Allegato 1 *al Regolamento UE n. 502/2018*

L'allegato IC del regolamento (UE) 2016/799 è così modificato:
1) l'indice è così modificato:
a) il punto 3.12.5 è sostituito dal s*eguente:*
*«3.12.5. Luoghi e posizioni dove iniziano e terminano i periodi di lavoro giornalieri e/o dove il periodo di guida cumulativo raggiung*e le 3 ore»;
b) il punto 4.5.3.2.16 è sostituito dal s*eguente:*
*«4.5.3.2.16 Dati relativi al luogo in cui si raggiungono le tre ore cumulativ*e di guida»;
c) il punto 4.5.4.2.14 è sostituito dal s*eguente:*
*«4.5.4.2.14 Dati relativi al luogo in cui si raggiungono le tre ore cumulativ*e di guida»;
d) il punto 6.2 è sostituito dal s*eguente:*
«6.2 Verifica dei componenti nuovi o riparati»;
2) il punto 1 è così modificato:
a) la definizione ll) è sostituita dalla s*eguente:*
*«ll) "dispositivo di comunicazione remota" o "dispositivo di diagnosi precoce remota", le dotazioni dell'unità elettronica di bordo utilizzate per svolgere controlli su stra*da mirati;»;
b) la definizione tt) è sostituita dalla s*eguente:*
«tt) «regolazione dell'ora», una regolazione dell'ora corrente; tale regolazione può essere automatica a intervalli regolari e usare come riferimento l'ora indicata dal ricevitore GNSS, oppure può essere effettuata nella modalità di taratura;»;
c) alla definizione yy), il primo trattino è sostituito dal s*eguente:*
*«- è montato e utilizzato soltanto sui veicoli delle categorie M1 e N1 (quali definiti nell'allegato II della direttiva 2007/46/CE del Parlamento europeo e del Consiglio (*), come modificata d*a ultimo);»;
d) è aggiunta una nuova definizio*ne fff):*
«fff) "periodo di guida cumulativo", un valore che rappresenta il totale cumulativo dei minuti di guida di un certo veicolo.
Il valore del periodo di guida cumulativo è un conteggio cumulativo di tutti i minuti considerati DI GUIDA dalla funzione di verifica delle attività di guida dell'apparecchio di controllo ed è utilizzato solo per attivare la memorizzazione della posizione del veicolo ogni volta che viene raggiunto un multiplo di tre ore cumulative di guida. Il conteggio cumulativo è avviato all'attivazione dell'apparecchio di controllo e non è influenzato da altre condizioni, come le condizioni«escluso dal campo di applicazione» o «attraversamento mediante traghetto/treno».
Il periodo di guida cumulativo non è destinato ad essere visualizzato, stampato o scaricato;»;
3) al punto 2.3, l'ultimo trattino del paragrafo 13 è sostituito dal s*eguente:*
«- in condizioni di funzionamento normali le unità elettroniche di bordo hanno un periodo di validità di 15 anni dalla data di efficacia dei relativi certificati, ma possono essere utilizzate per ulteriori 3 mesi per il solo trasferimento dei dati.»;
4) al punto 2.4, il primo comma è sostituito dal s*eguente:*
*«La sicurezza del sistema è intesa a proteggere la memoria di dati in modo da impedire l'accesso non autorizzato, la manipolazione dei dati e rilevarne eventuali tentativi, nonché da proteggere l'integrità e l'autenticità dei dati scambiati tra sensore di movimento e unità elettronica di bordo, l'integrità e l'autenticità dei dati scambiati tra l'apparecchio di controllo e le carte tachigrafiche, l'integrità e l'autenticità dei dati scambiati tra l'unità elettronico di bordo e il dispositivo GNSS esterno, se presente, la riservatezza, l'integrità e l'autenticità dei dati scambiati per finalità di controllo tramite la comunicazione remota a fini di diagnosi precoce e da verificare l'integrità e l'autenticità dei dati t*rasferiti.»;
5) al punto 3.2, il secondo trattino del paragrafo 27 è sostituito dal s*eguente:*
*«- delle posizioni dove il periodo di guida cumulativo raggiunge un multiplo d*i tre ore;»;
6) al punto 3.4, il paragrafo 49 è sostituito dal s*eguente:*
«49) Il primo passaggio di attività a INTERRUZIONE/RIPOSO o DISPONIBILITÀ che si verifica entro 120 secondi dalla selezione automatica di LAVORO dovuta all'arresto del veicolo va considerato avvenuto al momento dell'arresto del veicolo (annullando eventualmente il passaggio a LAVORO).»;
7) al punto 3.6.1, il paragrafo 59 è sostituito dal s*eguente:*
«59) Il conducente deve quindi immettere il luogo in cui si trova il veicolo in quel momento, che è considerato come un dato temporaneo.
Alle condizioni riportate di seguito sono convalidati (e quindi non saranno più sovrascritti) i dati temporanei immessi per ultimi prima dell'estrazione della carta:

- l'immissione relativa al luogo in cui inizia il periodo di lavoro giornaliero in corso durante l'immissione manuale conformemente al requisito 61;
- l'immissione successiva relativa al luogo in cui inizia il periodo di lavoro giornaliero in corso se il titolare della carta non immette alcun luogo di inizio o fine del periodo di lavoro nel corso dell'immissione manuale conformemente al requisito 61;
Alle condizioni riportate di seguito i dati temporanei immessi per ultimi prima dell'estrazione della carta sono sovrascritti e viene convalidato il nuovo valore:
*- l'immissione successiva relativa al luogo in cui finisce il periodo di lavoro giornaliero in corso se il titolare della carta non immette alcun luogo di inizio o fine del periodo di lavoro nel corso dell'immissione manuale conformemente al req*uisito 61.»;
8) al punto 3.6.2, il sesto e il settimo trattino sono sostituiti dai s*eguenti:*
«- il luogo in cui si è concluso il precedente periodo giornaliero di lavoro associato all'ora corrispondente (che va a sostituire e convalidare il dato inserito al momento dell'ultima estrazione della carta);
*- il luogo in cui ha inizio il periodo giornaliero di lavoro in corso associato all'ora corrispondente (che va a convalidare il dato temporaneo inserito al momento dell'ultima estrazione del*la carta).»;
9) il punto 3.9.15 è sostituito dal s*eguente:*
«3.9.15 Anomalia "Conflitto di orari"
*86) Questa anomalia deve attivarsi, quando non è attiva la modalità di taratura, quando la VU rileva una discrepanza di più di 1 minuto tra l'orario della funzione di misurazione del tempo dell'unità elettronica di bordo e l'orario proveniente dal ricevitore GNSS. Questa anomalia è registrata unitamente al valore dell'orologio interno dell'unità elettronica di bordo e accompagna un meccanismo automatico di regolazione dell'ora. Dopo che si è attivata un'anomalia 'Conflitto di orari', la VU non attiva altre anomalie dello stesso tipo per le successive 12 ore. Questa anomalia non deve attivarsi qualora nei precedenti 30 o più giorni non fosse rilevabile alcun segnale GNSS valido dal ricev*itore GNSS.»;
10) al punto 3.9.17 è aggiunto il trattino s*eguente:*
*«- guasto dell'interfaccia ITS (se ap*plicabile)»;
11) il punto 3.10 è così modificato:
i) al paragrafo 89, il testo che precede la tabella è sostituito dal s*eguente:*
«*L'apparecchio di controllo deve rilevare i guasti mediante prove automatiche e prove incorporate, secondo la tabella* seguente:»;
ii) alla tabella è aggiunta la riga seguente:"

«*Interfaccia ITS (opzionale)*	*Funzionamento corretto*»	

12) il secondo trattino del punto 3.12 è sostituito dal s*eguente:*
«- il numero medio di posizioni per ciascun giorno è inteso come almeno 6 posizioni in cui inizia il periodo di lavoro giornaliero, 6 posizioni in cui il periodo di guida cumulativo raggiunge un multiplo di tre ore e 6 posizioni in cui termina il periodo di lavoro giornaliero, per cui «365 giorni» comprende almeno 6570 posizioni,»;
13) il punto 3.12.5 è così modificato:
a) il titolo e il paragrafo 108 sono sostituiti dai s*eguenti:*
«3.12.5. Luoghi e posizioni dove iniziano e terminano i periodi di lavoro giornalieri e/o dove il periodo di guida cumulativo raggiunge le 3 ore
108) L'apparecchio di controllo deve registrare e memorizzare nella sua memoria di dati:
- i luoghi e le posizioni in cui il conducente e/o il secondo conducente iniziano il loro periodo di lavoro giornaliero;
- le posizioni in cui il periodo di guida cumulativo raggiunge un multiplo di tre ore;
*- i luoghi e le posizioni in cui il conducente e/o il secondo conducente terminano il loro periodo di lavoro gi*ornaliero.»;
b) il quarto trattino del paragrafo 110 è sostituito dal s*eguente:*
*«- il tipo di immissione (inizio, fine o 3 ore di periodo di guida cu*mulativo),»;
c) il paragrafo 111 è sostituito dal s*eguente:*
«111) La memoria di dati deve essere in grado di conservare per almeno 365 giorni i luoghi e le posizioni in cui iniziano e terminano i periodi di lavoro giornalieri e/o in cui il periodo di guida cumulativo raggiunge le 3 ore.»;
14) al punto 3.12.7, il paragrafo 116 è sostituito dal s*eguente:*
*«116) L'apparecchio di controllo deve registrare e memorizzare nella sua memoria di dati la velocità istantanea del veicolo e la data e l'ora di registrazione ogni secondo per almeno le ultime 24 ore di marcia de*l veicolo.»;
15) al punto 3.12.8 la tabella è così modificata:
a) la seguente voce è inserita tra *le voci «Assenza di informazioni sulla posizione provenienti dal ricev*itore *GNSS»*

e «Errore dei dati di movimento»:

«*Errore di comunicazione con il dispositivo GNSS esterno*	*- l'anomalia di maggiore durata per ciascuno degli ultimi 10 giorni in cui si è verificata,* *- le 5 anomalie di maggiore durata nel corso degli ultimi 365 giorni.*	*- data e ora di inizio dell'anomalia,* *- data e ora di fine dell'anomalia,* *- tipo, numero, Stato membro di rilascio e generazione delle carte inserite all'inizio e/o alla fine dell'anomalia,* *- numero di anomalie simili nel giorno in questione.*»

b) la voce "Dati contrastanti sull'ora" è sostituita dalla seguente:

«*Dati contrastanti sull'ora*	*- l'anomalia più grave per ciascuno degli ultimi 10 giorni in cui si è verificata (ovvero l'anomalia con la differenza maggiore tra data e ora dell'apparecchio di controllo e data e ora del GNSS).* *- le 5 anomalie più gravi nel corso degli ultimi 365 giorni.*	*- data e ora dell'apparecchio di controllo,* *- data e ora del GNSS,* *- tipo, numero, Stato membro di rilascio e generazione delle carte inserite all'inizio e/o alla fine dell'anomalia,* *- numero di anomalie simili nel giorno in questione.*»

16) al punto 3.20, il paragrafo 200 è sostituito dal s*eguente:*

*«200) L'apparecchio di controllo può anche essere munito di interfacce standardizzate che consentano di usare i dati registrati o generati dal tachigrafo nella modalità di funzionamento o di taratura mediante un dispositivo esterno. Nell'appendice 13 è specificata e standardizzata un'interfaccia ITS opzionale. Altre interfacce dell'unità elettronica di bordo possono coesistere, purché siano pienamente conformi ai requisiti dell'appendice 13 in termini di elenco minimo dei dati, sicurezza e consenso del conducente. Il consenso del conducente non riguarda i dati trasmessi dall'apparecchio di controllo alla rete del veicolo. Se i dati personali immessi nella rete del veicolo sono ulteriormente trattati al di fuori della rete del veicolo, è responsabilità del costruttore del veicolo accertarsi che la procedura di trattamento dei dati personali sia conforme al regolamento (UE) 2016/679 («regolamento generale sulla protezion*e dei dati»).

Il consenso del conducente non riguarda nemmeno i dati del tachigrafo trasferiti a un'impresa remota (requisito 193), poiché un tale scenario sarebbe controllato tramite i diritti di accesso della carta dell'azienda.

I seguenti requisiti si applicano ai dati ITS resi disponibili mediante tale interfaccia:

- tali dati sono una serie di dati esistenti scelti dal dizionario di dati del tachigrafo (appendice 1),
- un sottoinsieme di tali dati scelti è contrassegnato come "dati personali",
- il sottoinsieme "dati personali" è disponibile solo se è abilitato il consenso verificabile del conducente, con cui egli accetta che i propri dati personali possano lasciare la rete del veicolo,
- in qualsiasi momento il consenso del conducente può essere abilitato o disabilitato con i comandi del menù, purché la carta del conducente sia inserita,
- l'insieme e il sottoinsieme di dati sono trasmessi tramite protocollo wireless Bluetooth nel raggio della cabina del veicolo, con una frequenza di aggiornamento di 1 minuto,
- l'abbinamento del dispositivo esterno con l'interfaccia ITS è protetto da un PIN dedicato e casuale di almeno 4 cifre, registrate e disponibili mediante il dispositivo di visualizzazione di ciascuna unità elettronica di bordo,
- in ogni caso, la presenza dell'interfaccia ITS non deve perturbare o pregiudicare il corretto funzionamento e la sicurezza dell'unità elettronica di bordo.

Si possono trasmettere anche altri dati in aggiunta all'insieme di dati esistenti scelti, considerato l'elenco minimo, a condizione che tali dati non si possano considerare dati personali.

L'apparecchio di controllo deve essere in grado di comunicare lo stato del consenso del conducente ad altre piattaforme presenti nella rete del veicolo.

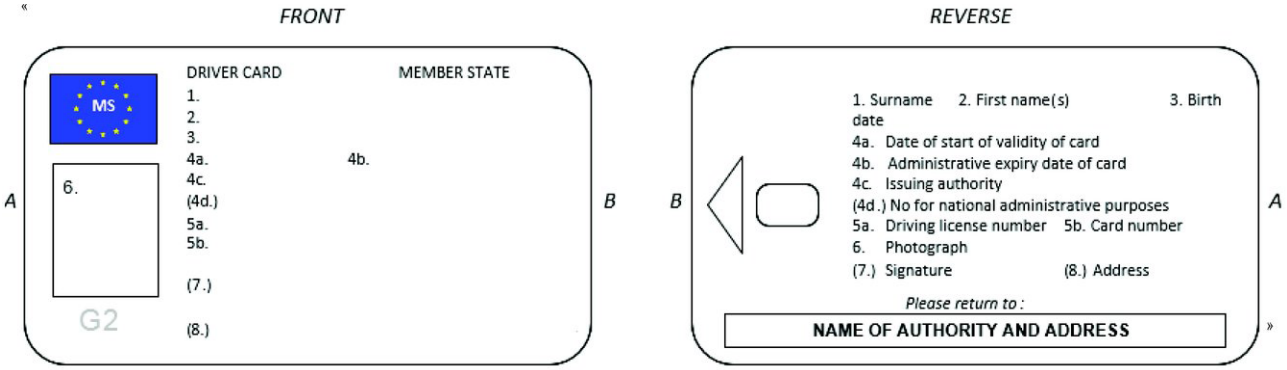
Quando l'accensione del veicolo è inserita, la trasmissione di tali dati deve essere continua.»

17) al punto 3.23, il paragrafo 211 è sostituito dal s*eguente:*

*«211) Le impostazioni dell'ora dell'orologio interno della VU devono essere regolate automaticamente ogni 12 ore. Se non è possibile regolare l'ora perché il segnale GNSS non è disponibile, la regolazione deve avvenire non appena la VU può accedere a un orario valido fornito dal ricevitore GNSS, secondo le condizioni di accensione del veicolo. Il riferimento temporale per l'impostazione automatica dell'ora dell'orologio interno della VU deve essere costituito dal ricevi*tore GNSS.»;

18) al punto 3.26, i paragrafi 225 e 226 sono sostituiti dai s*eguenti:*

«225) Una targhetta segnaletica deve essere affissa su ogni componente distinto dell'apparecchio di controllo e deve riportare le indicazioni seguenti:
- nome ed indirizzo del fabbricante,
- codice componente del fabbricante e anno di fabbricazione,
- numero di serie,
- marchio di omologazione.
226) Qualora lo spazio fisico non sia sufficiente per riportare tutte le indicazioni summenzionate, sulla targhetta segnaletica devono figurare almeno: il nome o il logo del fabbricante e il codice componente.»;
19) al punto 4.1 il disegno corrispondente al fronte e retro della carta del conducente è sostituito dal seguente:
«



»
20) al punto 4.5.3.1.8 il primo trattino del paragrafo 263 è sostituito dal s*eguente:*
*«- guasto della carta (se questa carta è l'oggetto de*l guasto),»;
21) al punto 4.5.3.2.8 il primo trattino del paragrafo 288 è sostituito dal s*eguente:*
*«- guasto della carta (se questa carta è l'oggetto de*l guasto),»;
22) il punto 4.5.3.2.16 è sostituito dal s*eguente:*
«4.5.3.2.16 Dati relativi al luogo in cui si raggiungono le tre ore cumulative di guida
305) La carta del conducente deve essere in grado di memorizzare i seguenti dati relativi alla posizione del veicolo quando il periodo di guida cumulativo del conducente raggiunge un multiplo di tre ore:
- la data e l'ora in cui il periodo di guida cumulativo raggiunge un multiplo di tre ore,
- la posizione del veicolo,
- l'accuratezza del GNSS, la data e l'ora in cui la posizione è stata determinata,
- il valore dell'odometro del veicolo.
*306) La carta del conducente deve essere in grado di memorizzare almeno 252 di tali regi*strazioni.»;
23) il punto 4.5.4.2.14 è sostituito dal s*eguente:*
«4.5.4.2.14 Dati relativi al luogo in cui si raggiungono le tre ore cumulative di guida
353) La carta dell'officina deve essere in grado di memorizzare i seguenti dati relativi alla posizione del veicolo quando il periodo di guida cumulativo del conducente raggiunge un multiplo di tre ore:
- la data e l'ora in cui il periodo di guida cumulativo raggiunge un multiplo di tre ore,
- la posizione del veicolo,
- l'accuratezza del GNSS, la data e l'ora in cui la posizione è stata determinata,
- il valore dell'odometro del veicolo.
*354) La carta dell'officina deve essere in grado di memorizzare almeno 18 di tali regi*strazioni.»;
24) al punto 5.2, il paragrafo 396 è sostituito dal s*eguente:*
«396) Sulla targhetta devono essere riportate almeno le indicazioni seguenti:
- nome, indirizzo o denominazione commerciale dell'installatore o dell'officina autorizzati,
- coefficiente caratteristico del veicolo, in forma di «w = … imp/km»,
- costante dell'apparecchio di controllo, in forma di «k = … imp/km»,
- circonferenza effettiva degli pneumatici delle ruote, in forma di «l = … mm»,
- dimensioni degli pneumatici,
- data in cui sono stati misurati il coefficiente caratteristico del veicolo e la circonferenza effettiva degli pneumatici delle ruote,
- numero di identificazione del veicolo,
- presenza (o meno) di un dispositivo GNSS esterno,
- numero di serie del dispositivo GNSS esterno (se del caso),
- numero di serie dell'eventuale dispositivo di comunicazione remota,
- numero di serie di tutti i sigilli apposti,
- parte del veicolo su cui è montato l'adattatore, se presente,

- parte del veicolo su cui è montato il sensore di movimento, se non è collegato alla scatola del cambio o se non viene utilizzato un adattatore,
- descrizione del colore del cavo che collega l'adattatore e la parte del veicolo che fornisce gli impulsi in entrata,
*- numero di serie del sensore di movimento incorporato nell'a*dattatore.»;
25) il punto 5.3 è così modificato:
a) è inserito un nuovo paragrafo 398a dopo il paragr*afo 398:*
*«398a) I sigilli summenzionati devono essere certificati conformemente alla norma EN 1*6882:2016.»;
b) al paragrafo 401 il secondo comma è sostituito dal seguente:
Questo numero di identificazione unico è così composto: MMNNNNNNNN, con iscrizione non rimovibile, dove MM è l'identificazione unica del fabbricante (registrazione nella banca dati gestita dalla CE) e NNNNNNNN il valore alfanumerico del sigillo, unico nel settore del fabbricante.";
c) il paragrafo 403 è sostituito dal s*eguente:*
*«403) I fabbricanti di sigilli, i cui modelli di sigillo sono certificati secondo la norma EN 16882:2016, devono essere registrati in una banca dati dedicata e devono rendere pubblici i loro numeri di identificazione dei sigilli attraverso una procedura che sarà stabilita dalla Commissio*ne europea.»;
d) il paragrafo 404 è sostituito dal s*eguente:*
*«404) Nel quadro del regolamento (UE) n. 165/2014, le officine e i costruttori di veicoli autorizzati devono usare esclusivamente sigilli certificati secondo la norma EN 16882:2016 provenienti dai fabbricanti di sigilli elencati nella suddetta b*anca dati.»;
26) il punto 6.2 è sostituito dal s*eguente:*
«6.2. Verifica dei componenti nuovi o riparati
*407) Di ogni singolo dispositivo, nuovo o riparato, vanno verificati il corretto funzionamento e l'esattezza delle letture e delle registrazioni, nei limiti fissati ai punti 3.2.1, 3.2.2, 3.*2.3 e 3.3.»;
27) al punto 6.3, il paragrafo 408 è sostituito dal s*eguente:*
«408) All'atto del montaggio sul veicolo, l'installazione nel suo complesso (compreso l'apparecchio di controllo) deve essere conforme alle disposizioni relative alle tolleranze massime di cui ai punti 3.2.1, 3.2.2, 3.2.3 e 3.3. L'installazione nel suo complesso deve essere sigillata conformemente al capitolo 5.3 e tarata.»;
28) il punto 8.1 è così modificato
a) al punto 8.1 il testo introduttivo che precede il paragrafo 425 è sostituito dal s*eguente:*
«Agli effetti della presente sezione, con «apparecchio di controllo» si intendono l'«apparecchio di controllo o i suoi componenti». Non è richiesta l'omologazione del cavo o dei cavi di collegamento tra il sensore di movimento e la VU, il dispositivo GNSS esterno e la VU o il dispositivo esterno di comunicazione remota e la VU. I fogli di carta impiegati dall'apparecchio di controllo devono considerarsi come un componente dell'apparecchio stesso.
Ciascun fabbricante può chiedere l'omologazione di uno o più componenti dell'apparecchio di controllo con qualsiasi altro componente (o componenti) dell'apparecchio di controllo, purché ciascun componente sia conforme ai requisiti del presente allegato. In alternativa, i fabbricanti possono anche chiedere l'omologazione dell'apparecchio di controllo.
Come indicato nella definizione 10), all'articolo 2 del presente regolamento, le unità elettroniche di bordo possono essere costituite da componenti assemblati in varianti diverse. A prescindere dalla variante di assemblaggio dei componenti, l'antenna esterna e (se del caso) il divisore dell'antenna connesso al ricevitore GNSS o al dispositivo di comunicazione remota non fanno parte dell'omologazione dell'unità elettronica di bordo.
Ciononostante, i fabbricanti che hanno ottenuto l'omologazione di un apparecchio di controllo devono tenere un elenco pubblicamente accessibile delle antenne e dei divisori compatibili con ciascun tipo di unità elettronica di bordo, di dispositivo GNSS esterno e di dispositivo esterno di comunicazione remota omologato.»;
b) il paragrafo 427 è sostituito dal s*eguente:*
«427) Le autorità di omologazione degli Stati membri non rilasciano la scheda di omologazione finché non siano stati loro presentati:
- un certificato di sicurezza (se richiesto a norma del presente allegato),
- un certificato funzionale,
*- un certificato di interoperabilità (se richiesto a norma del presente allegato), per l'apparecchio di controllo o la carta tachigrafica oggetto della domanda di om*ologazione.»;
29) l'appendice 1 è così modificata:
a) l'indice è così modificato:
i) il punto 2.63 è sostituito dal s*eguente:*
«2.63 Riservato per uso futuro»;
ii) il punto 2.78 è sostituito dal s*eguente:*
*«2.78 GNSSAccumula*tedDriving»;

iii) il punto 2.79 è sostituito dal s*eguente:*
*«2.79 GNSSAccumulatedDri*vingRecord»;
iv) il punto 2.111 è sostituito dal s*eguente:*
*«2.111 NoOfGNS*SADRecords»;
v) il punto 2.160 è sostituito dal s*eguente:*
«2.160 Riservato per uso futuro»;
vi) il punto 2.203 è sostituito dal s*eguente:*
*«2.203 VuGN*SSADRecord»;
vii) il punto 2.204 è sostituito dal s*eguente:*
*«2.204 VuGNSSADR*ecordArray»;
viii) il punto 2.230 è sostituito dal s*eguente:*
«2.230 Riservato per uso futuro»;
ix) il punto 2.231 è sostituito dal s*eguente:*
«2.231 Riservato per uso futuro»;
b) al punto 2 è aggiunto il seguente testo prima del pu*nto 2.1:*
*«Per i tipi di dati utilizzati nelle applicazioni di prima e seconda generazione, le dimensioni specificate nella presente appendice sono quelle valide per le applicazioni di seconda generazione. Si suppone che le dimensioni valide per le applicazioni di prima generazione siano già note al lettore. I riferimenti numerici dei requisiti dell'allegato IC legati a tali tipi di dati si riferiscono sia alle applicazioni di prima generazione, sia a quelle di seconda g*enerazione.»;
c) il punto 2.19 è sostituito dal s*eguente:*
«2.19. CardEventData
Prima generazione:
informazioni, memorizzate in una carta del conducente o dell'officina, relative alle anomalie associate al titolare della carta (requisiti 260 e 318 dell'allegato IC).

```
CardEventData ::= SEQUENCE SIZE(6) OF {
  cardEventRecords                    SET SIZE(NoOfEventsPerType) OF
                                      CardEventRecord
}
```

CardEventData è una sequenza di cardEventRecords ordinata in base al valore ascendente di EventFaultType (eccetto per le registrazioni relative ai tentativi di violazione della sicurezza, che sono raggruppate nell'ultima serie della sequenza).
cardEventRecords è una serie di registrazioni di anomalie di un determinato tipo (o categoria di anomalie relative ai tentativi di violazione della sicurezza).
Seconda generazione:
informazioni, memorizzate in una carta del conducente o dell'officina, relative alle anomalie associate al titolare della carta (requisiti 285 e 341 dell'allegato IC).

```
CardEventData ::= SEQUENCE SIZE(11) OF {
  cardEventRecords                    SET SIZE(NoOfEventsPerType) OF
                                      CardEventRecord
}
```

CardEventData è una sequenza di cardEventRecords ordinata in base al valore ascendente di EventFaultType (eccetto per le registrazioni relative ai tentativi di violazione della sicurezza, che sono raggruppate nell'ultima serie della sequenza).
*cardEventRecords è una serie di registrazioni di anomalie di un determinato tipo (o categoria di anomalie relative ai tentativi di violazione della s*icurezza).»
d) il punto 2.30 è sostituito dal s*eguente:*
«2.30. CardRenewalIndex
Il codice di rinnovo di una carta [definizione i)].

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

Value assignment: (cfr. capitolo 7 del presente allegato).
"0" Primo rilascio.
Ordine di incremento: "0, …, 9, A, …, Z"»;
e) al punto 2.61, il testo che segue i*l titolo «Seconda g*enerazione» è sostituito dal *seguente:*

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

Oltre alla prima generazione, sono utilizzati gli elementi di dati seguenti:

noOfGNSSADRecords è il numero di registrazioni del periodo guida cumulativo del GNSS che la carta è in grado di memorizzare.

noOfSpecificConditionRecords è il numero di registrazioni di condizioni particolari che la carta è in grado di memorizzare.

*noOfCardVehicleUnitRecords è il numero di registrazioni utilizzate delle unità elettroniche di bordo che la carta è in grado di me*morizzare.»;

f) il punto 2.63 è sostituito dal s*eguente: «2.63. Riservato per* uso futuro»;

g) al punto 2.67, il testo che segue i*l titolo "Seconda g*enerazione" è sostituito dal s*eguente:*

«Si usano gli stessi valori della prima generazione con le aggiunte seguenti:

```
--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: i valori della seconda generazione per la targa, l'adattatore e la connessione del dispositivo GNSS esterno e i valori della prima generazione per l'unità elettronica di bordo e il sensore di movimento possono essere utilizzati in SealRecord, se del caso.

Nota 2: nel campo CardHolderAuthorisation (CHA) dei certificati di seconda generazione i valori 1, 2 e 6 vanno interpretati come indicanti un certificato di autenticazione reciproca per il rispettivo tipo di apparecchio. Per indicare il rispettivo certificato allo scopo di creare una firma digitale, vanno usati i valori 17, 18 o 19.»;

h) al punto 2.70, il testo che segue i*l titolo "Seconda g*enerazione" è sostituito dal s*eguente:*

*«Seconda ge*nerazione:

'0x'H	*Anomalie generali,*
'00'H	*Nessun'altra informazione,*
'01'H	*Inserimento di una carta non valida,*
'02'H	*Conflitto di carte,*
'03'H	*Sovrapposizione di orari,*
'04'H	*Guida in assenza di una carta adeguata,*
'05'H	*Inserimento carta durante la guida,*
'06'H	*Chiusura errata ultima sessione carta,*
'07'H	*Superamento di velocità,*
'08'H	*Interruzione dell'alimentazione di energia,*
'09'H	*Errore dei dati di movimento,*
'0A'H	*Conflitto di dati sul movimento del veicolo,*
'0B'H	*Conflitto di orari (fra orologio del GNSS e orologio interno della VU),*
'0C'H	*Errore di comunicazione con il dispositivo di comunicazione remota,*
'0D'H	*Assenza di informazioni sulla posizione provenienti dal ricevitore GNSS,*
'0E'H	*Errore di comunicazione con il dispositivo GNSS esterno,*
'0F'H	*RFU,*

'1x'H	*Anomalie relative a tentativi di violazione della sicurezza riguardanti l'unità elettronica di bordo,*
'10'H	*Nessun'altra informazione,*
'11'H	*Mancata autenticazione del sensore di movimento,*
'12'H	*Mancata autenticazione della carta tachigrafica,*
'13'H	*Cambiamento non autorizzato di sensore di movimento,*
'14'H	*Errore di integrità nell'immissione dei dati della carta,*
'15'H	*Errore di integrità dei dati dell'utente memorizzati,*
'16'H	*Errore nel trasferimento interno di dati,*
'17'H	*Apertura non autorizzata dell'involucro,*
'18'H	*Sabotaggio di elementi hardware,*
'19'H	*Individuazione di manomissione del GNSS,*
'1A'H	*Mancata autenticazione del dispositivo GNSS esterno,*
'1B'H	*Certificato del dispositivo GNSS esterno scaduto,*
da '1C'H a '1F'H	*RFU,*
'2x'H	*Anomalie relative a tentativi di violazione della sicurezza riguardanti il sensore,*
'20'H	*Nessun'altra informazione,*
'21'H	*Autenticazione fallita,*
'22'H	*Errore di integrità dei dati memorizzati,*
'23'H	*Errore nel trasferimento interno di dati,*
'24'H	*Apertura non autorizzata dell'involucro,*
'25'H	*Sabotaggio di elementi hardware,*
da '26'H a '2F'H	*RFU,*
'3x'H	*Guasti dell'apparecchio di controllo,*
'30'H	*Nessun'altra informazione,*
'31'H	*Guasto all'interno della VU,*
'32'H	*Guasto della stampante,*
'33'H	*Guasto del dispositivo di visualizzazione,*
'34'H	*Guasto nel trasferimento di dati,*
'35'H	*Guasto del sensore,*
'36'H	*Ricevitore del GNSS interno,*
'37'H	*Dispositivo GNSS esterno,*
'38'H	*Dispositivo di comunicazione remota,*
'39'H	*Interfaccia ITS,*
da '3A'H a '3F'H	*RFU,*
'4x'H	*Guasti della carta,*
'40'H	*Nessun'altra informazione,*
da '41'H a '4F'H	*RFU,*
da '50'H a '7F'H	*RFU,*
da '80'H a 'FF'H	*Specifico del fabbricante.*»;

i) il punto 2.7.1 è sostituito dal s*eguente:*
«2.71. ExtendedSealIdentifier
Seconda generazione:
L'identificativo completo del sigillo identifica in modo univoco un sigillo (requisito 401 dell'allegato IC).

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

manufacturerCode è un codice del fabbricante del sigillo.
*sealIdentifier è un identificativo del sigillo che è unico per il fa*bbricante.»;
j) i punti 2.78 e 2.79 sono sostituiti dai s*eguenti:*
«2.78 GNSSAccumulatedDriving
Seconda generazione:

Informazioni, memorizzate in una carta del conducente o dell'officina, relative alla posizione del veicolo rilevata dal GNSS, se il periodo di guida cumulativo raggiunge un multiplo di tre ore (requisiti 306 e 354 dell'allegato IC).

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

gnssADPointerNewestRecord è l'indice della registrazione più aggiornata di guida cumulativa effettuata dal GNSS.
Value assignment è il numero corrispondente al numeratore della registrazione del periodo guida cumulativo effettuata dal GNSS, a partire da '0' per la prima volta in cui tale registrazione compare nella struttura.
gnssAccumulatedDrivingRecords è la serie di registrazioni contenenti la data e l'ora in cui il periodo guida cumulativo raggiunge un multiplo di tre ore e informazioni sulla posizione del veicolo.
2.79. GNSSAccumulatedDrivingRecord
Seconda generazione:
Informazioni, memorizzate in una carta del conducente o dell'officina, relative alla posizione del veicolo rilevata dal GNSS, se il periodo di guida cumulativo raggiunge un multiplo di tre ore (requisiti 305 e 353 dell'allegato IC).

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

timeStamp indica la data e l'ora in cui il periodo di guida cumulativo raggiunge un multiplo di tre ore.
gnssPlaceRecord contiene informazioni relative alla posizione del veicolo.
*vehicleOdometerValue è il valore odometrico del momento in cui il periodo di guida cumulativo raggiunge un multiplo d*i tre ore.»;
k) il punto 2.86 è sostituito dal s*eguente:*
«2.86. KeyIdentifier
*Identificativo univoco di una chiave pubblica utilizzato per codificare e selezionare la chiave. Identifica anche il titolare del*la *chiave.*

```
KeyIdentifier ::= CHOICE {
   extendedSerialNumber         ExtendedSerialNumber,
   certificateRequestID         CertificateRequestID,
   certificationAuthorityKID    CertificationAuthorityKID
}
```

La prima scelta (CHOICE) è adatta a codificare la chiave pubblica di un'unità elettronica di bordo, di una carta tachigrafica o di un dispositivo GNSS esterno.
La seconda scelta è adatta a codificare la chiave pubblica di un'unità elettronica di bordo (nei casi in cui il numero di serie dell'unità elettronica di bordo non sia noto al momento della generazione del certificato).
*La terza scelta è adatta a codificare la chiave pubblica di uno Sta*to membro.»;
l) il punto 2.92 è sostituito dal s*eguente:*
«2.92. MAC
Seconda generazione:
*Un totale di controllo crittografico di 8, 12 o 16 byte di lunghezza corrispondente alle cipher suites (sequenze crittografiche) di cui all'appe*ndice 11.

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

m) il punto 2.111 è sostituito dal s*eguente:*
«2.111. NoOfGNSSADRecords
Seconda generazione:
*Numero di registrazioni del periodo guida cumulativo del GNSS che una carta è in grado di me*morizzare.

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

*Assegnazione valore: cfr. ap*pendice 2.»;
n) al punto 2.120, l'assegnazione valore «16H» è sostituita dalla seguente:

```
'16'H    VuGNSSADRecord
```

o) il punto 2.160 è sostituito dal s*eguente:*
«2.160. Riservato per uso futuro»;
p) il punto 2.162 è sostituito dal s*eguente:*
«2.162. TimeReal
Codice per un campo combinato di data e ora, in cui la data e l'ora sono espresse in termini di secondi trascorsi a partire dalle 00h00min00s. del 1o gennaio 1970 *UTC.*

```
TimeReal {INTEGER:TimeRealRange} ::= INTEGER (0..TimeRealRange)
```

Assegnazione valore - Allineato all'ottetto: numero di secondi trascorsi a partire dalla mezzanotte del 1o gennaio 1970 UTC.
*La data/ora massima possibile è nell'*anno 2106.»;
q) il punto 2.179 è sostituito dal s*eguente:*
«2.179 VuCardRecord
Seconda generazione:
Informazioni, memorizzate in un'unità elettronica di bordo, relative ad una carta tachigrafica utilizzata (requisito 132 dell'allegato IC).

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

cardNumberAndGenerationInformation indica il numero completo e la generazione della carta utilizzata (tipo di dati 2.74).
cardExtendedSerialNumber quale letto nel file EF_ICC contenuto nel MF della carta.
cardStructureVersion quale letta nel file EF_Application_Identification contenuto nel DF_Tachograph_G2.
*cardNumber quale letto nel file EF_Identification contenuto nel DF_Tach*ograph_G2.»;
r) i punti 2.203 e 2.204 sono sostituiti dai s*eguenti:*
«2.203 VuGNSSADRecord
Seconda generazione:
*Informazioni, memorizzate in un'unità elettronica di bordo, relative alla posizione del veicolo rilevata dal GNSS, se il periodo di guida cumulativo raggiunge un multiplo di tre ore (requisiti 108 e 110 dell'alle*gato *IC).*

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

timeStamp indica la data e l'ora in cui il periodo di guida cumulativo raggiunge un multiplo di tre ore.
cardNumberAndGenDriverSlot identifica la carta, compresa la generazione, inserita nella sede (slot) del conducente.
cardNumberAndGenCodriverSlot identifica la carta, compresa la generazione, inserita nella sede (slot) del secondo conducente.
gnssPlaceRecord contiene informazioni relative alla posizione del veicolo.
vehicleOdometerValue è il valore odometrico del momento in cui il periodo di guida cumulativo raggiunge un multiplo di tre ore.
2.204. VuGNSSADRecordArray
Seconda generazione:
*Informazioni, memorizzate in un'unità elettronica di bordo, relative alla posizione del veicolo rilevata dal GNSS, se il periodo di guida cumulativo raggiunge un multiplo di tre ore (requisiti 108 e 110 dell'alle*gato *IC).*

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

recordType rappresenta il tipo di registrazione (VuGNSSADRecord).
Assegnazione valore: cfr. RecordType.
recordSize sono le dimensioni di VuGNSSADRecord in byte.
noOfRecords è il numero di registrazioni nella serie di registrazioni.
records è una serie di registrazioni di guida cumulativa rilevata dal GNSS.»;
s) i punti 2.230 e 2.231 sono sostituiti dai seguenti:
«2.230. Riservato per u*so futuro*
2.231. Riservato per uso futuro»;
t) al punto 2.234, il testo che segue il titolo "Seconda generazione" è sostituito dal seguente:

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

Oltre alla prima generazione, sono utilizzati gli elementi di dati seguenti:
noOfGNSSADRecords è il numero di registrazioni del periodo guida cumulativo del GNSS che la carta è in grado di memorizzare.
noOfSpecificConditionRecords è il numero di registrazioni di condizioni particolari che la carta è in grado di memorizzare.
*noOfCardVehicleRecords è il numero di registrazioni relative alle unità elettroniche di bordo che la carta è in grado di me*morizzare.»;
30) l'appendice 2 è così modificata:
a) al punto 1.1 sono aggiunte le seguenti abbrev*iazioni:*
«CHA Autorizzazione del titolare del certificato
*DO Gget*to di dati»;
b) il punto 3.3 è così modificato:
i) il paragrafo TCS_24 è sostituito dal s*eguente:*
«TCS_24 Queste condizioni di sicurezza possono essere collegate nei modi seguenti:
AND: devono essere soddisfatte tutte le condizioni di sicurezza
OR: deve essere soddisfatta almeno una condizione di sicurezza
*Le norme di accesso per il file system, vale a dire per i comandi SELECT, UPDATE BINARY e READ BINARY, sono specificate nel capitolo 4. Le norme di accesso per gli altri comandi sono specificate nelle tabelle riportate di seguito. L'espressione «Non applicabile» si usa quando non vi sono requisiti a supporto del comando. In questo caso il comando può essere o può non essere supportato, ma la condizione di accesso è esclusa dal campo di app*licazione.»;
ii) al paragrafo TCS_25, la tabella è sostituita dalla seguente:

«**Comando**	**Carta del conducente**	**Carta dell'officina**	**Carta di controllo**	**Carta dell'azienda**
External Authenticate				
- Per l'autenticazione di prima generazione	*ALW*	*ALW*	*ALW*	*ALW*
- Per l'autenticazione di seconda generazione	*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	*Non applicabile*	*Non applicabile*	*Non applicabile*	*Non applicabile*
PSO: Compute Digital Signature	*ALW OR SM-MAC-G2*	*ALW OR SM-MAC-G2*	*Non applicabile*	*Non applicabile*
PSO: Hash	*Non applicabile*	*Non applicabile*	*ALW*	*Non applicabile*
PERFORM HASH OF FILE	*ALW OR SM-MAC-G2*	*ALW OR SM-MAC-G2*	*Non applicabile*	*Non applicabile*
PSO: Verify Certificate	*ALW*	*ALW*	*ALW*	*ALW*
PSO: Verify Digital Signature	*Non applicabile*	*Non applicabile*	*ALW*	*Non applicabile*
Verify	*Non applicabile*	*ALW*	*Non applicabile*	*Non applicabile*»

iii) al paragrafo TCS_26, la tabella è sostituita dalla seguente:

«**Comando**	**Carta del conducente**	**Carta dell'officina**	**Carta di controllo**	**Carta dell'azienda**
External Authenticate				
- Per l'autenticazione di prima generazione	*Non applicabile*	*Non applicabile*	*Non applicabile*	*Non applicabile*
- Per l'autenticazione di seconda generazione	*ALW*	*PWD*	*ALW*	*ALW*
Internal Authenticate	*Non applicabile*	*Non applicabile*	*Non applicabile*	*Non applicabile*
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	*Non applicabile*	*ALW*	*ALW*	*Non applicabile*
PSO: Compute Digital Signature	*ALW OR SM-MAC-G2*	*ALW OR SM-MAC-G2*	*Non applicabile*	*Non applicabile*
PSO: Hash	*Non applicabile*	*Non applicabile*	*ALW*	*Non applicabile*
PERFORM HASH OF FILE	*ALW OR SM-MAC-G2*	*ALW OR SM-MAC-G2*	*Non applicabile*	*Non applicabile*
PSO: Verify Certificate	*ALW*	*ALW*	*ALW*	*ALW*
PSO: Verify Digital Signature	*Non applicabile*	*Non applicabile*	*ALW*	*Non applicabile*
Verify	*Non applicabile*	*ALW*	*Non applicabile*	*Non applicabile*»

iv) al paragrafo TCS_27, la tabella è sostituita dalla seguente:

«**Comando**	**Carta del conducente**	**Carta dell'officina**	**Carta di controllo**	**Carta dell'azienda**
External Authenticate				
- Per l'autenticazione di prima generazione	*Non applicabile*	*Non applicabile*	*Non applicabile*	*Non applicabile*
- Per l'autenticazione di seconda generazione	*ALW*	*PWD*	*ALW*	*ALW*
Internal Authenticate	*Non applicabile*	*Non applicabile*	*Non applicabile*	*Non applicabile*
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	*Non applicabile*	*Non applicabile*	*Non applicabile*	*Non applicabile*
PSO: Compute Digital Signature	*Non applicabile*	*Non applicabile*	*Non applicabile*	*Non applicabile*
PSO: Hash	*Non applicabile*	*Non applicabile*	*Non applicabile*	*Non applicabile*
PERFORM HASH OF FILE	*Non applicabile*	*Non applicabile*	*Non applicabile*	*Non applicabile*
PSO: Verify Certificate	*ALW*	*ALW*	*ALW*	*ALW*
PSO: Verify Digital Signature	*Non applicabile*	*Non applicabile*	*Non applicabile*	*Non applicabile*
Verify	*Non applicabile*	*ALW*	*Non applicabile*	*Non applicabile*»

c) al punto 3.4 il paragrafo TCS_29 è sostituito dal s*eguente:*

«TCS_29 Le parole di stato SW1 SW2 sono inviate in ogni messaggio di risposta ed indicano lo stato di elaborazione del comando.

SW1	***SW2***	***Significato***
90	*0*	*Elaborazione normale.*
61	*XX*	*Elaborazione normale. XX= numero di byte di risposta disponibili*
62	*81*	*Elaborazione con avvertimento. Parte dei dati inviati in risposta potrebbe essere danneggiata.*
63	*0*	*Autenticazione fallita (avvertimento).*
63	*CX*	*CHV (PIN) errato. Contatore tentativi rimasti fornito da 'X'.*
64	*0*	*Errore di esecuzione - Stato della memoria non volatile immutato. Errore di integrità.*
65	*0*	*Errore di esecuzione - Stato della memoria non volatile mutato.*
65	*81*	*Errore di esecuzione - Stato della memoria non volatile mutato - Errore di memoria.*
66	*88*	*Errore di sicurezza: totale di controllo crittografico errato (durante messaggistica sicura), o certificato errato (durante verifica certificato), o crittogramma errato (durante autenticazione esterna), o firma errata (durante verifica firma).*
67	*0*	*Lunghezza errata (Lc o Le errata).*
68	*83*	*Ultimo comando della catena atteso.*
69	*0*	*Comando vietato (risposta non disponibile in T= 0).*
69	*82*	*Condizione di sicurezza non soddisfatta.*
69	*83*	*Metodo di autenticazione bloccato.*
69	*85*	*Condizioni di impiego non soddisfatte.*
69	*86*	*Comando non consentito (nessun EF in corso).*
69	*87*	*Oggetti di dati previsti in messaggistica sicura mancanti.*
69	*88*	*Oggetti di dati in messaggistica sicura non corretti.*
6A	*80*	*Parametri errati nel campo di dati.*
6A	*82*	*File non trovato.*
6A	*86*	*Parametri P1-P2 errati.*
6A	*88*	*Dati indicati non trovati.*
6B	*0*	*Parametri errati (scostamento al di fuori dell'EF).*
6C	*XX*	*Lunghezza errata, SW2 indica la lunghezza esatta. Non viene inviato alcun campo di dati in risposta.*
6D	*0*	*Codice di istruzione non previsto o non valido.*
6E	*0*	*Classe non supportata.*
6F	*0*	*- Altri errori di controllo.*

Possono essere inviate in risposta altre parole di stato definite dalla norma ISO/IEC 7816-4 se il loro comportamento non è esplicitamente menzionato nella presente appendice.
Per esempio possono essere inviate in risposta le parole di stato seguenti:
6881: Canale logico non supportato
6882: Messaggistica sicura non supportata»;
d) al punto 3.5.1.1, l'ultimo trattino del paragrafo TCS_38 è sostituito dal s*eguente:*
«- Se l'applicazione selezionata è considerata danneggiata (negli attributi del file è rilevato un errore di integrità), lo stato di elaborazione inviato in risposta è "6400" o "6500".»;
e) al punto 3.5.1.2, l'ultimo trattino del paragrafo TCS_41 è sostituito dal s*eguente:*
«- Se il file selezionato è considerato danneggiato (negli attributi del file è rilevato un errore di integrità), lo stato di elaborazione inviato in risposta è "6400" o "6500".»;
f) al punto 3.5.2.1, il sesto trattino del paragrafo TCS_43 è sostituito dal s*eguente:*
«- Se negli attributi del file è rilevato un errore di integrità, la carta deve considerare tale file danneggiato e irrecuperabile; lo stato di elaborazione inviato in risposta è '6400' o '6500'.»;
g) il punto 3.5.2.1.1 è così modificato:
i) al paragrafo TCS_45, la tabella è sostituita dalla seguente:

«***Byte***	***Lunghezza***	***Valore***	***Descrizione***
#1	*1*	*"81h"*	*TPV: tag per i dati in chiaro*
#2	*L*	*"NNh" o "81 NNh"*	*LPV: lunghezza dei dati inviati in risposta (= Le originale). L è 2 byte se LPV>127 byte*
#(2+L) - #(1+L+NN)	*NN*	*"XX..XXh"*	*Dati in chiaro*
#(2+L+NN)	*1*	*"99h"*	*Tag per lo stato di elaborazione (SW1-SW2) - facoltativo per la messaggistica sicura di prima generazione*
#(3+L+NN)	*1*	*"02h"*	*Lunghezza dello stato di elaborazione - facoltativo per la messaggistica sicura di prima generazione*
#(4+L+NN) - #(5+L+NN)	*2*	*"XX XXh"*	*Stato di elaborazione della risposta APDU non protetta - facoltativo per la messaggistica sicura di prima generazione*
#(6+L+NN)	*1*	*"8Eh"*	*TCC: tag per il totale di controllo crittografico*
#(7+L+NN)	*1*	*"XXh"*	*"LCC: lunghezza del totale di controllo crittografico successivo* *"04h" per la messaggistica sicura di prima generazione (cfr. appendice 11, parte A)* *"08h", "0Ch" o "10h" secondo la lunghezza della chiave AES per la messaggistica sicura di seconda generazione (cfr. appendice 11, parte B)"*
#(8+L+N-N)-#(7+M+L+NN)	*M*	*"XX..XXh"*	*Totale di controllo crittografico*
SW	*2*	*"XXXXh"*	*Parole di stato (SW1, SW2)*»

ii) al paragrafo TCS_46, la tabella è sostituita dalla seguente:

«***Byte***	***Lunghezza***	***Valore***	***Descrizione***
#1	*1*	*"87h"*	*TPI CG: tag per i dati criptati (crittogramma)*
#2	*L*	*"MMh" o '81 MMh'*	*"LPI CG: lunghezza dei dati criptati inviati in risposta (diversa da Le originale del comando a causa del riempimento) L è 2 byte se LPI CG>127 byte."*
#(2+L)-#(1+L+MM)	*MM*	*"01XX..XXh"*	*Dati criptati: indicatore di riempimento e crittogramma*
#(2+L+MM)	*1*	*"99h"*	*Tag per lo stato di elaborazione (SW1-SW2) - facoltativo per la messaggistica sicura di prima generazione*
#(3+L+MM)	*1*	*"02h"*	*Lunghezza dello stato di elaborazione - facoltativo per la messaggistica sicura di prima generazione*

#(4+L+MM) - #(5+L+MM)	*2*	*“XX XXh”*	*Stato di elaborazione della risposta APDU non protetta - facoltativo per la messaggistica sicura di prima generazione*
#(6+L+MM)	*1*	*“8Eh”*	*TCC: tag per il totale di controllo crittografico*
#(7+L+MM)	*1*	*“XXXXh”*	*"LCC: lunghezza del totale di controllo crittografico successivo* *“04h” per la messaggistica sicura di prima generazione (cfr. appendice 11, parte A)* *“08h”, “0Ch” o “10h” secondo la lunghezza della chiave AES per la messaggistica sicura di seconda generazione (cfr. appendice 11, parte B)"*
# (8 + L + M - M)-#(7+N+L+MM)	*N*	*“XX..XXh”*	*Totale di controllo crittografico*
SW	*2*	*“XXXXh”*	*Parole di stato (SW1, SW2)*»

h) al punto 3.5.2.2, il sesto trattino del paragrafo TCS_50 è sostituito dal s*eguente:*
«- Se negli attributi del file è rilevato un errore di integrità, la carta deve considerare tale file danneggiato e irrecuperabile; lo stato di elaborazione inviato in risposta è “6400” o “6500”.»;
i) al punto 3.5.2.3, il paragrafo TCS_52 è così modificato:
i) l’ultima riga della tabella è sostituita dalla seguente:

«*Le*	*1*	*’XXh’*	*Secondo la norma ISO/IEC 7816-4*»

ii) è aggiunta la frase s*eguente:*
«Nei casi in cui T=0, la carta assume il valore Le=“00h” se non è applicata la messaggistica sicura.
Nei casi in cui T=1, lo stato di elaborazione inviato in risposta è “6700” se Le=“01h”.»;
j) al punto 3.5.2.3, il sesto trattino del paragrafo TCS_53 è sostituito dal s*eguente:*
«- Se negli attributi del file è rilevato un errore di integrità, la carta deve considerare tale file danneggiato e irrecuperabile; lo stato di elaborazione inviato in risposta è “6400” o “6500”.»;
k) al punto 3.5.3.2, il sesto trattino del paragrafo TCS_63 è sostituito dal s*eguente:*
«- Se negli attributi del file è rilevato un errore di integrità, la carta deve considerare tale file danneggiato e irrecuperabile; lo stato di elaborazione inviato in risposta è “6400” o “6500”.»;
l) al punto 3.5.5, il paragrafo TCS_72 è sostituito dal s*eguente:*
*«TCS_72 Il PIN inserito dall’utente deve essere codificato in ASCII e riempito a destra dall’IFD con byte “FFh”, fino a raggiungere la lunghezza di 8 byte; cfr. anche il tipo di dati WorkshopCardPIN nell’ap*pendice 1.»;
m) al punto 3.5.8, il paragrafo TCS_95 è sostituito dal s*eguente:*
«TCS_95 Se il comando INTERNAL AUTHENTICATE ha esito positivo, la chiave di sessione corrente di prima generazione, se presente, viene cancellata e non è più disponibile. Per avere a disposizione una nuova chiave di sessione di prima generazione, il comando EXTERNAL AUTHENTICATE per il meccanismo di autenticazione di prima generazione dev’essere eseguito con esito positivo.
*Nota: per le chiavi di sessione di seconda generazione cfr. appendice 11, CSM_193 e CSM_195. Se sono stabilite chiavi di sessione di seconda generazione e la carta tachigrafica riceve il comando in chiaro INTERNAL AUTHENTICATE APDU, la carta interrompe la sessione di messaggistica sicura di seconda generazione e distrugge le chiavi di sessione di seconda g*enerazione.»;
n) al punto 3.5.9, il paragrafo TCS_97 è sostituito dal s*eguente:*
«TCS_97 La variante di comando per l’autenticazione reciproca VU-carta di seconda generazione può essere eseguita nell’MF, nel DF Tachograph e nel DF Tachograph_G2, cfr. anche TCS_34. Se questo comando EXTERNAL AUTHENTICATE di seconda generazione ha esito positivo, la chiave di sessione corrente di prima generazione, se presente, viene cancellata e non è più disponibile.
*Nota: per le chiavi di sessione di seconda generazione cfr. appendice 11, CSM_193 e CSM_195. Se sono stabilite chiavi di sessione di seconda generazione e la carta tachigrafica riceve il comando in chiaro EXTERNAL AUTHENTICATE APDU, la carta interrompe la sessione di messaggistica sicura di seconda generazione e distrugge le chiavi di sessione di seconda g*enerazione.»;
o) al punto 3.5.10, paragrafo TCS_101, nella tabella è aggiunta la riga seguente:

«*5 + L + 1*	*1*	*’00h’*	*Secondo la norma ISO/IEC 7816-4*»

p) al punto 3.5.11.2.3, paragrafo TCS_114, è aggiunto il testo seguente:

«*- Se il currentAuthenticatedTime della carta è successivo alla data di scadenza della chiave pubblica selezionata, lo stato di elaborazione inviato in risposta è "6A88".*

Nota: in caso di comando MSE: SET AT per l'autenticazione della VU, la chiave indicata è una chiave pubblica VU_MA. La carta deve impostare la chiave pubblica VU_MA per l'uso, se disponibile nella sua memoria, che coincide con il riferimento del titolare del certificato (CHR) indicato nel campo di dati del comando (la carta può identificare le chiavi pubbliche VU_MA tramite il campo CHA del comando). Se è disponibile solo la chiave pubblica VU_Sign o se non è disponibile alcuna chiave pubblica dell'unità elettronica di bordo, in risposta a questo comando la carta deve inviare lo stato "6A88". Cfr. la definizione del campo CHA nell'appendice 11 e la definizione del tipo di dati equipmentType nell'appendice 1.

Allo stesso modo, qualora venga inviata a una carta di controllo un comando MSE: SET DST con un riferimento a un EQT (cioè una VU o una carta), conformemente a CSM_234, la chiave indicata è sempre una chiave EQT_Sign che va utilizzata per la verifica di una firma digitale. Come illustrato nella figura 13 dell'appendice 11, la carta di controllo avrà sempre memorizzato la chiave pubblica EQT_Sign pertinente. In alcuni casi la carta di controllo potrebbe aver memorizzato la chiave pubblica EQT_MA corrispondente. La carta di controllo deve sempre impostare l'uso della chiave pubblica EQT_Sign quando riceve il comando MSE: SET DST.»;

q) il punto 3.5.13 è così modificato:

(i) il paragrafo TCS_121 è sostituito dal seguente:

«*TCS_121 Il valore Hash of File temporaneamente memorizzato deve essere cancellato se è calcolato un nuovo valore Hash of File tramite il comando PERFORM HASH of FILE, se è selezionato un DF o se la carta tachigrafica è azzerata.*»;

ii) il paragrafo TCS_123 è sostituito dal seguente:

«*TCS_123 L'applicazione del tachigrafo di seconda generazione deve supportare l'algoritmo SHA-2 (SHA-256, SHA-384 o SHA-512), specificato dalla sequenza crittografica di cui all'appendice 11, parte B, per la chiave di firma della carta Card_Sign.*»;

iii) al paragrafo TCS_124, la tabella è sostituita dalla seguente:

«***Byte***	***Lunghezza***	***Valore***	***Descrizione***
CLA	*1*	*"80h"*	*CLA*
INS	*1*	*"2Ah"*	*Esecuzione operazione di sicurezza*
P1	*1*	*"90h"*	*Tag: Hash*
P2	*1*	*"00h"*	*Algoritmo implicitamente noto* *Per l'applicazione tachigrafica di prima generazione: SHA-1* *Per l'applicazione tachigrafica di seconda generazione: l'algoritmo SHA-2, (SHA-256, SHA-384 o SHA-512), specificato dalla sequenza crittografica di cui all'appendice 11, parte B, per la chiave di firma della carta Card_Sign.*»

r) il punto 3.5.14 è così modificato: il testo che segue il titolo e arriva fino al paragrafo TCS_126 è sostituito dal seguente:

«*Questo comando è usato per calcolare la firma digitale del codice hash precedentemente calcolato (cfr. PERFORM HASH OF FILE, al punto 3.5.13).*

Solo la carta del conducente e la carta dell'officina devono supportare questo comando nel DF Tachograph e nel DF Tachograph_G2.

Altri tipi di carte tachigrafiche possono eseguire o meno questo comando. Nel caso dell'applicazione dei tachigrafi di seconda generazione, solo la carta del conducente e la carta dell'officina dispongono di una chiave di firma di seconda generazione; altre carte non sono in grado di eseguire il comando e di terminare con un codice di errore idoneo.

Il comando può essere accessibile o meno nell'MF. Se il comando non è accessibile nell'MF, deve terminare con un codice di errore idoneo.

Questo comando è conforme alla norma ISO/IEC 7816-8. Il suo uso è limitato rispetto a quello previsto dalla norma.»;

s) il punto 3.5.15 è così modificato:

i) al paragrafo TCS_133, la tabella è sostituita dalla seguente:

«***Byte***	***Lunghezza***	***Valore***	***Descrizione***
CLA	*1*	*"00h"*	*CLA*
INS	*1*	*"2Ah"*	*Esecuzione operazione di sicurezza*
P1	*1*	*"00h"*	
P2	*1*	*"A8h"*	*Tag: il campo di dati contiene DO pertinenti per la verifica*

Lc	*1*	*"XXh"*	*Lunghezza Lc del campo di dati successivo*
#6	*1*	*"9Eh"*	*Tag per la firma digitale*
#7 o #7-#8	*L*	*"NNh" o "81 NNh"*	*Lunghezza della firma digitale (L è 2 byte se la firma digitale è più lunga di 127 byte):* *128 byte codificati conformemente all'appendice 11, parte A, per l'applicazione tachigrafica di prima generazione.* *Secondo la curva selezionata per l'applicazione tachigrafica di seconda generazione (cfr. appendice 11, parte B)*
# (7 + L) - #(6+L+NN)	*NN*	*"XX..XXh"*	*Contenuto della firma digitale*»

ii) al paragrafo TCS_134 è aggiunto il trattino seguente:

«- *Se la chiave pubblica selezionata (usata per verificare la firma digitale) ha una CHA.LSB (CertificateHolderAuthorisation.equipmentType) non idonea alla verifica della firma digitale secondo l'appendice 11, lo stato di elaborazione inviato in risposta è "6985".*»;

t) il punto 3.5.16 è così modificato:

i) al paragrafo TCS_138, nella tabella è aggiunta la riga seguente:"

5 + L + 1	1	"00h"	Secondo la norma ISO/IEC 7816-4

ii) al paragrafo TCS_139 è aggiunto il comma seguente:

«- *"6985" indica che il time stamp di 4 byte riportato nel campo di dati del comando è anteriore a cardValidityBegin o posteriore a cardExpiryDate.*»;

u) il punto 4.2.2 è così modificato:

i) Nella struttura dei dati di cui al paragrafo TCS_154, le righe da DF Tachograph G2 a EF CardMA_Certificate e le righe da EF GNSS_Places alla fine del paragrafo sono sostituite dalle seguenti:

File / Elemento di dati	Numero di registrazioni	Dimensioni (in byte) Min.	Max.	Valori standard
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) al paragrafo TCS_155, l'elemento
NoOfGNSSCDRecords
della tabella è sostituito dal seguente:

« n_g	*NoOfGNSSADRecords*	*252*	*336»*

v) al punto 4.3.1, paragrafo TCS_156, il testo corrispondente all'abbreviazione SC4 è sostituito dal seguente:
«*SC4 Per il comando READ BINARY con byte INS pari:*
(SM-C-MAC-G1 AND SM-R-ENC-MAC-G1) OR
(SM-C-MAC-G2 AND SM-R-ENC-MAC-G2)
Per il comando READ BINARY con byte INS dispari (se supportato): NEV»;
w) il punto 4.3.2 è così modificato:
i) Nella struttura dei dati di cui al paragrafo TCS_162, le righe da DF Tachograph G2 a EF CardMA_Certificate, da EF Calibration a extendedSealIdentifier e da EF GNSS_Places a vehicleOdometer Value sono sostituite dalle seguenti:

File / Elemento di dati	Numero di registrazioni	Dimensioni (in byte) Min.	Max.	Valori standard
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) l'elemento NoOfGNSSCDRecords della tabella contenuta nel paragrafo TCS_163 è sostituito dal seguente:

«n_g	*NoOfGNSSADRecords*	*18*	*24*»

31) all'appendice 3, il punto 2 è così modificato:
a) al di sotto della riga dei pittogrammi «*Luogo in cui inizia il periodo di lavoro giornaliero*» e «*Luogo in cui termina il periodo di lavoro giornaliero*» è inserita la riga seguente:
«  *Posizione dopo 3 ore di periodo di guida cumulativo*»;
b) la combinazione di pittogrammi «*Regolazione dell'ora (in officina)*» è sostituita dalla seguente:
«  *Dati contrastanti sull'ora o regolazione dell'ora (in officina)*»;
c) All'elenco delle anomalie sono aggiunte le combinazioni di pittogrammi seguenti:
«  *Assenza di informazioni sulla posizione provenienti dal ricevitore GNSS o errore di comunicazione con il dispositivo GNSS esterno*»;
«  *Errore di comunicazione con il dispositivo di comunicazione remota*»;
32) l'appendice 4 è così modificata:
a) il punto 2 è così modificato:
i) il blocco numero 11.4 è sostituito dal seguente:"

«*11.4*	*Immissione del luogo in cui inizia e/o termina un periodo di lavoro giornaliero*	
	pi = pittogramma luogo inizio / termine, ora, paese, regione *longitudine della posizione registrata* *latitudine della posizione registrata* *timestamp in cui è stata determinata la posizione* *Odometro*	*pihh:mm Cou Reg* *lon ±DDDoMM.M'* *lat ± DDoMM.M'* *hh:mm* *x xxx xxx km*»

ii) il blocco numero 11.5 è sostituito dal seguente:

«*11.5*	*Posizioni dopo 3 ore di periodo di guida cumulativo* *pi=posizione dopo 3 ore di periodo di guida cumulativo*	
	ora *longitudine della posizione registrata* *latitudine della posizione registrata* *timestamp in cui è stata determinata la posizione* *Odometro*	pihh:mm lon ± DDD°MM.M' lat ± DD°MM.M ' hh:mm x xxx xxx **km**»

b) al punto 3.1, la posizione 11.5 del formato della stampa giornaliera è sostituita dalla seguente:"

11.5	Posizioni dopo 3 ore di periodo di guida cumulativo in ordine cronologico

c) al punto 3.2, il formato della stampa giornaliera è sostituito dal seguente:"

1	Data e ora di stampa del documento
2	Tipo di stampa
3	Identificazione del titolare della carta (per tutte le carte inserite nella VU + GEN)

4	Identificazione del veicolo (veicolo da cui si ottiene la stampa)
5	Identificazione della VU (VU da cui si ottiene la stampa + GEN)
6	Ultima taratura di questa VU
7	Ultimo controllo di questo tachigrafo
9	Delimitatore delle attività del conducente
10	Delimitatore della sede (slot) del conducente (slot 1)
10a	Condizione «escluso dal campo di applicazione» all'inizio del giorno in questione
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Attività in ordine cronologico [sede (slot) conducente]
10	Delimitatore della sede (slot) del secondo conducente (slot s)
10a	Condizione «escluso dal campo di applicazione» all'inizio del giorno in questione
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Attività in ordine cronologico [sede (slot) secondo conducente]
11	Delimitatore del riepilogo giornaliero
11.1	Riepilogo dei periodi senza carta nella sede (slot) del conducente
11.4	Luoghi immessi in ordine cronologico
11.5	Posizioni dopo 3 ore di periodo di guida cumulativo in ordine cronologico
11.7	Totali delle attività
11.2	Riepilogo dei periodi senza carta nella sede (slot) del secondo conducente
11.4	Luoghi immessi in ordine cronologico
11.5	Posizioni dopo 3 ore di periodo di guida cumulativo in ordine cronologico
11.8	Totali delle attività
11.3	Riepilogo delle attività per un conducente, comprese entrambe le sedi (slot)
11.4	Luoghi immessi da tale conducente in ordine cronologico
11.5	Posizioni dopo 3 ore di periodo di guida cumulativo in ordine cronologico
1.9	Totali delle attività per questo conducente
13.1	Delimitatore di anomalie e guasti
13.4	Registrazione di anomalie/guasti (ultime 5 anomalie/guasti memorizzati o in corso nella VU)
22.1	Luogo del controllo
22.2	Firma dell'agente incaricato del controllo
22.3	Dalle ore (spazio disponibile per consentire a un conducente senza carta di indicare
22.4	Alle ore quali periodi sono pertinenti per lui)
22.5	Firma del conducente

d) al punto 3.7, il paragrafo PRT_014 è sostituito dal seguente:
«*PRT_014 La stampa della cronologia delle carte inserite deve rispettare il formato seguente:*

1	*Data e ora di stampa del documento*
2	*Tipo di stampa*
3	*Identificazione del titolare della carta (per tutte le carte inserite nella VU)*
23	*Carta più recente inserita nella VU*
23,1	*Carte inserite (fino a 88 registrazioni)*
12.3	*Delimitatore dei guasti*»

33) l'appendice 7 è così modificata:
a) il punto 1.1 è sostituito dal seguente:
«*1.1. Campo di applicazione*

Il trasferimento di dati a un ESM può avvenire:
- da un'unità elettronica di bordo mediante un apparecchio intelligente dedicato (Intelligent dedicated equipment - IDE) collegato alla VU,
- da una carta tachigrafica mediante un IDE dotato di interfaccia della carta (IFD),
- da una carta tachigrafica e attraverso l'unità elettronica di bordo mediante un IDE collegato alla VU.
Per consentire la verifica dell'autenticità e dell'integrità dei dati trasferiti e memorizzati in un ESM, i dati vengono trasferiti allegando una firma digitale conformemente all'appendice 11 (Meccanismi comuni di sicurezza). Vengono inoltre trasferiti i dati relativi all'identificazione dell'apparecchio di provenienza (VU o carta tachigrafica) e i relativi certificati di sicurezza (Stato membro e apparecchio). Chi è preposto alla verifica dei dati deve essere in possesso di una chiave pubblica europea fidata.
I dati trasferiti da una VU sono firmati utilizzando i meccanismi comuni di sicurezza di cui all'appendice 11, parte B (Sistema tachigrafico di seconda generazione), tranne quando il controllo dei conducenti è effettuato da un'autorità di controllo non UE che utilizza una carta di controllo di prima generazione, nel qual caso i dati sono firmati utilizzando i meccanismi comuni di sicurezza di cui all'appendice 11, parte A (Sistema tachigrafico di prima generazione), come previsto dall'appendice 15, Migrazione: requisito MIG_015.
La presente appendice specifica pertanto due tipi di trasferimento di dati dalla VU:
- trasferimento di dati da una VU di seconda generazione, che fornisce la struttura dei dati di seconda generazione, firmati utilizzando i meccanismi comuni di sicurezza di cui all'appendice 11, parte B,
- trasferimento di dati da una VU di prima generazione, che fornisce la struttura dei dati di prima generazione, firmati utilizzando i meccanismi comuni di sicurezza di cui all'appendice 11, parte A.
Analogamente esistono due tipi di trasferimento di dati da carte del conducente di seconda generazione inserite in una VU, come specificato ai paragrafi 3 e 4 della presente appendice.»;
b) il punto 2.2.2 è così modificato:
i) la tabella è sostituita dalla seguente:

«***Struttura del messaggio***		***Max 4 Byte Intestazione***				***Max 255 Byte Dati***			***1 Byte Totale***
IDE ->	*<- VU*	*FMT*	*TGT*	*SRC*	*LEN*	*SID*	*DS_ / TRTP*	*DATA*	*CS*
Richiesta di inizio comunicazione		*81*	*EE*	*F0*		*81*			*E0*
Risposta positiva di inizio comunicazione		*80*	*F0*	*EE*	*3*	*C1*		*EA, 8F*	*9B*
Richiesta di inizio sessione diagnostica		*80*	*EE*	*F0*	*2*	*10*	*81*		*F1*
Risposta positiva di inizio sessione diagnostica		*80*	*F0*	*EE*	*2*	*50*	*81*		*31*
Servizi di controllo del collegamento									
Verifica della frequenza di baud (fase 1)									
9 600 Bd		*80*	*EE*	*F0*	*4*	*87*		*01,01,01*	*EC*
19 200 Bd		*80*	*EE*	*F0*	*4*	*87*		*01,01,02*	*ED*
38 400 Bd		*80*	*EE*	*F0*	*4*	*87*		*01,01,03*	*EE*
57 600 Bd		*80*	*EE*	*F0*	*4*	*87*		*01,01,04*	*EF*
115 200 Bd		*80*	*EE*	*F0*	*4*	*87*		*01,01,05*	*F0*
Risposta positiva verifica della frequenza di baud		*80*	*F0*	*EE*	*2*	*C7*		*1*	*28*
Frequenza di baud di transizione (fase 2)		*80*	*EE*	*F0*	*3*	*87*		*02.03*	*ED*
Richiesta di invio dati		*80*	*EE*	*F0*	*0A*	*35*		*00,00,00,00, 00,FF,FF,FF,FF*	*99*
Risposta positiva di invio dati		*80*	*F0*	*EE*	*3*	*75*		*00,FF*	*D5*
Richiesta di trasferimento dati									
Riepilogo		*80*	*EE*	*F0*	*2*	*36*	*01 o 21*		*97*
Attività		*80*	*EE*	*F0*	*6*	*36*	*02 o 22*	*Data*	*CS*
Anomalie e guasti		*80*	*EE*	*F0*	*2*	*36*	*03 o 23*	*Data*	*99*

Dati dettagliati relativi alla velocità	*80*	*EE*	*F0*	*2*	*36*	*04 o 24*	*Data*	*9A*
Dati tecnici	*80*	*EE*	*F0*	*2*	*36*	*05 o 25*	*Data*	*9B*
Trasferimento dei dati della carta	*80*	*EE*	*F0*	*2*	*36*	*6*	*Slot*	*CS*
Risposta positiva di trasferimento dati	*80*	*F0*	*EE*	*Len*	*76*	*TREP*	*Dati*	*CS*
Richiesta di chiusura trasferimento	*80*	*EE*	*F0*	*1*	*37*			*96*
Risposta positiva richiesta di chiusura trasferimento	*80*	*F0*	*EE*	*1*	*77*			*D6*
Richiesta di termine comunicazione	*80*	*EE*	*F0*	*1*	*82*			*E1*
Risposta positiva di termine comunicazione	*80*	*F0*	*EE*	*1*	*C2*			*21*
Riconoscimento sottomessaggio	*80*	*EE*	*F0*	*Len*	*83*		*Dati*	*CS*
Risposte negative								
Rifiuto generico	*80*	*F0*	*EE*	*3*	*7F*	*Sid Req*	*10*	*CS*
Servizio non supportato	*80*	*F0*	*EE*	*3*	*7F*	*Sid Req*	*11*	*CS*
Sottofunzione non supportata	*80*	*F0*	*EE*	*3*	*7F*	*Sid Req*	*12*	*CS*
Lunghezza del messaggio non corretta	*80*	*F0*	*EE*	*3*	*7F*	*Sid Req*	*13*	*CS*
Condizioni non soddisfatte o errore nella sequenza di richiesta	*80*	*F0*	*EE*	*3*	*7F*	*Sid Req*	*22*	*CS*
Richiesta fuori valori limite	*80*	*F0*	*EE*	*3*	*7F*	*Sid Req*	*31*	*CS*
Invio dati rifiutato	*80*	*F0*	*EE*	*3*	*7F*	*Sid Req*	*50*	*CS*
Risposta pendente	*80*	*F0*	*EE*	*3*	*7F*	*Sid Req*	*78*	*CS*
Dati non disponibili	*80*	*F0*	*EE*	*3*	*7F*	*Sid Req*	*FA*	*CS*»

ii) alle note in calce alla tabella sono aggiunti i trattini seguenti:
«*- i TRTP da 21 a 25 sono usati per richieste di trasferimento dati da VU di seconda generazione, i TRTP da 01 a 05 sono usati per richieste di trasferimento dati da VU di prima generazione, le quali possono essere accettate dalla VU solo nel quadro di controlli dei conducenti effettuati da un'autorità di controllo non UE che utilizza una carta di controllo di prima generazione,*
- i TRTP da 11 a 19 e da 31 a 39 sono riservati per richieste di trasferimento dati specifiche del fabbricante.»;
c) il punto 2.2.2.9 è così modificato:
i) il paragrafo DDP_011 è sostituito dal seguente:
«*DDP_011 La richiesta di trasferimento dati è inviata dall'IDE per specificare alla VU il tipo di dati da trasferire. Un parametro di richiesta di trasferimento (TRTP) di un byte indica il tipo di trasferimento.*
Vi sono sei tipi di trasferimento dati. Per il trasferimento di dati VU possono essere utilizzati due diversi TRTP per ciascun tipo di trasferimento:

Tipo di trasferimento dati	***Valore TRTP per trasferimento dati da VU di prima generazione***	***Valore TRTP per trasferimento dati da VU di seconda generazione***
Riepilogo	*1*	*21*
Attività relative a una data specifica	*2*	*22*
Anomalie e guasti	*3*	*23*
Dati dettagliati relativi alla velocità	*4*	*24*
Dati tecnici	*5*	*25*

Tipo di trasferimento dati	*Valore TRTP*
Trasferimento dei dati della carta	*06*»

ii) il paragrafo DDP_054 è sostituito dal seguente:
«*DDP_054 L'IDE deve obbligatoriamente richiedere il trasferimento dati in modalità ispezione (TRTP 01 o 21) durante una sessione di trasferimento, poiché solo in tal modo i certificati della VU vengono registrati nei file trasferiti (e permettono così la verifica della firma digitale).*
Nel secondo caso (TRTP 02 o 22) il messaggio Richiesta di trasferimento dati comprende l'indicazione del giorno

di calendario (formatoTimeReal) da trasferire.»;
d) al punto 2.2.2.10, il paragrafo DDP_055 è sostituito dal seguente:
«*DDP_055 Nel primo caso (TREP 01) la VU invia i dati utili all'operatore dell'IDE per individuare i dati che intende trasferire. Le informazioni contenute all'interno del messaggio in questione riguardano:*
- certificati di sicurezza,
- identificazione del veicolo,
- data e ora correnti della VU,
- estremi temporali minimo e massimo dei dati disponibili per il trasferimento (dati VU),
- indicazione della presenza di carte nella VU,
- precedente trasferimento dati a un'impresa,
- blocchi di un'impresa,
- controlli precedenti.»;
e) al punto 2.2.2.16, l'ultimo trattino del paragrafo DDP_018 è sostituito dal seguente:
«*- dati FA non disponibili*
I dati oggetto di una richiesta di trasferimento non sono di disponibili nella VU (ad esempio non vi è alcuna carta inserita, richiesta di trasferimento dati da VU di prima generazione fuori dall'ambito di un controllo dei conducenti da parte di un'autorità di controllo non UE …).»;
f) il punto 2.2.6.1 è così modificato:
i) al paragrafo DDP_029, il primo comma è sostituito dal seguente:
«*Il campo di dati del messaggio «Risposta positiva di trasferimento dati ispezione» fornisce nell'ordine sotto indicato i seguenti dati corrispondenti ai valori esadecimali SID 76 Hex e TREP 01 o 21 Hex, nonché alla suddivisione e al conteggio appropriati dei sottomessaggi:*»;
ii) il titolo "Struttura dei dati generazione 1" è sostituito dal seguente:
«*Struttura dei dati di prima generazione (TREP 01 Hex)*»;
iii) il titolo "Struttura dei dati generazione 2" è sostituito dal seguente:
«*Struttura dei dati di seconda generazione (TREP 21 Hex)*»;
g) il punto 2.2.6.2 è così modificato:
i) al paragrafo DDP_030, il primo comma è sostituito dal seguente:
«*Il campo di dati del messaggio «Risposta positiva di trasferimento dati relativi alle attività» fornisce nell'ordine sotto indicato i seguenti dati corrispondenti ai valori esadecimali SID 76 Hex e TREP 02 o 22 Hex, nonché alla suddivisione e al conteggio appropriati dei sottomessaggi:*»;
ii) il titolo «*Struttura dei dati generazione 1*» è sostituito dal seguente:
«*Struttura dei dati di prima generazione (TREP 02 Hex)*»;
iii) il titolo «*Struttura dei dati generazione 2*» è sostituito dal seguente:
«*Struttura dei dati di seconda generazione (TREP 22 Hex)*»;
iv) l'elemento VuGNSSCDRecordArray che segue il titolo «*Struttura dei dati di seconda generazione (TREP 22 Hex)*» è sostituito dal seguente:

« VuGNSSADRecordArray		*Posizioni GNSS del veicolo nel momento in cui il periodo di guida cumulativo raggiunge un multiplo di tre ore. Se la sezione è vuota, viene inviata un'intestazione di array con noOfRecords = 0.*»

h) il punto 2.2.6.3 è così modificato:
i) al paragrafo DDP_031, il primo comma è sostituito dal seguente:
«*Il campo di dati del messaggio «Risposta positiva di trasferimento dati relativi ad anomalie e guasti» fornisce nell'ordine sotto indicato i seguenti dati corrispondenti ai valori esadecimali SID 76 Hex e TREP 03 o 23 Hex, nonché alla suddivisione e al conteggio appropriati dei sottomessaggi:*»;
ii) il titolo "Struttura dei dati generazione 1" è sostituito dal seguente:
«*Struttura dei dati di prima generazione (TREP 03 Hex)*»;
iii) il titolo "Struttura dei dati generazione 2" è sostituito dal seguente:
«*Struttura dei dati di seconda generazione (TREP 23 Hex)*»;
iv) l'elemento VuTimeAdjustmentGNSSRecordArray che segue il titolo «*Struttura dei dati di generazione 2 (TREP 23 Hex)*» è soppresso;
i) il punto 2.2.6.4 è così modificato:
i) al paragrafo DDP_032, il primo comma è sostituito dal seguente:
«*Il campo di dati del messaggio «Risposta positiva di trasferimento dati dettagliati relativi alla velocità» fornisce*

nell'ordine sotto indicato i seguenti dati corrispondenti ai valori esadecimali SID 76 Hex e TREP 04 o 24 Hex, nonché alla suddivisione e al conteggio appropriati dei sottomessaggi:»;
ii) il titolo "Struttura dei dati generazione 1" è sostituito dal seguente:
«*Struttura dei dati di prima generazione (TREP 04)*»;
iii) il titolo «*Struttura dei dati generazione 2*» è sostituito dal seguente:
«*Struttura dei dati di seconda generazione (TREP 24)*»;
j) il punto 2.2.6.5 è così modificato:
i) al paragrafo DDP_033, il primo comma è sostituito dal seguente: «*Il campo di dati del messaggio «Risposta positiva di trasferimento dati tecnici» fornisce nell'ordine sotto indicato i seguenti dati corrispondenti ai valori esadecimali SID 76 Hex e TREP 05 o 25 Hex, nonché alla suddivisione e al conteggio appropriati dei sottomessaggi:*»;
ii) il titolo «*Struttura dei dati generazione 1*» è sostituito dal seguente:
«*Struttura dei dati di prima generazione (TREP 05)*»;
iii) il titolo «*Struttura dei dati generazione 2*» è sostituito dal seguente:
«*Struttura dei dati di seconda generazione (TREP 25)*»;
k) al punto 3.3, il paragrafo DDP_035 è sostituito dal seguente:
«*DDP_035 Il trasferimento dei dati di una carta tachigrafica comprende le fasi seguenti:*
- Trasferimento negli EF ICC e IC dell'informazione comune relativa alla carta. Questa informazione è facoltativa e non è resa sicura mediante firma digitale.
- (per le carte tachigrafiche di prima e seconda generazione) trasferimento negli EF all'interno del Tachograph DF:
- Trasferimento degli EF Card_Certificate e CA_Certificate. Questa informazione non è resa sicura mediante firma digitale. Il trasferimento dei file in questione è obbligatorio per ogni sessione di trasferimento.
- Trasferimento degli altri EF di dati relativi alle diverse applicazioni (all'interno del Tachograph DF) ad eccezione dell'EF Card_Download. Questa informazione è resa sicura mediante firma digitale utilizzando i meccanismi comuni di sicurezza di cui all'appendice 11, parte A.
- Per ogni sessione di trasferimento è obbligatorio il trasferimento almeno degli EF Application_Identification e Identification.
- Nel trasferire i dati relativi alla carta del conducente è obbligatorio trasferire anche gli EF seguenti:

— Driver_Activity_Data,
— Vehicles_Used,
— Places,
— Events_Data,
— Control_Activity_Data,
— Faults_Data,
— Specific_Conditions,

- (solo per le carte tachigrafiche di seconda generazione) Tranne nel caso in cui il trasferimento dei dati relativi alla carta del conducente inserita in una VU sia effettuato da un'autorità di controllo non UE che utilizza una carta di controllo di prima generazione, trasferimento negli EF all'interno del Tachograph_G2 DF:
- Trasferimento degli EF CardSignCertificate, CA_Certificate and Link_Certificate (se del caso). Questa informazione non è resa sicura mediante firma digitale.
Il trasferimento dei file in questione è obbligatorio per ogni sessione di trasferimento.
- Trasferimento degli altri EF di dati relativi alle diverse applicazioni (all'interno del Tachograph_G2 DF) ad eccezione di EF Card_Download. Questa informazione è resa sicura mediante firma digitale utilizzando i meccanismi comuni di sicurezza di cui all'appendice 11, parte B.
- Per ogni sessione di trasferimento è obbligatorio il trasferimento almeno degli EF Application_Identification e Identification.
- Nel trasferire i dati relativi alla carta del conducente è obbligatorio trasferire anche gli EF seguenti:

— Events_Data,
— Faults_Data,
— Driver_Activity_Data,
— Vehicles_Used,
— Places,
— Control_Activity_Data,
— Specific_Conditions,
— VehicleUnits_Used,
— GNSS Places.

- Nel trasferimento dei dati relativi alla carta del conducente, aggiornare LastCardDownload nell'EF Card_Download e, se del caso, nei DF Tachograph_G2
- Nel trasferimento dei dati relativi alla carta dell'officina, reinizializzare il contatore di taratura nell'EF Card_Download nei DF Tachograph e, se del caso, Tachograph_G2.
- Nel trasferimento dei dati relativi alla carta dell'officina, l'EF Sensor_Installation_Data nei DF Tachograph e, se del caso, Tachograph_G2, non va scaricato.»;
l) al punto 3.3.2, il primo punto del paragrafo DDP_037 è sostituito dal seguente:
«*La sequenza per il trasferimento degli EF ICC, IC, Card_Certificate (o CardSignCertificate per il DF Tachograph_G2), CA_Certificate e Link_Certificate (solo per il DF Tachograph_G2) è la seguente:*»;
m) al punto 3.3.3, la tabella è sostituita dalla seguente:"

Carta	Dir	IDE/IFD	Significato/Osservazioni
	⇦	Seleziona file	
OK	⇨		
	⇦	Esegui Hash of file	- Calcola il valore di hash sul contenuto dei dati del file selezionato, mediante l'algoritmo di hash conformemente all'appendice 11, parte A o B. Il comando in questione non è del tipo ISO
Calcola il valore di hash del file e memorizza temporaneamente tale valore			
OK	⇨		
	⇦	Read Binary	Se il file contiene più dati della dimensione buffer del lettore o della carta, è necessario ripetere il comando fino all'avvenuta lettura del file completo
File dati OK	⇨	Invio dati ricevuti in memoria a ESM	secondo 3.4 Controllo inserimento ed estrazione carte
	⇦	PSO: Compute Digital Signature	
Esegue l'operazione di sicurezza «Compute Digital Signature» mediante il valore di hash temporaneamente memorizzato			
Signature OK	⇨	Aggiungi dati a quelli precedentemente memorizzati nell'ESM	secondo 3.4 Controllo inserimento ed estrazione carte

n) al punto 3.4.2, il paragrafo DDP_046 è sostituito dal seguente:
«*DDP_046 Una firma deve essere memorizzata come l'oggetto TLV immediatamente successivo all'oggetto TLV contenente i dati del file.*

Definizione	***Significato***	***Lunghezza***
FID (2 byte) || «00»	*Tag per EF (FID) all'interno del DF Tachograph o per l'informazione comune relativa alla carta.*	*3 byte*
FID (2 byte) || «01»	*Tag per firma di EF (FID) all'interno del DF Tachograph*	*3 byte*
FID (2 byte) || «02»	*Tag per firma di EF (FID) all'interno del DF Tachograph_G2*	*3 byte*
FID (2 byte) || «03»	*Tag per firma di EF (FID) all'interno del DF Tachograph_G2*	*3 byte*
xx xx	*Lunghezza campo valori*	*2 byte*

Esempio di dati contenuti in un file trasferito nell'ESM:

Tag	***Lunghezza***	***Valore***
00 02 00	*00 11*	*- Dati dell'EF ICC*
C1 00 00	*00 C2*	*- Dati dell'EF Card_Certificate*

		- …
05 05 00	*0A 2E*	*Dati dell'EF Vehicles_Used (all'interno del DF Tachograph)*
05 05 01	*00 80*	*Firma dell'EF Vehicles_Used (all'interno del DF Tachograph)*
05 05 02	*0A 2E*	*Dati dell'EF Vehicles_Used (all'interno del DF Tachograph_G2)*
05 05 03	*xx xx*	*Firma dell'EF Vehicles_Used (all'interno del DF Tachograph_G2)* »

o) al punto 4, il paragrafo DDP_049 è sostituito dal seguente:
«*DDP_049 Carte del conducente di prima generazione: i dati vanno trasferiti utilizzando il protocollo di trasferimento dati di prima generazione; i dati trasferiti devono avere lo stesso formato dei dati trasferiti da un'unità elettronica di bordo di prima generazione.*
Carte del conducente di seconda generazione: la VU trasferisce quindi l'intero contenuto della carta, file dopo file, in conformità del protocollo di trasferimento dati della carta illustrato al punto 3, e invia tutti i dati ricevuti dalla carta all'IDE nel formato file TLV appropriato (cfr. 3.4.2) e incapsulati all'interno di un messaggio "Risposta positiva di trasferimento dati»;
34) al punto 2 dell'appendice 8, il paragrafo che segue il titolo "Riferimenti" è sostituito dal seguente:
«*ISO 14230-2: Road Vehicles -Diagnostic Systems — Keyword Protocol 2000- Part 2: Data Link Layer. First edition: 1999.*»;
35) l'appendice 9 è così modificata:
a) nell'indice, il punto 6 è sostituito dal seguente:
«*6. PROVE DEL DISPOSITIVO ESTERNO DI COMUNICAZIONE REMOTA*»;
b) al punto 1.1 il primo trattino è sostituito dal seguente:
«*- una certificazione di sicurezza, basata sulle specifiche dei criteri comuni rispetto ad un obiettivo di sicurezza pienamente conforme all'appendice 10 del presente allegato,*»;
c) al punto 2, la tabella delle prove funzionali per l'unità elettronica di bordo è sostituita dalla seguente:"

«***N.***	***Prova***	***Descrizione***	***Requisiti applicabili***
1	***Esame amministrativo***		
1.1	Documentazione	Correttezza della documentazione	
1.2	Risultati delle prove del fabbricante	Risultati delle prove effettuate dal fabbricante durante l'integrazione Attestati cartacei	88, 89.91
2	***Esame visivo***		
2.1	Conformità alla documentazione		
2.2	Identificazione/marcature		da 224 a 226
2.3	Materiali		da 219 a 223
2.4	Sigillatura		398, da 401 a 405
2.5	Interfacce esterne		
3	***Prove funzionali***		
3.1	*Funzioni*		*02, 03, 04, 05, 07, 382*
3.2	*Modalità di funzionamento*		*da 09 a 11*, 134, 135*
3.3	*Funzioni e diritti di accesso ai dati*		*12* 13*, 382, 383, da 386 a 389*
3.4	*Controllo inserimento ed estrazione carte*		*15, 16, 17, 18, 19*, 20*, 134*
3.5	*Misurazione di velocità e distanza*		*da 21 a 31*
3.6	*Misurazione del tempo (prova effettuata a 20 °C)*		*da 38 a 43*
3.7	*Controllo delle attività del conducente*		*da 44 a 53, 134*

3.8	*Controllo delle condizioni di guida*	*54, 55, 134*
3.9	*Immissioni manuali*	*da 56 a 62*
3.10	*Gestione dei blocchi di un'impresa*	*da 63 a 68*
3.11	*Verifica delle attività di controllo*	*69, 70*
3.12	*Rilevamento di anomalie e/o guasti*	*da 71 a 88, 134*
3.13	*Dati di identificazione dell'apparecchio*	*93*, 94*, 97, 100*
3.14	*Dati relativi all'inserimento e all'estrazione della carta del conducente*	*da 102* a 104**
3.15	*Dati relativi all'attività del conducente*	*da 105* a 107**
3.16	*Dati relativi ai luoghi e alle posizioni*	*da 108* a 112**
3.17	*Dati relativi all'odometro*	*da 113* a 115**
3.18	*Dati dettagliati relativi alla velocità*	*116**
3.19	*Dati relativi alle anomalie*	*117**
3.20	*Dati relativi ai guasti*	*118**
3.21	*Dati relativi alla taratura*	*da 119* a 121**
3.22	*Dati relativi alla regolazione dell'ora*	*124*, 125**
3.23	*Dati relativi alle attività di controllo*	*126*, 127**
3.24	*Dati relativi ai blocchi di un'impresa*	*128**
3.25	*Dati relativi alle attività di trasferimento*	*129**
3.26	*Dati relativi a condizioni particolari*	*130*, 131**
3.27	*Registrazione e memorizzazione nelle carte tachigrafiche*	*136, 137, 138*, 139*, 141*, 142, 143, 144, 145, 146*, 147*, 148*, 149, 150*
3.28	*Visualizzazione*	*90, 134, da 151 a 168, PIC_001, DIS_001*
3.29	*Stampa*	*90, 134, da 169 a 181, PIC_001, da PRT_001 a PRT_014*
3.30	*Avviso*	*134, da 182 a 191, PIC_001*
3.31	*Trasferimento di dati verso un dispositivo esterno*	*90, 134, da 192 a 196*
3.32	*Comunicazione remota per controlli su strada mirati*	*da 197 a 199*
3.33	*Trasmissione di dati ad altri dispositivi esterni*	*200, 201*
3.34	*Taratura*	*da 202 a 206*, 383, 384, da 386 a 391*
3.35	*Controlli su strada della taratura*	*da 207 a 209*
3.36	*Regolazione dell'ora*	*da 210 a 212**
3.37	*Non interferenza di funzioni supplementari*	*06, 425*
3.38	*Interfaccia del sensore di movimento*	*02, 122*
3.39	*Dispositivo GNSS esterno*	*03, 123*
3.40	*Verificare che la VU individui, registri e memorizzi le anomalie e/o i guasti definiti dal fabbricante della VU quando un sensore di movimento abbinato reagisce ai campi magnetici che ostacolano il rilevamento dei dati di movimento del veicolo.*	*217*
3.41	*Cypher suite e parametri Domain standardizzati*	*CSM_48, CSM_50*
4	***Prove ambientali***	

4.1	*Temperatura:*	*Verificare la funzionalità mediante:* *prova conformemente alla norma ISO 16750-4, capitolo 5.1.1.2: Prova di funzionamento a bassa temperatura (72 h a -20 °C)* *Questa prova si riferisce alla norma IEC 60068-2-1: Prove ambientali - Parti 2-1: Prove - Prova A: freddo* *Prova conformemente a ISO 16750-4: Capitolo 5.1.2.2: Prova di funzionamento ad alta temperatura (72 h a 70 °C)* *Questa prova si riferisce alla norma IEC 60068-2-2: Procedure di prove ambientali di base; Parte 2: Prove; Prove B: calore secco* *Prova conformemente a ISO 16750-4: Capitolo 5.3.2: Cambiamento rapido di temperatura con durata specifica della transizione (-20 °C/70 °C, 20 cicli, tempo di permanenza di 2h a ogni temperatura)* *Si può effettuare una serie ridotta di prove (fra quelle definite alla sezione 3 della presente tabella) alla temperatura più bassa, alla temperatura più alta e durante i cicli di temperature*	*213*
4.2	*Umidità*	*Verificare che l'unità elettronica di bordo possa sopportare un'umidità ciclica (prova termica) secondo la norma IEC 60068-2-30, prova Db, sei cicli di 24 ore, ciascuno con temperature che variano da +25 °C a +55 °C e un'umidità relativa del 97 % a +25 °C e del 93 % a +55 °C*	*214*
4.3	*Prove meccaniche*	*1. Vibrazioni sinusoidali.* *Verificare che l'unità elettronica di bordo possa sopportare vibrazioni sinusoidali aventi le seguenti caratteristiche:* *spostamento costante tra 5 e 11 Hz: picco di 10 mm* *accelerazione costante tra 11 e 300 Hz: 5g* *Questo requisito si verifica in base alla norma IEC 60068-2-6, prova Fc, con una durata minima della prova di 3×12 ore (12 ore per asse)* *La norma ISO 16750-3 non prescrive una prova di vibrazione sinusoidale per i dispositivi posizionati nella cabina del veicolo staccata.* *2. Vibrazioni casuali:* *Prova conformemente a ISO 16750-3: Capitolo 4.1.2.8: Prova VIII: Veicolo commerciale, cabina del veicolo staccata* *Prova delle vibrazioni casuali, 10…2000 Hz, RMS verticale 21,3 m/s2, RMS longitudinale 11,8 m/s2, RMS laterale 13,1 m/s2, 3 assi, 32 h per asse, incluso il ciclo di temperatura -20…70 °C.* *Questa prova si riferisce alla norma IEC 60068-2-64: Prove ambientali - Parti 2-64: Prove - Prova Fh: vibrazioni, a banda larga casuali e guida* *3. Urti:* *urto meccanico con mezzo seno 3g conformemente a ISO 16750.* *Le prove sopra descritte sono effettuate su campioni diversi del modello di apparecchio sottoposto alle prove*	*219*

4.4	*Protezione contro l'acqua e i corpi estranei*	*Prova conformemente a ISO 20653: Veicoli stradali – Grado di protezione (codice IP) – Protezione delle apparecchiature da oggetti estranei, dall'acqua e dall'accesso (senza modifica dei parametri); Valore minimo IP 40*	*220, 221*
4.5	*Protezione contro sovratensione*	*Verificare che l'unità elettronica di bordo possa sopportare un'alimentazione di: versioni da 24 V: 34V a + 40 °C 1 ora versioni da 12 V: 17V a + 40 °C 1 ora (ISO 16750-2)*	*216*
4.6	*Protezione contro polarità inversa*	*Verificare che l'unità elettronica di bordo possa sopportare un'inversione dell'alimentazione (ISO 16750-2)*	*216*
4.7	*Protezione contro cortocircuiti*	*Verificare che i segnali in ingresso e in uscita siano protetti contro i cortocircuiti rispetto ad alimentazione e massa (ISO 16750-2)*	*216*
5	***Prove della compatibilità elettromagnetica***		
5.1	*Emissioni irradiate e sensibilità ai disturbi*	*Conformità al regolamento ECE R10*	*218*
5.2	*Scariche elettrostatiche*	*Conformità alla norma ISO 10605 :2008 + Rettifica tecnica :2010 + AMD1 :2014: +/- 4kV per il contatto e +/- 8kV per lo scarico di aria*	*218*
5.3	*Sensibilità ai transitori condotti nell'alimentazione*	*Per le versioni da 24 V: conformità alla norma ISO 7637-2 + regolamento ECE n. 10 Rev. 3: impulso 1a: Vs = -450V Ri = 50 ohm impulso 2a: Vs = +37V Ri = 2 ohm impulso 2b: Vs = +20V Ri = 0,05 ohm impulso 3a: Vs = -150V Ri = 50 ohm impulso 3b: Vs = +150V Ri = 50 ohm impulso 4: Vs = -16V Va = -12V t6 = 100ms impulso 5: Vs = +120V Ri = 2,2 ohm td = 250ms Per le versioni da 12 V: conformità alla norma ISO 7637-1 + regolamento ECE n. 10 Rev. 3: impulso 1: Vs = -75V Ri = 10 ohm impulso 2a: Vs = +37V Ri = 2 ohm impulso 2b: Vs = +10V Ri = 0,05 ohm impulso 3a: Vs = -112V Ri = 50 ohm impulso 3b: Vs = +75V Ri = 50 ohm impulso 4: Vs = -6V Va = -5V t6 = 15ms impulso 5: Vs = +65V Ri = 3ohm td = 100ms L'impulso 5 va controllato solo per le unità elettroniche di bordo destinate al montaggio in veicoli per i quali non è prevista una protezione comune esterna contro le cadute della potenza di carico Per la proposta relativa alle cadute della potenza di carico fare riferimento alla norma ISO 16750-2, 4a edizione, capitolo 4.6.4.*	*218*»

d) il punto 6 è sostituito dal seguente

:

«*6. PROVE DEL DISPOSITIVO ESTERNO DI COMUNICAZIONE REMOTA*

N.	*Prova*	*Descrizione*	*Requisiti applicabili*
1.	*Esame amministrativo*		
1.1	*Documentazione*	*Correttezza della documentazione*	
2.	*Esame visivo*		
2.1.	*Conformità alla documentazione*		
2.2.	*Identificazione/marcature*		*225, 226*
2.3	*Materiali*		*da 219 a 223*
3.	*Prove funzionali*		
3.1	*Comunicazione remota per controlli su strada mirati*		*4, da 197 a 199*
3.2	*Registrazione e memorizzazione nella memoria di dati*		*91*
3.3	*Comunicazione con l'unità elettronica di bordo*		*Appendice 14, da DSC_66 a DSC_70, da DSC_71 a DSC_76*
4.	*Prove ambientali*		
4.1	*Temperatura:*	*"Verificare la funzionalità mediante:* *prova conformemente alla norma ISO 16750-4, capitolo 5.1.1.2: Prova di funzionamento a bassa temperatura (72 h a -20 °C)* *Questa prova si riferisce alla norma IEC 60068-2-1: Prove ambientali - Parti 2-1: Prove - Prova A: freddo* *Prova conformemente a ISO 16750-4: Capitolo 5.1.2.2: Prova di funzionamento ad alta temperatura (72 h a 70 °C)* *Questa prova si riferisce alla norma IEC 60068-2-2: Procedure di prove ambientali di base; Parte 2: Prove; Prove B: calore secco* *Prova conformemente a ISO 16750-4: Capitolo 5.3.2: Cambiamento rapido di temperatura con durata specifica della transizione (-20 °C/70 °C, 20 cicli, tempo di permanenza di 1 h a ogni temperatura)* *Si può effettuare una serie ridotta di prove (fra quelle definite alla sezione 3 della presente tabella) alla temperatura più bassa, alla temperatura più alta e durante i cicli di temperature"*	*213*
4.2	*Protezione contro l'acqua e i corpi estranei*	*Prova conformemente a ISO 20653: Veicoli stradali – Grado di protezione (codice IP) – Protezione delle apparecchiature da oggetti estranei, dall'acqua e dall'accesso (valore target IP40)*	*220, 221*
5	*Prove della compatibilità elettromagnetica*		
5.1	*Emissioni irradiate e sensibilità ai disturbi*	*Conformità al regolamento ECE R10*	*218*
5.2	*Scariche elettrostatiche*	*Conformità alla norma ISO 10605 :2008 + Rettifica tecnica :2010 + AMD1 :2014: +/- 4kV per il contatto e +/- 8kV per lo scarico di aria*	*218*

5.3	*Sensibilità ai transitori condotti nell'alimentazione*	*"Per le versioni da 24 V: conformità alla norma ISO 7637-2 + regolamento ECE n. 10 Rev. 3:* *impulso 1a: Vs = -450V Ri = 50 ohm* *impulso 2a: Vs = +37V Ri = 2 ohm* *impulso 2b: Vs = +20V Ri = 0,05 ohm* *impulso 3a: Vs = -150V Ri = 50 ohm* *impulso 3b: Vs = +150V Ri = 50 ohm* *impulso 4: Vs = -16V Va = -12V t6 = 100ms* *impulso 5: Vs = +120V Ri = 2,2 ohm td = 250ms* *Per le versioni da 12 V: conformità alla norma ISO 7637-1 + regolamento ECE n. 10 Rev. 3:* *impulso 1: Vs = -75V Ri = 10 ohm* *impulso 2a: Vs = +37V Ri = 2 ohm* *impulso 2b: Vs = +10V Ri = 0,05 ohm* *impulso 3a: Vs = -112V Ri = 50 ohm* *impulso 3b: Vs = +75V Ri = 50 ohm* *impulso 4: Vs = -6V Va = -5V t6 = 15ms* *impulso 5: Vs = +65V Ri = 3ohm td = 100ms* *L'impulso 5 va controllato solo per le unità elettroniche di bordo destinate al montaggio in veicoli per i quali non è prevista una protezione comune esterna contro le cadute della potenza di carico* *Per la proposta relativa alle cadute della potenza di carico fare riferimento alla norma ISO 16750-2, 4a edizione, capitolo 4.6.4."*	*218*»

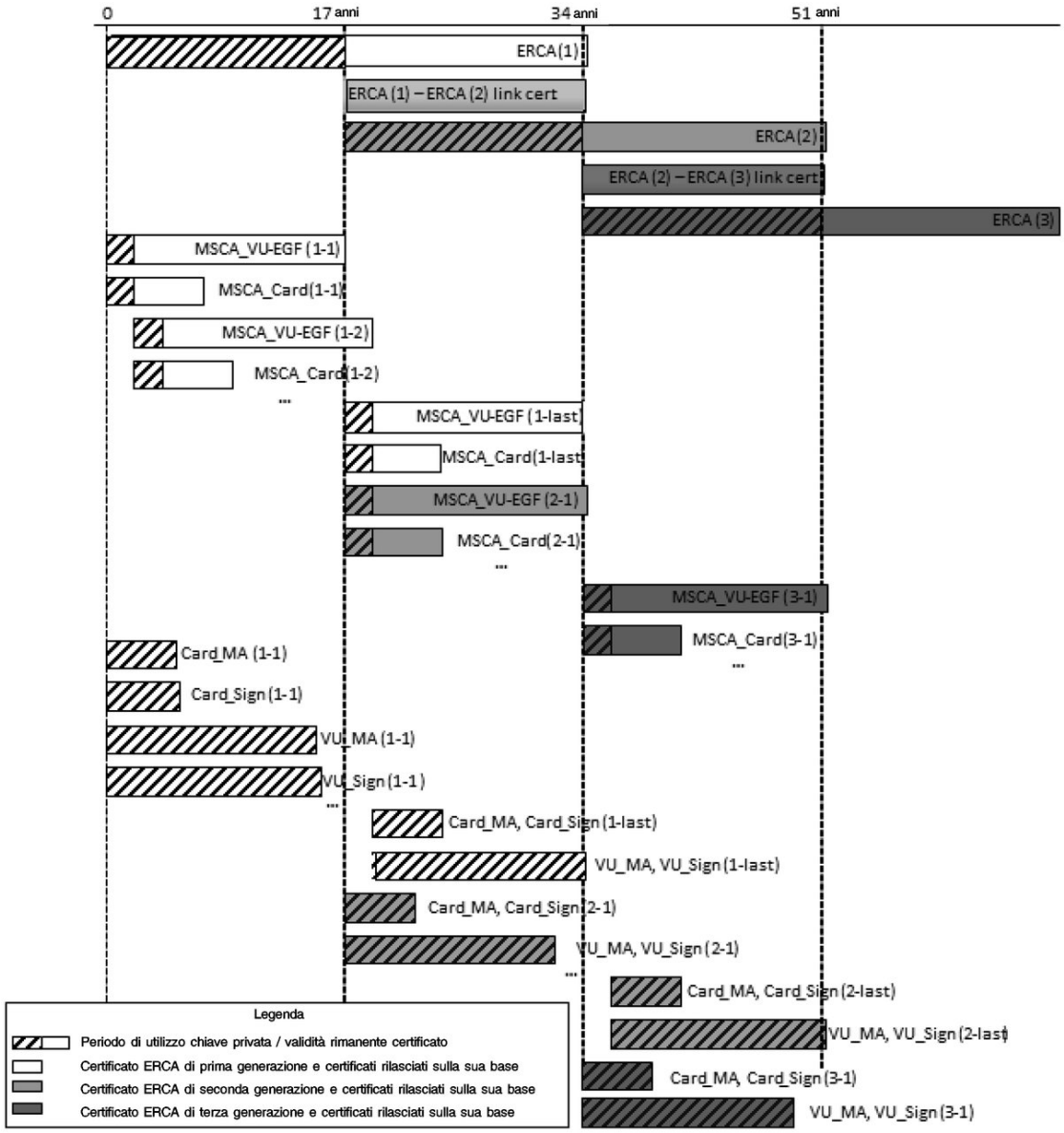
e) al punto 8, «*Prove di interoperabilità*», la tabella è sostituita dalla seguente:

N.	Prova	Descrizione
8.1 Prove di interoperabilità tra unità elettroniche di bordo e carte tachigrafiche		
1	Autenticazione reciproca	Verificare che l'autenticazione reciproca tra l'unità elettronica di bordo e la carta tachigrafica funzioni normalmente
2	Prove di scrittura/lettura	Predisporre uno scenario di attività tipico sull'unità elettronica di bordo. Lo scenario deve essere adattato al tipo di carta sottoposta alla prova e prevedere la scrittura nel maggior numero possibile di EF nella carta Verificare mediante un trasferimento dei dati dell'unità elettronica di bordo che tutte le registrazioni corrispondenti siano state effettuate correttamente Verificare mediante un trasferimento dei dati della carta che tutte le registrazioni corrispondenti siano state effettuate correttamente Verificare mediante stampe giornaliere che tutte le registrazioni corrispondenti si possano leggere correttamente
8.2 Prove di interoperabilità tra unità elettroniche di bordo e sensori di movimento		
1	Abbinamento	Verificare che l'abbinamento delle unità elettroniche di bordo e dei sensori di movimento funzioni normalmente
2	Prove delle attività	Predisporre uno scenario di attività tipico sul sensore di movimento. Lo scenario deve includere un'attività normale e creare il maggior numero possibile di anomalie o guasti. Verificare mediante un trasferimento dei dati dell'unità elettronica di bordo che tutte le registrazioni corrispondenti siano state effettuate correttamente Verificare mediante un trasferimento dei dati della carta che tutte le registrazioni corrispondenti siano state effettuate correttamente Verificare mediante una stampa giornaliera che tutte le registrazioni corrispondenti si possano leggere correttamente

8.3 Prove di interoperabilità tra unità elettroniche di bordo e dispositivi GNSS esterni (se applicabile)		
1	Autenticazione reciproca	Verificare che l'autenticazione reciproca (accoppiamento) tra l'unità elettronica di bordo e il modulo GNSS esterno funzioni normalmente
2	Prove delle attività	Predisporre uno scenario di attività tipico sul GNSS esterno. Lo scenario deve includere un'attività normale e creare il maggior numero possibile di anomalie o guasti. Verificare mediante un trasferimento dei dati dell'unità elettronica di bordo che tutte le registrazioni corrispondenti siano state effettuate correttamente Verificare mediante un trasferimento dei dati della carta che tutte le registrazioni corrispondenti siano state effettuate correttamente Verificare mediante una stampa giornaliera che tutte le registrazioni corrispondenti si possano leggere correttamente

36) l'appendice 11 è così modificata:
a) al punto 8.2.3, il paragrafo CSM_49 è sostituito dal seguente:
«*CSM_49 Le unità elettroniche di bordo, le carte tachigrafiche e i dispositivi GNSS esterni devono essere compatibili con gli algoritmi SHA-256, SHA-384 e SHA-512, come specificato in [SHS].*»;
b) al punto 9.1.2, il primo comma del paragrafo CSM_58 è sostituito dal seguente:
«*CSM_58 Ogni volta che si crea una nuova coppia di chiavi radice europee, la ERCA deve creare un certificato di collegamento (link certificate) per la nuova chiave pubblica europea e deve firmarlo con la precedente chiave privata europea. Il periodo di validità di un certificato di collegamento deve essere di 17 anni più 3 mesi. Anch'esso è indicato nella figura 1, sezione 9.1.7.*»;
c) al punto 9.1.4, il paragrafo CSM_72 è sostituito dal seguente:
«*CSM_72 Per ciascuna unità elettronica di bordo devono essere generate due coppie di chiavi uniche ECC, denominate VU_MA e VU_Sign. Questo compito spetta ai fabbricanti di VU. Ogniqualvolta si genera una coppia di chiavi della VU, la parte che genera la chiave deve inviare la chiave pubblica alla MSCA di competenza, in modo da ottenere il certificato VU corrispondente firmato dalla MSCA. La chiave privata deve essere usata solo dall'unità elettronica di bordo.*»;
d) il punto 9.1.5 è così modificato:
i) il paragrafo CSM_83 è sostituito dal seguente:
«*CSM_83 Per ciascuna carta tachigrafica deve essere generata una coppia unica di chiavi ECC, denominata Card_MA. Inoltre, per ciascuna carta del conducente e per ciascuna carta dell'officina deve essere generata una seconda coppia unica di chiavi ECC, denominata Card_Sign. Questa operazione può essere svolta dai fabbricanti della carta o da chi personalizza la carta. Ogniqualvolta si genera una coppia di chiavi della carta, la parte che genera la chiave deve inviare la chiave pubblica alla MSCA di competenza, in modo da ottenere il certificato della carta corrispondente firmato dalla MSCA. La chiave privata deve essere usata solo dalla carta tachigrafica.*»;
ii) il paragrafo CSM_88 è sostituito dal seguente:
«*CSM_88 Il periodo di validità di un certificato Card_MA deve essere il seguente:*
- per le carte del conducente: 5 anni;
- per le carte dell'azienda: 5 anni;
- per le carte di controllo: 2 anni;
- per le carte dell'officina: 1 anno»;
iii) al paragrafo CSM_91 è aggiunto il testo seguente:
«*- Inoltre, solo per le carte di controllo, le carte dell'azienda e le carte dell'officina, e solo se tali carte sono rilasciate durante i primi tre mesi del periodo di validità di un nuovo certificato EUR: il certificato EUR di due generazioni precedenti, se esistente.*
Nota all'ultimo trattino: per esempio, nei primi tre mesi dall'emissione del certificato ERCA(3) (cfr. figura 1), dette carte devono contenere il certificato ERCA(1). Ciò è necessario per garantire che queste carte possano essere utilizzate per effettuare il trasferimento di dati dalle VU ERCA (1) il cui normale periodo di trasferimento dati di 15 anni più tre mesi scade durante questi mesi; cfr. l'allegato IC, ultimo trattino del requisito 13»;
e) il punto 9.1.6 è così modificato:

i) il paragrafo CSM_93 è sostituito dal seguente:
«*CSM_93 Per ogni dispositivo GNSS esterno deve essere generata una coppia unica di chiavi ECC, denominata EGF_MA. Questo compito spetta ai fabbricanti di dispositivi GNSS esterni. Ogniqualvolta si genera una coppia di chiavi EGF_MA, la parte che genera la chiave deve inviare la chiave pubblica alla MSCA di competenza, in modo da ottenere il certificato EGF_MA corrispondente firmato dalla MSCA. La chiave privata deve essere usata solo dal dispositivo GNSS esterno.*»;
ii) il paragrafo CSM_95 è sostituito dal seguente:
«*CSM_95 Un dispositivo GNSS esterno deve usare la propria coppia di chiavi EGF_MA, composta da una chiave privata EGF_MA.SK e da una chiave pubblica EGF_MA.PK, esclusivamente per eseguire l'autenticazione reciproca e l'accordo sulle chiavi di sessione nei confronti delle unità elettroniche di bordo, come specificato al punto 11.4 della presente appendice.*»;
f) il punto 9.1.7 è così modificato:
i) la figura 1 è sostituita dalla seguente:
«Figura 1
Rilascio e uso di diverse generazioni di certificati radice ERCA, certificati di collegamento ERCA, certificati MSCA e certificati di dispositivo



ii) nelle note alla figura 1, il paragrafo 6 è sostituito dal seguente:
«*6. Per motivi di spazio, la differenza del periodo di validità tra i certificati Card_MA e Card_Sign è indicata solo per la prima generazione.*»;
g) il punto 9.2.1.1 è così modificato:
i) al paragrafo CSM_106, il primo trattino è sostituito dal seguente:
«- *Per le chiavi master dei sensori di movimento a 128 bit: CV = 'B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5D 83'*»;
ii) al paragrafo CSM_107, il primo comma è sostituito dal seguente:

«*Ciascun fabbricante di sensori di movimento deve generare una chiave di abbinamento KP unica e casuale per ciascun sensore di movimento e deve inviare ciascuna chiave di accoppiamento all'autorità di certificazione dello Stato membro (MSCA) di competenza. La MSCA deve criptare separatamente ciascuna chiave di abbinamento con la chiave master del sensore di movimento KM e deve fornire la chiave criptata al fabbricante del sensore di movimento. Per ciascuna chiave criptata, la MSCA deve comunicare al fabbricante del sensore di movimento il numero di versione della KM associata.*»;

iii) il paragrafo CSM_108 è sostituito dal seguente:

«*CSM_108 Ciascun fabbricante di sensori di movimento deve generare un numero di serie unico per ciascun sensore di movimento e deve inviare tutti i numeri di serie all'autorità di certificazione dello Stato membro (MSCA) di competenza. La MSCA deve criptare separatamente ciascun numero di serie con la chiave di identificazione del sensore di movimento KID e deve fornire il numero di serie criptato al fabbricante del sensore di movimento. Per ciascun numero di serie criptato, la MSCA deve comunicare al fabbricante del sensore di movimento il numero di versione della KID associata.*»;

h) il punto 9.2.2.1 è così modificato:

i) il paragrafo CSM_123 è sostituito dal seguente:

«*CSM_123 Per ciascuna VU, il fabbricante di VU deve generare un numero di serie unico della VU e inviare tale numero alla rispettiva MSCA in una richiesta volta ad ottenere un insieme di due chiavi DSRC specifiche della VU. Il tipo di dati del numero di serie della VU deve essere VuSerialNumber.*

Nota:

- il numero di serie della VU deve essere identico all'elemento VuSerialNumber contenuto in VuIdentification (cfr. appendice 1) e al riferimento del titolare del certificato indicato nei certificati della VU.

- Il numero di serie della VU può non essere noto nel momento in cui il produttore della VU richiede le chiavi DSRC specifiche della VU. In tal caso, il fabbricante della VU deve inviare al suo posto l'identificativo unico della richiesta di certificato usato nella domanda di certificati della VU; cfr. CSM_153. Tale identificativo della richiesta di certificato deve quindi coincidere con il riferimento del titolare del certificato indicato nei certificati della VU.»;

ii) al paragrafo CSM_124, il requisito info della fase 2 è sostituito dal seguente:

«*info= numero di serie o identificativo della richiesta di certificato della VU come specificato in CSM_123*»;

iii) il paragrafo CSM_128 è sostituito dal seguente:

«*CSM_128 La MSCA deve registrare tutte le chiavi DSRC specifiche della VU che ha generato, il loro numero di versione e il numero di serie o l'identificativo della richiesta di certificato della VU usato per ricavarle.*»;

i) al punto 9.3.1, il primo comma del paragrafo CSM_135 è sostituito dal seguente: «*Per la codifica degli oggetti di dati all'interno dei certificati vanno usate le regole di codifica distinte (DER), conformemente alla norma [ISO 8825-1]. La tabella 4 mostra l'intera codifica dei certificati, compresi tutti i tag e i byte di lunghezza.*»;

j) al punto 9.3.2.3, il paragrafo CSM_141 è sostituito dal seguente:

«*CSM_141 L'autorizzazione del titolare del certificato deve essere usata per identificare il tipo di certificato. Si compone dei sei byte più significativi dell'ID dell'applicazione tachigrafica, concatenati con il tipo di apparecchio cui si riferisce il certificato. Nel caso di un certificato della VU, della carta del conducente o della carta dell'officina, il tipo di apparecchio si usa anche per distinguere tra un certificato di autenticazione reciproca e un certificato per la creazione di firme digitali (cfr. appendice 1, punto 9.1, tipo di dati EquipmentType).*»;

k) al punto 9.3.2.5, paragrafo CSM_146, è aggiunto il comma seguente:

«*Nota: per un certificato della carta, il valore del CHR deve coincidere con il valore cardExtendedSerialNumber nell'EF_ICC; cfr. appendice 2. Per un certificato EGF, il valore del CHR deve coincidere con il valore sensorGNSSSerialNumber nell'EF_ICC; cfr. appendice 14. Per un certificato della VU, il valore del CHR deve coincidere con il l'elemento vuSerialNumber contenuto in VuIdentification, cfr. appendice 1, a meno che al momento della richiesta del certificato il fabbricante non conoscesse il numero di serie specifico del fabbricante.*»;

l) al punto 9.3.2.6, il paragrafo CSM_148 è sostituito dal seguente:

«*CSM_148 La data di efficacia del certificato deve indicare la data e l'ora di inizio del periodo di validità del certificato.*»;

m) il punto 9.3.3 è così modificato:

i) al paragrafo CSM_151, il primo comma è sostituito dal seguente:

«*Per la richiesta di un certificato, la MSCA deve inviare i seguenti dati alla ERCA:*»;

ii) il paragrafo CSM_153 è sostituito dal seguente:

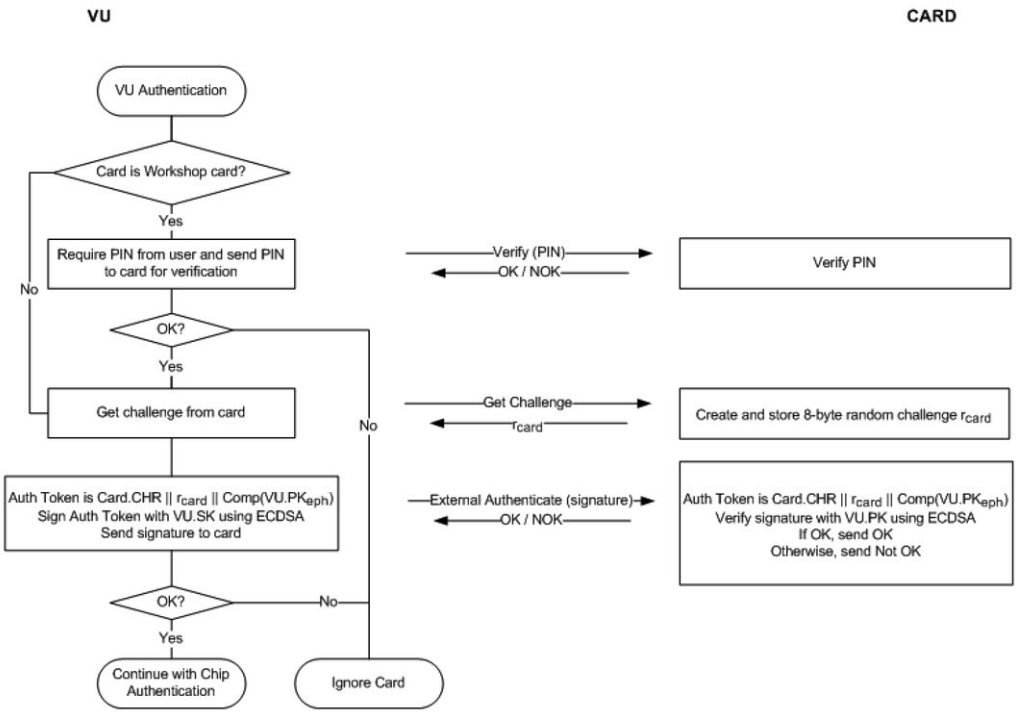
«*CSM_153 Il fabbricante dell'apparecchiatura deve inviare i seguenti dati in una richiesta di certificato alla MSCA, consentendole di creare il riferimento del titolare del certificato relativo al nuovo certificato dell'apparecchiatura:*

- se noto (cfr. CSM_154), un numero di serie per l'apparecchio, univocamente associato al fabbricante, al tipo di apparecchio e al mese di fabbricazione. Altrimenti, un identificativo unico della richiesta di certificato;

- il mese e l'anno di fabbricazione dell'apparecchio o della richiesta di certificato.

Il fabbricante deve garantire che tali dati siano corretti e che il certificato rilasciato dalla MSCA sia inserito

nell'apparecchio cui è destinato.»;
n) il punto 10.2.1 è così modificato:
i) al paragrafo CSM_157, il testo che precede le note alla figura 4 è sostituito dal seguente:
«*Le VU devono usare il protocollo illustrato nella figura 4 per la verifica della catena di certificati di una carta tachigrafica. Per ogni certificato che legge dalla carta, la VU deve verificare che l'informazione contenuta nel campo «autorizzazione del titolare del certificato» (CHA) sia corretta:*
- Il campo CHA del certificato Card deve indicare un certificato di autenticazione reciproca della carta (cfr. appendice 1, tipo di dati EquipmentType).
- Il campo CHA del certificato Card.CA deve indicare una MSCA.
- Il campo CHA del certificato Card.Link deve indicare la ERCA.»;
ii) al paragrafo CSM_159 è aggiunta la frase seguente:
«*Sebbene la memorizzazione di tutti gli altri tipi di certificato sia facoltativa, la VU deve obbligatoriamente memorizzare i certificati nuovi presentati da una carta.*»;
o) il punto 10.2.2 è così modificato:
i) al paragrafo CSM_161, il testo che precede la figura 5 è sostituito dal seguente:
«*Le carte tachigrafiche devono usare il protocollo illustrato nella figura 5 per la verifica della catena di certificati di una VU. Per ogni certificato presentato dalla VU, la carta deve verificare che l'informazione contenuta nel campo «autorizzazione del titolare del certificato» (CHA) sia corretta:*
- Il campo CHA del certificato VU.Link deve indicare la ERCA.
- Il campo CHA del certificato VU.CA deve indicare una MSCA.
- Il campo CHA del certificato VU deve indicare un certificato VU di autenticazione reciproca (cfr. appendice 1, tipo di dati EquipmentType).»;
ii) il paragrafo CSM_165 è sostituito dal seguente:
«*CSM_165 Se il comando MSE: Set AT ha esito positivo, la carta deve impostare il VU.PK indicato per l'uso successivo durante l'autenticazione del veicolo e memorizzare temporaneamente il Comp(VU.PKeph). Nel caso in cui due o più comandi MSE: Set AT siano inviati con esito positivo prima dell'accordo sulla chiave di sessione, la carta deve memorizzare solo l'ultimo Comp(VU.PKeph) ricevuto. La carta deve azzerare Comp(VU.PKeph) una volta che il comando GENERAL AUTHENTICATE ha avuto esito positivo.*»;
p) il punto 10.3 è così modificato:
i) al paragrafo CSM_170, il primo comma è sostituito dal seguente:
«*Accanto alla sfida (challenge) della carta, la VU deve includere nella firma il riferimento al titolare del certificato preso dal certificato della carta.*»;
ii) al paragrafo CSM_171, la figura 6 è sostituita dalla seguente:
«Figura 6
Protocollo di autenticazione della VU



iii) il paragrafo CSM_174 è sostituito dal seguente:
«CSM_174 Al ricevimento della firma della VU in un comando EXTERNAL AUTHENTICATE, la carta deve:
- calcolare il token di autenticazione concatenando Card.CHR, la sfida (challenge) della carta rcard e l'identificativo della chiave pubblica temporanea della VU Comp(VU.PKeph),
- verificare la firma della VU utilizzando l'algoritmo ECDSA, in combinazione con l'algoritmo di hash collegato alle dimensioni della coppia di chiavi VU_MA della VU, come specificato in CSM_50, in combinazione con VU.PK e il token di autenticazione calcolato.»;
q) al punto 10.4, il paragrafo CSM_176 è così modificato:
i) il punto 2 è sostituito dal seguente:
«2. La VU invia alla carta il punto pubblico VU.PKeph della sua coppia di chiavi temporanee. Il punto pubblico deve essere convertito in stringhe di ottetti, come specificato in [TR-03111]. Deve essere usato il formato di codifica non compresso. Come spiegato in CSM_164, la VU ha generato questa coppia di chiavi temporanee prima della verifica della catena di certificati della VU. La VU ha inviato alla carta l'identificativo della chiave pubblica temporanea Comp(VU.PKeph) e la carta lo ha memorizzato.»;
ii) il punto 6 è sostituito dal seguente:
«6. Usando KMAC, la carta calcola un token di autenticazione sul punto pubblico temporaneo della VU: TPICC= CMAC(KMAC, VU.PKeph). Il punto pubblico deve avere il formato utilizzato dalla VU (cfr. punto 2 in alto). La carta invia NPICC e TPICC all'unità elettronica di bordo.»;
r) al punto 10.5.2, il paragrafo CSM_191 è sostituito dal seguente:
«CSM_191 Qualsiasi oggetto di dati da criptare deve essere riempito conformemente alla norma [ISO 7816-4] usando l'indicatore di contenuto di riempimento '01'. Per il calcolo del MAC, gli oggetti di dati nell'APDU devono essere riempiti secondo la norma [ISO 7816-4].
Nota: il riempimento per la messaggistica sicura è sempre eseguito a livello di messaggistica sicura e non dagli algoritmi CMAC o CBC.
Riepilogo ed esempi

Un comando APDU con messaggistica sicura applicata avrà la seguente struttura, a seconda del caso del rispettivo comando non sicuro (DO corrisponde a oggetto di dati):
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 pari): CLA INS P1 P2 || Lc' || DO '81' || DO '8E' || Le
Caso 3 (byte INS dispari): CLA INS P1 P2 || Lc' || DO 'B3' || DO '8E' || Le
Caso 4 (byte INS pari): CLA INS P1 P2 || Lc' || DO '81' || DO '97' || DO '8E' || Le
Caso 4 (byte INS dispari): CLA INS P1 P2 || Lc' || DO 'B3' || DO '97' || DO '8E' || Le
dove Le = '00' o '00 00' a seconda che siano usati campi brevi o lunghi; cfr. [ISO 7816-4].

Una risposta APDU con messaggistica sicura applicata avrà la seguente struttura, a seconda del caso della rispettiva risposta non sicura:
Caso 1 o 3: DO '99' || DO '8E' || SW1SW2
Caso 2 o 4 (byte INS pari) non criptato: DO '81' || DO '99' || DO '8E' || SW1SW2
Caso 2 o 4 (byte INS pari) criptato: DO '87' || DO '99' || DO '8E' || SW1SW2
Caso 2 o 4 (byte INS dispari) non criptato: DO 'B3' || DO '99' || DO '8E' || SW1SW2

Nota: il caso 2 o 4 (byte INS dispari) criptato non è mai usato nella comunicazione tra una VU e una carta.
Di seguito tre esempi di trasformazioni APDU per comandi con codice INS pari. La figura 8 mostra un comando APDU caso 4 autenticato, la figura 9 una risposta APDU caso 1/caso 3 autenticata e la figura 10 una risposta APDU, caso 2/caso 4 autenticata e criptata.

Figura 8
Trasformazione di un comando APDU caso 4 autenticato

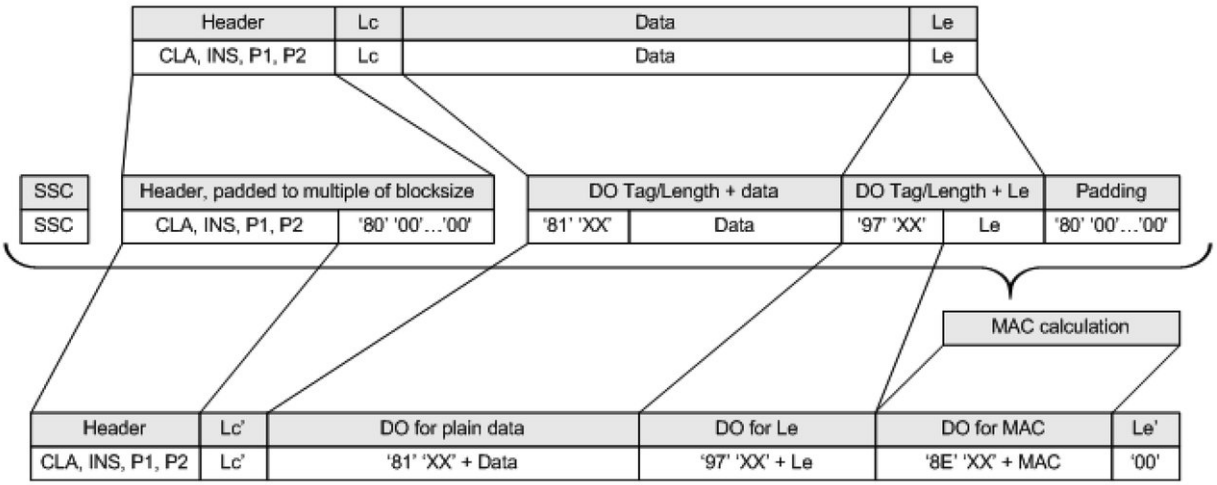


Figura 9
Trasformazione di una risposta APDU caso 1 / caso 3 autenticata

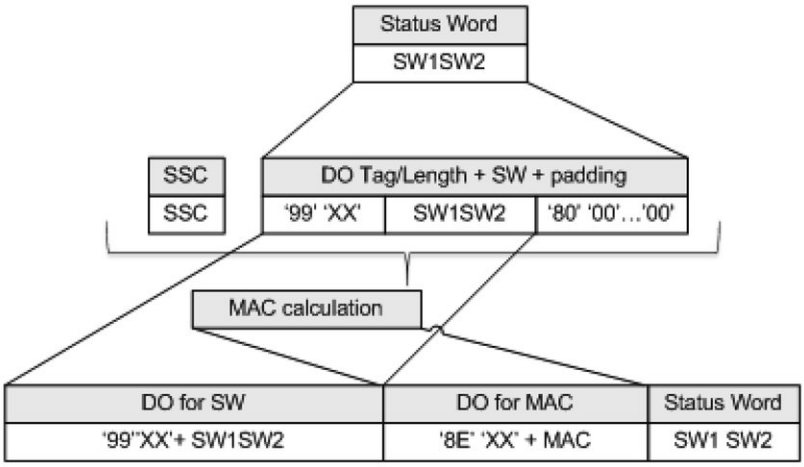
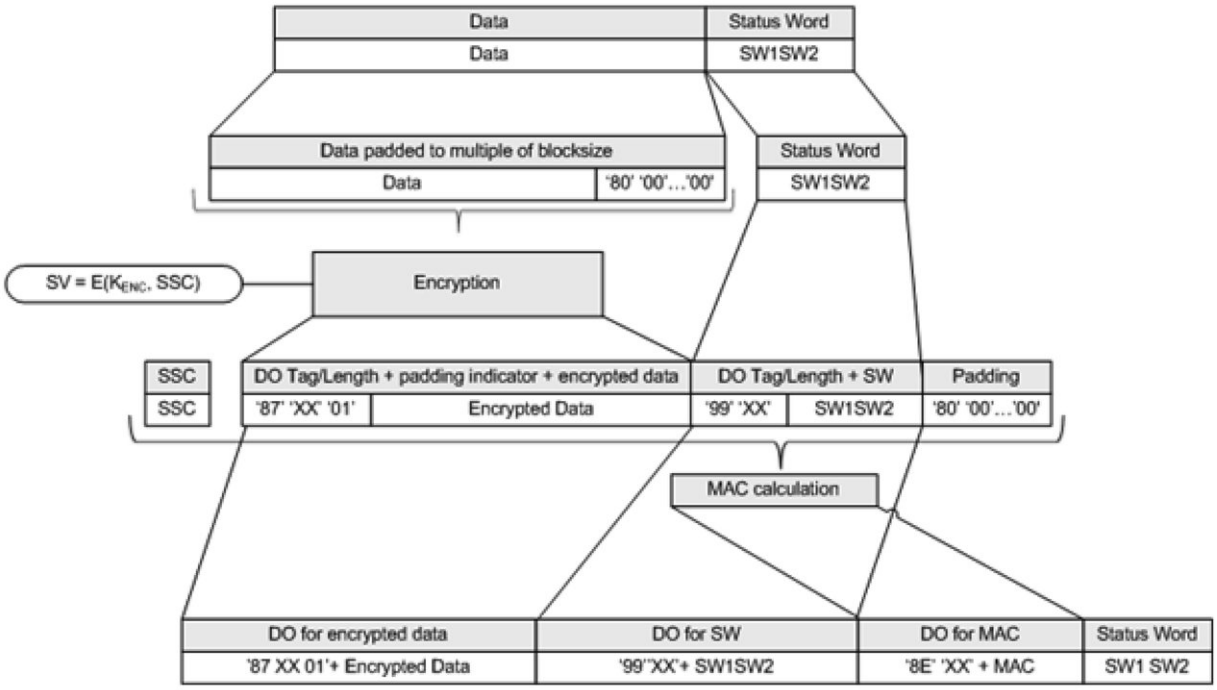


Figura 10
Trasformazione di una risposta APDU caso 2 / caso 4 criptata e autenticata



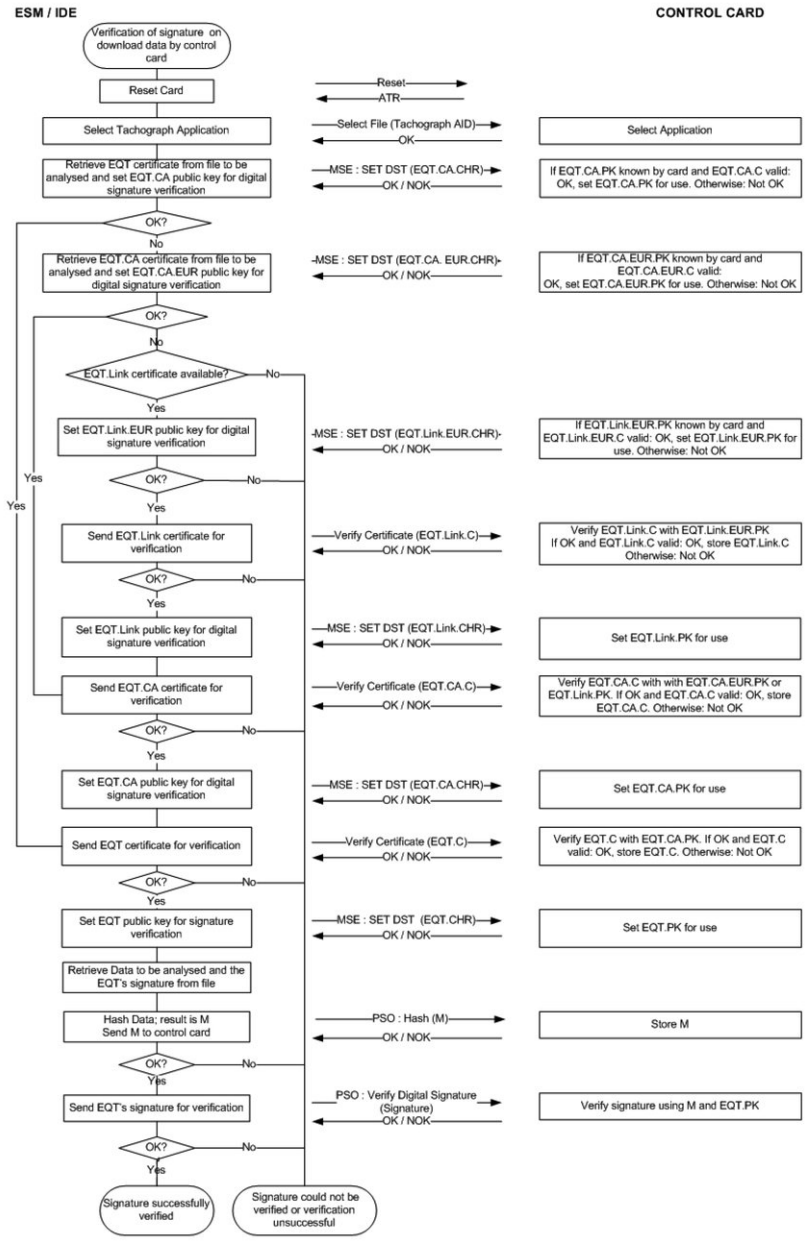
s) al punto 10.5.3, il paragrafo CSM_193 è sostituito dal seguente:
«*CSM_193 Una carta tachigrafica deve interrompere una sessione di messaggistica sicura in corso se e solo se si verifica una delle seguenti condizioni:*
- la carta tachigrafica riceve un comando APDU in chiaro;

- la carta tachigrafica individua un errore di messaggistica sicura in un comando APDU:
- manca un oggetto di dati atteso in messaggistica sicura, l'ordine degli oggetti di dati è errato o è incluso un oggetto di dati sconosciuto,
- un oggetto di dati in messaggistica sicura non è corretto, ad esempio il valore MAC non è corretto o la struttura TLV non è corretta;
- la carta non è più alimentata o viene reinizializzata;
- la VU inizia la procedura di autenticazione della VU;
- è stato raggiunto il limite per il numero di comandi e di risposte associate nell'ambito della sessione corrente. Per una data carta, tale limite deve essere definito dal suo fabbricante, tenendo conto dei requisiti di sicurezza dell'hardware usato, con un valore massimo di 240 comandi di SM e risposte associate per sessione.»;
t) il punto 11.3.2 è così modificato:
i) il primo comma del paragrafo CSM_208 è sostituito dal seguente:
«*Durante l'accoppiamento alla VU, il dispositivo GNSS esterno deve usare il protocollo illustrato nella figura 5 (punto 10.2.2) per verificare la catena di certificati della VU.*»;
ii) il paragrafo CSM_210 è sostituito dal seguente:
«*CSM_210 Dopo la verifica del certificato VU_MA, il dispositivo GNSS esterno deve memorizzare tale certificato da usare durante il funzionamento normale; cfr. sezione 11.3.3.*»;
u) al punto 11.3.3, il primo comma del paragrafo CSM_211 è sostituito dal seguente:
«*Durante il funzionamento normale, la VU e l'EGF devono usare il protocollo della figura 11 per verificare la validità temporale del certificato EGF_MA memorizzato e per impostare la chiave pubblica VU_MA per la successiva autenticazione della VU. Durante il normale funzionamento non deve aver luogo nessun'altra verifica reciproca delle catene di certificati.*»;
v) al punto 12.3, la tabella 6 è sostituita dalla seguente:
«*Tabella 6*
Numero di byte di dati di testo in chiaro (plaintext) e criptati per istruzione definiti in [ISO 16844-3]

Istruzione	***Richiesta / risposta***	***Descrizione dei dati***	***# di byte di dati di testo in chiaro (plaintext) secondo [ISO 16844-3]***	***# di byte di dati di testo in chiaro (plaintext) usando chiavi AES***	***# di byte di dati criptati usando chiavi AES di lunghezza (in bit)***		
					128	***192***	***256***
10	*richiesta*	*Dati di autenticazione + numero del file*	*8*	*8*	*16*	*16*	*16*
11	*risposta*	*Dati di autenticazione + contenuto del file*	*16 o 32 a seconda del file*	*16 o 32 a seconda del file*	*32/48*	*32/48*	*32/48*
41	*richiesta*	*Numero di serie MoS*	*8*	*8*	*16*	*16*	*16*
41	*risposta*	*Chiave di abbinamento*	*16*	*16 / 24 / 32*	*16*	*32*	*32*
42	*richiesta*	*Chiave di sessione*	*16*	*16 / 24 / 32*	*16*	*32*	*32*
43	*richiesta*	*Informazioni di abbinamento*	*24*	*24*	*32*	*32*	*32*
50	*risposta*	*Informazioni di abbinamento*	*24*	*24*	*32*	*32*	*32*
70	*richiesta*	*Dati di autenticazione*	*8*	*8*	*16*	*16*	*16*
80	*risposta*	*Valore del contatore del MoS + dati di autenticazione*	*8*	*8*	*16*	*16*	*16*»

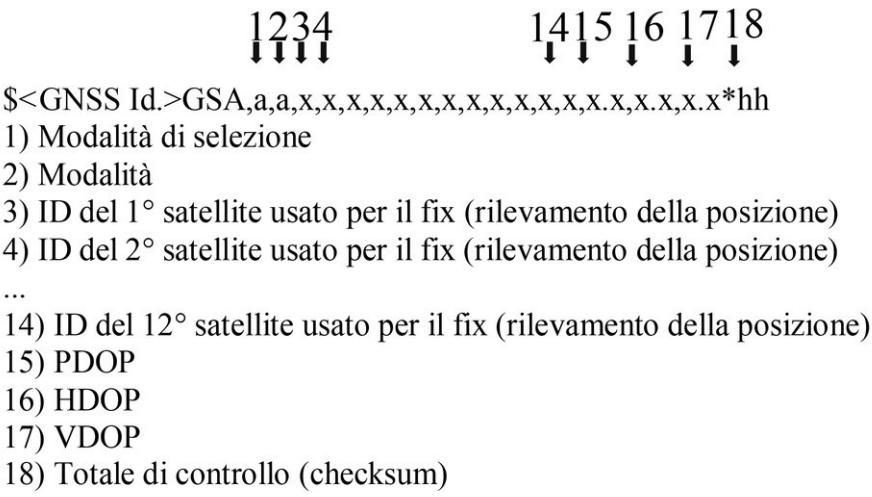
w) al punto 13.1, paragrafo CSM_224, il requisito relativo al numero di serie della VU è sostituito dal seguente:
«*Numero di serie della VU*
Il numero di serie della VU o l'identificativo della richiesta di certificato (tipo di dati VuSerialNumber o CertificateRequestID) – cfr. CSM_123.»;
x) al punto 13.3 il secondo punto del paragrafo CSM_228 è sostituito dal seguente:
«*2. La carta di controllo deve usare la chiave master DSRC indicata in combinazione con il numero di serie della VU o l'identificativo della richiesta di certificato nei dati di sicurezza DSRC per calcolare le chiavi DSRC specifiche della VU K_VUDSRC_ENC e K_VUDSRC_MAC, come specificato in CSM_124.*»;
y) il punto 14.3 è così modificato:

i) al paragrafo CSM_234, il testo che precede le note alla figura 13 è sostituito dal seguente:
«*Un IDE può verificare la firma sui dati trasferiti oppure può usare una carta di controllo per questo scopo. Nel caso usi una carta di controllo, la verifica della firma può avvenire come illustrato in figura 13. Per verificare la validità temporale del certificato presentato dall'IDE, la carta di controllo deve usare l'ora corrente memorizzata internamente, come specificato in CSM_167. La carta di controllo deve aggiornare la propria ora corrente se la data di efficacia di un certificato «sorgente di tempo valida» è più recente dell'ora corrente della carta. La carta deve accettare come sorgente di tempo valida solo i certificati seguenti:*
- certificati di collegamento ERCA di seconda generazione;
- certificati MSCA di seconda generazione;
- certificati VU_Sign o Card_Sign di seconda generazione rilasciati dallo stesso paese del certificato della carta di controllo.
Nel caso verifichi esso stesso la firma, l'IDE deve verificare l'autenticità e la validità di tutti i certificati della catena di certificati nel file di dati e la firma sui dati che seguono lo schema di firma definito in [DSS]. In entrambi i casi, per ciascun certificato letto dal file di dati è necessario verificare che l'informazione contenuta nel campo «autorizzazione del titolare del certificato» (CHA) sia corretta:
- Il campo CHA del certificato EQT deve indicare un certificato VU o Card (a seconda dei casi) usato per la firma (cfr. appendice 1, tipo di dati EquipmentType).
- Il campo CHA del certificato EQT.CA deve indicare una MSCA.
- Il campo CHA del certificato EQT.Link deve indicare la ERCA.»;
ii) la figura 13 è sostituita dalla seguente:
«*Figura 13*
Protocollo di verifica della firma su un file di dati trasferiti



37) l'appendice 12 è così modificata:
a) il punto 3 è così modificato:
i) al paragrafo GNS_4, il secondo comma dopo la figura 2 è sostituito dal seguente:
«*La risoluzione della posizione è basata sul formato della frase RMC di cui sopra. La prima parte dei campi 3) e 5) è usata per rappresentare i gradi. La parte restante è usata per rappresentare i minuti con tre decimali. La risoluzione è quindi 1/1000 di minuto o 1/60000 di grado (poiché un minuto è 1/60 di un grado).*»;
ii) il paragrafo GNS_5 è sostituito dal seguente:
«*GNS_5 L'unità elettronica di bordo deve conservare nella propria banca dati le informazioni sulla posizione per latitudine e longitudine con una risoluzione di 1/10 di min o 1/600 di grado, come descritto nell'appendice 1 per il tipo GeoCoordinates.*
Il comando GPS DOP e satelliti attivi (GSA) può essere usato dalla VU per determinare e registrare la disponibilità e la precisione del segnale. In particolare HDOP è usato per fornire un'indicazione circa il livello di precisione dei dati di localizzazione registrati (cfr. 4.2.2). La VU memorizzerà il valore HDOP (Horizontal Dilution of Precision), calcolato come il valore HDOP minimo tra quelli raccolti dai sistemi GNSS disponibili.
L'identificativo GNSS indica l'identificativo NMEA corrispondente per ogni costellazione GNSS e sistema di potenziamento basato su satelliti (Satellite-Based Augmentation System — SBAS).

Figura 3
Struttura della frase GSA



iii) il paragrafo GNS_6 è sostituito dal seguente:
«*GNS_6 La frase GSA deve essere memorizzata con i numeri di registrazione da '02' a '06'.*»;
b) il punto 4.2.1 è così modificato:
i) il paragrafo GNS_16 è sostituito dal seguente:
«*GNS_16 I campi lunghi non devono essere supportati nel protocollo di comunicazione.*»;
ii) il paragrafo GNS_18 è sostituito dal seguente:
«*GNS_18 Per quanto riguarda le funzioni di 1) raccolta e distribuzione dei dati GNSS, 2) raccolta dei dati di configurazione del dispositivo GNSS esterno e 3) protocollo di gestione, il ricetrasmettitore sicuro GNSS deve simulare una smart card, l'architettura del cui file system è composta da un file master (MF) e da un file dedicato (DF), con l'identificativo dell'applicazione specificato nell'appendice 1, capitolo 6.2 ("FF 44 54 45 47 4D") e con tre EF contenenti i certificati e un solo file elementare (EF.EGF) con l'identificativo uguale a "2F2F" come illustrato nella tabella 1.*»;
iii) il paragrafo GNS_20 è sostituito dal seguente:
«*GNS_20 Il ricetrasmettitore sicuro GNSS deve servirsi di una memoria per conservare i dati e deve essere in grado di eseguire almeno 20 milioni di cicli di scrittura/lettura. A parte questo aspetto, la progettazione interna e l'implementazione del ricetrasmettitore sicuro GNSS è a discrezione dei fabbricanti.*
La mappatura dei numeri di registrazione e dei dati è illustrata nella tabella 1. Da notare che vi sono cinque frasi GSA per le costellazioni GNSS e il sistema satellitare di potenziamento basato su satelliti (SBAS).»;
c) al punto 4.2.2, paragrafo GNS_23, il punto 5 è sostituito dal seguente:
«*5. Il processore della VU verifica i dati ricevuti ed estrae le informazioni (ad esempio latitudine, longitudine, ora) dalla frase NMEA RMC. La frase NMEA RMC comprende le informazioni sulla validità della posizione. Se la posizione non è valida, i dati di localizzazione non sono ancora disponibili e non possono essere usati per registrare*

la posizione del veicolo. Se la posizione è valida, il processore della VU estrae anche i valori di HDOP dalle frasi NMEA GSA e calcola il valore minimo sui sistemi satellitari disponibili (vale a dire quando il fix è disponibile).»;
d) al punto 4.4.1, il paragrafo GNS_28 è sostituito dal seguente:
«*GNS_28 Se non riesce a comunicare col dispositivo GNSS esterno cui è accoppiata per più di 20 minuti consecutivi, la VU deve generare e registrare al suo interno un'anomalia di tipo EventFaultType con il valore di enum '0E'H Communication error with the external GNSS facility (errore di comunicazione con il dispositivo GNSS esterno) e con la marcatura oraria (timestamp) dell'ora corrente. L'anomalia sarà generata solo se sono date le due condizioni seguenti: a) il tachigrafo intelligente non è in modalità taratura e b) il veicolo è in movimento. In questo contesto, si attiva un errore di comunicazione quando il ricetrasmettitore sicuro VU non riceve un messaggio di risposta dopo un messaggio di richiesta come descritto in 4.2.*»;
e) al punto 4.4.2, il paragrafo GNS_29 è sostituito dal seguente:
«*GNS_29 Se il dispositivo GNSS esterno è stato violato, il ricetrasmettitore sicuro GNSS deve cancellare tutta la sua memoria, incluso il materiale crittografico. Come descritto in GNS_25 e GNS_26, la VU deve rilevare le manomissioni se lo stato della risposta è '6690'. La VU deve quindi generare un'anomalia di tipo EventFaultType enum '19'H Tamper detection of GNSS (rilevamento manomissione GNSS). In alternativa, il dispositivo GNSS esterno potrebbe non rispondere più alle richieste esterne.*»;
f) al punto 4.4.3, il paragrafo GNS_30 è sostituito dal seguente:
«*GNS_30 Se non riceve dati dal ricevitore GNSS per più di 3 ore consecutive, il ricetrasmettitore sicuro GNSS deve generare un messaggio di risposta al comando REAR RECORD con il numero di registrazione (RECORD number) uguale a '01' e un campo di dati di 12 byte impostati tutti su 0xFF. Alla ricezione del messaggio di risposta con tale valore del campo di dati, la VU deve generare e registrare un'anomalia di tipo EventFaultType enum '0D'H Absence of position information from GNSS receiver (assenza di informazioni sulla posizione provenienti dal ricevitore GNSS) con la marcatura oraria (timestamp) dell'ora corrente solo se sono date le due seguenti condizioni: a) il tachigrafo intelligente non è in modalità taratura e b) il veicolo è in movimento.*»;
g) al punto 4.4.4, il testo del paragrafo GNS_31 che arriva fino alla figura 4 è sostituito dal seguente:
«*Se rileva che il certificato EGF usato per l'autenticazione reciproca non è più valido, la VU deve generare e registrare un'anomalia dell'apparecchio di registrazione di tipo EventFaultType enum '1B'H External GNSS facility certificate expired (certificato del dispositivo GNSS esterno scaduto) con la marcatura oraria (timestamp) dell'ora corrente. La VU deve comunque continuare a usare i dati sulla posizione GNSS ricevuti.*»;
h) al punto 5.2.1, il paragrafo GNS_34 è sostituito dal seguente:
«*GNS_34 Se non riceve dati dal ricevitore GNSS per più di 3 ore consecutive, la VU deve generare e registrare un'anomalia di tipo EventFaultType enum '0D'H Absence of position information from GNSS receiver (assenza di informazioni sulla posizione provenienti dal ricevitore GNSS) con la marcatura oraria (timestamp) dell'ora corrente solo se sono date le due condizioni seguenti: a) il tachigrafo intelligente non è in modalità taratura e b) il veicolo è in movimento.*»;
i) il punto 6 è sostituito dal seguente:
«*6. CONFLITTO DI ORARI DEL GNSS*
Se rileva una discrepanza di più di 1 minuto tra l'orario della funzione di misurazione dell'ora dell'unità elettronica di bordo e l'orario proveniente dal ricevitore GNSS, la VU registrerà un evento di tipo EventFaultType enum '0B'H Time conflict (GNSS versus VU internal clock) [conflitto di orari (tra GNSS e orologio interno della VU)]. Dopo che si è attivata un'anomalia «Conflitto di orari», la VU non verificherà la discrepanza di orario per le successive 12 ore. Questa anomalia non deve attivarsi qualora nei precedenti 30 giorni non fosse rilevabile alcun segnale GNSS valido dal ricevitore GNSS.»;
38) l'appendice 13 è così modificata:
a) al punto 2, il quarto comma è sostituito dal seguente:
«*Per chiarire, la presente appendice non specifica:*
- la raccolta dei dati relativi al funzionamento e alla gestione all'interno della VU (che sarà specificata altrove nel regolamento oppure sarà una funzione della progettazione del prodotto);
- la forma di presentazione dei dati raccolti all'applicazione installata nel dispositivo esterno;
- le disposizioni sulla sicurezza dei dati superiore a quella fornita da Bluetooth® (ad esempio cifratura) per quanto riguarda il contenuto dei dati [che saranno specificate altrove nel regolamento (Appendice 11 Meccanismi comuni di sicurezza)];
- i protocolli Bluetooth® utilizzati dall'interfaccia ITS.»;
b) al punto 4.2, il terzo comma è sostituito dal seguente:
«*Quando un dispositivo esterno entra nel raggio della VU per la prima volta può iniziare il processo di abbinamento Bluetooth® (cfr. anche allegato 2). I dispositivi condividono i propri indirizzi, nomi, profili e chiave segreta*

comune (common secret key) che consente l'abbinamento automatico in futuro. In seguito, il dispositivo esterno è considerato affidabile ed è in grado di iniziare le richieste di trasferimento dati dal tachigrafo. Non si prevede di aggiungere meccanismi di cifratura supplementari rispetto a quelli forniti da Bluetooth®. Tuttavia se sono necessari ulteriori meccanismi di sicurezza, essi saranno aggiunti conformemente ai meccanismi comuni di sicurezza di cui all'appendice 11.»;

c) il punto 4.3 è così modificato:

i) il primo comma è sostituito dal seguente:

«*Per motivi di sicurezza la VU disporrà un sistema di autorizzazione con codice PIN separato rispetto all'abbinamento Bluetooth. Ogni VU deve essere in grado di generare codici PIN ai fini dell'autenticazione composti da almeno 4 cifre. Ogni volta che un dispositivo esterno si abbina alla VU deve fornire il codice PIN corretto prima di ricevere dati.*»;

ii) il terzo paragrafo che segue la tabella 1 è sostituito dal seguente:

«*Il fabbricante può offrire la possibilità di modificare il codice PIN direttamente tramite la VU, ma il codice PUC non deve essere modificabile. La modifica del codice PIN, se prevista, deve richiedere l'inserimento del codice PIN valido direttamente nella VU.*»;

d) al punto 4.4, il secondo comma che segue il titolo «Campo dati» è sostituito dal seguente:

«*Se il volume dei dati da trattare è superiore allo spazio disponibile in un messaggio, i dati saranno suddivisi in diversi sottomessaggi. Ogni sottomessaggio deve avere la stessa intestazione e SID, ma comprendere un contatore da 2 byte, un contatore corrente [Counter Current (CC)] e un contatore massimo [Counter Max (CM)] per indicare il numero del sottomessaggio. Per abilitare la verifica degli errori e interrompere la trasmissione dati il dispositivo che riceve i dati conferma tutti i sottomessaggi. Il dispositivo che riceve i dati può: accettare un sottomessaggio, chiedere che sia ritrasmesso, richiedere al dispositivo che ha inviato il messaggio di ricominciare o interrompere la trasmissione.*»;

e) l'allegato 1 è così modificato:

i) il titolo è sostituito dal seguente:

«*1) ELENCO DEI DATI DISPONIBILI MEDIANTE L'INTERFACCIA ITS*»;

ii) nella tabella al punto 3, sotto l'elemento «*Assenza di informazioni sulla posizione provenienti dal ricevitore GNSS*», è inserito l'elemento seguente:

«*Errore di comunicazione con il dispositivo GNSS esterno*	*- l'anomalia di maggiore durata per ciascuno degli ultimi 10 giorni in cui si è verificata,* *- le 5 anomalie di maggiore durata nel corso degli ultimi 365 giorni.*	*- data e ora di inizio dell'anomalia,* *- data e ora di fine dell'anomalia,* *- tipo, numero, Stato membro di rilascio e generazione delle carte inserite all'inizio e/o alla fine dell'anomalia,* *- numero di anomalie simili nel giorno in questione.*»

iii) al punto 5 è aggiunto il trattino seguente:

«*- guasto dell'interfaccia ITS (se applicabile)*»;

f) all'allegato 3, le specifiche ASN.1 sono così modificate:

i) al di sotto della riga 206 sono inserite le righe da 206a a 206e seguenti:

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

ii) le righe da 262 a 264 sono sostituite dalle seguenti:

```
«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 riga 275 è sostituita dalla seguente:

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

iv) le righe da 288 a 310 sono sostituite dalle seguenti:

```
«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) le righe da 362 a 363 sono sostituite dalle seguenti:

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

vi) al di sotto della riga 410 sono inserite le righe 410a e 410b seguenti:

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

vii) al di sotto della riga 539 sono inserite le righe da 539a a 539j seguenti:

```
«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) l'appendice 14 è così modificata:

a) l'elemento 5.5 dell'indice è sostituito dal seguente:

«*5.5 Conformità alla direttiva (UE) 2015/719…490*»;

b) al punto 2, il terzo comma è sostituito dal seguente:

«*In questo scenario, il tempo a disposizione per la comunicazione è limitato, perché la comunicazione è mirata e a corto raggio. Il mezzo di comunicazione usato per il monitoraggio a distanza del tachigrafo (RTM) può essere inoltre usato dalle autorità di controllo competenti anche per altre applicazioni [ad esempio per i pesi massimi e le dimensioni massime dei veicoli commerciali pesanti definiti nella direttiva (UE) 2015/719] e tali operazioni possono essere separate o in sequenza a discrezione delle autorità di controllo competenti.*»;

c) il punto 5.1 è così modificato:

i) al paragrafo DSC_19, il dodicesimo trattino è sostituito dal seguente:

«- *L'antenna DSRC-VU deve essere posizionata in modo da ottimizzare la comunicazione DSRC tra il veicolo e l'antenna del lettore a lato della strada, se il lettore è installato a 15 metri di distanza di fronte al veicolo e a due metri di altezza dal suolo ed è orientato al centro del parabrezza del veicolo sugli assi orizzontale e verticale. Sui veicoli leggeri è appropriato installarla nella parte superiore del parabrezza. Su tutti gli altri veicoli l'antenna DSRC dovrebbe essere installata in prossimità della parte inferiore o della parte superiore del parabrezza.*»;

ii) al paragrafo DSC_22, il primo comma è sostituito dal seguente:

«*Il fattore di forma dell'antenna non è definito ed è una decisione commerciale, purché la DSRC-VU montata soddisfi i requisiti di conformità definiti nel paragrafo 5 che segue. L'antenna deve essere posizionata come de-*

terminato in DSC_19 e deve supportare efficacemente i casi d'impiego descritti ai paragrafi 4.1.2 e 4.1.3.»;
d) al punto 4.5.3, la sequenza 7 è sostituita dalla seguente:

«*7*	*REDCR*	*>*	*DSRC-VU*	*Invia GET.request per i dati di attributo diverso (se del caso)*»

e) al punto 5.4.4, paragrafo DCS_40, la definizione del modulo ASN.1 alè così modificata:
(i) la prima riga della sequenza per TachographPayload è sostituita dalla seguente:

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

ii) è aggiunta la nota 1 seguente:
«*1. Se un LPN contiene un indicatore alfabetico LatinAlphabetNo2 o latinCyrillicAlphabet, i caratteri speciali sono rimappati dall'unità di strada dell'interrogatore applicando le norme speciali di cui all'allegato E della norma ISO/DIS 14 906,2*»;
iii) nella riga in cui è definito il timestamp del record attuale («timestamp of current record»), l'apice numerico «2» è soppresso;
iv) la definizione del modulo ASN.1 per RtmTransferAck è sostituita dalla seguente:

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

f) al punto 5.4.5, l'elemento RTM12 della tabella 14.3 è sostituito dal seguente:

«*RTM12* *Guasto del sensore*	*La VU deve generare un valore intero per l'elemento di dati RTM12.* *La VU deve assegnare alla variabile sensorFault un valore di:* *- 1 se è stata registrata un'anomalia di tipo '35'H «Guasto del sensore» negli ultimi 10 giorni,* *- 2 se è stata registrata un'anomalia di tipo «Guasto del ricevitore GNSS» (interno o esterno con i valori enum '36'H o '37'H) negli ultimi 10 giorni.* *- 3 se è stata registrata un'anomalia di tipo '0E'H «Errore di comunicazione con il dispositivo GNSS esterno» negli ultimi 10 giorni.* *- 4 se sono stati registrati sia un guasto del sensore sia guasti del ricevitore GNSS negli ultimi 10 giorni.* *- 5 se sono stati registrati sia un guasto del sensore sia un errore di comunicazione con il dispositivo GNSS esterno negli ultimi 10 giorni.* *- 6 se sono stati registrati sia un guasto del ricevitore GNSS sia un errore di comunicazione con il dispositivo GNSS esterno negli ultimi 10 giorni.* *- 7 se sono stati registrati tutti e tre i guasti del sensore negli ultimi 10 giorni. In TUTTI GLI ALTRI CASI deve assegnare un valore «0» se non sono state registrate anomalie negli ultimi 10 giorni.*	*–Guasto del sensore, un ottetto secondo il dizionario di dati*	`sensorFault INTEGER (0..255),;`

g) al punto 5.4.6, il paragrafo DSC_43 è sostituito dal seguente:
«*DSC_43 Per tutti gli altri scambi DSRC, i dati devono essere codificati usando le PER (regole di codifica del pacchetto) SENZA ALLINEAMENTO, tranne nel caso di TachographPayload e OwsPayload; , che devono essere codificati usando le OER (regole di codifica all'ottetto) definite dalla norma ISO/IEC 8825-7, Rec. ITU-T X.696.*»;
h) al punto 5.4.7, nella quarta colonna della tabella 14.9, il testo nella casella che descrive Rtm-ContexMark;
è sostituito dal seguente:
«*Identificativo dell'oggetto della norma, della parte e della versione supportate. Esempio: ISO (1) Norma (0) TARV (15638) Parte 9 (9) Versione 1 (1).*
Il primo ottetto è 06H, che è l'identificativo dell'oggetto; il secondo ottetto è 06H, che è la sua lunghezza. I 6 ottetti successivi codificano l'identificativo dell'oggetto preso come esempio.»;

i) i punti 5.5 e 5.5.1 sono sostituiti dai seguenti:
«*5.5. Conformità alla direttiva (UE) 2015/719*
5.5.1. Riepilogo
DSC_59 Per conformarsi alla direttiva (UE) 2015/719 sulle dimensioni massime e i pesi massimi dei veicoli commerciali pesanti, il protocollo della transazione per scaricare i dati OWS tramite il collegamento dell'interfaccia DSRC 5,8 GHz sarà lo stesso usato per i dati RTM (cfr. 5.4.1), con l'unica differenza che l'identificativo dell'oggetto relativo alla norma TARV riguarderà la norma ISO 15638 (TARV) parte 20 concernente i WOB/OWS.»;
j) al punto 5.6.1, il punto a) del paragrafo DSC_68 è sostituito dal seguente:
«*a) al fine di consentire l'acquisto di VU, DSCR-VU e di diversi lotti di DSRC-VU da fornitori diversi, il collegamento tra la VU e la DSRC-VU non interno alla VU deve essere un collegamento standard aperto. La VU deve collegarsi alla DSRC-VU:*»;
k) al punto 5.7.1, il paragrafo DSC_77 è sostituito dal seguente:
«*DSC_77 I dati devono essere forniti, già sicuri, dalla funzione VUSM alla DSRC-VU. La VUSM deve verificare che i dati registrati nella DSRC-VU siano stati registrati correttamente. La registrazione e la comunicazione degli eventuali errori nel trasferimento dei dati dalla VU alla memoria della DSRC-VU devono essere registrate insieme al timestamp come EventFaultType e con il valore enum impostato a '0C'H (corrispondente all'anomalia «Errore di comunicazione con il dispositivo di comunicazione remota»).*»;
40) l'appendice 15 è così modificata:
a) il primo comma del punto 2.2 è sostituito dal seguente:
«*È sottinteso che le carte tachigrafiche di prima generazione sono interoperabili con le unità elettroniche di bordo di prima generazione conformemente all'allegato IB del regolamento (CEE) n. 3821/85, mentre le carte tachigrafiche di seconda generazione sono interoperabili con le unità elettroniche di bordo di seconda generazione conformemente all'allegato IC del presente regolamento. Inoltre si applicano i requisiti riportati di seguito.*»;
b) al punto 2.4.1, il paragrafo MIG_011 è così modificato:
i) il primo trattino è sostituito dal seguente:
«*- EF IC e ICC non firmati (facoltativo),*»;
ii) il terzo trattino è sostituito dal seguente:
«*- gli altri EF dei dati applicativi (all'interno del DF Tachograph) richiesti dal protocollo di trasferimento della carta di prima generazione. Tali informazioni devono essere rese sicure mediante una firma digitale conformemente ai meccanismi di sicurezza di prima generazione.*
Tale trasferimento di dati non deve includere gli EF dei dati applicativi presenti solo nelle carte del conducente (e dell'officina) di seconda generazione (EF dei dati applicativi all'interno del DF Tachograph_G2).»;
c) al punto 2.4.3, i paragrafi MIG_014 e MIG_015 sono sostituiti dai seguenti:
«*MIG_014 Tranne che nel caso dei controlli dei conducenti da parte di un'autorità di controllo non UE, i dati devono essere trasferiti da un'unità elettronica di bordo di seconda generazione utilizzando i meccanismi di sicurezza di seconda generazione e il protocollo di trasferimento dati di cui all'appendice 7 del presente allegato.*
MIG_015 Per consentire il controllo dei conducenti da parte di autorità non UE, facoltativamente può essere reso possibile il trasferimento dei dati da unità elettroniche di bordo di seconda generazione utilizzando meccanismi di sicurezza di prima generazione. I dati trasferiti devono quindi avere lo stesso formato dei dati trasferiti da un'unità elettronica di bordo di prima generazione. Questa facoltà può essere selezionata mediante i comandi del menù.»;