibilidad electromagnética**		
5.1	Emisiones radiadas y susceptibilidad	Cumplimiento del Reglamento n.º 10 de la CEPE.	218
5.2	Descarga electrostática	Cumplimiento de la norma ISO 10605:2008 + Corrigendum Técnico 2010 + AMD1:2014: +/– 4 kV para contacto +/– 8 kV para descarga de aire.	218

N.º	Prueba	Descripción	Condiciones correspondientes
5.3	Susceptibilidad transitoria conducida en la fuente de alimentación	Para versiones 24 V: cumplimiento de la ISO 7637-2 + Reglamento n.º 10 de la CEPE, Rev. 3: impulso 1a: Vs = – 450 V, Ri = 50 ohmios impulso 2a: Vs = + 37 V, Ri = 2 ohmios impulso 2b: Vs = + 20 V, Ri = 0,05 ohmios impulso 3a: Vs = – 150 V, Ri = 50 ohmios impulso 3b: Vs = + 150 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. Para versiones 12 V: cumplimiento de la ISO 7637-1 + Reglamento n.º 10 de la CEPE, Rev. 3: impulso 1: Vs = – 75 V, Ri = 10 ohmios impulso 2a: Vs = + 37 V, Ri = 2 ohmios impulso 2b: Vs = + 10 V, Ri = 0,05 ohmios impulso 3a: Vs = – 112 V, Ri = 50 ohmios impulso 3b: Vs = + 75 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. Para las propuestas de volcado de la carga, remítase a la ISO 16750-2, 4.ª edición, apartado 4.6.4.	218»

d) el apartado 6 se sustituye por el texto siguiente:

«6. PRUEBAS DEL DISPOSITIVO DE COMUNICACIÓN A DISTANCIA EXTERNO

N.º	Prueba	Descripción	Condiciones correspondientes
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		225, 226
2.3.	Materiales		219 a 223
3.	**Pruebas funcionales**		
3.1.	Comunicación remota para pruebas en carretera específicas		4, 197 a 199

N.º	Prueba	Descripción	Condiciones correspondientes
3.2.	Registro y almacenamiento de datos en la memoria		91
3.3.	Comunicación con la unidad instalada en el vehículo		Apéndice 14, DSC_66 a DSC_70, DSC_71 a DSC_76
4.	**Pruebas ambientales**		
4.1.	Temperatura	Verificar la funcionalidad mediante: Prueba en virtud de la ISO 16750-4, apartado 5.1.1.2: prueba de funcionamiento a temperatura baja (72 h a – 20 °C). Esta prueba se refiere a la IEC 60068-2-1: Verificación medioambiental – Parte 2-1: Pruebas – Prueba A: Frío Prueba en virtud de la ISO 16750-4: apartado 5.1.2.2: prueba de funcionamiento a temperatura alta (72 h a 70 °C). Esta prueba se refiere a la IEC 60068-2-2: Procedimientos básicos de verificación medioambiental; Parte 2: pruebas; Prueba B: Calor seco. Prueba en virtud de la ISO 16750-4, apartado 5.3.2: cambio rápido de temperatura con una duración de transición específica (– 20 °C / 70 °C, 20 ciclos, tiempo: 1 hora en cada temperatura). Es posible llevar a cabo un conjunto reducido de pruebas (de 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.	213
4.2.	Protección frente a la penetración de agua y cuerpos extraños	Prueba en virtud de la ISO 20653: Vehículos de carretera – Niveles de protección (código IP) – Protección del equipo eléctrico frente a objetos extraños, al agua y al acceso (valor objetivo IP40)	220, 221
5.	**Pruebas de compatibilidad electromagnética**		
5.1.	Emisiones radiadas y susceptibilidad	Cumplimiento del Reglamento n.º 10 de la CEPE.	218
5.2.	Descarga electrostática	Cumplimiento de la norma ISO 10605:2008 + Corrigendum Técnico 2010 + AMD1:2014:+/– 4 kV para contacto +/– 8 kV para descarga de aire.	218

N.º	Prueba	Descripción	Condiciones correspondientes
5.3.	Susceptibilidad transitoria conducida en la fuente de alimentación	Para versiones 24 V: cumplimiento de la ISO 7637-2 + Reglamento n.º 10 de la CEPE, Rev. 3: impulso 1a: Vs = – 450 V, Ri = 50 ohmios impulso 2a: Vs = + 37 V, Ri = 2 ohmios impulso 2b: Vs = + 20 V, Ri = 0,05 ohmios impulso 3a: Vs = – 150 V, Ri = 50 ohmios impulso 3b: Vs = + 150 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. Para versiones 12 V: cumplimiento de la ISO 7637-1 + Reglamento n.º 10 de la CEPE, Rev. 3: impulso 1: Vs = – 75 V, Ri = 10 ohmios impulso 2a: Vs = + 37 V, Ri = 2 ohmios impulso 2b: Vs = + 10 V, Ri = 0,05 ohmios impulso 3a: Vs = – 112 V, Ri = 50 ohmios impulso 3b: Vs = + 75 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. Para las propuestas de volcado de la carga, remítase a la ISO 16750-2, 4.ª edición, apartado 4.6.4.	218»

e) en el apartado 8, el cuadro sobre las pruebas de interoperabilidad se sustituye por el siguiente:

«N.º	Prueba	Descripción
	8.1 Pruebas de interoperabilidad entre las unidades intravehiculares y las tarjetas de tacógrafo	
1	Autenticación mutua	Comprobar que la autenticación mutua entre la unidad instalada en el vehículo y la tarjeta de tacógrafo funciona normalmente.
2	Pruebas de lectura/escritura	Ejecutar un escenario de actividad típico en la unidad instalada en el vehículo. Dicho escenario deberá adaptarse al tipo de tarjeta que se esté verificando y deberá incluir pruebas de escritura en tantos EF como sea posible en la tarjeta. Verificar mediante una transferencia de la unidad instalada en el vehículo que todos los registros correspondientes se han realizado correctamente. Verificar mediante una transferencia de la tarjeta que todos los registros correspondientes se han realizado correctamente. Verificar mediante una impresión diaria que todos los registros correspondientes se pueden leer correctamente.

N.º	Prueba	Descripción
8.2 Pruebas de interoperabilidad entre las unidades intravehiculares y los sensores de movimiento		
1	Emparejamiento	Comprobar que el emparejamiento entre las unidades intravehiculares y los sensores de movimiento funciona normalmente.
2	Pruebas de actividad	Ejecutar un escenario de actividad típico en el sensor de movimiento. El escenario incluirá una actividad normal y creará el mayor número de incidentes o fallos posible. Verificar mediante una transferencia de la unidad instalada en el vehículo que todos los registros correspondientes se han realizado correctamente. Verificar mediante una transferencia de la tarjeta que todos los registros correspondientes se han realizado correctamente. Verificar mediante una impresión diaria que todos los registros correspondientes se pueden leer correctamente.
8.3 Pruebas de interoperabilidad entre las unidades intravehiculares y las instalaciones GNSS externas (si procede)		
1	Autenticación mutua	Comprobar que la autenticación mutua (acoplamiento) entre la unidad instalada en el vehículo y el módulo GNSS externo funciona normalmente.
2	Pruebas de actividad	Ejecutar un escenario de actividad típico en el módulo GNSS externo. El escenario incluirá una actividad normal y creará el mayor número de incidentes o fallos posible. Verificar mediante una transferencia de la unidad instalada en el vehículo que todos los registros correspondientes se han realizado correctamente. Verificar mediante una transferencia de la tarjeta que todos los registros correspondientes se han realizado correctamente. Verificar mediante una impresión diaria que todos los registros correspondientes se pueden leer correctamente.»

36) El apéndice 11 se modifica como sigue:

a) en el apartado 8.2.3, el punto CSM_49 se sustituye por el texto siguiente:

«CSM_49 Las unidades instaladas en los vehículos, las tarjetas de tacógrafo y los dispositivos GNSS externos admitirán los algoritmos SHA-256, SHA-384 y SHA-512 especificados en [SHS].»;

b) en el apartado 9.1.2, el primer párrafo del punto CSM_58 se sustituye por el texto siguiente:

«CSM_58 Siempre que genere un nuevo par de claves raíz europeo, la ERCA creará un certificado de enlace para la nueva clave pública europea y la firmará con la clave privada europea anterior. El período de validez del certificado de enlace será de 17 años y 3 meses. Lo anterior se indica asimismo en la figura 1 de la sección 9.1.7.»;

c) en el apartado 9.1.4, el punto CSM_72 se sustituye por el texto siguiente:

«CSM_72 Para cada unidad instalada en el vehículo se generarán dos pares de claves ECC únicos, designados VU_MA y VU_Sign. Esta tarea es efectuada por los fabricantes de VU. Siempre que se genere un nuevo par de claves VU, la parte que genere la clave enviará la clave pública a la MSCA, a fin de obtener el certificado VU correspondiente firmado por la MSCA. La clave privada será utilizada solamente por la unidad instalada en el vehículo.»;

d) el apartado 9.1.5 se modifica como sigue:

i) el punto CSM_83 se sustituye por el texto siguiente:

«CSM_83 Para cada tarjeta de tacógrafo se generará un par de claves ECC único, designado Card_MA. Además, para cada tarjeta de conductor y cada tarjeta de taller se generará un segundo par de claves ECC único, designado Card_Sign. Esta tarea puede ser efectuada por los fabricantes de tarjetas o los personalizadores de tarjetas. Siempre que se genere un nuevo par de claves de tarjeta, la parte que genere la clave enviará la clave pública a la MSCA, a fin de obtener el certificado de la tarjeta correspondiente firmado por la MSCA. La clave privada será utilizada solamente por la tarjeta de tacógrafo.»;

ii) el punto CSM_88 se sustituye por el texto siguiente:

«CSM_88 El período de validez de un certificado Card_MA será el siguiente:

— Para las tarjetas de conductor: 5 años

— Para las tarjetas de empresa: 5 años

— Para las tarjetas de control: 2 años

— Para las tarjetas de taller: 1 año»;

iii) se añade el guion siguiente al punto CSM_91:

«— Además, para las tarjetas de control, las tarjetas de empresa y las tarjetas de taller, y solo si estas tarjetas se expiden durante los tres primeros meses del período de validez del nuevo certificado EUR: el certificado EUR que sea dos generaciones más antiguo, de existir este.

Nota al último guion: por ejemplo, en los tres primeros meses del certificado ERCA (3) (véase la figura 1), las mencionadas tarjetas contendrán el certificado ERCA (1). Esto es necesario para garantizar que estas tarjetas pueden utilizarse para realizar transferencias de datos desde VU con certificado ERCA (1) cuyo período de vida normal de quince años más el período de tres meses para transferir los datos expira durante estos meses; véase el último guion del requisito 13 del anexo IC.»;

e) el apartado 9.1.6 se modifica como sigue:

i) el punto CSM_93 se sustituye por el texto siguiente:

«CSM_93 Para cada dispositivo GNSS externo se generará un par de claves ECC único designado EGF_MA. Esta tarea es efectuada por los fabricantes de dispositivos GNSS externos. Siempre que se genere un nuevo par de claves EGF_MA, la parte que genere la clave enviará la clave pública a la MSCA, a fin de obtener el certificado EGF_MA correspondiente firmado por la MSCA. La clave privada será utilizada solamente por el dispositivo GNSS externo.»;

ii) el punto CSM_95 se sustituye por el texto siguiente:

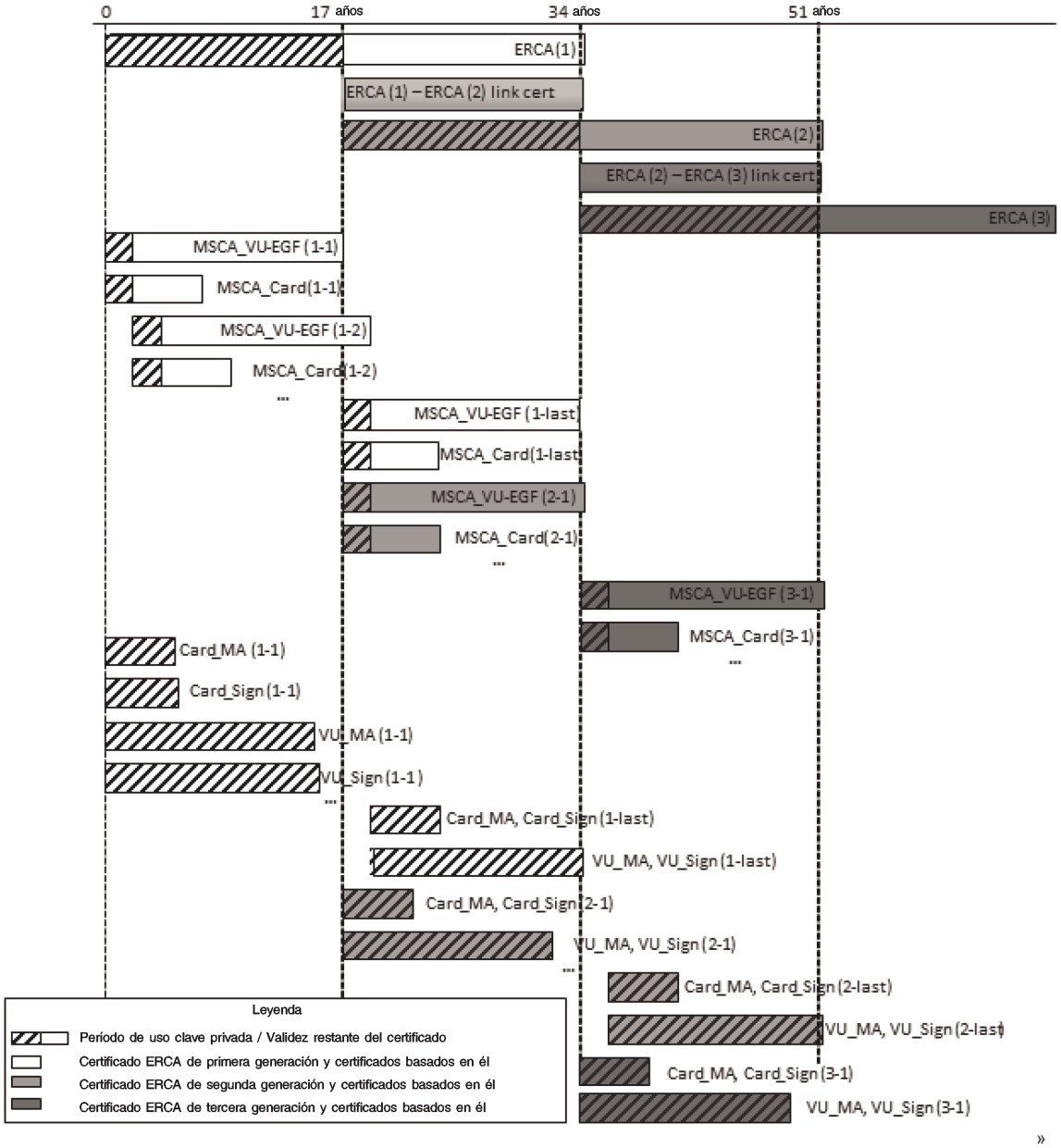
«CSM_95 Una dispositivo GNSS externo utilizará su par de claves EGF_MA, compuesto por la clave privada EGF_MA.SK y la clave pública EGF_MA.PK, exclusivamente para efectuar la autenticación mutua y establecer la clave de sesión con las unidades instaladas en los vehículos, tal como se especifica en el apartado 11.4 del presente apéndice.»;

f) el apartado 9.1.7 se modifica como sigue:

i) la figura 1 se sustituye por lo siguiente:

«*Figura 1*

Expedición y uso de las diferentes generaciones de certificados raíz ERCA, certificados de enlace ERCA, certificados MSCA y certificados de equipos



»

ii) la nota 6 de la figura 1 se sustituye por la siguiente:

«6. Por limitaciones de espacio, solamente se indica la diferencia entre los períodos de validez de los certificados Card_MA y Card_Sign de la primera generación.»;

g) el apartado 9.2.1.1 se modifica como sigue:

i) en el punto CSM_106, el primer guion se sustituye por el texto siguiente:

«— Para las claves maestras de sensor de movimiento de 128 bits: CV = "B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5D 83" »;

ii) en el punto CSM_107, el párrafo primero se sustituye por el texto siguiente:

«Cada fabricante de sensores de movimiento generará una clave de emparejamiento K_P aleatoria y única para cada sensor de movimiento y enviará cada clave de emparejamiento a la autoridad de certificación de su Estado miembro. La MSCA cifrará cada clave de emparejamiento separadamente con la clave maestra K_M del sensor de movimiento y devolverá la clave cifrada al fabricante del sensor de movimiento. Para cada clave cifrada, la MSCA notificará al fabricante del sensor de movimiento el número de versión de la K_M asociada.»;

iii) el punto CSM_108 se sustituye por el texto siguiente:

«CSM_108 Cada fabricante de sensores de movimiento generará un número de serie único para cada sensor de movimiento y enviará todos los números de serie a la autoridad de certificación de su Estado miembro. La MSCA cifrará cada número de serie separadamente con la clave de identificación maestra K_{ID} y devolverá el número de serie cifrado al fabricante del sensor de movimiento. Para cada número de serie cifrado, la MSCA notificará al fabricante del sensor de movimiento el número de versión de la K_{ID} asociada.»;

h) el apartado 9.2.2.1 se modifica como sigue:

i) el punto CSM_123 se sustituye por el texto siguiente:

«CSM_123 Para cada unidad instalada en el vehículo, el fabricante de la unidad instalada en el vehículo creará un número de serie de la VU único y lo enviará a la autoridad de certificación de su Estado miembro en una solicitud de obtención de un conjunto de dos claves DSRC específicas de la VU. El número de serie de la VU tendrá el tipo de dato `VuSerialNumber`.

Nota:

— Este número de serie de la VU será idéntico al elemento vuSerialNumber de VuIdentification, véase el apéndice 1 y la referencia del titular del certificado en los certificados de la VU.

— El número de serie de la VU puede no conocerse en el momento en que el fabricante de la unidad instalada en el vehículo solicita las claves DSRC específicas de la VU. En este caso, el fabricante de la VU enviará el identificador único de la solicitud de certificado que utilizó al solicitar los certificados de la VU; véase CSM_153. Dicho identificador de la solicitud de certificado será, por tanto, igual a la referencia del titular del certificado de los certificados de la VU.»;

ii) en el punto CSM_124, el requisito de información del paso 2 se sustituye por el texto siguiente:

«*info* = número de serie o identificador de la solicitud de certificado de la VU tal como se especifica en CSM_123»;

iii) el punto CSM_128 se sustituye por el texto siguiente:

«CSM_128 La MSCA llevará un registro de todas las claves DSRC específicas de VU que haya generado, su número de versión y el número de serie o el identificador de la solicitud de certificado de la VU utilizados para derivarlas.»;

i) en el apartado 9.3.1, el primer párrafo del punto CSM_135 se sustituye por el texto siguiente:

«A fin de codificar los objetos de datos en los certificados, se utilizarán las reglas de codificación distinguida (DER) de acuerdo con la norma [ISO 8825-1]. La tabla 4 muestra la codificación completa del certificado, incluidas todas las etiquetas y los bytes de longitud.»;

j) en el apartado 9.3.2.3, el punto CSM_141 se sustituye por el texto siguiente:

«CSM_141 La autorización del titular del certificado servirá para identificar el tipo de certificado. Se compone de los seis bytes más significativos del identificador de la aplicación del tacógrafo, concatenados con el tipo de equipo, que indica el tipo de equipo al que está destinado el certificado. En el caso de un certificado de la VU, un certificado de la tarjeta de conductor o un certificado de la tarjeta de taller, el tipo de equipo también se utiliza para diferenciar entre un certificado para la autenticación mutua y un certificado para la creación de firmas digitales (véanse el apartado 9.1 y el apéndice 1, tipo de datos EquipmentType).»;

k) en el apartado 9.3.2.5, se añade el siguiente párrafo en el punto CSM_146:

«*Nota*: En el caso de un certificado de la tarjeta, el valor de la CHR será igual al valor del cardExtendedSerial-Number del archivo EF_ICC; véase el apéndice 2. En el caso de un certificado EGF, el valor de la CHR será igual al valor del sensorGNSSSerialNumber del archivo EF_ICC; véase el apéndice 14. En el caso de un certificado de VU, el valor de la CHR será igual al valor del elemento vuSerialNumber de VuIdentification, véase el apéndice 1, a menos que el fabricante no conozca el número de serie específico del fabricante en el momento de solicitar el certificado.»;

l) en el apartado 9.3.2.6, el punto CSM_148 se sustituye por el texto siguiente:

«CSM_148 La fecha efectiva del certificado indicará la fecha y hora de inicio del período de validez del certificado.»;

m) el apartado 9.3.3 se modifica como sigue:

i) en el punto CSM_151, el párrafo primero se sustituye por el texto siguiente:

«Al solicitar un certificado, la MSCA enviará los siguientes datos a su ERCA:»;

ii) el punto CSM_153 se sustituye por el texto siguiente:

«CSM_153 En una solicitud de certificado, un fabricante de equipos enviará los siguientes datos a la MSCA a fin de permitirle crear la referencia del titular del certificado del nuevo certificado de equipo:

— si se conoce (véase CSM_154), un número de serie para el equipo, único para el fabricante, el tipo de equipo, y el mes de fabricación. En caso contrario, un identificador único de la solicitud de certificado.

— El mes y año de fabricación del equipo o de solicitud del certificado.

El fabricante garantizará que estos datos sean correctos y que el certificado devuelto por la MSCA sea insertado en el equipo previsto.»;

n) el apartado 10.2.1 se modifica como sigue:

i) en el punto CSM_157, el texto que precede a las notas de la figura 4 se sustituye por el texto siguiente:

«Las unidades instaladas en el vehículo utilizarán el protocolo ilustrado en la figura 4 para verificar la cadena de certificados de una tarjeta de tacógrafo. Para cada certificado que lea en la tarjeta, la VU verificará que el campo "Autorización del titular del certificado" (CHA) sea correcto:

— El campo CHA del certificado Card indicará un certificado de tarjeta para la autenticación mutua (véase apéndice 1, tipo de datos EquipmentType).

— El campo CHA del certificado Card.CA indicará una MSCA.

— El campo CHA del certificado Card.Link indicará una ERCA.»;

ii) en el punto CSM_159 se añade la frase siguiente:

«Mientras que el almacenamiento de todos los demás tipos de certificados es facultativo, es obligatorio que la VU almacene todo nuevo certificado de enlace presentado por una tarjeta.»;

o) el apartado 10.2.2 se modifica como sigue:

i) en el punto CSM_161, el texto que precede a la figura 5 se sustituye por el texto siguiente:

«Las tarjetas de tacógrafo utilizarán el protocolo ilustrado en la figura 5 para verificar la cadena de certificados de una VU. Para cada certificado presentado por la VU, la tarjeta verificará que el campo "Autorización del titular del certificado" (CHA) sea correcto:

— El campo CHA del certificado VU.Link indicará una ERCA.

— El campo CHA del certificado VU.CA indicará una MSCA.

— El campo CHA del certificado VU indicará un certificado de VU para la autenticación mutua (véase apéndice 1, tipo de datos EquipmentType).»;

ii) el punto CSM_165 se sustituye por el texto siguiente:

«CSM_165 Si el comando MSE: Set AT se ejecuta correctamente, la tarjeta establecerá la VU.PK indicada para su uso posterior durante la autenticación del vehículo, y almacenará temporalmente Comp(VU.PKeph). En el caso de que se envíen dos o más comandos MSE: Set AT ejecutados correctamente antes de efectuar el acuerdo de claves de sesión, la tarjeta almacenará únicamente la última Comp(VU.PKeph) recibida. La tarjeta reiniciará Comp(VU.PKeph) después de un comando GENERAL AUTHENTICATE ejecutado correctamente.»;

p) el apartado 10.3 se modifica como sigue:

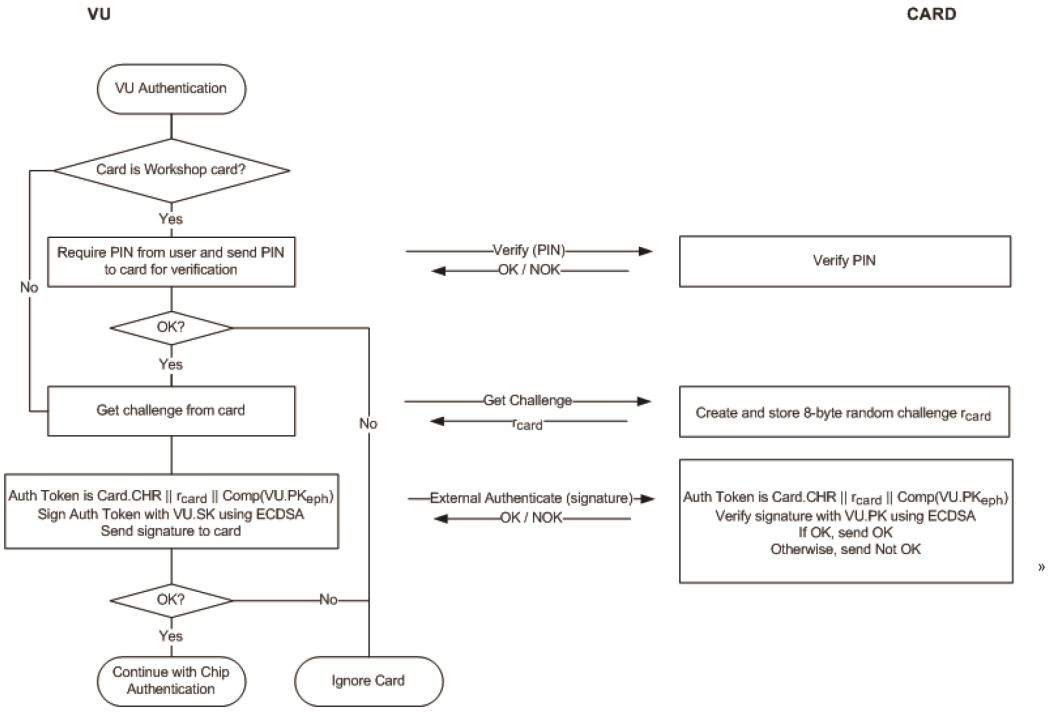
i) el primer párrafo del punto CSM_170 se sustituye por el texto siguiente:

«Junto a la comprobación de la tarjeta, la VU incluirá en la firma la referencia del titular del certificado extraída del certificado de la tarjeta.»;

ii) en el punto CSM_171, la figura 6 se sustituye por la siguiente:

«*Figura 6*

Protocolo de autenticación de VU



»

iii) el punto CSM_174 se sustituye por el texto siguiente:

«CSM_174 Al recibir la firma de la VU en un comando EXTERNAL AUTHENTICATE, la tarjeta:

— calculará el token de autenticación concatenando Card.CHR, la comprobación de tarjeta rcard y el identificador de la clave pública efímera de la VU Comp(VU.PKeph);

— verificará la firma de la VU mediante el algoritmo ECDSA, en combinación con el algoritmo hash relacionado con el tamaño de clave del par de claves VU_MA de la VU, tal como se especifica en CSM_50, y en combinación con la clave VU.PK y el token de autenticación calculado.»;

q) en el apartado 10.4, el punto CSM_176 queda modificado como sigue:

i) el punto 2 se sustituye por el texto siguiente:

«2. La VU envía el punto público $VU.PK_{eph}$ de su par de claves efímero a la tarjeta. El punto público se convertirá en una cadena de octetos tal como se especifica en la directriz técnica [TR-03111]. Se utilizará el formato de codificación descomprimido. Como se indica en CSM_164, la VU generó este par de claves efímero antes de la verificación de la cadena de certificados de la VU. La VU envió el identificador de la clave pública efímera $Comp(VU.PK_{eph})$ a la tarjeta, y la tarjeta lo almacenó.»;

ii) el punto 6 se sustituye por el texto siguiente:

«6. Mediante la clave K_{MAC}, la tarjeta computa un token de autenticación a través del identificador del punto público efímero de la VU: $T_{PICC} = CMAC(K_{MAC}, VU.PK_{eph})$. El punto público deberá estar en el formato utilizado por la VU (véase el punto 2). La tarjeta envía N_{PICC} y T_{PICC} a la unidad instalada en el vehículo.»;

r) en el apartado 10.5.2, el punto CSM_191 se sustituye por el texto siguiente:

«CSM_191 Los objetos de datos que deban cifrarse se rellenarán de acuerdo con la norma [ISO 7816-4] mediante el indicador de contenido de relleno '01'. Para el cálculo del MAC, los objetos de datos de la APDU se rellenarán conforme a la norma [ISO 7816-4].

Nota: El relleno para la mensajería segura siempre es efectuado por la capa de mensajería segura, no por los algoritmos CMAC o CBC.

Resumen y ejemplos

Un comando APDU con mensajería segura aplicada tendrá la siguiente estructura, dependiendo del caso del comando no securizado correspondiente (DO significa objeto de datos):

Caso 1: CLA INS P1 P2 || Lc' || DO '8E' || Le

Caso 2: CLA INS P1 P2 || Lc' || DO '97' || DO '8E' || Le

Caso 3 (byte INS par): CLA INS P1 P2 || Lc' || DO '81' || DO '8E' || Le

Caso 3: (byte INS impar): CLA INS P1 P2 || Lc' || DO 'B3' || DO '8E' || Le

Caso 4 (byte INS par): CLA INS P1 P2 || Lc' || DO '81' || DO '97' || DO '8E' || Le

Caso 4 (byte INS impar): CLA INS P1 P2 || Lc' || DO 'B3' || DO '97' || DO '8E' || Le

donde Le = '00' o '00 00', dependiendo de si se usan campos de corta longitud o de longitud extendida; véase la norma [ISO 7816-4].

Una respuesta APDU con mensajería segura aplicada tendrá la siguiente estructura, dependiendo del caso del comando no securizado correspondiente:

Caso 1o 3: DO '99' || DO '8E' || SW1SW2

Caso 2 o 4 (byte INS par) sin cifrado: DO '81' || DO '99' || DO '8E' || SW1SW2

Caso 2 o 4 (byte INS par) con cifrado: DO '87' || DO '99' || DO '8E' || SW1SW2

Caso 2 o 4 (byte INS impar) sin cifrado: DO 'B3' || DO '99' || DO '8E' || SW1SW2

Nota: El caso 2 o 4 (byte INS impar) con cifrado no se usa nunca en la comunicación entre una VU y una tarjeta.

A continuación figuran tres ejemplos de transformaciones APDU para comandos con código INS par. La figura 8 muestra un comando APDU de caso 4 autenticado, la figura 9 muestra una respuesta APDU de caso 1/caso 3 autenticada, y la figura 10 muestra una respuesta APDU de caso 2/caso 4 cifrada y autenticada.

Figura 8

Transformación de un comando APDU de caso 4 autenticado

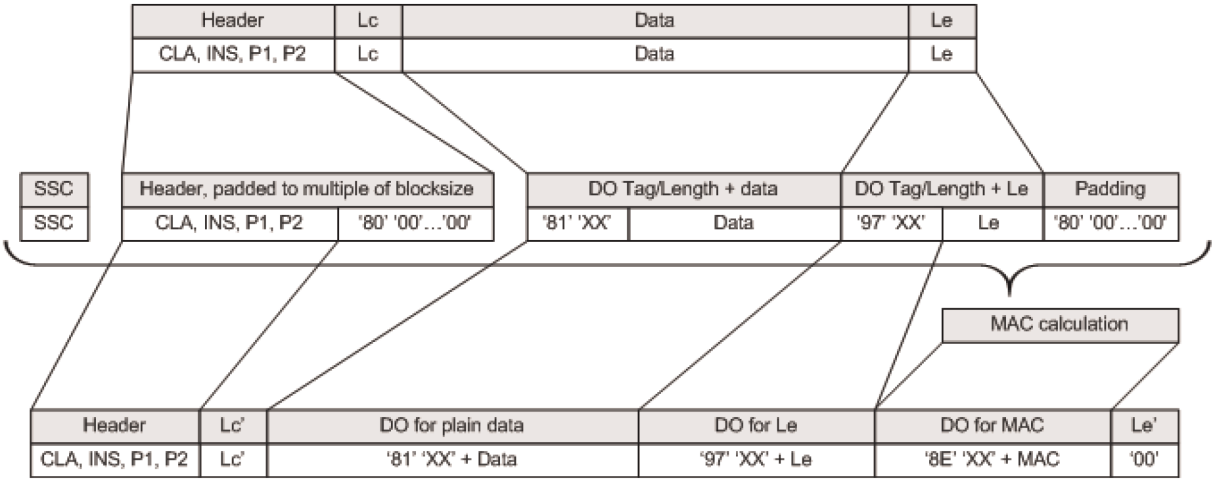


Figura 9

Transformación de una respuesta APDU de caso 1 / caso 3 autenticada

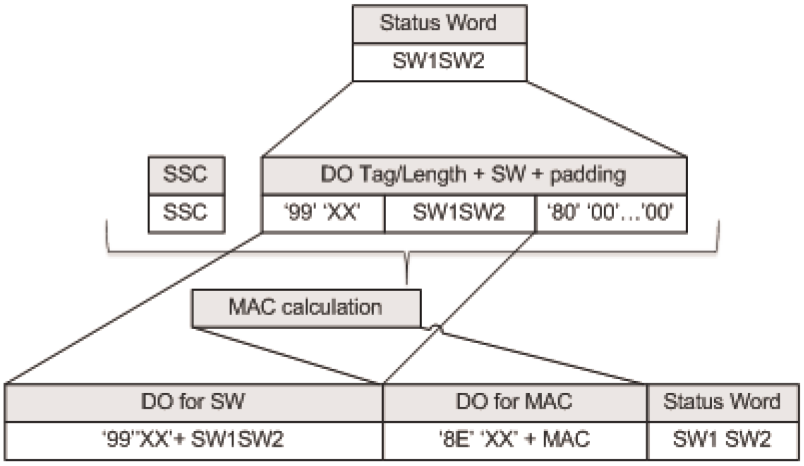
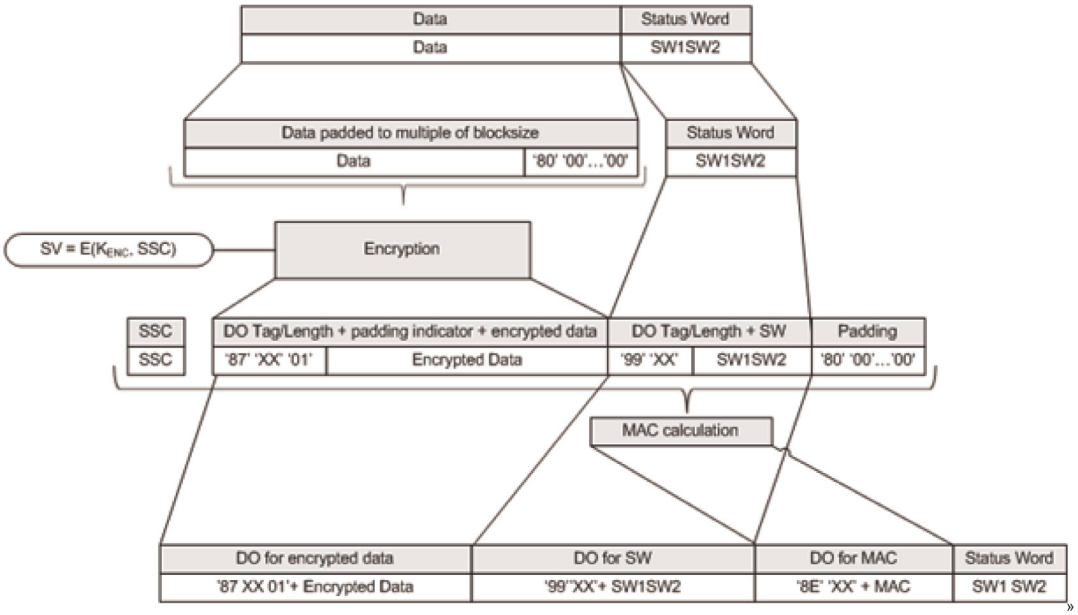


Figura 10

Transformación de una respuesta APDU de caso 2 / caso



»

s) en el apartado 10.5.3, el punto CSM_193 se sustituye por el texto siguiente:

«CSM_193 Una tarjeta de tacógrafo abortará una sesión de mensajería segura en curso solamente si se da una de las condiciones siguientes:

— recibe un comando APDU plano;

— detecta un error de mensajería segura en un comando APDU:

— falta un objeto de datos de mensajería segura esperado, el orden de los objetos de datos es incorrecto, o hay incluido un objeto de datos desconocido;

— un objeto de datos de mensajería segura es incorrecto, por ejemplo, el valor MAC es incorrecto o la estructura TLC es incorrecta;

— no recibe alimentación eléctrica o ha sido restaurada;

— la VU inicia el proceso de autenticación de la VU;

— se ha alcanzado el límite de número de comandos y respuestas asociadas en la sesión actual. Este límite lo definirá para cada tarjeta concreta su fabricante, teniendo en cuenta los requisitos de seguridad del soporte físico utilizado, con un valor máximo de 240 comandos y respuestas asociadas de SM por sesión.»;

t) el apartado 11.3.2 se modifica como sigue:

i) el primer párrafo del punto CSM_208 se sustituye por el texto siguiente:

«Durante el acoplamiento a una VU, un dispositivo GNSS externo utilizará el protocolo ilustrado en la figura 5 (sección 10.2.2) para verificar la cadena de certificados de la VU.»;

ii) el punto CSM_210 se sustituye por el texto siguiente:

«CSM_210 Una vez verificado el certificado VU_MA, el dispositivo GNSS externo almacenará el certificado para utilizarlo durante el funcionamiento normal. Véase el apartado 11.3.3.»;

u) en el apartado 11.3.3, el primer párrafo del punto CSM_211 se sustituye por el texto siguiente:

«Durante el funcionamiento normal, una unidad instalada en el vehículo y una EGF utilizarán el protocolo ilustrado en la figura 11 para verificar la validez temporal del certificado EGF_MA almacenado y para configurar la clave pública VU_MA para la posterior autenticación de la VU. Durante el funcionamiento normal no se efectuará ninguna nueva verificación mutua de las cadenas de certificados.»;

v) en el apartado 12.3, la tabla 6 se sustituye por la siguiente:

«Tabla 6

Número de bytes de datos de texto plano y cifrados por instrucción definido en la norma [ISO 16844-3]

Instrucción	Solicitud/ respuesta	Descripción de los datos	# de bytes de texto plano según la norma [ISO 16844-3]	# de bytes de datos de texto plano mediante claves AES	# de bytes de datos cifrados mediante claves AES de longitud en bits de		
					128	192	256
10	solicitud	Datos de autenticación + número de archivo	8	8	16	16	16
11	respuesta	Datos de autenticación + contenido de archivo	16 o 32, según el archivo	16 o 32, según el archivo	32 / 48	32 / 48	32 / 48
41	solicitud	N.º de serie del sensor	8	8	16	16	16
41	respuesta	Clave de emparejamiento	16	16 / 24 / 32	16	32	32
42	solicitud	Clave de sesión	16	16 / 24 / 32	16	32	32
43	solicitud	Información de emparejamiento	24	24	32	32	32
50	respuesta	Información de emparejamiento	24	24	32	32	32
70	solicitud	Datos de autenticación	8	8	16	16	16
80	respuesta	Valor de contador del sensor + datos de autenticación	8	8	16	16	16»

w) en el apartado 13.1, el requisito relativo al número de serie de la VU que aparece en el punto CSM_224 se sustituye por el texto siguiente:

«**N.º de serie de la VU** el número de serie de la VU o el identificador de la solicitud de certificado (tipo de dato VuSerialNumber o CertificateRequestID), véase CSM_123»;

x) en el apartado 13.3, el apartado 2 del punto CSM_228 se sustituye por el texto siguiente:

«2. La tarjeta de control usará la clave maestra DSRC indicada en combinación con el número de serie de la VU o el identificador de la solicitud de certificado en los datos de seguridad DSRC para derivar las claves DSRC K_VU_{DSRC}_ENC y K_VU_{DSRC}_MAC específicas de la VU, tal como se especifica en CSM_124.»;

y) el apartado 14.3 se modifica como sigue:

i) en el punto CSM_234, el texto que precede a las notas de la figura 13 se sustituye por el texto siguiente:

«Un IDE puede efectuar por sí mismo la verificación de una firma en los datos descargados o utilizar una tarjeta de control a tal efecto. En el caso de que utilice la tarjeta de control, la verificación de la firma se efectuará tal como muestra la Figure 13. Para verificar la validez temporal de un certificado presentado por el IDE, la tarjeta de control utilizará su reloj interno, tal como se especifica en el punto CSM_167. La tarjeta de control actualizará su hora actual si la fecha efectiva de un certificado auténtico de 'fuente válida de hora' es más reciente que la hora actual de la tarjeta. La tarjeta solamente aceptará los certificados siguientes como fuente válida de hora:

— Certificados de enlace ERCA de segunda generación

— Certificados de enlace MSCA de segunda generación

— Certificados VU_Sign o Card_Sign de segunda generación expedidos por el mismo país que el propio certificado de tarjeta de la tarjeta de control.

En el caso de que efectúe la verificación de la firma por sí mismo, el IDE verificará la autenticidad y validez de todos los certificados de la cadena de certificados en el archivo de datos y verificará asimismo la firma en los datos de acuerdo con el esquema de firma definido en la norma [DSS]. En ambos casos, para cada certificado que lea del archivo de datos, es necesario verificar que el campo "Autorización del titular de la tarjeta" (CHA) sea correcto:

— El campo CHA del certificado EQT indicará un certificado de VU o de tarjeta (según proceda) para la firma (véase apéndice 1, tipo de datos EquipmentType).

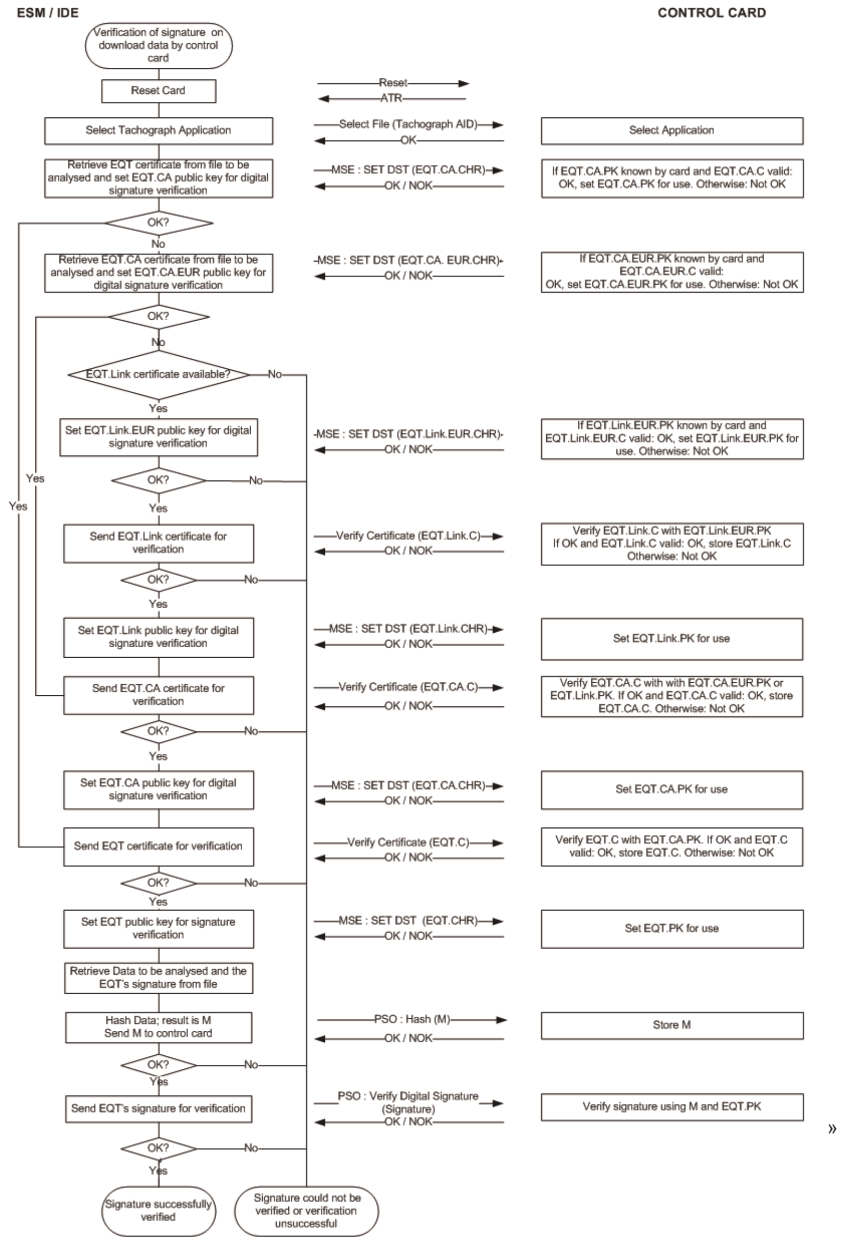
— El campo CHA del certificado EQT.CA indicará una MSCA.

— El campo CHA del certificado EQT.Link indicará una ERCA.»;

ii) la figura 13 se sustituye por lo siguiente:

«*Figura 13*

Protocolo para la verificación de la firma en un archivo de datos descargado



»

37) El apéndice 12 se modifica como sigue:

a) el apartado 3 se modifica como sigue:

i) en el punto GNS_4, el párrafo segundo después del gráfico 2 se sustituye por el texto siguiente:

«La resolución de la posición se basa en el formato de la secuencia RMC anteriormente descrita. La primera parte de los campos 3 y 5 sirve para representar los grados. El resto se emplea para representar los minutos con tres decimales. Por consiguiente, la resolución es de 1/1 000 de minuto o 1/60 000 de grado (puesto que un minuto es 1/60 de un grado).»;

ii) el punto GNS_5 se sustituye por el texto siguiente:

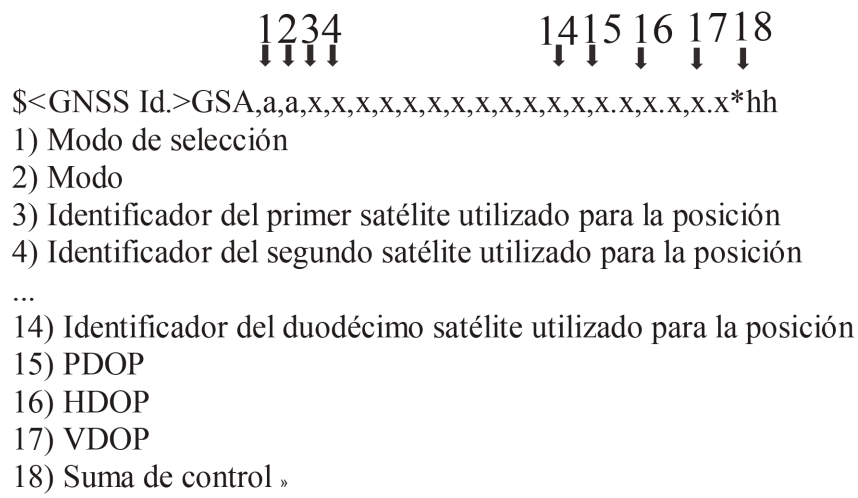
«GNS_5 La unidad instalada en el vehículo almacenará en su base de datos la información de posición relativa a la latitud y a la longitud con una resolución de 1/10 de minuto o 1/600 de grado, tal y como se describe en el apéndice 1 para las geocoordenadas.

La VU puede utilizar el comando DOP del GPS y satélites activos (GSA) para definir y registrar la disponibilidad y la precisión de la señal. En concreto, la HDOP se emplea para facilitar una indicación del nivel de precisión de los datos de localización registrados (véase el apartado 4.2.2). La VU almacenará el valor de la HDOP calculado como el mínimo de los valores HDOP recogidos en los sistemas GNSS disponibles.

El identificador del sistema GNSS indica el identificador NMEA correspondiente a cada sistema satélite y el sistema de aumentación basado en satélites (SBAS).

Gráfico 3

Estructura de la secuencia GSA



iii) el punto GNS_6 se sustituye por el texto siguiente:

«GNS_6 La secuencia GSA se almacenará con el número de registro “02” a “06”.»;

b) el apartado 4.2.1 se modifica como sigue:

i) el punto GNS_16 se sustituye por el texto siguiente:

(no afecta a la versión española)

ii) el punto GNS_18 se sustituye por el texto siguiente:

«GNS_18 Para las funciones 1 (recogida y distribución de datos GNSS), 2 (recogida de los datos de configuración del dispositivo GNSS externo) y 3 (protocolo de administración), el transceptor seguro GNSS simulará una tarjeta inteligente con una arquitectura de archivos del sistema formada por: un archivo principal (MF); un archivo dedicado (DF) con el identificador de aplicación especificado en el apéndice 1, apartado 6.2 ("FF 44 54 45 47 4D") y con tres EF que contengan certificados; y un archivo elemental único (EF.EGF) con el identificador igual a "2F2F", tal y como se describe en la tabla 1.»;

iii) el punto GNS_20 se sustituye por el texto siguiente:

«GNS_20 El transceptor seguro GNSS utilizará una memoria para almacenar los datos y podrá realizar al menos veinte millones de ciclos de escritura/lectura. A excepción de este elemento, el diseño interno y la aplicación del transceptor seguro GNSS queda en manos de los fabricantes.

El mapeado de los números de registro y de los datos se detalla en la tabla 1. Cabe señalarse que hay cinco secuencias GSA para los sistemas satélite y el sistema de aumentación basado en satélites (SBAS).»;

c) en el apartado 4.2.2, el apartado 5 del punto GNS_23 se sustituye por el texto siguiente:

«5. El procesador de la VU verifica los datos recibidos (por ejemplo, latitud, longitud o tiempo) al extraer la información de la secuencia RMC NMEA. La secuencia RMC NMEA incluye la información si la posición es válida. Si la posición no es válida, aún no dispone de datos de localización y no pueden emplearse para registrar la posición del vehículo. Si la posición es válida, el procesador de la VU también extrae los valores de HDOP de las secuencias GSA NMEA y calcula el valor mínimo en los sistemas de satélite disponibles (es decir, cuando se disponga de una posición).»;

d) en el apartado 4.4.1, el punto GNS_28 se sustituye por el texto siguiente:

«GNS_28 Si la VU no consigue comunicarse con el dispositivo GNSS externo acoplado durante más de veinte minutos seguidos, la VU generará y registrará en la VU un incidente de tipo EventFaultType con el valor de la enumeración "0EH"" Communication error with the external GNSS facility" (error de comunicación con el dispositivo GNSS externo) y con la hora en que se produzca como marca de tiempo. El incidente se generará exclusivamente si se cumplen las siguientes dos condiciones: a) el tacógrafo inteligente no está en modo calibración y b) el vehículo está en movimiento. En este contexto, se genera un error de comunicación cuando el transceptor seguro de la VU no recibe ningún mensaje de respuesta tras un mensaje de petición enviado según se describe en el apartado 4.2.»;

e) en el apartado 4.4.2, el punto GNS_29 se sustituye por el texto siguiente:

«GNS_29 Si se ha manipulado el dispositivo GNSS externo, el transceptor seguro GNSS borrará toda su memoria, incluido el material criptográfico. Tal y como se describe en GNS_25 y en GNS_26, la VU detectará la manipulación si se ha enviado un mensaje de respuesta con el estado "6690". A continuación, la VU generará un incidente de tipo EventFaultType con la enumeración "19H Tamper detection of GNSS" (detección de manipulación del GNSS). De manera alternativa, el dispositivo GNSS externo podría no responder a ninguna otra solicitud externa más.»;

f) en el apartado 4.4.3, el punto GNS_30 se sustituye por el texto siguiente:

«GNS_30 Si el transceptor seguro GNSS no recibe datos del receptor GNSS durante más de tres horas seguidas, el transceptor seguro GNSS generará un mensaje de respuesta con el comando READ RECORD (leer registro) con el número de registro "01" y con un campo de datos de 12 bytes, todos ellos fijados en 0xFF. Una vez recibido el mensaje de respuesta con este valor del campo de datos, la VU solamente generará y registrará un incidente de tipo EventFaultType con la enumeración "0DH Absence of position information from GNSS receiver" (ausencia de información de posición del receptor GNSS) y con la hora en que se produzca como marca de tiempo si se cumplen las siguientes dos condiciones: a) el tacógrafo inteligente no está en modo calibración y b) el vehículo está en movimiento.»;

g) en el apartado 4.4.4, el texto del punto GNS_31 hasta el gráfico 4 se sustituye por el texto siguiente:

«Si la VU detecta que el certificado EGF empleado para las autenticaciones mutuas ya no es válido, generará y registrará un fallo del aparato de control de tipo EventFaultType con la enumeración "*1BH External GNSS facility certificate expired*" (certificado del dispositivo GNSS externo expirado) con la hora en que se produzca como marca de tiempo. La VU seguirá utilizando los datos GNSS de posición recibidos.»;

h) en el apartado 5.2.1, el punto GNS_34 se sustituye por el texto siguiente:

«GNS_34 Si la VU no recibe datos del receptor GNSS durante más de tres horas seguidas, solamente generará y registrará un incidente de tipo EventFaultType con la enumeración "0DH Absence of position information from GNSS receiver" (ausencia de información de posición del receptor GNSS) y con la hora en que se produzca como marca de tiempo si se cumplen las siguientes dos condiciones: a) el tacógrafo inteligente no está en modo calibración y b) el vehículo está en movimiento.»;

i) el apartado 6 se sustituye por el texto siguiente:

«6. ERROR DE SINCRONIZACIÓN DEL GNSS

Si la VU detecta una discrepancia de más de un minuto entre el tiempo de la función de medición del tiempo de la unidad instalada en el vehículo y el tiempo procedente del receptor GNSS, generará y registrará un incidente de tipo EventFaultType con la enumeración "*0BH Time conflict (GNSS versus VU internal clock)*" (discrepancia temporal entre el GNSS y el reloj interno de la VU). Cuando se produzca una discrepancia temporal, la VU no comprobará el desajuste hasta pasadas doce horas. Este incidente no se producirá cuando no hubiera una señal GNSS válida detectable por el receptor GNSS en los últimos treinta días.».

38) El apéndice 13 se modifica como sigue:

a) en el apartado 2, el párrafo cuarto se sustituye por el texto siguiente:

«A efectos de aclaración, el presente apéndice no especifica:

— La operación y gestión de la recogida de *los datos* en la VU (que se especificarán en otro punto del *Reglamento*, o que de otra manera serán una función del diseño del producto).

— La forma de presentación de los datos recogidos a la aplicación alojada en el dispositivo externo.

— Las disposiciones sobre seguridad de los datos más allá de la proporcionada por Bluetooth® (como el cifrado) en lo que se refiere al contenido de *los datos* [que se especificarán en otro punto del *Reglamento* (apéndice 11, Mecanismos de seguridad comunes)].

— Los protocolos Bluetooth® usados por la interfaz ITS.»;

b) en el apartado 4.2, el párrafo tercero se sustituye por el texto siguiente:

«Cuando un dispositivo externo entra dentro del radio de alcance de la VU por primera vez, puede iniciarse el proceso de emparejamiento de Bluetooth® (véase también el anexo 2). Los dispositivos comparten sus direcciones, nombres y perfiles y clave secreta común, que les permite conectarse cada vez que entren en contacto en el futuro. Una vez finalizado este paso, el dispositivo externo es de confianza y está en situación de iniciar solicitudes de descarga de datos del tacógrafo. No está previsto añadir mecanismos de cifrado más allá de los facilitados por Bluetooth®. No obstante, si se necesitan mecanismos de seguridad adicionales se procederá de conformidad con lo establecido en el apéndice 11, Mecanismos de seguridad comunes.»;

c) el apartado 4.3 se modifica como sigue:

i) el párrafo primero se sustituye por el texto siguiente:

«Por razones de seguridad, la VU requerirá un sistema de autorización mediante código PIN separado del emparejamiento Bluetooth. Cada VU será capaz de generar códigos PIN con fines de autenticación compuestos de al menos cuatro cifras. Cada vez que un dispositivo externo se empareje con la VU deberá introducir el código PIN correcto antes de recibir datos.»;

ii) el párrafo tercero después de la tabla 1 se sustituye por el texto siguiente:

(no afecta a la versión española)

d) en el apartado 4.4, el segundo párrafo que aparece después del encabezamiento «Campo de datos» se sustituye por el texto siguiente:

«Si los datos que hay que gestionar son mayores que el espacio disponible en un mensaje, se dividirán entre varios submensajes. Cada submensaje tendrá la misma cabecera y SID, pero contendrá un contador de 2 bytes, Counter Current (CC) y Counter Max (CM), para indicar el número de submensajes. Al objeto de permitir la verificación de errores y la cancelación, el dispositivo receptor confirma cada uno de los submensajes. El dispositivo de recepción puede aceptar el submensaje, solicitar su retransmisión, pedir al dispositivo de envío que comience de nuevo o abortar la transmisión.»;

e) el anexo 1 se modifica como sigue:

i) el título se sustituye por el texto siguiente:

«1) LISTA DE DATOS DISPONIBLES A TRAVÉS DE LA INTERFAZ ITS»;

ii) se inserta el siguiente elemento en el cuadro del punto 3, después del elemento «Ausencia de información de posición del receptor del GNSS»:

«Error de comunicación con el dispositivo GNSS externo	— el incidente de mayor duración ocurrido cada uno de los últimos 10 días, — los 5 incidentes de mayor duración ocurridos en los últimos 365 días.	— fecha y hora de comienzo del incidente, — fecha y hora de finalización del incidente, — tipo de tarjeta(s), número, Estado miembro emisor y generación de cualquier tarjeta insertada al comenzar o al terminar el incidente, — número de incidentes similares ocurridos ese día.»

iii) en el punto 5, se añade el guion siguiente:

«— fallo de la interfaz ITS (si procede)»;

f) las especificaciones ASN.1 del anexo 3 se modifican como sigue:

i) se insertan las siguientes filas 206a a 206e tras la fila 206:

```
»206a
206b       DriverID ::= SEQUENCE{
206c       issuingMemberState OCTET STRING (SIZE(3)),
206d       cardNumber OCTET STRING (SIZE(16))
206e }»;
```

ii) las filas 262 a 264 se sustituyen por lo siguiente:

```
«262    driveRecognize BIT STRING ('00'B UNION '01'B),
263     driverCardDriver1 BIT STRING ('00'B UNION '01'B),
264     driverCardDriver2 BIT STRING ('00'B UNION '01'B), »;
```

iii) la fila 275 se sustituye por lo siguiente:

```
«275    outOfScopeCondition BIT STRING ('00'B UNION '01'B),«;
```

iv) las filas 288 a 310 se sustituyen por lo siguiente:

```
«288    driver1WorkingState BIT STRING ('000'B UNION '001'B UNION '010'B UNION
289     '011'B UNION '100'B UNION '101'B …),
290     driver2WorkingState BIT STRING ('000'B UNION '001'B UNION '010'B UNION
291     '011'B UNION '100'B UNION '101'B …),
292
293     driver1TimeRelatedStates BIT STRING ('0000'B UNION '0001'B
294     UNION '0010'B UNION '0011'B UNION '0100'B UNION '0101'B UNION
295     '0110'B UNION '0111'B UNION '1000'B UNION '1001'B UNION '1010'B
296     UNION '1011'B UNION '1100'B UNION '1101'B …),
297
298
299     driver2TimeRelatedStates BIT STRING ('0000'B UNION '0001'B
300     UNION '0010'B UNION '0011'B UNION '0100'B UNION '0101'B UNION
301     '0110'B UNION '0111'B UNION '1000'B UNION '1001'B UNION '1010'B
302     UNION '1011'B UNION '1100'B UNION '1101'B …),
303
304
305
306     overSpeed BIT STRING ('00 'B UNION '01 'B),
307     driver1Identification DriverID,
308     driver2Identification DriverID,
309
310»
```

v) las filas 362 y 363 se sustituyen por lo siguiente:

```
«362    driver1MaximumDailyDrivingTime BIT STRING (SIZE(4)),
363     driver2MaximumDailyDrivingTime BIT STRING (SIZE(4)),»;
```

vi) se insertan las siguientes filas 410a y 410b tras la fila 410:

```
«410a   comErrorWithExternalGNSSFacility
410b    CommunicationErrorWithTheExternalGNSSFacility,»;
```

vii) se insertan las siguientes filas 539a a 539j tras la fila 539:

```
«539a     CommunicationErrorWithTheExternalGNSSFacility ::= SEQUENCE{
539b      beginDate GeneralizedTime,
539c      endDate GeneralizedTime,
539d      cardsType SEQUENCE OF UTF8String,
539e      cardsNumber SEQUENCE OF INTEGER,
539f      issuingMemberState SEQUENCE OF NationAlpha,
539g      cardsGeneration SEQUENCE OF INTEGER,
539h      numberOfSimilarEvent INTEGER
539i            }
539j»;
```

39) El apéndice 14 se modifica como sigue:

a) el apartado 5.5 del índice se sustituye por el siguiente:

«5.5 Cumplimiento de la Directiva (UE) 2015/719 ..... p. 490»;

b) en el apartado 2, el párrafo tercero se sustituye por el texto siguiente:

«En estas circunstancias, el tiempo de que se dispone para la comunicación es limitado porque *la Comunicación* es específica y tiene un diseño de corto alcance. Además, las autoridades de control competentes pueden aprovechar el mismo medio de comunicación utilizado en la supervisión a distancia de tacógrafos (RTM) para otras aplicaciones [como los pesos máximos y las dimensiones de vehículos pesados que se establecen en la Directiva (UE) 2015/719] y estas operaciones pueden realizarse por separado o de manera consecutiva según el criterio de las autoridades de control competentes.»;

c) el apartado 5.1 se modifica como sigue:

i) en el punto DSC_19, el duodécimo guion se sustituye por el texto siguiente:

«— La antena de la DSRC-VU se colocará en una posición en la que optimice la comunicación DSRC entre el vehículo y la antena del lector del lado de la carretera, cuando el lector esté instalado a quince metros de distancia por delante del vehículo y a dos metros de altura, apuntando al centro vertical y horizontal del parabrisas. En vehículos ligeros, puede instalarse perfectamente en la parte superior del parabrisas. En el caso de los demás vehículos, la antena de la DSRC se instalará, bien cerca la parte inferior del parabrisas, o bien cerca de su parte superior.»;

ii) en el punto DSC_22, el párrafo primero se sustituye por el texto siguiente:

«El factor de forma de la antena no se define y constituirá una decisión comercial, siempre que la DSRC-VU instalada cumpla los requisitos de conformidad establecidos en la sección 5. La antena se colocará del modo establecido en DSC_19 y responderá de manera eficaz a los ejemplos de uso descritos en los apartados 4.1.2 y 4.1.3.»;

d) en el apartado 5.4.3, la secuencia 7 se sustituye por el texto siguiente:

(no afecta a la versión española)

e) en el apartado 5.4.4, la definición del módulo ASN.1 del punto DCS_40 se modifica como sigue:

i) la primera línea de la secuencia para `TachographPayload` se sustituye por el texto siguiente:

```
«tp15638VehicleRegistrationPlate LPN – Vehicle Registration Plate as per EN 15509[1]»
```

ii) se añade la siguiente nota 1:

«1. si una LPN contiene un AlphabetIndicator LatinAlphabetNo2 o latinCyrillicAlphabet, los caracteres especiales se remapean en la unidad del interrogador de carretera aplicando normas especiales de acuerdo con el anexo E de la norma ISO/DIS 14 906,2.»;

iii) se elimina el superíndice 2 de la línea «Timestamp of current record»;

iv) la definición de `RtmTransferAck` del módulo ASN.1 se sustituye por la siguiente:

```
«RtmTransferAck ::= INTEGER {
                    Ok (1),
                    NoK (2)
                    } (1..255)»;
```

f) en el apartado 5.4.5, el elemento RTM12 del cuadro 14.3 se sustituye por lo siguiente:

«**RTM12** **Fallo de sensor**	La VU generará un valor entero para el elemento de datos RTM12. La VU deberá asignar a la variable sensorFault un valor de: — 1 si se ha registrado un incidente de tipo '35'H Fallo de sensor en los últimos diez días — 2 si se ha registrado un incidente de tipo Fallo del receptor GNSS (interno o externo con valores de enumeración '36'H o '37'H) en los diez últimos días — 3 si se ha registrado un incidente del tipo '0E'H Error de comunicación con el dispositivo GNSS externo en los diez últimos días — 4 si se han registrado fallos tanto del sensor como del receptor GNSS en los diez últimos días — 5 si se han registrado incidentes tanto de tipo Fallo del sensor como de tipo Error de comunicación con el dispositivo GNSS externo en los diez últimos días — 6 si se han registrado incidentes tanto de tipo Fallo del receptor GNSS como de tipo Error de comunicación con el dispositivo GNSS externo en los diez últimos días — 7 si se han registrado fallos en los tres sensores en los diez últimos días DE LO CONTRARIO, deberá asignarse un valor de 0 si no se han registrado incidentes en los diez últimos días	–fallo del sensor un octeto según el diccionario de datos	`sensorFault INTEGER (0..255),;` »

g) en el apartado 5.4.6, el punto DSC_43 se sustituye por el texto siguiente:

«DSC_43 En todos los intercambios DSRC, los datos se codificarán utilizando PER (Reglas de Codificación por Paquetes) NO ALINEADAS, excepto por lo que se refiere a `TachographPayload` y `OwsPayload`;, que se codificarán utilizando OER (Reglas de Codificación por Octetos), definidas en la norma ISO/CEI 8825-7, Rec. ITU-T X.696.»;

h) en el apartado 5.4.7, en la cuarta columna del cuadro 14.9, el texto en la celda que describe `Rtm-ContextMark`; se sustituye por el texto siguiente:

«Identificador de objeto de la norma admitida, parte y versión. Ejemplo: ISO (1) Standard (0) TARV (15638) part9 (9) Version1 (1).

El primer octeto es 06H, que es el identificador del objeto. El segundo octeto es 06H, que es su longitud. Los seis octetos siguientes codifican el identificador de objeto de ejemplo.»;

i) los apartados 5.5 y 5.5.1 se sustituyen por el texto siguiente:

«5.5 **Cumplimiento de la Directiva (UE) 2015/719**

5.5.1 *Resumen*

DSC_59 Con el fin de cumplir la Directiva (UE) 2015/719, relativa a las dimensiones y los pesos máximos de vehículos pesados, el protocolo de transacciones para descargar los datos OWS a través de un enlace de interfaz DSRC de 5,8 GHz será el mismo que el utilizado para los datos RTM (véase el apartado 5.4.1), con la salvedad de que el identificador de objetos que se refiere a la norma TARV se ajustará a la parte 20 de la norma ISO 15638 (TARV) relativa a WOB/OWS.»;

j) en el apartado 5.6.1, la letra a) del punto DSC_68 se sustituye por el texto siguiente:

«a) con el fin de poder contratar a varios proveedores el suministro de la VU y la DSRC-VU, e incluso diferentes lotes de DSRC-VU, la conexión entre la VU y la DSRC-VU no interna será una conexión de norma abierta. La VU se conectará con la DSRC-VU:»;

k) en el apartado 5.7.1, el punto DSC_77 se sustituye por el texto siguiente:

«DSC_77 *Los Datos* deberán ser suministrados, ya protegidos, por la función *VUSM* a la *DSRC-VU*. La *VUSM* verificará que los datos registrados en la *DSRC-VU* se han grabado correctamente. El registro y la notificación de errores en la transferencia de datos de la *VU* a la memoria de la *DSRC-VU* se llevarán a cabo con el tipo EventFaultType y el valor de enumeración fijado en '0C'H Error de comunicación con el dispositivo de comunicación a distancia, junto con la indicación temporal.».

40) El apéndice 15 se modifica como sigue:

a) el primer párrafo del apartado 2.2 se sustituye por el texto siguiente:

«Se entiende que las tarjetas de tacógrafo de primera generación son interoperables con las unidades instaladas en el vehículo de primera generación [de conformidad con el anexo IB del Reglamento (CEE) n.º 3821/85], mientras que las tarjetas de tacógrafo de segunda generación son interoperables con las unidades instaladas en el vehículo de segunda generación, de conformidad con el anexo IC del presente Reglamento. Asimismo, serán de aplicación los siguientes requisitos:»;

b) en el apartado 2.4.1, el punto MIG_11 queda modificado como sigue:

i) el primer guion se sustituye por el texto siguiente:

«— EF (archivos elementales) IC e ICC no firmados (opcional),»;

ii) el tercer guion se sustituye por el texto siguiente:

«— el resto de EF con datos de aplicación (dentro del DF tacógrafo) requeridos por el protocolo de transferencia de datos de la tarjeta de primera generación. Esta información debe estar protegida con una firma digital, conforme a los mecanismos de seguridad de la primera generación.

Dicha trasferencia de datos no incluirá EF con datos de aplicación solo presentes en las tarjetas de conductor (y de taller) de segunda generación (EF con datos de aplicación dentro del DF tacógrafo_G2).»;

c) en el apartado 2.4.3, los puntos MIG_014 y MIG_015 se sustituyen por el texto siguiente:

«MIG_014 Fuera del marco de la supervisión del conductor realizada por las autoridades de control de países no pertenecientes a la UE, los datos serán transferidos desde las unidades instaladas en el vehículo de segunda generación utilizando los mecanismos de seguridad de segunda generación, y el protocolo de transferencia de datos especificado en el apéndice 7 del presente anexo.

MIG_015 Para permitir el control de los conductores por parte de autoridades de control no pertenecientes a la UE, también podría ser posible la opción de realizar la trasferencia de datos desde unidades instaladas en el vehículo de segunda generación utilizando los mecanismos de seguridad de la primera generación. Los datos transferidos deberán tener entonces el formato de los datos transferidos desde una unidad instalada en el vehículo de primera generación. Esta capacidad podrá seleccionarse mediante los comandos del menú.».

ANEXO II

El anexo II del Reglamento (UE) 2016/799 se modifica como sigue:

1) En el capítulo I, apartado 1, la letra b) se sustituye por el texto siguiente:

«b) un número de homologación correspondiente al número del certificado de homologación que se haya asignado al prototipo del aparato de control o de la hoja de registro o de la tarjeta de tacógrafo, colocado en cualquier posición cerca del rectángulo.».

2) En el capítulo III, el punto 5 se sustituye por el texto siguiente:

«5. Presentado para su homologación el .....».

3) En el capítulo IV, el punto 5 se sustituye por el texto siguiente:

«5. Presentado para su homologación el .....».