I

(Atti per i quali la pubblicazione è una condizione di applicabilità)

REGOLAMENTO (CE) Nº 1360/2002 DELLA COMMISSIONE

del 13 giugno 2002

che adegua per la settima volta al progresso tecnico il regolamento (CEE) n. 3821/85 del Consiglio relativo all'apparecchio di controllo nel settore dei trasporti su strada

(Testo rilevante ai fini del SEE)

LA COMMISSIONE DELLE COMUNITÀ EUROPEE,

visto il trattato che istituisce la Comunità europea,

visto il regolamento (CEE) n. 3821/85 del Consiglio, del 20 dicembre 1985, relativo all'apparecchio di controllo nel settore dei trasporti su strada ([1]), modificato da ultimo dal regolamento (CE) n. 2135/98 ([2]), in particolare gli articoli 17 e 18,

considerando quanto segue:

(1) Le specifiche tecniche di cui all'allegato I B del regolamento (CEE) n. 3821/85 devono essere adeguate al progresso tecnico, prestando particolare attenzione alla sicurezza generale del sistema e all'interoperabilità tra l'apparecchio di controllo e le carte del conducente.

(2) Per l'adeguamento dell'apparecchio è inoltre necessario adeguare l'allegato II del regolamento (CEE) n. 3821/85, in cui sono definiti i marchi e le schede di omologazione.

(3) Il Comitato istituito dall'articolo 18 del regolamento (CEE) n. 3821/85 non ha espresso un parere sulle misure contenute nella proposta e la Commissione ha quindi presentato al Consiglio una proposta concernente tali misure.

(4) Trascorso il periodo di cui all'articolo 18, paragrafo 5, lettera b), del regolamento (CEE) n. 3821/85, il Consiglio non aveva deliberato e spetta quindi alla Commissione adottare tali misure,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

L'allegato del regolamento (CE) n. 2135/98 è sostituito dall'allegato del presente regolamento.

Articolo 2

L'allegato II del regolamento (CEE) n. 3821/85 è modificato come segue:

1) Il capitolo I, punto 1, primo trattino è modificato come segue:
   — il segno distintivo per la Grecia «GR» è sostituito da «23»;
   — il segno distintivo per l'Irlanda «IRL» è sostituito da «24»;
   — il segno distintivo «12» è aggiunto per l'Austria;
   — il segno distintivo «17» è aggiunto per la Finlandia;
   — il segno distintivo «5» è aggiunto per la Svezia.
2) Il capitolo I, punto 1, secondo trattino è modificato come segue:
   — dopo la parola «foglio» sono aggiunte le parole «o della carta tachigrafica».
3) Il capitolo I, punto 2, è modificato come segue:
   — dopo le parole «foglio di registrazione» sono aggiunte le parole «e su ogni carta tachigrafica».
4) Al titolo del capitolo II sono aggiunte le parole «DEI PRODOTTI CONFORMI ALL'ALLEGATO I».

([1]) GU L 370 del 31.12.1985, pag. 8.
([2]) GU L 274 del 9.10.1998, pag. 1.

5) È aggiunto il seguente capitolo III:

«III. SCHEDA DI OMOLOGAZIONE DEI PRODOTTI CONFORMI ALL'ALLEGATO I B

Lo Stato che ha effettuato l'omologazione rilascia al richiedente una scheda di omologazione di cui viene riprodotto un modello qui di seguito. Per la comunicazione agli altri Stati membri delle omologazioni accordate o degli eventuali ritiri, ciascuno Stato membro utilizza copie di questo documento.

SCHEDA DI OMOLOGAZIONE DEI PRODOTTI CONFORMI ALL'ALLEGATO I B

Nome dell'amministrazione competente: .....

Comunicazione concernente (*):

☐ l'omologazione di

☐ il ritiro dell'omologazione di

☐ un modello di apparecchio di controllo

☐ un componente dell'apparecchio di controllo (**) .....

☐ una carta del conducente

☐ una carta dell'officina

☐ una carta dell'azienda

☐ una carta di controllo

N. di omologazione .....

1. Marchio di fabbrica o di commercio .....
2. Denominazione del modello .....
3. Nome del fabbricante .....
4. Indirizzo del fabbricante .....
5. Presentato all'omologazione di .....
6. Laboratorio/i .....
7. Data e numero delle prove .....
8. Data dell'omologazione .....
9. Data del ritiro dell'omologazione .....
10. Modello di componente/i dell'apparecchio di controllo con il quale il componente è destinato ad essere utilizzato .....
11. Luogo .....
12. Data .....
13. Documenti illustrativi allegati .....

---

14. Osservazioni (compresa la posizione di eventuali sigilli)

.....

(Firma)

(*) Barrare la casella corrispondente.
(**) Indicare il componente oggetto della comunicazione.»

Articolo 3

Il presente regolamento entra in vigore il ventesimo giorno successivo a quello della pubblicazione nella *Gazzetta ufficiale delle Comunità europee*.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il 13 giugno 2002.

Per la Commissione
Loyola DE PALACIO
Vicepresidente

ALLEGATO

«ALLEGATO I B

REQUISITI PER LA COSTRUZIONE, LA PROVA, IL MONTAGGIO E IL CONTROLLO

Al fine di preservare l'interoperabilità dei programmi delle apparecchiature definite nel presente allegato, alcune sigle, alcuni termini o espressioni di programmazione informatica sono stati mantenuti nella lingua d'origine in cui è stato redatto il testo, ossia in inglese. Tuttavia, delle traduzioni letterali sono state inserite, tra parentesi e per informazione, accanto ad alcune espressioni per facilitarne la comprensione.

INDICE

I. DEFINIZIONI

Ai sensi del presente allegato, s'intende per:

a) **attivazione**:

la fase in cui l'apparecchio di controllo diventa pienamente efficiente e in grado di assolvere tutte le sue funzioni, comprese quelle di sicurezza.

L'attivazione di un apparecchio di controllo richiede l'impiego di una carta dell'officina e l'immissione del relativo codice di identificazione personale;

b) **autenticazione**:

la funzione di identificazione e verifica dell'identità indicata;

c) **autenticità**:

la caratteristica secondo cui un'informazione proviene da una fonte di cui si può verificare l'identità;

d) **prova incorporata**:

le prove effettuate su richiesta, azionate dall'operatore o da un apparecchio esterno;

e) **giorno di calendario**:

una giornata che va dalle ore 00.00 alle ore 24.00. Tutti i giorni di calendario si riferiscono al tempo UTC (Tempo universale coordinato);

f) **calibratura**:

l'aggiornamento o la conferma dei parametri del veicolo da conservare nei dati memorizzati. Tali parametri comprendono l'identificazione del veicolo (VIN, VRN e Stato membro di immatricolazione) e le caratteristiche del veicolo [w, k, l, dimensioni dei pneumatici, regolazione del limitatore di velocità (se applicabile), ora corrente (UTC), valore corrente dell'odometro].

La calibratura di un apparecchio di controllo richiede l'impiego di una carta dell'officina;

g) **numero della carta**:

un numero di 16 caratteri alfanumerici che identifica in modo inequivocabile una carta tachigrafica all'interno di uno Stato membro. Il numero della carta comprende un codice di serie (se applicabile), un codice di sostituzione e un codice di rinnovo.

Una carta è quindi identificata in modo inequivocabile dal codice dello Stato membro di rilascio e dal numero della carta;

h) **codice di serie della carta**:

il 14º carattere alfanumerico del numero della carta inteso a differenziare le diverse carte rilasciate ad un'impresa o ad un organismo autorizzati ad ottenere più carte tachigrafiche. L'impresa o l'organismo sono identificati in modo inequivocabile dai primi 13 caratteri del numero della carta;

i) **codice di rinnovo della carta**:

il 16º carattere alfanumerico del numero della carta, che viene aumentato di un'unità ad ogni rinnovo della carta tachigrafica;

j) **codice di sostituzione della carta**:

il 15º carattere alfanumerico del numero della carta, che viene aumentato di un'unità ad ogni sostituzione di una carta tachigrafica;

k) **coefficiente caratteristico del veicolo**:

la caratteristica numerica che esprime il valore del segnale di uscita emesso dalla parte del veicolo collegata all'apparecchio di controllo (albero del cambio o asse) quando il veicolo percorre la distanza di un chilometro in condizioni normali di prova (cfr. capitolo VI, punto 5). Il coefficiente caratteristico è espresso in impulsi per chilometro (w = … imp/km);

l) **carta dell'azienda**:

una carta tachigrafica rilasciata dalle autorità di uno Stato membro al proprietario o detentore di veicoli muniti di apparecchio di controllo.

La carta dell'azienda identifica l'impresa e consente la visualizzazione, il trasferimento e la stampa dei dati memorizzati nell'apparecchio di controllo su cui tale impresa ha attivato un blocco;

m) **costante dell'apparecchio di controllo**:

la caratteristica numerica che esprime il valore del segnale di entrata necessario per ottenere l'indicazione e la registrazione della distanza percorsa di 1 chilometro; la costante è espressa in impulsi per chilometro (k = … imp/km);

n) **periodo di guida continuo (calcolato all'interno dell'apparecchio di controllo)** ([1]):

la somma corrente dei periodi di guida accumulati da un determinato conducente, a partire dal termine del suo ultimo periodo di DISPONIBILITÀ o INTERRUZIONE/RIPOSO o periodo NON NOTO ([2]) di 45 o più minuti (questo periodo può essere ripartito in diversi periodi di 15 o più minuti). I calcoli tengono conto, a seconda della necessità, delle attività precedenti memorizzate sulla carta del conducente. Qualora il conducente non abbia inserito la sua carta, i calcoli si basano sulle registrazioni nella memoria di dati riferite al periodo corrente durante il quale la carta non era inserita e relative alla sede (slot) pertinente;

o) **carta di controllo**:

una carta tachigrafica rilasciata dalle autorità di uno Stato membro alle autorità nazionali competenti per i controlli.

La carta di controllo identifica l'organismo preposto ai controlli, e possibilmente l'agente incaricato dei controlli, e consente di accedere ai dati memorizzati nella memoria o nelle carte del conducente ai fini della lettura, della stampa e/o del trasferimento;

p) **periodo cumulato di interruzione (calcolato all'interno dell'apparecchio di controllo)** ([1]):

il periodo cumulato di interruzione della guida è calcolato come la somma corrente dei periodi di DISPONIBILITÀ o INTERRUZIONE/RIPOSO o periodi NON NOTI ([2]) di 15 o più minuti accumulati da un determinato conducente, a partire dal termine del suo ultimo periodo di DISPONIBILITÀ o INTERRUZIONE/RIPOSO o periodo NON NOTO ([2]) di 45 o più minuti (questo periodo può essere ripartito in diversi periodi di 15 o più minuti).

I calcoli tengono conto, a seconda della necessità, delle attività precedenti memorizzate sulla carta del conducente. I periodi non noti di durata negativa (inizio del periodo non noto > termine del periodo non noto), dovuti a sovrapposizioni di orari tra due diversi apparecchi di controllo, non sono presi in considerazione.

Qualora il conducente non abbia inserito la sua carta, i calcoli si basano sulle registrazioni nella memoria di dati riferite al periodo corrente durante il quale la carta non era inserita e relative alla sede (slot) pertinente;

q) **memoria di dati**:

un dispositivo elettronico di memorizzazione di dati, incorporato nell'apparecchio di controllo;

r) **firma digitale**:

i dati aggiunti a un blocco di dati, o una trasformazione crittografica dello stesso, che consentono al destinatario del blocco di dati di verificarne l'autenticità e l'integrità;

s) **trasferimento**:

la copia, insieme alla firma digitale, di una parte o di tutti i dati registrati nella memoria di dati del veicolo o nella memoria di una carta tachigrafica.

Il trasferimento non deve alterare o cancellare alcun dato memorizzato;

([1]) Questo metodo di calcolare il periodo di guida continuo e il periodo cumulato di interruzione consente all'apparecchio di controllo di calcolare gli avvisi relativi al periodo di guida continuo. Esso non pregiudica l'interpretazione giuridica da dare a tali periodi.

([2]) I periodi NON NOTI corrispondono ai periodi durante i quali la carta del conducente non era inserita in un apparecchio di controllo e per i quali non è stata effettuata l'immissione manuale delle attività del conducente.

t) **carta del conducente**:

una carta tachigrafica assegnata dalle autorità di uno Stato membro a ciascun conducente.

La carta del conducente identifica il conducente e consente la memorizzazione dei dati relativi alle sue attività;

u) **circonferenza effettiva dei pneumatici delle ruote**:

la media delle distanze percorse da ciascuna delle ruote che imprimono il movimento al veicolo (ruote motrici) durante una rotazione completa. La misurazione di queste distanze deve essere effettuata in condizioni normali di prova (cfr. capitolo VI, punto 5) ed è espressa con: "l = … mm". I costruttori di veicoli possono sostituire la misurazione di queste distanze con un calcolo teorico che tenga conto della ripartizione del peso sugli assi, con veicolo a vuoto in normali condizioni di marcia ([1]). I metodi di tale calcolo teorico devono essere approvati dalle autorità competenti degli Stati membri;

v) **anomalia**:

un'operazione anomala rilevata dall'apparecchio di controllo che può essere dovuta a un tentativo di frode;

w) **guasto**:

un'operazione anomala rilevata dall'apparecchio di controllo che può essere dovuta al cattivo funzionamento o al guasto di un apparecchio;

x) **montaggio**:

l'installazione dell'apparecchio di controllo in un veicolo;

y) **sensore di movimento**:

un elemento dell'apparecchio di controllo che fornisce un segnale corrispondente alla velocità del veicolo e/o alla distanza percorsa;

z) **carta non valida**:

una carta riscontrata difettosa, o la cui autenticazione iniziale è stata respinta, o la cui data di inizio di validità non è ancora stata raggiunta, o la cui data di scadenza è stata superata;

aa) **escluso dal campo di applicazione**:

la circostanza in cui non è prescritto l'uso dell'apparecchio di controllo, secondo le disposizioni del regolamento (CEE) n. 3820/85 del Consiglio;

bb) **superamento di velocità**:

il superamento della velocità autorizzata del veicolo, definito come ogni periodo di durata superiore a 60 secondi durante il quale la velocità misurata del veicolo supera il limite del valore di regolazione del limitatore di velocità stabilito dalla direttiva 92/6/CEE del Consiglio, del 10 febbraio 1992, concernente il montaggio e l'impiego di limitatori di velocità per talune categorie di veicoli nella Comunità ([2]);

cc) **controllo periodico**:

un insieme di operazioni effettuate per verificare il corretto funzionamento dell'apparecchio di controllo e la corrispondenza tra i valori di regolazione e i parametri del veicolo;

dd) **stampante**:

un componente dell'apparecchio di controllo che fornisce documenti stampati dei dati memorizzati;

ee) **apparecchio di controllo**:

l'insieme delle apparecchiature destinate ad essere montate a bordo di veicoli stradali per indicare, registrare e memorizzare in modo automatico o semiautomatico i dati sulla marcia di questi veicoli e su determinati periodi di lavoro dei loro conducenti;

([1]) Direttiva 97/27/CE del Parlamento europeo e del Consiglio, del 22 luglio 1997, concernente le masse e le dimensioni di alcune categorie di veicoli a motore e dei loro rimorchi e che modifica la direttiva 70/156/CEE (GU L 233 del 25.8.1997, pag. 1).

([2]) GU L 57 del 2.3.1992, pag. 27.

ff) **rinnovo**:

il rilascio di una nuova carta tachigrafica quando una carta esistente raggiunge il termine del suo periodo di validità, o non funziona correttamente e viene restituita alle autorità di rilascio. Il rinnovo implica sempre la certezza che due carte valide non coesistono;

gg) **riparazione**:

ogni riparazione di un sensore di movimento o di un'unità elettronica di bordo che comporta l'interruzione dell'alimentazione di energia, o il disinnesto da altri componenti dell'apparecchio di controllo, o l'apertura dello stesso;

hh) **sostituzione**:

il rilascio di una carta tachigrafica in sostituzione di una carta esistente, dichiarata smarrita, rubata o non funzionante, che non viene restituita alle autorità di rilascio. La sostituzione implica sempre il rischio che possano coesistere due carte valide;

ii) **certificazione della sicurezza**:

la procedura, condotta da un organismo di certificazione ITSEC ([1]), volta a certificare che l'apparecchio di controllo (o suo componente) o la carta tachigrafica in esame soddisfa i requisiti di sicurezza definiti all'appendice 10, Obiettivi generali di sicurezza;

jj) **prova automatica**:

le prove cicliche ed automatiche effettuate dall'apparecchio di controllo per rilevare eventuali guasti;

kk) **carta tachigrafica**:

una carta intelligente da impiegare con l'apparecchio di controllo. Le carte tachigrafiche consentono l'identificazione, da parte dell'apparecchio di controllo, dell'identità (o gruppo di identità) del titolare della carta e il trasferimento e la memorizzazione di dati. Sono usati i seguenti tipi di carta tachigrafica:

— carta del conducente,

— carta di controllo,

— carta dell'officina,

— carta dell'azienda;

ll) **omologazione**:

la procedura in base alla quale uno Stato membro certifica che l'apparecchio di controllo (o suo componente) o la carta tachigrafica in esame soddisfa i requisiti del presente regolamento;

mm) **dimensioni dei pneumatici**:

l'indicazione delle dimensioni dei pneumatici (ruote motrici esterne), in conformità della direttiva 92/23/CEE ([2]);

nn) **identificazione del veicolo**:

i numeri che identificano il veicolo: numero di immatricolazione del veicolo (VRN), con indicazione dello Stato membro di immatricolazione, e numero di identificazione del veicolo (VIN) ([3]);

oo) **unità elettronica di bordo (VU)**:

l'apparecchio di controllo, escluso il sensore di movimento e i cavi di collegamento del sensore di movimento. L'unità elettronica di bordo può consistere in un unico dispositivo o in diversi dispositivi distribuiti a bordo del veicolo, purché sia conforme ai requisiti di sicurezza previsti dal presente regolamento;

([1]) Raccomandazione 95/144/CE del Consiglio, del 7 aprile 1995, su criteri comuni per la valutazione della sicurezza delle tecnologie d'informazione (GU L 93 del 26.4.1995, pag. 27).
([2]) GU L 129 del 14.5.1992, pag. 95.
([3]) Direttiva 76/114/CEE del 18.12.1975 (GU L 24 del 30.1.1976, pag. 1).

pp) **settimana (ai fini dei calcoli interni dell'apparecchio di controllo)**:

il periodo compreso tra le ore 00.00 UTC del lunedì e le ore 24.00 UTC della domenica;

qq) **carta dell'officina**:

una carta tachigrafica assegnata dalle autorità di uno Stato membro ai fabbricanti di apparecchi di controllo, ai montatori, ai costruttori di veicoli o alle officine, approvati dallo Stato membro in questione.

La carta dell'officina identifica il titolare della carta e consente la prova, la calibratura e/o il trasferimento dei dati dell'apparecchio di controllo.

II. CARATTERISTICHE GENERALI E FUNZIONI DELL'APPARECCHIO DI CONTROLLO

000 I veicoli su cui è montato un apparecchio di controllo conforme alle disposizioni del presente allegato devono essere muniti di un indicatore di velocità e di un odometro. Tali funzioni possono essere incorporate nell'apparecchio di controllo.

1. **Caratteristiche generali**

L'apparecchio di controllo ha lo scopo di registrare, memorizzare, indicare, stampare e trasmettere dati relativi alle attività del conducente.

001 L'apparecchio di controllo comprende i cavi, un sensore di movimento e un'unità elettronica di bordo.

002 L'unità elettronica di bordo è costituita da un'unità di elaborazione, una memoria di dati, un orologio in tempo reale, due interfacce per carte intelligenti (conducente e secondo conducente), una stampante, un dispositivo di visualizzazione, un avvisatore visivo, un connettore di calibratura/trasferimento dati e dispositivi per l'immissione di dati da parte dell'utente.

L'apparecchio di controllo può essere collegato ad altri dispositivi attraverso connettori aggiuntivi.

003 L'eventuale presenza nell'apparecchio di controllo o collegamento ad esso di altre funzioni o dispositivi, omologati o meno, non deve interferire direttamente o indirettamente con il funzionamento corretto e sicuro dell'apparecchio di controllo e con le disposizioni del regolamento.

Gli utenti dell'apparecchio di controllo sono identificati dall'apparecchio per mezzo di carte tachigrafiche.

004 L'apparecchio di controllo fornisce diritti di accesso selettivi ai dati e alle funzioni, a seconda del tipo e/o dell'identità dell'utente.

L'apparecchio di controllo registra e memorizza dati nella sua memoria di dati e sulle carte tachigrafiche.

Questa operazione è effettuata in conformità della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati ([1]).

2. **Funzioni**

005 L'apparecchio di controllo garantisce le seguenti funzioni:

— controllo dell'inserimento e dell'estrazione delle carte,

— misurazione della velocità e della distanza,

— misurazione del tempo,

— controllo delle attività del conducente,

— controllo delle condizioni di guida,

— immissioni manuali da parte del conducente:

  — luogo in cui inizia e/o termina il periodo di lavoro giornaliero,

  — attività del conducente,

  — condizioni particolari,

([1]) GU L 281 del 23.11.1995, pag. 31.

— gestione dei blocchi di un'impresa,

— verifica delle attività di controllo,

— rilevamento di anomalie e/o guasti,

— prove incorporate e prove automatiche,

— lettura della memoria di dati,

— registrazione e memorizzazione nella memoria di dati,

— lettura delle carte tachigrafiche,

— registrazione e memorizzazione nelle carte tachigrafiche,

— visualizzazione,

— stampa,

— avviso,

— trasferimento di dati su dispositivi esterni,

— trasmissione di dati a dispositivi esterni aggiuntivi,

— calibratura,

— regolazione dell'ora.

3. **Modalità di funzionamento**

006 L'apparecchio di controllo prevede quattro modalità di funzionamento:

— modo funzionamento,

— modo controllo,

— modo calibratura,

— modo azienda.

007 L'apparecchio di controllo deve passare alla modalità di funzionamento sotto riportata, a seconda delle carte tachigrafiche in corso di validità inserite nelle interfacce:

Modalità di funzionamento		Sede (slot) "conducente"				
		Carta assente	Carta del conducente	Carta di controllo	Carta dell'officina	Carta dell'azienda
Sede (slot) "secondo conducente"	Carta assente	funzionamento	funzionamento	controllo	calibratura	azienda
	Carta del conducente	funzionamento	funzionamento	controllo	calibratura	azienda
	Carta di controllo	controllo	controllo	controllo (*)	funzionamento	funzionamento
	Carta dell'officina	calibratura	calibratura	funzionamento	calibratura (*)	funzionamento
	Carta dell'azienda	azienda	azienda	funzionamento	funzionamento	azienda (*)

008 (*) In questi casi l'apparecchio di controllo usa solo la carta tachigrafica inserita nella sede "conducente".

009 L'apparecchio di controllo ignora le carte non valide inserite, fatta salva la possibilità di visualizzare, stampare o trasferire i dati memorizzati su una carta scaduta.

010 Tutte le funzioni elencate al capitolo II, punto 2, devono essere disponibili in ogni modalità di funzionamento, con le seguenti eccezioni:

— la funzione di calibratura è accessibile solo nel modo calibratura,

— la funzione di regolazione dell'ora è limitata quando non è attivo il modo calibratura,

— le funzioni di immissione manuale da parte del conducente sono disponibili solo nei modi funzionamento e calibratura,

— la funzione di gestione dei blocchi di un'impresa è disponibile solo nel modo azienda,

— la verifica delle attività di controllo è disponibile solo nel modo controllo,

— la funzione di trasferimento dati non è disponibile nel modo funzionamento (fatto salvo quanto disposto dal requisito 150).

011 L'apparecchio di controllo può trasmettere qualsiasi dato al dispositivo di visualizzazione, alla stampante o a dispositivi esterni, con le seguenti eccezioni:

— nel modo funzionamento, è omessa ogni identificazione personale (cognome e nome/i) non corrispondente a una carta tachigrafica inserita ed è parzialmente omesso (un carattere sì e uno no, da sinistra a destra) ogni numero di carta non corrispondente a una carta tachigrafica inserita,

— nel modo azienda, si possono trasmettere ad altri dispositivi solo i dati relativi al conducente (requisiti 081, 084 e 087) riferiti a periodi per cui non è stato attivato un blocco da un'altra impresa (identificata dai primi 13 caratteri del numero di carta dell'azienda),

— se nell'apparecchio di controllo non è inserita una carta, si possono trasmettere ad altri dispositivi solo i dati relativi al conducente riferiti al giorno corrente e agli 8 giorni di calendario precedenti.

4. **Sicurezza**

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 proteggere l'integrità e l'autenticità dei dati scambiati tra sensore di movimento e unità elettronica di bordo, proteggere l'integrità e l'autenticità dei dati scambiati tra l'apparecchio di controllo e le carte tachigrafiche e verificare l'integrità e l'autenticità dei dati trasferiti.

012 Al fine di garantire la sicurezza del sistema, l'apparecchio di controllo deve soddisfare i requisiti specificati negli obiettivi generali di sicurezza per il sensore di movimento e per l'unità elettronica di bordo (appendice 10).

III. REQUISITI PER LA COSTRUZIONE E IL FUNZIONAMENTO DELL'APPARECCHIO DI CONTROLLO

1. **Controllo dell'inserimento e dell'estrazione delle carte**

013 L'apparecchio di controllo deve rilevare ogni inserimento ed estrazione di carte nelle relative interfacce.

014 All'atto dell'inserimento, l'apparecchio di controllo deve verificare se la carta inserita è una carta tachigrafica in corso di validità ed in tal caso identificarne il tipo.

015 L'apparecchio di controllo deve essere realizzato in modo tale che le carte tachigrafiche vengano bloccate in posizione quando sono inserite correttamente nelle relative interfacce.

016 Le carte tachigrafiche devono poter essere estratte solo a veicolo fermo e dopo la memorizzazione dei dati pertinenti nelle carte stesse. L'estrazione della carta deve richiedere l'intervento fisico dell'utilizzatore.

2. **Misurazione della velocità e della distanza**

017 Questa funzione deve misurare costantemente ed essere in grado di fornire il valore dell'odometro corrispondente alla distanza totale percorsa dal veicolo.

018 Questa funzione deve misurare costantemente ed essere in grado di fornire la velocità del veicolo.

019 La funzione di misurazione della velocità indica inoltre se il veicolo è in marcia o fermo. Il veicolo è considerato in marcia non appena la funzione rileva più di 1 imp/sec per almeno 5 secondi sul sensore di movimento, in caso contrario il veicolo si considera fermo.

I dispositivi che visualizzano la velocità (tachimetro) e la distanza totale percorsa (odometro), montati su ogni veicolo munito di un apparecchio di controllo conforme alle prescrizioni del presente regolamento, devono rispettare i requisiti relativi alle tolleranze massime fissate nel presente allegato (capitolo III, punti 2.1 e 2.2).

2.1. ***Misurazione della distanza percorsa***

020 La distanza percorsa può essere misurata:

— a marcia avanti e a marcia indietro, oppure

— unicamente a marcia avanti.

021 L'apparecchio di controllo deve misurare la distanza da 0 a 9 999 999,9 km.

022 La distanza misurata deve rispettare le tolleranze seguenti (distanze di almeno 1 000 m):

— ± 1 % prima del montaggio,

— ± 2 % all'atto del montaggio e del controllo periodico,

— ± 4 % durante l'impiego.

023 La distanza misurata deve avere una risoluzione maggiore o uguale a 0,1 km.

2.2. ***Misurazione della velocità***

024 L'apparecchio di controllo deve misurare la velocità compresa tra 0 e 220 km/h.

025 Per garantire una tolleranza massima sulla velocità visualizzata di ± 6 km/h durante l'impiego, tenuto conto di:

— una tolleranza di ± 2 km/h per le variazioni in ingresso (variazioni dei pneumatici, ecc.),

— una tolleranza di ± 1 km/h per le misurazioni effettuate durante il montaggio o i controlli periodici,

l'apparecchio di controllo deve misurare la velocità, per velocità comprese tra 20 e 180 km/h e per coefficienti caratteristici del veicolo compresi tra 4 000 e 25 000 con una tolleranza di ± 1 km/h (a velocità costante).

Nota: La risoluzione della memorizzazione dei dati apporta una tolleranza supplementare di ± 0,5 km/h alla velocità memorizzata dall'apparecchio di controllo.

025a La velocità deve essere misurata correttamente, rispettando le tolleranze normali, entro 2 secondi dalla fine di una variazione di velocità, quando il tasso di variazione di velocità è inferiore o uguale a $2 m/s^2$.

026 La misurazione della velocità deve avere una risoluzione maggiore o uguale a 1 km/h.

3. **Misurazione del tempo**

027 La funzione di misurazione del tempo deve misurare costantemente ed indicare data e ora UTC in formato digitale.

028 La data e l'ora UTC sono usati per datare tutti i dati dell'apparecchio di controllo (registrazioni, documenti stampati, scambio di dati, visualizzazione, ecc.).

029 Al fine di visualizzare l'ora locale, deve essere possibile regolare l'ora visualizzata in intervalli di mezz'ora.

030 Lo sfasamento dell'ora non deve superare ± 2 secondi al giorno in condizioni di omologazione.

031 L'ora misurata deve avere una risoluzione maggiore o uguale a 1 secondo.

032 La misurazione dell'ora non deve essere compromessa da un'interruzione dell'alimentazione esterna inferiore a 12 mesi in condizioni di omologazione.

4. **Controllo delle attività del conducente**

033 Questa funzione deve controllare costantemente e separatamente le attività di un conducente e di un secondo conducente.

034 Le attività del conducente sono GUIDA, LAVORO, DISPONIBILITÀ e INTERRUZIONE/RIPOSO.

035 Il conducente e/o il secondo conducente devono poter selezionare manualmente LAVORO, DISPONIBILITÀ o INTERRUZIONE/RIPOSO.

036 Quando il veicolo è in marcia, si seleziona automaticamente GUIDA per il conducente e DISPONIBILITÀ per il secondo conducente.

037 Quando il veicolo si arresta, si seleziona automaticamente LAVORO per il conducente.

038 Il primo cambio di attività che si verifica entro 120 secondi dalla selezione automatica di LAVORO dovuta all'arresto del veicolo si considera avvenuto al momento dell'arresto del veicolo (eventualmente si annulla quindi la selezione di LAVORO).

039 Questa funzione deve trasmettere i cambi di attività alle funzioni di registrazione con una risoluzione di un minuto.

040 Se durante un dato intervallo di un minuto si verifica l'attività GUIDA, l'intero minuto viene considerato come GUIDA.

041 Dato un intervallo di un minuto, se entro il minuto immediatamente precedente e il minuto immediatamente successivo si verifica l'attività GUIDA, l'intero minuto viene considerato come GUIDA.

042 Dato un intervallo di un minuto non considerato come GUIDA in base ai requisiti precedenti, l'intero minuto viene considerato come attività dello stesso tipo di quella continua di maggiore durata verificatasi entro tale minuto (o, nel caso di più attività di pari durata, dell'ultima di esse).

043 Questa funzione controlla inoltre costantemente il periodo di guida continuo e il periodo cumulato di interruzione del conducente.

5. **Controllo delle condizioni di guida**

044 Questa funzione controlla costantemente ed automaticamente le condizioni di guida.

045 La condizione di guida EQUIPAGGIO viene selezionata quando nell'apparecchio sono inserite due carte del conducente in corso di validità; in ogni altro caso viene selezionata la condizione di guida SINGOLA.

6. **Immissioni manuali da parte del conducente**

6.1. ***Immissione del luogo in cui inizia e/o termina il periodo di lavoro giornaliero***

046 Questa funzione consente l'immissione del luogo in cui inizia e/o termina il periodo di lavoro giornaliero di un conducente e/o di un secondo conducente.

047 Per luogo s'intende il paese e, se del caso, anche la regione.

048 All'atto dell'estrazione di una carta del conducente (o dell'officina), l'apparecchio di controllo invita il conducente (o il secondo conducente) ad immettere il "luogo in cui termina il periodo di lavoro giornaliero".

049 L'apparecchio di controllo deve consentire di ignorare questa richiesta.

050 Il luogo in cui inizia e/o termina il periodo di lavoro giornaliero deve poter essere immesso senza carta o in momenti diversi da quello dell'inserimento o dell'estrazione della carta.

6.2. ***Immissione manuale delle attività del conducente***

050a All'atto dell'inserimento della carta del conducente (o dell'officina), ed esclusivamente in tale momento, l'apparecchio di controllo:

— ricorda al titolare della carta la data e l'ora dell'ultima estrazione della sua carta, e

— chiede al titolare della carta di indicare se l'inserimento della carta rappresenta una continuazione del periodo di lavoro giornaliero in corso.

L'apparecchio di controllo deve consentire al titolare della carta di ignorare la richiesta, di dare una risposta affermativa o di dare una risposta negativa:

— nel caso in cui la richiesta sia ignorata, l'apparecchio di controllo invita il titolare della carta ad inserire il "luogo in cui inizia il periodo di lavoro giornaliero". Questa richiesta deve poter essere ignorata. Se viene immesso un luogo, l'informazione viene registrata nella memoria di dati e nella carta tachigrafica e riferita all'ora di inserimento della carta;

— nel caso di risposta negativa o affermativa, l'apparecchio di controllo invita il titolare della carta ad inserire le attività manualmente, con la rispettiva data e ora di inizio e termine, indicando esclusivamente LAVORO o DISPONIBILITÀ o INTERRUZIONE/RIPOSO, rigorosamente rientranti nel periodo compreso tra l'ultima estrazione della carta e l'inserimento della carta in atto, e senza consentire la sovrapposizione reciproca di tali attività. Questo va effettuato in base alle procedure seguenti:

  — in caso di risposta affermativa, l'apparecchio di controllo invita il titolare della carta a inserire le attività manualmente, in ordine cronologico, per il periodo compreso tra l'ultima estrazione della carta e l'inserimento in atto. La procedura è completata quando l'ora in cui termina un'attività inserita manualmente corrisponde all'ora di inserimento della carta;

  — in caso di risposta negativa, l'apparecchio di controllo:

    — invita il titolare della carta ad inserire manualmente le attività in ordine cronologico dall'ora di estrazione della carta fino all'ora in cui termina il relativo periodo di lavoro giornaliero (o l'attività relativa a tale veicolo nel caso in cui il periodo di lavoro giornaliero prosegua su un foglio di registrazione). L'apparecchio di controllo invita quindi il titolare della carta, prima di consentire l'immissione manuale di ogni attività, ad indicare se l'ora in cui termina l'ultima attività registrata rappresenta la fine di un periodo di lavoro precedente (cfr. nota seguente).

      Nota: Nel caso in cui il titolare della carta non indichi l'ora in cui è terminato il periodo di lavoro precedente ed inserisca manualmente un'attività la cui ora di termine corrisponda all'ora di inserimento della carta, l'apparecchio di controllo:

      — considera che il periodo di lavoro giornaliero sia terminato all'inizio del primo periodo di RIPOSO (o periodo NON NOTO rimanente) successivo all'estrazione della carta o all'ora di estrazione della carta qualora non sia stato inserito alcun periodo di riposo (ed in assenza di un periodo rimanente NON NOTO),

      — considera che l'ora di inizio (cfr. infra) corrisponda all'ora di inserimento della carta,

      — procede secondo le fasi sotto indicate;

    — quindi, se l'ora del termine del relativo periodo di lavoro è diversa dall'ora di estrazione della carta, o se in tale momento non era stato inserito il luogo in cui era terminato il periodo di lavoro giornaliero, invita il titolare della carta a "confermare o inserire il luogo in cui è terminato il periodo di lavoro giornaliero" (l'apparecchio di controllo deve consentire di ignorare la richiesta). Se viene inserito un luogo, l'informazione viene registrata nella carta tachigrafica soltanto se è diversa da quella inserita al momento dell'estrazione della carta (se era stata inserita), e riferita all'ora in cui è terminato il periodo di lavoro;

    — invita quindi il titolare della carta ad "inserire un'ora di inizio" del periodo di lavoro giornaliero in corso (o dell'attività relativa al veicolo corrente nel caso in cui il titolare della carta abbia precedentemente usato un foglio di registrazione durante tale periodo), nonché ad inserire un "luogo in cui inizia il periodo di lavoro giornaliero" (l'apparecchio di controllo deve consentire di ignorare la richiesta). Se viene inserito un luogo, l'informazione viene registrata sulla carta tachigrafica e riferita all'ora di inizio. Se l'ora di inizio corrisponde all'ora di inserimento della carta, il luogo viene registrato anche nella memoria di dati;

    — invece, se l'ora di inizio è diversa dall'ora di inserimento della carta, invita il titolare ad inserire manualmente le attività in ordine cronologico a partire da tale ora di inizio fino all'ora di inserimento della carta. La procedura è completata quando l'ora del termine di un'attività inserita manualmente corrisponde all'ora di inserimento della carta.

  — L'apparecchio di controllo deve consentire al titolare della carta di modificare ogni attività inserita manualmente, fino alla conferma mediante un apposito comando, e quindi impedire ogni altra modifica.

  — L'apparecchio di controllo interpreta le risposte alle richieste iniziali non seguite dall'inserimento di un'attività come se il titolare della carta avesse ignorato la richiesta.

Durante l'intera procedura, l'apparecchio di controllo attende l'inserimento di informazioni entro e non oltre i seguenti limiti di tempo:

— se non avviene alcuna interazione con l'interfaccia uomo-macchina dell'apparecchio durante 1 minuto (con un avviso visivo e possibilmente acustico dopo 30 secondi), o

— se la carta viene estratta o viene inserita un'altra carta del conducente (o dell'officina), o

— non appena il veicolo si mette in marcia,

in questo caso l'apparecchio di controllo conferma le informazioni già inserite.

6.3. ***Immissione di condizioni particolari***

050b L'apparecchio di controllo deve consentire al conducente di inserire, in tempo reale, le due condizioni particolari seguenti:

— "ESCLUSO DAL CAMPO DI APPLICAZIONE" (inizio, fine)

— "ATTRAVERSAMENTO MEDIANTE TRAGHETTO/TRENO"

Un "ATTRAVERSAMENTO MEDIANTE TRAGHETTO/TRENO" non può verificarsi se è stata aperta la condizione "ESCLUSO DAL CAMPO DI APPLICAZIONE".

La condizione "ESCLUSO DAL CAMPO DI APPLICAZIONE" aperta deve essere chiusa automaticamente dall'apparecchio di controllo se viene inserita o estratta una carta del conducente.

7. **Gestione dei blocchi di un'impresa**

051 Questa funzione consente di gestire i blocchi previsti da un'impresa per limitare a se stessa l'accesso ai dati nel modo azienda.

052 I blocchi di un'impresa consistono in una data/ora di inizio (attivazione blocco) e in una data/ora di termine (disattivazione blocco), associate all'identificazione dell'impresa risultante dal numero della carta dell'azienda (all'attivazione del blocco).

053 I blocchi possono essere attivati o disattivati solo in tempo reale.

054 Il blocco deve poter essere disattivato solo dall'impresa il cui blocco è attivo (identificata dai primi 13 caratteri del numero della carta dell'azienda), oppure

055 la disattivazione del blocco avviene automaticamente se un'altra impresa attiva un blocco.

055a Nel caso in cui un'impresa attiva un blocco e che il blocco precedente sia stato effettuato dalla stessa impresa, allora si riterrà che il blocco precedente non è stato disattivato e che è tuttora attivato.

8. **Verifica delle attività di controllo**

056 Questa funzione verifica le attività di VISUALIZZAZIONE, STAMPA, TRASFERIMENTO dati della VU e della carta nel modo controllo.

057 La funzione verifica inoltre le attività di CONTROLLO SUPERAMENTO DI VELOCITÀ nel modo controllo. Un controllo del superamento di velocità si considera avvenuto quando, nel modo controllo, l'informazione "superamento di velocità" viene inviata alla stampante o al dispositivo di visualizzazione, o quando i dati relativi ad "anomalie e guasti" vengono trasferiti dalla memoria di dati della VU.

9. **Rilevamento di anomalie e/o guasti**

058 Questa funzione rileva le anomalie e/o guasti seguenti:

9.1. ***Anomalia "Inserimento di una carta non valida"***

059 Questa anomalia si attiva all'inserimento di una carta non valida e/o quando una carta inserita in corso di validità raggiunge la data di scadenza.

9.2. ***Anomalia "Conflitto di carte"***

060 Questa anomalia si attiva quando si verifica una combinazione di carte in corso di validità indicata con X nella tabella seguente:

Conflitto di carte		Sede (slot) "conducente"				
		Carta assente	Carta del conducente	Carta di controllo	Carta dell'officina	Carta dell'azienda
Sede (slot) "secondo conducente"	Carta assente					
	Carta del conducente				X	
	Carta di controllo			X	X	X
	Carta dell'officina		X	X	X	X
	Carta dell'azienda			X	X	X

9.3. ***Anomalia "Sovrapposizione di orari"***

061 Questa anomalia si attiva quando la data/ora dell'ultima estrazione di una carta del conducente, letta sulla carta, è successiva alla data/ora corrente dell'apparecchio di controllo in cui è inserita la carta.

9.4. ***Anomalia "Guida in assenza di una carta adeguata"***

062 Questa anomalia si attiva per ogni combinazione di carte tachigrafiche indicata con X nella tabella seguente, quando l'attività del conducente passa a GUIDA, o quando si verifica un cambio di modalità di funzionamento mentre l'attività del conducente è GUIDA:

Guida in assenza di una carta adeguata		Sede (slot) "conducente"				
		Carta assente (o carta non valida)	Carta del conducente	Carta di controllo	Carta dell'officina	Carta dell'azienda
Sede (slot) "secondo conducente"	Carta assente (o carta non valida)	X		X		X
	Carta del conducente	X		X	X	X
	Carta di controllo	X	X	X	X	X
	Carta dell'officina	X	X	X		X
	Carta dell'azienda	X	X	X	X	X

9.5. ***Anomalia "Inserimento carta durante la guida"***

063 Questa anomalia si attiva quando una carta tachigrafica viene inserita in qualsiasi sede, mentre l'attività del conducente è GUIDA.

9.6. ***Anomalia "Chiusura errata ultima sessione carta"***

064 Questa anomalia si attiva quando all'inserimento della carta l'apparecchio di controllo rileva che, nonostante le prescrizioni di cui al capitolo III, punto 1, la sessione precedente della carta non è stata chiusa in modo corretto (la carta è stata estratta prima che tutti i dati pertinenti fossero memorizzati sulla carta stessa). Questa anomalia riguarda solo le carte del conducente e dell'officina.

9.7. ***Anomalia "Superamento di velocità"***

065 Questa anomalia si attiva ad ogni superamento della velocità autorizzata.

9.8. ***Anomalia "Interruzione dell'alimentazione di energia"***

066 Eccetto per il modo calibratura, questa anomalia si attiva nel caso di un'interruzione dell'alimentazione del sensore di movimento e/o dell'unità elettronica di bordo di durata superiore a 200 millisecondi. La soglia di interruzione è definita dal costruttore. La caduta di alimentazione dovuta all'avviamento del motore del veicolo non deve attivare questa anomalia.

9.9. ***Anomalia "Errore dati di marcia"***

067 Questa anomalia si attiva in caso di interruzione del normale flusso di dati tra il sensore di movimento e l'unità elettronica di bordo e/o nel caso di un errore di integrità dei dati o di autenticazione dei dati durante lo scambio di dati tra il sensore di movimento e l'unità elettronica di bordo.

9.10. ***Anomalia "Tentata violazione della sicurezza"***

068 Eccetto per il modo calibratura, questa anomalia si attiva in caso di ogni altra anomalia che influisca sulla sicurezza del sensore di movimento e/o dell'unità elettronica di bordo, come specificato dagli obiettivi generali di sicurezza per questi componenti.

9.11. ***Guasto "Carta"***

069 Questo guasto si attiva in caso di funzionamento difettoso della carta tachigrafica.

9.12. ***Guasto "Apparecchio di controllo"***

070 Eccetto per il modo calibratura, questo guasto si attiva in ciascuno dei casi seguenti:

— guasto all'interno del VU

— guasto della stampante

— guasto del dispositivo di visualizzazione

— guasto nel trasferimento di dati

— guasto del sensore.

10. **Prove incorporate e automatiche**

071 L'apparecchio di controllo rileva automaticamente i guasti mediante le prove automatiche e le prove incorporate, secondo la tabella seguente:

Sottoinsieme sottoposto a prova	Prova automatica	Prova incorporata
Software		Integrità
Memoria di dati	Accesso	Accesso, integrità dei dati
Interfacce delle carte	Accesso	Accesso
Tastiera		Controllo manuale
Stampante	(definita dal fabbricante)	Documento stampato
Dispositivo di visualizzazione		Controllo visivo
Trasferimento di dati (eseguita solo durante il trasferimento)	Corretto funzionamento	
Sensore	Corretto funzionamento	Corretto funzionamento

11. **Lettura della memoria di dati**

072 L'apparecchio di controllo deve essere in grado di leggere ogni dato memorizzato nella sua memoria di dati.

12. **Registrazione e memorizzazione nella memoria di dati**

Agli effetti del presente punto:

— per "365 giorni" s'intende 365 giorni di calendario di attività media del conducente su un veicolo. L'attività media giornaliera su un veicolo è intesa come almeno 6 conducenti o secondi conducenti, 6 cicli di inserimento ed estrazione della carta e 256 cambi di attività. "365 giorni" comprende quindi almeno 2 190 conducenti (o secondi conducenti), 2 190 cicli di inserimento ed estrazione della carta e 93 440 cambi di attività,

— se non diversamente specificato, i tempi sono registrati con una risoluzione di un minuto,

— i valori dell'odometro sono registrati con una risoluzione di un chilometro,

— le velocità sono registrate con una risoluzione di 1 km/h.

073 I dati memorizzati nella memoria di dati non devono essere compromessi da un'interruzione dell'alimentazione esterna di durata inferiore a dodici mesi in condizioni di omologazione.

074 L'apparecchio di controllo deve essere in grado di registrare e memorizzare implicitamente o esplicitamente nella sua memoria di dati le informazioni sotto elencate.

12.1. ***Dati di identificazione dell'apparecchio***

12.1.1. *Dati di identificazione dell'unità elettronica di bordo*

075 L'apparecchio di controllo deve essere in grado di memorizzare nella sua memoria i seguenti dati di identificazione dell'unità elettronica di bordo:

— nome del fabbricante,

— indirizzo del fabbricante,

— codice componente,

— numero di serie,

— numero di versione del software,

— data di installazione della versione del software,

— anno di fabbricazione dell'apparecchio,

— numero di omologazione.

076 I dati di identificazione dell'unità elettronica di bordo sono registrati e memorizzati una sola volta dal fabbricante dell'unità, eccetto per i dati relativi al software e il numero di omologazione, che si possono modificare in caso di aggiornamento del software.

12.1.2. *Dati di identificazione del sensore di movimento*

077 Il sensore di movimento deve essere in grado di memorizzare nella sua memoria i seguenti dati di identificazione:

— nome del fabbricante,

— codice componente,

— numero di serie,

— numero di omologazione,

— identificativo del componente di sicurezza incorporato (per es., codice componente chip/processore interno),

— identificativo del sistema operativo (per es., numero di versione del software).

078 I dati di identificazione del sensore di movimento sono registrati e memorizzati una sola volta dal fabbricante del sensore.

079 L'unità elettronica di bordo deve essere in grado di registrare e memorizzare nella sua memoria i seguenti dati di identificazione del sensore di movimento cui è accoppiata:

— numero di serie,

— numero di omologazione,

— data del primo accoppiamento.

12.2. ***Elementi di sicurezza***

080 L'apparecchio di controllo deve essere in grado di memorizzare i seguenti elementi di sicurezza:

— chiave pubblica europea,

— certificato dello Stato membro,

— certificato dell'apparecchio,

— chiave privata dell'apparecchio.

Gli elementi di sicurezza dell'apparecchio di controllo sono inseriti nell'apparecchio dal fabbricante dell'unità elettronica di bordo.

12.3. ***Dati relativi all'inserimento e all'estrazione della carta del conducente***

081 Per ogni ciclo di inserimento ed estrazione dall'apparecchio di una carta del conducente o dell'officina, l'apparecchio di controllo registra e memorizza nella sua memoria di dati:

— cognome e nome del titolare della carta, memorizzato nella carta stessa,

— numero della carta, Stato membro di rilascio e data di scadenza, memorizzati nella carta stessa,

— data e ora di inserimento,

— valore dell'odometro del veicolo all'atto dell'inserimento,

— sede (slot) in cui è inserita la carta,

— data e ora di estrazione,

— valore dell'odometro del veicolo all'atto dell'estrazione,

— le seguenti informazioni relative al veicolo usato in precedenza dal conducente, memorizzate nella carta:

  — VRN e Stato membro di immatricolazione,

  — data e ora di estrazione della carta,

  un indicatore (flag) che segnali se, all'atto dell'inserimento della carta, il titolare della carta abbia o meno inserito manualmente le attività.

082 La memoria di dati deve essere in grado di conservare tali informazioni per almeno 365 giorni.

083 Qualora si esaurisca la capacità di memorizzazione, i nuovi dati sostituiscono quelli meno recenti.

12.4. ***Dati relativi all'attività del conducente***

084 L'apparecchio di controllo registra e memorizza nella sua memoria di dati, ogniqualvolta si verifichi un cambio di attività del conducente e/o del secondo conducente e/o ogniqualvolta si verifichi una variazione della condizione di guida e/o ogniqualvolta venga inserita o estratta una carta del conducente o dell'officina:

— la condizione di guida (EQUIPAGGIO, SINGOLA),

— la sede (slot) (CONDUCENTE, SECONDO CONDUCENTE),

— la condizione della carta nella relativa sede (slot) (INSERITA, NON INSERITA) (cfr. Nota),

— l'attività (GUIDA, DISPONIBILITÀ, LAVORO, INTERRUZIONE/RIPOSO),

— la data e l'ora del cambiamento.

Nota: INSERITA significa che una carta del conducente o dell'officina in corso di validità è inserita nella sede (slot). NON INSERITA significa il contrario, cioè che nella sede non è inserita una carta del conducente o dell'officina in corso di validità (per es., è inserita una carta dell'azienda oppure non è inserita alcuna carta).

Nota: I dati relativi all'attività inseriti manualmente dal conducente non vengono registrati nella memoria di dati.

085 La memoria di dati deve essere in grado di conservare i dati relativi all'attività del conducente per almeno 365 giorni.

086 Qualora si esaurisca la capacità di memorizzazione, i nuovi dati sostituiscono quelli meno recenti.

12.5. ***Luogo in cui inizia e/o termina il periodo di lavoro giornaliero***

087 L'apparecchio di controllo registra e memorizza nella sua memoria di dati ogni occasione in cui un conducente (o secondo conducente) inserisce il luogo in cui inizia e/o termina un periodo di lavoro giornaliero:

— se del caso, il numero di carta del conducente (o secondo conducente) e lo Stato membro di rilascio,

— la data e l'ora di immissione (o la data/ora relativa all'immissione, se questa viene effettuata durante la procedura di immissione manuale),

— il tipo di immissione (inizio o termine, condizione di immissione),

— il paese e la regione inseriti,

— il valore dell'odometro del veicolo.

088 La memoria di dati deve essere in grado di conservare i dati relativi all'inizio e al termine del periodo di lavoro giornaliero per almeno 365 giorni (nell'ipotesi che un conducente inserisca tali informazioni due volte al giorno).

089 Qualora si esaurisca la capacità di memorizzazione, i nuovi dati sostituiscono quelli meno recenti.

12.6. ***Dati relativi all'odometro***

090 L'apparecchio di controllo registra nella sua memoria di dati il valore dell'odometro del veicolo e la data di registrazione alle ore 00.00 di ogni giorno di calendario.

091 La memoria di dati deve essere in grado di memorizzare i valori dell'odometro registrati alle ore 00.00 per almeno 365 giorni di calendario.

092 Qualora si esaurisca la capacità di memorizzazione, i nuovi dati sostituiscono quelli meno recenti.

12.7. ***Dati dettagliati relativi alla velocità***

093 L'apparecchio di controllo registra e memorizza 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 del veicolo.

12.8. ***Dati relativi alle anomalie***

Agli effetti del presente punto, l'ora deve essere registrata con una risoluzione di 1 secondo.

094 L'apparecchio di controllo registra e memorizza nella sua memoria i dati sotto elencati per ogni anomalia rilevata, in base alle seguenti regole di memorizzazione:

Anomalia	Regole di memorizzazione	Dati da registrare per ogni anomalia
Conflitto di carte	— le ultime 10 anomalie	— data e ora di inizio dell'anomalia — data e ora di termine dell'anomalia — tipo e numero delle carte e Stato membro di rilascio delle due carte che creano il conflitto
Guida in assenza di una carta adeguata	— 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 termine dell'anomalia — tipo e numero delle carte e Stato membro di rilascio di ogni carta inserita all'inizio e/o termine dell'anomalia — numero di anomalie analoghe verificatesi in tale data
Inserimento carta durante la guida	— l'ultima anomalia per ciascuno degli ultimi 10 giorni in cui si è verificata	— data e ora dell'anomalia — tipo e numero della carta e Stato membro di rilascio — numero di anomalie analoghe verificatesi in tale data
Chiusura errata ultima sessione carta	— le ultime 10 anomalie	— data e ora di inserimento della carta — tipo e numero della carta e Stato membro di rilascio — dati relativi all'ultima sessione letti sulla carta: — data e ora di inserimento della carta — VRN e Stato membro di immatricolazione
Superamento di velocità ([1])	— l'anomalia più grave per ciascuno degli ultimi 10 giorni in cui si è verificata (cioè quella con la più alta velocità media) — le 5 anomalie più gravi nel corso degli ultimi 365 giorni — la prima anomalia verificatasi dopo l'ultima calibratura	— data e ora di inizio dell'anomalia — data e ora di termine dell'anomalia — velocità massima misurata durante l'anomalia — media aritmetica della velocità misurata durante l'anomalia — tipo e numero della carta e Stato membro di rilascio del conducente (se applicabile) — numero di anomalie analoghe verificatesi in tale data

Anomalia	Regole di memorizzazione	Dati da registrare per ogni anomalia
Interruzione dell'alimentazione ([2])	— 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 termine dell'anomalia — tipo e numero delle carte e Stato membro di rilascio di ogni carta inserita all'inizio e/o termine dell'anomalia — numero di anomalie analoghe verificatesi in tale data
Errore dati di marcia	— 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 termine dell'anomalia — tipo e numero delle carte e Stato membro di rilascio di ogni carta inserita all'inizio e/o termine dell'anomalia — numero di anomalie analoghe verificatesi in tale data
Tentata violazione della sicurezza	— le ultime 10 anomalie per ogni tipo di anomalia	— data e ora di inizio dell'anomalia — data e ora di termine dell'anomalia (se pertinente) — tipo e numero delle carte e Stato membro di rilascio di ogni carta inserita all'inizio e/o termine dell'anomalia — tipo di anomalia

095 ([1]) L'apparecchio di controllo registra e memorizza nella sua memoria anche i dati seguenti:
— la data e l'ora dell'ultimo CONTROLLO SUPERAMENTO VELOCITÀ,
— la data e l'ora del primo superamento di velocità in seguito a tale CONTROLLO SUPERAMENTO VELOCITÀ,
— il numero di anomalie per superamento di velocità in seguito all'ultimo CONTROLLO SUPERAMENTO VELOCITÀ.
([2]) Questi dati si possono registrare solo al reinserimento dell'alimentazione di energia, l'ora deve essere nota con una precisione di un minuto.

12.9. ***Dati relativi ai guasti***

Agli effetti del presente punto, l'ora deve essere registrata con una risoluzione di 1 secondo.

096 L'apparecchio di controllo deve cercare di registrare e memorizzare nella sua memoria i dati sotto elencati per ciascun guasto rilevato, in base alle seguenti regole di memorizzazione:

Guasto	Regole di memorizzazione	Dati da registrare per ogni guasto
Guasto della carta	— gli ultimi 10 guasti della carta del conducente	— data e ora di inizio del guasto — data e ora di termine del guasto — tipo e numero della carta e Stato membro di rilascio
Guasti dell'apparecchio di controllo	— gli ultimi 10 guasti per ogni tipo di guasto — il primo guasto dopo l'ultima calibratura	— data e ora di inizio del guasto — data e ora di termine del guasto — tipo di guasto — tipo e numero delle carte e Stato membro di rilascio di ogni carta inserita all'inizio e/o termine del guasto

12.10. ***Dati relativi alla calibratura***

097 L'apparecchio di controllo registra e memorizza nella sua memoria le seguenti informazioni:

— parametri di calibratura noti al momento dell'attivazione,

— prima calibratura successiva all'attivazione,

— prima calibratura sul veicolo in cui è montato (identificato dal VIN),

— ultime 5 calibrature (se si effettuano diverse calibrature nello stesso giorno di calendario, deve essere memorizzata soltanto l'ultima del giorno).

098 Per ciascuna di tali calibrature si devono registrare i dati seguenti:

— scopo della calibratura (attivazione, primo montaggio, montaggio, controllo periodico),

— nome e indirizzo dell'officina,

— numero di carta dell'officina, Stato membro di rilascio della carta e data di scadenza della carta,

— identificazione del veicolo,

— parametri aggiornati o confermati: w, k, l, dimensioni dei pneumatici, regolazione del limitatore di velocità, odometro (vecchio e nuovo valore), data e ora (vecchio e nuovo valore).

099 Il sensore di movimento registra e memorizza nella sua memoria i seguenti dati di montaggio del sensore stesso:

— primo accoppiamento con una VU (data, ora, numero di omologazione della VU, numero di serie della VU),

— ultimo accoppiamento con una VU (data, ora, numero di omologazione della VU, numero di serie della VU).

12.11. ***Dati relativi alla regolazione dell'ora***

100 L'apparecchio di controllo registra e memorizza nella sua memoria le seguenti informazioni:

— ultima regolazione dell'ora,

— ultime 5 maggiori regolazioni dell'ora, in seguito all'ultima calibratura,

effettuate in modo calibratura al di fuori di un ciclo ordinario di calibratura (def. f).

101 Per ciascuna di tali regolazioni dell'ora si devono registrare i dati seguenti:

— data e ora, vecchio valore,

— data e ora, nuovo valore,

— nome e indirizzo dell'officina,

— numero di carta dell'officina, Stato membro di rilascio e data di scadenza della carta.

12.12. ***Dati relativi alle attività di controllo***

102 L'apparecchio di controllo registra e memorizza nella sua memoria i dati seguenti relativi alle ultime 20 attività di controllo:

— data e ora del controllo,

— numero della carta di controllo e Stato membro di rilascio della carta,

— tipo di controllo (visualizzazione e/o stampa e/o trasferimento dati VU e/o trasferimento dati carta).

103 Nel caso del trasferimento, si devono registrare anche le date del giorno meno recente e del giorno più recente cui si riferiscono i dati trasferiti.

12.13. ***Dati relativi ai blocchi di un'impresa***

104 L'apparecchio di controllo registra e memorizza nella sua memoria i dati seguenti relativi agli ultimi 20 blocchi di un'azienda:

— data e ora di attivazione blocco,

— data e ora di disattivazione blocco,

— numero di carta dell'azienda e Stato membro di rilascio della carta,

— nome e indirizzo dell'impresa.

12.14. ***Dati relativi al trasferimento***

105 L'apparecchio di controllo registra e memorizza nella sua memoria i dati seguenti, relativi all'ultimo trasferimento della memoria di dati su un dispositivo esterno in modo azienda o calibratura:

— data e ora del trasferimento,

— numero di carta dell'azienda o dell'officina e Stato membro di rilascio della carta,

— nome dell'impresa o dell'officina.

12.15. ***Dati relativi a condizioni particolari***

105a L'apparecchio di controllo deve registrare e memorizzare nella sua memoria i dati seguenti, relativi a condizioni particolari:

— data e ora dell'inserimento,

— tipo di condizione particolare.

105b La memoria di dati deve essere in grado di conservare i dati relativi alle condizioni particolari per almeno 365 giorni (nell'ipotesi che in media si apra e si chiuda 1 condizione al giorno). Qualora si esaurisca la capacità di memorizzazione, i dati nuovi sostituiscono quelli meno recenti.

13. **Lettura delle carte tachigrafiche**

106 L'apparecchio di controllo deve essere in grado di leggere sulle carte tachigrafiche, se del caso, i dati necessari a:

— identificare il tipo di carta, il titolare della carta, il veicolo usato in precedenza, la data e l'ora dell'ultima estrazione della carta e l'attività selezionata in tale momento,

— verificare che l'ultima sessione della carta sia stata chiusa in modo corretto,

— calcolare il periodo di guida continuo del conducente, il periodo cumulato di interruzione e i periodi cumulati di guida per la settimana corrente e per quella precedente,

— stampare i documenti relativi ai dati registrati su una carta del conducente,

— trasferire i dati di una carta del conducente su un dispositivo esterno.

107 In caso di errore di lettura, l'apparecchio di controllo riprova, un massimo di tre volte, ad inviare il medesimo comando di lettura; quindi, se l'errore persiste, dichiara la carta guasta e non valida.

14. **Registrazione e memorizzazione nelle carte tachigrafiche**

108 L'apparecchio di controllo imposta i "dati relativi alla sessione della carta" nella carta del conducente o dell'officina immediatamente dopo l'inserimento della carta.

109 L'apparecchio di controllo aggiorna i dati memorizzati in una carta valida del conducente, dell'officina e/o di controllo con tutti i dati necessari relativi al periodo durante il quale la carta è inserita e relativi al titolare della carta. I dati memorizzati in tali carte sono specificati al capitolo IV.

109a L'apparecchio di controllo aggiorna i dati relativi all'attività del conducente e alla località (specificati al capitolo IV, punti 5.2.5 e 5.2.6), memorizzati su una carta valida del conducente e/o dell'officina, con i dati relativi all'attività e alla località inseriti manualmente dal titolare della carta.

110 L'aggiornamento dei dati delle carte tachigrafiche deve avvenire in modo tale che, all'occorrenza e tenuto conto della capacità di memorizzazione effettiva della carta, i nuovi dati sostituiscano quelli meno recenti.

111 In caso di errore di scrittura, l'apparecchio di controllo riprova, un massimo di tre volte, ad inviare il medesimo comando di scrittura; quindi, se l'errore persiste, dichiara la carta guasta e non valida.

112 Prima di consentire l'estrazione di una carta del conducente, e dopo avere memorizzato nella carta tutti i dati pertinenti, l'apparecchio di controllo deve azzerare i "dati relativi alla sessione della carta".

15. **Visualizzazione**

113 Il dispositivo di visualizzazione comprende almeno 20 caratteri.

114 La dimensione minima dei caratteri è di 5 mm in altezza e 3,5 mm in larghezza.

114a Il dispositivo di visualizzazione deve gestire gli insiemi di caratteri grafici dell'alfabeto latino n. 1 e greco, definiti dalla norma ISO 8859, parti 1 e 7, come specificato all'appendice 1, capitolo 4 "Insiemi di caratteri". Il dispositivo di visualizzazione può usare caratteri semplificati (per es. le lettere accentate possono apparire senza l'accento, o le lettere minuscole possono apparire come maiuscole).

115 Il dispositivo di visualizzazione deve essere munito di un'illuminazione adeguata antiabbagliante.

116 Le indicazioni devono essere visibili dall'esterno dell'apparecchio di controllo.

117 L'apparecchio di controllo deve essere in grado di visualizzare:

— i dati predefiniti,

— i dati relativi agli avvisi,

— i dati relativi all'accesso guidato da menù,

— altri dati richiesti dall'utente.

L'apparecchio di controllo può visualizzare altre informazioni, a condizione che siano chiaramente distinte da quelle di cui sopra.

118 Il dispositivo di visualizzazione dell'apparecchio di controllo usa i pittogrammi o le combinazioni di pittogrammi elencati all'appendice 3. Il dispositivo di visualizzazione può prevedere altri pittogrammi o combinazioni di pittogrammi, purché siano chiaramente distinti da quelli summenzionati.

119 Il dispositivo di visualizzazione deve essere sempre acceso durante la marcia del veicolo.

120 L'apparecchio di controllo può prevedere un comando manuale o automatico per spegnere il dispositivo di visualizzazione quando il veicolo non è in marcia.

Il formato di visualizzazione è specificato all'appendice 5.

15.1. ***Visualizzazione predefinita***

121 In assenza di altre informazioni da visualizzare, l'apparecchio di controllo visualizza, come impostazione predefinita, quanto segue:

— l'ora locale (risultante dall'ora UTC, con regolazione effettuata dal conducente),

— la modalità di funzionamento,

— l'attività in corso del conducente e del secondo conducente,

— informazioni relative al conducente:

  — se l'attività in corso è GUIDA, il corrente periodo di guida continuo e il corrente periodo cumulato di interruzione,

  — se l'attività in corso non è GUIDA, la durata di tale attività (a partire dal momento in cui è stata selezionata) e il corrente periodo cumulato di interruzione,

— informazioni relative al secondo conducente:

  — la durata della sua attività (a partire dal momento in cui è stata selezionata).

122 La visualizzazione dei dati relativi a ciascun conducente deve essere chiara, semplice ed inequivocabile. Qualora non sia possibile visualizzare contemporaneamente le informazioni relative al conducente e al secondo conducente, l'apparecchio di controllo deve visualizzare per definizione le informazioni relative al conducente e consentire all'utente di visualizzare le informazioni relative al secondo conducente.

123 Qualora l'ampiezza del dispositivo non consenta di visualizzare per definizione la modalità di funzionamento, ad ogni variazione l'apparecchio di controllo deve visualizzare brevemente la nuova modalità di funzionamento.

124 L'apparecchio di controllo deve visualizzare brevemente il nome del titolare all'atto dell'inserimento della carta.

124a Qualora si apra una condizione "ESCLUSO DAL CAMPO DI APPLICAZIONE", la visualizzazione predefinita deve indicare, mediante l'apposito pittogramma, che la condizione è aperta (è ammesso che l'attività in corso del conducente non sia indicata nel contempo).

15.2. ***Visualizzazione degli avvisi***

125 L'apparecchio di controllo visualizza gli avvisi utilizzando principalmente i pittogrammi di cui all'appendice 3, integrati, se necessario, da un codice numerico supplementare. Si può anche aggiungere una descrizione dell'avviso nella lingua abituale del conducente.

15.3. ***Accesso guidato da menù***

126 L'apparecchio di controllo deve fornire i comandi necessari attraverso un'apposita struttura a menù.

15.4. ***Visualizzazione di altre informazioni***

127 Deve essere possibile visualizzare selettivamente, su richiesta:

— la data e l'ora UTC,

— la modalità di funzionamento (se non indicata per definizione),

— il periodo di guida continuo e il periodo cumulato di interruzione del conducente,

— il periodo di guida continuo e il periodo cumulato di interruzione del secondo conducente,

— il periodo di guida cumulato del conducente relativo alla settimana corrente e a quella precedente,

— il periodo di guida cumulato del secondo conducente relativo alla settimana corrente e a quella precedente,

— il contenuto di ciascuno dei sei documenti stampati nello stesso formato dei documenti stessi.

128 La visualizzazione del contenuto dei documenti stampati deve essere sequenziale, riga per riga. Qualora l'ampiezza del dispositivo di visualizzazione sia inferiore a 24 caratteri, l'utente deve poter ottenere le informazioni complete mediante un sistema adeguato (più righe, scorrimento del testo, ecc.). Ai fini della visualizzazione si possono omettere le righe dei documenti stampati riservate alle informazioni da riportare a mano.

16. **Stampa**

129 L'apparecchio di controllo deve essere in grado di stampare le seguenti informazioni contenute nella sua memoria di dati e/o nelle carte tachigrafiche, in modo da ottenere i documenti stampati seguenti:

— stampa giornaliera delle attività del conducente contenute nella carta,

— stampa giornaliera delle attività del conducente contenute nell'unità elettronica di bordo,

— stampa di anomalie e guasti contenuti nella carta,

— stampa di anomalie e guasti contenuti nell'unità elettronica di bordo,

— stampa dei dati tecnici,

— stampa dei superamenti di velocità.

Il formato e il contenuto precisi di tali documenti stampati sono specificati all'appendice 4.

Alla fine dei documenti stampati si possono riportare anche altre informazioni.

L'apparecchio di controllo può inoltre fornire altri documenti stampati, purché siano chiaramente distinguibili dai sei documenti summenzionati.

130 I documenti "stampa giornaliera delle attività del conducente contenute nella carta" e "stampa di anomalie e guasti contenuti nella carta" devono essere disponibili solo se una carta del conducente o una carta del centro di controllo è inserita nell'apparecchio di controllo. L'apparecchio di controllo deve aggiornare i dati contenuti nella carta prima di iniziare la stampa.

131 Per produrre il documento "stampa giornaliera delle attività del conducente contenute nella carta" o il documento "stampa di anomalie e guasti contenuti nella carta", l'apparecchio di controllo deve:

— selezionare automaticamente la carta del conducente o la carta del centro di controllo se solo una delle due è inserita, oppure

— prevedere un comando per selezionare la carta da cui attingere i dati o selezionare la carta inserita nella sede (slot) "conducente", se due di tali carte sono inserite nell'apparecchio di controllo.

132 La stampante deve essere in grado di stampare 24 caratteri per riga.

133 La dimensione minima dei caratteri è di 2,1 mm in altezza e 1,5 mm in larghezza.

133a La stampante gestisce gli insiemi di caratteri grafici dell'alfabeto latino n. 1 e greco, definiti dalla norma ISO 8859, parti 1 e 7, come specificato all'appendice 1, capitolo 4 "Insiemi di caratteri".

134 Le stampanti sono progettate in modo da fornire i suddetti documenti stampati con un grado di definizione atto ad evitare qualsiasi ambiguità nella lettura.

135 I documenti stampati devono conservare le loro dimensioni e le loro registrazioni in condizioni normali di umidità (10-90 %) e di temperatura.

136 La carta usata per la stampa deve portare il marchio di omologazione pertinente e l'indicazione del tipo o dei tipi di apparecchio di controllo con cui si può usare. I documenti stampati devono rimanere chiaramente leggibili ed identificabili in condizioni normali di conservazione, per quanto riguarda l'intensità luminosa, l'umidità e la temperatura, per almeno un anno.

137 Deve inoltre essere possibile apportare su questi documenti iscrizioni manuali supplementari, come la firma del conducente.

138 L'apparecchio di controllo deve gestire anomalie del tipo "mancanza carta" durante la stampa, riavviando la stampa dall'inizio del documento in seguito al caricamento della carta o continuando la stampa e fornendo un riferimento inequivocabile alla parte già stampata.

17. **Avvisi**

139 L'apparecchio di controllo invia un segnale di avviso al conducente quando rileva un'anomalia e/o un guasto.

140 L'avviso di un'anomalia dovuta ad interruzione dell'alimentazione può attivarsi anche solo dopo il ripristino dell'alimentazione stessa.

141 L'apparecchio di controllo invia un segnale di avviso al conducente 15 minuti prima del superamento di 4 h 30 min. di periodo di guida continuo e al momento in cui tale limite viene superato.

142 I segnali di avviso sono visivi. Si possono anche prevedere avvisi acustici in aggiunta a quelli visivi.

143 Gli avvisi visivi devono essere chiaramente riconoscibili dall'utente, devono rientrare nel campo visivo del conducente ed essere chiaramente leggibili sia di giorno che di notte.

144 Gli avvisi visivi sono incorporati nell'apparecchio di controllo e/o collocati in posizione remota dall'apparecchio di controllo.

145 In quest'ultimo caso devono recare il simbolo "T" ed essere di colore giallo ambra o arancione.

146 Gli avvisi hanno una durata di almeno 30 secondi, se non confermati dall'utente con la pressione di un qualsiasi tasto dell'apparecchio di controllo. Questa prima conferma non deve annullare la visualizzazione della causa dell'avviso menzionata al paragrafo successivo.

147 La causa dell'avviso deve essere visualizzata sull'apparecchio di controllo e rimanere visibile fino alla conferma da parte dell'utente mediante l'uso di un apposito tasto o comando dell'apparecchio di controllo.

148 Si possono prevedere altri avvisi, purché non confondano i conducenti in relazione a quelli sopra definiti.

18. **Trasferimento di dati verso un dispositivo esterno**

149 L'apparecchio di controllo deve essere in grado di trasferire su richiesta i dati contenuti nella sua memoria o in una carta del conducente ad un dispositivo di memorizzazione esterno attraverso il connettore di calibratura/trasferimento. L'apparecchio di controllo deve aggiornare i dati contenuti nella carta prima di iniziare il trasferimento.

150 Inoltre, e a titolo facoltativo, in qualsiasi modalità di funzionamento l'apparecchio di controllo può trasferire i dati attraverso un altro connettore ad un'impresa autenticata attraverso questo canale. In tal caso, al trasferimento si applicano i diritti di accesso ai dati del modo azienda.

151 Il trasferimento di dati non deve modificare o cancellare i dati memorizzati.

L'interfaccia elettrica del connettore di calibratura/trasferimento è specificata all'appendice 6.

I protocolli di trasferimento sono specificati all'appendice 7.

19. **Trasmissione di dati ad altri dispositivi esterni**

152 Se l'apparecchio di controllo non prevede le funzioni di visualizzazione della velocità e/o dell'odometro, l'apparecchio deve fornire uno o più segnali in uscita che consentano di visualizzare la velocità del veicolo (tachimetro) e/o la distanza totale percorsa dal veicolo (odometro).

153 L'unità elettronica di bordo deve inoltre essere in grado di trasmettere i dati seguenti attraverso un apposito collegamento seriale dedicato, indipendente da una connessione linea CAN opzionale (ISO 11898 Veicoli stradali — Interscambio di informazioni digitali — Controller Area Network (CAN) per comunicazioni ad alta velocità), per consentirne l'elaborazione da parte di altre unità elettroniche presenti sul veicolo:

— data e ora UTC corrente,

— velocità del veicolo,

— distanza totale percorsa dal veicolo (odometro),

— attività del conducente e del secondo conducente selezionate,

— indicazione della presenza o meno di una carta tachigrafica nella sede (slot) "conducente" e "secondo conducente" e, se applicabile, informazioni sull'identificazione delle carte (numero della carta e Stato membro di rilascio).

Oltre a questo elenco minimo si possono trasmettere anche altri dati.

Ad accensione del veicolo inserita, tali dati devono essere costantemente trasmessi. Se l'accensione del veicolo non è inserita, almeno ogni cambio di attività del conducente o del secondo conducente e/o ogni inserimento o estrazione di una carta tachigrafica devono generare la trasmissione della relativa informazione. Nel caso in cui la trasmissione dei dati sia sospesa durante il periodo in cui l'accensione del veicolo non è inserita, tali informazioni devono essere rese disponibili non appena l'accensione del veicolo viene nuovamente inserita.

20. **Calibratura**

154 La funzione di calibratura consente:

— l'accoppiamento automatico del sensore di movimento alla VU,

— l'adattamento digitale della costante dell'apparecchio di controllo (k) al coefficiente caratteristico del veicolo (w) (i veicoli con due o più rapporti al ponte devono essere muniti di un dispositivo di commutazione mediante il quale questi diversi rapporti vengano riportati automaticamente al rapporto per cui l'apparecchio di controllo è stato adattato al veicolo),

— la regolazione (senza limitazioni) dell'ora,

— la regolazione del valore corrente dell'odometro,

— l'aggiornamento dei dati di identificazione del sensore di movimento memorizzati nella memoria di dati,

— l'aggiornamento o la conferma di altri parametri noti all'apparecchio di controllo: identificazione del veicolo, w, l, dimensioni dei pneumatici e regolazione del limitatore di velocità, se applicabile.

155 L'accoppiamento del sensore di movimento alla VU prevede, almeno:

— l'aggiornamento dei dati di montaggio del sensore di movimento in esso contenuti (all'occorrenza),

— la copia, nella memoria di dati della VU, dei dati di identificazione del sensore necessari.

156 La funzione di calibratura deve essere in grado di immettere i dati necessari attraverso il connettore di calibratura/trasferimento o in base al protocollo di calibratura definito all'appendice 8. La funzione di calibratura può anche immettere i dati necessari attraverso altri connettori.

21. **Regolazione dell'ora**

157 La funzione di regolazione dell'ora consente di regolare l'ora in intervalli di massimo 1 minuto con una frequenza non inferiore a 7 giorni.

158 Questa funzione consente di regolare l'ora senza limitazioni in modo calibratura.

22. **Caratteristiche di funzionamento**

159 L'unità elettronica di bordo deve essere in grado di funzionare correttamente nel campo di temperatura compreso tra − 20 °C e 70 °C e il sensore di movimento nel campo di temperatura compreso tra − 40 °C e 135 °C. La memoria di dati deve essere in grado di conservare il suo contenuto fino alla temperatura minima di − 40 °C.

160 L'apparecchio di controllo deve essere in grado di funzionare correttamente nel campo di umidità compreso tra 10 % e 90 %.

161 L'apparecchio di controllo deve essere protetto contro sovratensione, inversione di polarità dell'alimentazione e corto circuiti.

162 L'apparecchio di controllo deve essere conforme alla direttiva 95/54/CE della Commissione [1], che adegua al progresso tecnico la direttiva 72/245/CEE del Consiglio, concernente la compatibilità elettromagnetica, e deve essere protetto contro le scariche elettrostatiche ed i transitori.

23. **Materiali**

163 Tutti gli elementi costitutivi dell'apparecchio di controllo devono essere realizzati con materiali dotati di stabilità e di resistenza meccanica sufficienti e di caratteristiche elettriche e magnetiche stabili.

164 Per le normali condizioni di impiego, tutti gli elementi interni dell'apparecchio devono essere protetti contro l'umidità e la polvere.

165 L'unità elettronica di bordo deve soddisfare il grado di protezione IP 40 e il sensore di movimento il grado di protezione IP 64, secondo la norma IEC 529.

---

[1] GU L 266 dell' 8.11.1995, pag. 1.

166 L'apparecchio di controllo deve essere conforme alle specifiche tecniche applicabili in materia di ergonomia.

167 L'apparecchio di controllo deve essere protetto contro i danni accidentali.

24. **Iscrizioni**

168 Se l'apparecchio di controllo visualizza il valore dell'odometro e la velocità, sul dispositivo di visualizzazione devono figurare le seguenti iscrizioni:

— in prossimità della cifra che indica la distanza, l'unità di misura della distanza espressa dal simbolo "km",

— in prossimità della cifra che indica la velocità, l'indicazione "km/h".

L'apparecchio di controllo deve inoltre consentire la visualizzazione della velocità in miglia all'ora, nel qual caso l'unità di misura della velocità sarà espressa dall'indicazione "mph".

169 Una targhetta segnaletica deve essere affissa ad ogni componente distinto dell'apparecchio di controllo e deve riportare le seguenti indicazioni:

— nome e indirizzo del fabbricante dell'apparecchio,

— codice componente del fabbricante e anno di fabbricazione dell'apparecchio,

— numero di serie dell'apparecchio,

— marchio di omologazione del tipo di apparecchio.

170 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 dell'apparecchio.

IV. REQUISITI COSTRUTTIVI E FUNZIONAMENTO DELLE CARTE TACHIGRAFICHE

1. **Dati visibili**

Il lato anteriore della carta contiene:

171 i termini "Carta del conducente" o "Carta di controllo" o "Carta dell'officina" o "Carta dell'azienda" stampati in carattere largo nella lingua o nelle lingue ufficiali dello Stato membro che rilascia la carta, a seconda del tipo di carta;

172 gli stessi termini nelle altre lingue ufficiali della Comunità, come stampa di fondo della carta:

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

173 il nome dello Stato membro che rilascia la carta (facoltativo);

174 il segno distintivo dello Stato membro che rilascia la carta, stampato in negativo in un rettangolo azzurro e circondato da dodici stelle gialle. I simboli distintivi sono i seguenti:

B Belgio

DK Danimarca

D Germania

GR Grecia

E Spagna

F Francia

IRL Irlanda

I Italia

L Lussemburgo

NL Paesi Bassi

A Austria

P Portogallo

FIN Finlandia

S Svezia

UK Regno Unito

175 le informazioni specifiche della carta, nell'ordine seguente:

	Carta del conducente	Carta di controllo	Carta dell'azienda o dell'officina
1.	Cognome del conducente	Nome dell'organismo di controllo	Nome dell'azienda o dell'officina
2.	Nome/i del conducente	Cognome dell'agente incaricato del controllo (se applicabile)	Cognome del titolare della carta (se applicabile)
3.	Data di nascita del conducente	Nome/i dell'agente incaricato del controllo (se applicabile)	Nome/i del titolare della carta (se applicabile)
4.(a)	Data di inizio validità della carta		
(b)	Data di scadenza della carta (se prevista)		
(c)	Denominazione dell'autorità che rilascia la carta (si può stampare sul retro)		
(d)	Un numero, diverso da quello indicato alla voce 5, da utilizzare per fini amministrativi (facoltativo)		
5.(a)	Numero della patente di guida (alla data di rilascio della carta del conducente)		
5.(b)	Numero della carta		
6.	Fotografia del conducente	Fotografia dell'agente incaricato del controllo (facoltativo)	—
7.	Firma del conducente	Firma del titolare (facoltativo)	
8.	Luogo di residenza normale, o indirizzo postale del titolare (facoltativo)	Indirizzo postale dell'organismo di controllo	Indirizzo postale dell'azienda o dell'officina

176 le date devono essere indicate nel formato "gg/mm/aaaa" o "gg.mm.aaaa" (giorno, mese, anno).

Il retro della carta contiene:

177 la spiegazione delle voci numerate che appaiono sul lato anteriore della carta;

178 se del caso e con l'assenso specifico scritto del titolare, anche altre informazioni che non si riferiscono alla gestione della carta, purché tale aggiunta non modifichi in alcun modo l'impiego del modello come carta tachigrafica.

MODELLO COMUNITARIO DI CARTA TACHIGRAFICA

LATO ANTERIORE — *RETRO*

CARTA DEL CONDUCENTE — STATO MEMBRO

MS

1.
2.
3.
4a. 4b.
4c.
(4d.)
5a.
5b.
7.
(8.)

6.

TARJETA DEL CONDUCTOR
FØRERKORT
FAHRERKARTE
ΚΑΡΤΑ ΟΔΗΓΟΥ
DRIVER CARD
CARTE DE CONDUCTEUR
CARTA TOMANAI
CARTA DEL CONDUCENTE
BESTUURDERSKAART
CARTÃO DE CONDUTOR
KULJETTAJAKORTTILLA
FÖRARKORT

A — B — B — A

1. Cognome 2. Nome/i 3. Data di nascita
4a. Data di inizio validità della carta
4b. Data di scadenza della carta
4c. Autorità che rilascia la carta
(4d.) Numero da utilizzare per fini amministrativi
5a. Numero della patente di guida 5b. Numero della carta
6. Fotografia
7. Firma (8.) Indirizzo

Pregasi restituire a

NOME E INDIRIZZO DELL'AUTORITÀ

CARTA DI CONTROLLO — STATO MEMBRO

MS

1.
(2.)
(3.)
4a. (4b.)
4c.
(4d.)
5b.
(7.)
8.

(6.)

TARJETA DE CONTROL
KONTROLKORT
KONTROLLKARTE
ΚΑΡΤΑ ΕΛΕΓΧΟΥ
CONTROL CARD
CARTE DE CONTRÔLEUR
CARTA STEIRTHA
CARTA DI CONTROLLO
CONTROLEKAART
CARTÃO DE CONTROLO
VALVONTAKORTTILLA
KONTROLLKORT

1. Organismo di controllo 2. Cognome 3. Nome/i
4a. Data di inizio validità della carta
(4b.) Data di scadenza della carta
4c. Autorità che rilascia la carta
(4d.) Numero da utilizzare per fini amministrativi
5b. Numero della carta
6. Fotografia
7. Firma (8.) Indirizzo

Pregasi restituire a

NOME E INDIRIZZO DELL'AUTORITÀ

CARTA DELL'OFFICINA — STATO MEMBRO

MS

1.
(2.)
(3.)
4a. 4b.
4c.
(4d.)
5b.
(7.)
8.

TARJETA DEL CENTRO DE ENSAYO
VÆRKSTEDSKORT
WERKSTATTKARTE
ΚΑΡΤΑ ΚΕΝΤΡΟΥ ΜΟΜΟΝ
WORKSHOP CARD
CARTE D'ATELIER
CÁRTA GEARDLANNE
CARTA DELL'OFFICINA
WERKPLAATSKAART
CARTÃO DO CENTRO DE ENSAIO
TESTAUSASEMAKORTTILLA
VERKSTADSKORT

1. Nome dell'officina 2. Cognome 3. Nome/i
4a. Data di inizio validità della carta
4b. Data di scadenza della carta
4c. Autorità che rilascia la carta
(4d.) Numero da utilizzare per fini amministrativi
5b. Numero della carta
7. Firma (8.) Indirizzo

Pregasi restituire a

NOME E INDIRIZZO DELL'AUTORITÀ

CARTA DELL'AZIENDA — STATO MEMBRO

MS

1.
(2.)
(3.)
4a. 4b.
4c.
(4d.)
5b.
(7.)
8.

TARJETA DE LA EMPRESA
VIRKSOMHEDSKORT
UNTERNEHMENSKARTE
ΚΑΡΤΑ ΕΠΙΧΕΙΡΗΣΗΣ
COMPANY CARD
CARTE D'ENTREPRISE
CÁRTA COMHLACHTA
CARTA DELL'AZIENDA
BEDRIJFSKAART
CARTÃO DE EMPRESA
YRITYSKORTTILLA
FÖRETAGSKORT

1. Nome dell'azienda 2. Cognome 3. Nome/i
4a. Data di inizio validità della carta
4b. Data di scadenza della carta
4c. Autorità che rilascia la carta
(4d.) Numero da utilizzare per fini amministrativi
5b. Numero della carta
7. Firma (8.) Indirizzo

Pregasi restituire a

NOME E INDIRIZZO DELL'AUTORITÀ

179 Le carte tachigrafiche sono stampate con i seguenti colori di fondo predominanti:

— carta del conducente: bianco

— carta di controllo: azzurro

— carta dell'officina: rosso

— carta dell'azienda: giallo

180 Le carte tachigrafiche devono presentare almeno le caratteristiche seguenti ai fini della protezione contro la falsificazione e la manomissione della carta stessa:

— stampa policroma del fondo di sicurezza finemente arabescato,

— sovrapposizione del fondo di sicurezza e della fotografia,

— almeno una linea bicromatica microstampata.

181 Salve restando le altre prescrizioni del presente allegato e previa consultazione della Commissione, gli Stati membri possono aggiungere altri colori o iscrizioni, come i simboli nazionali ed altre caratteristiche di sicurezza.

2. **Sicurezza**

La sicurezza del sistema è intesa a proteggere l'integrità e l'autenticità dei dati scambiati tra le carte e l'apparecchio di controllo, proteggere l'integrità e l'autenticità dei dati trasferiti dalle carte, consentire talune operazioni di scrittura sulle carte solo all'apparecchio di controllo, escludere ogni possibilità di falsificazione dei dati memorizzati sulle carte, impedire la manomissione e rilevarne eventuali tentativi.

182 Al fine di garantire la sicurezza del sistema, le carte tachigrafiche devono soddisfare i requisiti specificati negli obiettivi generali di sicurezza per le carte tachigrafiche (appendice 10).

183 Le carte tachigrafiche devono poter essere lette da altri apparecchi, come i personal computer.

3. **Norme**

184 Le carte tachigrafiche devono essere conformi alle norme seguenti:

— ISO/IEC 7810 Carte di identificazione — Caratteristiche fisiche

— ISO/IEC 7816 Carte di identificazione — Circuiti integrati con contatti:

  — Parte 1: Caratteristiche fisiche

  — Parte 2: Dimensione e posizione dei contatti

  — Parte 3: Segnali elettronici e protocolli di trasmissione

  — Parte 4: Comandi interindustriali per gli scambi

  — Parte 8: Sicurezza relativa ai comandi interindustriali

ISO/IEC 10373 Carte di identificazione — Metodi di prova.

4. **Specifiche ambientali ed elettriche**

185 Le carte tachigrafiche devono essere in grado di funzionare correttamente in tutte le condizioni climatiche abituali nel territorio della Comunità e almeno nel campo di temperatura compreso tra — 25 °C e + 70 °C, con picchi occasionali fino a + 85 °C , dove per "occasionale" s'intende non superiore a 4 ore per volta e non superiore a 100 volte nell'intero periodo di durata della carta.

186 Le carte tachigrafiche devono essere in grado di funzionare correttamente nel campo di umidità compreso tra 10 % e 90 %.

187 Le carte tachigrafiche devono essere in grado di funzionare correttamente per un periodo di cinque anni, se impiegate nel rispetto delle specifiche ambientali ed elettriche.

188 Per quanto riguarda il funzionamento, le carte tachigrafiche devono essere conformi alla direttiva 95/54/CE della Commissione, del 31 ottobre 1995 ([1]), concernente la compatibilità elettromagnetica, e devono essere protette contro le scariche elettrostatiche.

5. **Memorizzazione dei dati**

Agli effetti del presente punto,

— se non diversamente specificato, i tempi sono registrati con una risoluzione di un minuto,

— i valori dell'odometro sono registrati con una risoluzione di un chilometro,

— le velocità sono registrate con una risoluzione di 1 km/h.

Le funzioni, i comandi e le strutture logiche delle carte tachigrafiche che soddisfano i requisiti di memorizzazione sono specificati all'appendice 2.

([1]) GU L 266 dell'8.11.1995, pag. 1.

189 Il presente paragrafo specifica la capacità minima di memorizzazione per i file di dati destinati alle diverse applicazioni. Le carte tachigrafiche devono essere in grado di indicare all'apparecchio di controllo la capacità effettiva di memorizzazione di tali file di dati.

Eventuali dati supplementari da memorizzare nelle carte tachigrafiche, relativi ad altre applicazioni eventualmente previste dalla carta, devono essere memorizzati in conformità della direttiva 95/46/CE ([1]).

5.1. ***Identificazione della carta e dati di sicurezza***

5.1.1. *Identificazione dell'applicazione*

190 Le carte tachigrafiche devono essere in grado di memorizzare i seguenti dati di identificazione dell'applicazione:

— identificazione dell'applicazione tachigrafica,

— identificazione del tipo di carta tachigrafica.

5.1.2. *Identificazione del chip*

191 Le carte tachigrafiche devono essere in grado di memorizzare i seguenti dati di identificazione del circuito integrato:

— numero di serie del circuito integrato,

— riferimenti di fabbricazione del circuito integrato.

5.1.3. *Identificazione della carta a circuito integrato*

192 Le carte tachigrafiche devono essere in grado di memorizzare i seguenti dati di identificazione delle carte intelligenti:

— numero di serie della carta (compresi i riferimenti di fabbricazione),

— numero di omologazione della carta,

— identificazione personalizzata della carta (ID),

— identificazione dell'assemblatore della carta,

— identificativo del circuito integrato.

5.1.4. *Elementi di sicurezza*

193 Le carte tachigrafiche devono essere in grado di memorizzare i seguenti elementi di sicurezza:

— chiave pubblica europea,

— certificato dello Stato membro,

— certificato della carta,

— chiave privata della carta.

5.2. ***Carta del conducente***

5.2.1. *Identificazione della carta*

194 La carta del conducente deve essere in grado di memorizzare i seguenti dati di identificazione della carta:

— numero della carta,

— Stato membro di rilascio, denominazione dell'autorità di rilascio, data di rilascio,

— data di inizio validità della carta, data di scadenza della carta.

([1]) GU L 281 del 23.11.1995, pag. 31.

5.2.2. *Identificazione del titolare della carta*

195 La carta del conducente deve essere in grado di memorizzare i seguenti dati di identificazione del titolare:

— cognome del titolare,

— nome/i del titolare,

— data di nascita,

— lingua abituale.

5.2.3. *Informazioni sulla patente di guida*

196 La carta del conducente deve essere in grado di memorizzare i seguenti dati relativi alla patente di guida:

— Stato membro di rilascio, denominazione dell'autorità di rilascio,

— numero della patente di guida (alla data di rilascio della carta).

5.2.4. *Dati relativi ai veicoli impiegati*

197 La carta del conducente deve essere in grado di memorizzare, per ogni giorno di calendario in cui la carta viene usata e per ogni periodo di impiego di un determinato veicolo in tale giorno (un periodo di impiego comprende tutti i cicli consecutivi di inserimento/estrazione della carta nel veicolo, dal punto di vista della singola carta), i dati seguenti:

— data e ora del primo impiego del veicolo (cioè il primo inserimento della carta per questo periodo di impiego del veicolo, o 00h00 se il periodo di impiego è in corso in tale momento),

— valore dell'odometro del veicolo in tale momento,

— data e ora dell'ultimo impiego del veicolo (cioè l'ultima estrazione della carta per questo periodo di impiego del veicolo, o 23h59 se il periodo di impiego è in corso in tale momento),

— valore dell'odometro del veicolo in tale momento,

— VRN e Stato membro di immatricolazione del veicolo.

198 La carta del conducente deve essere in grado di memorizzare almeno 84 di tali registrazioni.

5.2.5. *Dati relativi all'attività del conducente*

199 La carta del conducente deve essere in grado di memorizzare, per ciascun giorno di calendario in cui la carta viene usata o ogniqualvolta il conducente inserisca manualmente un'attività, i dati seguenti:

— la data,

— un contatore di presenza giornaliera (aumentato di un'unità per ogni giorno di calendario in cui la carta viene usata),

— la distanza totale percorsa dal conducente durante tale giorno,

— la condizione del conducente a 00h00,

— ad ogni cambio di attività del conducente e/o cambio di condizione di guida e/o inserimento o estrazione della carta:

  — la condizione di guida (EQUIPAGGIO, SINGOLA)

  — la sede (slot) (CONDUCENTE, SECONDO CONDUCENTE),

  — la condizione della carta (INSERITA, NON INSERITA),

  — l'attività (GUIDA, DISPONIBILITÀ, LAVORO, INTERRUZIONE/RIPOSO).

  — l'ora del cambiamento.

200 La memoria della carta del conducente deve essere in grado di conservare i dati relativi all'attività del conducente per almeno 28 giorni (l'attività media di un conducente è intesa come 93 cambi di attività al giorno).

201 I dati elencati ai requisiti 197 e 199 devono essere memorizzati in modo da consentire il reperimento delle attività nell'ordine in cui hanno avuto luogo, anche in caso di sovrapposizione di orari.

5.2.6. *Luogo in cui inizia e/o termina il periodo di lavoro giornaliero*

202 La carta del conducente deve essere in grado di memorizzare i dati seguenti relativi al luogo in cui inizia e/o termina il periodo di lavoro giornaliero, inseriti dal conducente:

— la data e l'ora dell'immissione (o la data/ora relativa all'immissione, se questa viene effettuata durante la procedura di immissione manuale),

— il tipo di immissione (inizio o termine, condizione di immissione),

— il paese e la regione inseriti,

— il valore dell'odometro del veicolo.

203 La memoria della carta del conducente deve essere in grado di conservare almeno 42 coppie di tali registrazioni.

5.2.7. *Dati relativi alle anomalie*

Agli effetti del presente punto, l'ora deve essere memorizzata con una risoluzione di 1 secondo.

204 La carta del conducente deve essere in grado di memorizzare i dati relativi alle anomalie seguenti, rilevate dall'apparecchio di controllo a carta inserita:

— sovrapposizione di orari (se questa carta è la causa dell'anomalia),

— inserimento della carta durante la guida (se questa carta è l'oggetto dell'anomalia),

— chiusura errata ultima sessione carta (se questa carta è l'oggetto dell'anomalia),

— interruzione dell'alimentazione di energia,

— errore dati di marcia,

— tentata violazione della sicurezza.

205 Per tali anomalie, la carta del conducente deve essere in grado di memorizzare i dati seguenti:

— codice dell'anomalia,

— data e ora di inizio dell'anomalia (o di inserimento della carta se l'anomalia era in atto in tale momento),

— data e ora di termine dell'anomalia (o di estrazione della carta se l'anomalia era in atto in tale momento),

— VRN e Stato membro di immatricolazione del veicolo in cui si è verificata l'anomalia.

Nota: Per l'anomalia "Sovrapposizione di orari":

— la data e l'ora di inizio dell'anomalia devono corrispondere alla data e all'ora di estrazione della carta dal veicolo precedente,

— la data e l'ora di termine dell'anomalia devono corrispondere alla data e all'ora di inserimento della carta nel veicolo in uso,

— i dati relativi al veicolo devono corrispondere al veicolo in uso su cui si verifica l'anomalia.

Nota: Per l'anomalia "Chiusura errata ultima sessione carta":

— la data e l'ora di inizio dell'anomalia devono corrispondere alla data e all'ora di inserimento della carta per la sessione chiusa in modo errato,

— la data e l'ora di termine dell'anomalia devono corrispondere alla data e all'ora di inserimento della carta per la sessione durante la quale è stata rilevata l'anomalia (sessione in corso),

— i dati relativi al veicolo devono corrispondere al veicolo in cui la sessione è stata chiusa in modo errato.

206 La carta del conducente deve essere in grado di memorizzare i dati relativi alle sei anomalie più recenti di ciascun tipo (cioè 36 anomalie).

5.2.8. *Dati relativi ai guasti*

Agli effetti del presente punto, l'ora deve essere registrata con una risoluzione di 1 secondo.

207 La carta del conducente deve essere in grado di memorizzare i dati relativi ai guasti seguenti, rilevati dall'apparecchio di controllo a carta inserita:

— guasto della carta (se questa carta è l'oggetto del guasto),

— guasto dell'apparecchio di controllo.

208 Per tali guasti, la carta del conducente deve essere in grado di memorizzare i dati seguenti:

— codice del guasto,

— data e ora di inizio del guasto (o di inserimento della carta se il guasto era in atto in tale momento),

— data e ora di termine del guasto (o di estrazione della carta se il guasto era in atto in tale momento),

— VRN e Stato membro di immatricolazione del veicolo in cui si è verificato il guasto.

209 La carta del conducente deve essere in grado di memorizzare i dati relativi ai dodici guasti più recenti di ciascun tipo (cioè 24 guasti).

5.2.9. *Dati relativi alle attività di controllo*

210 La carta del conducente deve essere in grado di memorizzare i dati seguenti, relativi alle attività di controllo:

— data e ora del controllo,

— numero della carta di controllo e Stato membro di rilascio,

— tipo di controllo [visualizzazione e/o stampa e/o trasferimento dati VU e/o trasferimento dati carta (cfr. nota)],

— periodo trasferito, in caso di trasferimento,

— VRN e Stato membro di immatricolazione del veicolo in cui è stato effettuato il controllo.

Nota: I requisiti di sicurezza prevedono che il trasferimento dei dati della carta sia registrato soltanto se viene effettuato attraverso un apparecchio di controllo.

211 La carta del conducente deve essere in grado di conservare una di tali registrazioni.

5.2.10. *Dati relativi alla sessione della carta*

212 La carta del conducente deve essere in grado di memorizzare i dati relativi al veicolo che ha aperto la sessione in corso:

— data e ora di apertura della sessione (cioè inserimento della carta) con una risoluzione di un secondo,

— VRN e Stato membro di immatricolazione.

5.2.11. *Dati relativi a condizioni particolari*

212a La carta del conducente deve essere in grado di memorizzare i dati seguenti, relativi a condizioni particolari immesse a carta inserita (in qualsiasi sede):

— data e ora di immissione,

— tipo di condizione particolare.

212b La carta del conducente deve essere in grado di memorizzare 56 di tali registrazioni.

5.3. ***Carta dell'officina***

5.3.1. *Elementi di sicurezza*

213 La carta dell'officina deve essere in grado di memorizzare un numero di identificazione personale (codice PIN).

214 La carta dell'officina deve essere in grado di memorizzare le chiavi crittografiche necessarie per l'accoppiamento dei sensori di movimento con le unità elettroniche di bordo.

5.3.2. *Identificazione della carta*

215 La carta dell'officina deve essere in grado di memorizzare i seguenti dati di identificazione della carta:

— numero della carta,

— Stato membro di rilascio, denominazione dell'autorità di rilascio, data di emissione,

— data di inizio validità della carta, data di scadenza della carta.

5.3.3. *Identificazione del titolare della carta*

216 La carta dell'officina deve essere in grado di memorizzare i seguenti dati di identificazione del titolare della carta:

— nome dell'officina,

— indirizzo dell'officina,

— cognome del titolare,

— nome/i del titolare,

— lingua abituale.

5.3.4. *Dati relativi ai veicoli impiegati*

217 La carta dell'officina deve essere in grado di memorizzare i dati relativi ai veicoli impiegati allo stesso modo della carta del conducente.

218 La carta dell'officina deve essere in grado di memorizzare almeno 4 di tali registrazioni.

5.3.5. *Dati relativi all'attività del conducente*

219 La carta dell'officina deve essere in grado di memorizzare i dati relativi all'attività del conducente allo stesso modo della carta del conducente.

220 La carta dell'officina deve essere in grado di conservare tali dati per almeno 1 giorno di attività media del conducente.

5.3.6. *Dati relativi all'inizio e/o termine del periodo di lavoro giornaliero*

221 La carta dell'officina deve essere in grado di memorizzare i dati relativi all'inizio e/o termine del periodo di lavoro giornaliero allo stesso modo della carta del conducente.

222 La carta dell'officina deve essere in grado di conservare almeno 3 coppie di tali registrazioni.

5.3.7. *Dati relativi ad anomalie e guasti*

223 La carta dell'officina deve essere in grado di memorizzare i dati relativi alle anomalie e ai guasti allo stesso modo della carta del conducente.

224 La carta dell'officina deve essere in grado di memorizzare i dati relativi alle tre anomalie più recenti di ciascun tipo (cioè 18 anomalie) e ai sei guasti più recenti di ciascun tipo (cioè 12 guasti).

5.3.8. *Dati relativi alle attività di controllo*

225 La carta dell'officina deve essere in grado di memorizzare i dati relativi alle attività di controllo allo stesso modo della carta del conducente.

5.3.9. *Dati relativi a calibratura e regolazione dell'ora*

226 La carta dell'officina deve essere in grado di conservare i dati relativi alle calibrature e/o regolazioni dell'ora effettuate a carta inserita nell'apparecchio di controllo.

227 Ogni registrazione relativa alla calibratura deve essere in grado di contenere i dati seguenti:

— scopo della calibratura (primo montaggio, montaggio, controllo periodico),

— identificazione del veicolo,

— parametri aggiornati o confermati (w, k, l, dimensioni dei pneumatici, regolazione del limitatore di velocità, odometro (vecchio e nuovo valore), data e ora (vecchio e nuovo valore),

— identificazione dell'apparecchio di controllo (codice componente della VU, numero di serie della VU, numero di serie del sensore di movimento).

228 La carta dell'officina deve essere in grado di memorizzare almeno 88 di tali registrazioni.

229 La carta dell'officina deve contenere un contatore che indichi il numero totale di calibrature effettuate con la carta stessa.

230 La carta dell'officina deve contenere un contatore che indichi il numero di calibrature effettuate a partire dall'ultimo trasferimento dei suoi dati.

5.3.10. *Dati relativi a condizioni particolari*

230a La carta dell'officina deve essere in grado di memorizzare i dati relativi a condizioni particolari allo stesso modo della carta del conducente. La carta dell'officina deve essere in grado di memorizzare 2 di tali registrazioni.

5.4. ***Carta di controllo***

5.4.1. *Identificazione della carta*

231 La carta di controllo deve essere in grado di memorizzare i seguenti dati di identificazione della carta:

— numero della carta,

— Stato membro di rilascio, denominazione dell'autorità di rilascio, data di rilascio,

— data di inizio validità della carta, data di scadenza della carta (se prevista).

5.4.2. *Identificazione del titolare della carta*

232 La carta di controllo deve essere in grado di memorizzare i seguenti dati di identificazione del titolare:

— nome dell'organismo di controllo,

— indirizzo dell'organismo di controllo,

— cognome del titolare,

— nome/i del titolare,

— lingua abituale.

5.4.3. *Dati relativi alle attività di controllo*

233 La carta di controllo deve essere in grado di memorizzare i dati seguenti, relativi alle attività di controllo:

— data e ora del controllo,

— tipo di controllo (visualizzazione e/o stampa e/o trasferimento dati VU e/o trasferimento dati carta),

— periodo cui si riferiscono i dati trasferiti (se del caso),

— VRN e autorità dello Stato membro di immatricolazione del veicolo controllato,

— numero della carta e Stato membro di rilascio della carta del conducente controllata.

234 La carta di controllo deve essere in grado di conservare almeno 230 di tali registrazioni.

5.5. ***Carta dell'azienda***

5.5.1. *Identificazione della carta*

235 La carta dell'azienda deve essere in grado di memorizzare i seguenti dati di identificazione della carta:

— numero della carta,

— Stato membro di rilascio, denominazione dell'autorità di rilascio, data di rilascio,

— data di inizio validità della carta, data di scadenza della carta (se presente).

5.5.2. *Identificazione del titolare della carta*

236 La carta dell'azienda deve essere in grado di memorizzare i seguenti dati di identificazione del titolare:

— nome dell'azienda,

— indirizzo dell'azienda.

5.5.3. *Dati relativi alle attività dell'impresa*

237 La carta dell'azienda deve essere in grado di memorizzare i dati seguenti, relativi alle attività dell'impresa:

— data e ora dell'attività,

— tipo di attività (attivazione e/o disattivazione blocco VU e/o trasferimento dati VU e/o trasferimento dati carta),

— periodo cui si riferiscono i dati trasferiti (se del caso),

— VRN e autorità dello Stato membro di immatricolazione del veicolo,

— numero della carta e Stato membro di rilascio (in caso di trasferimento dei dati della carta).

238 La carta dell'azienda deve essere in grado di conservare almeno 230 di tali registrazioni.

V. MONTAGGIO DELL'APPARECCHIO DI CONTROLLO

1. **Montaggio**

239 Gli apparecchi di controllo nuovi devono essere consegnati prima dell'attivazione ai montatori o ai costruttori di veicoli, con tutti i parametri di calibratura, elencati al capitolo III, punto 20, impostati su valori predefiniti corretti e validi. In assenza di un valore corretto, i parametri alfabetici devono essere impostati come stringhe di "?" e i parametri numerici devono essere impostati su "0".

240 Prima dell'attivazione, l'apparecchio di controllo deve consentire l'accesso alla funzione di calibratura anche in modalità di funzionamento diverse dal modo calibratura.

241 Prima dell'attivazione, l'apparecchio di controllo non deve registrare né memorizzare i dati menzionati al capitolo III, dal punto 12.3. al punto 12.9. e dal punto 12.12 al punto 12.14. inclusi.

242 Durante il montaggio, i costruttori di veicoli devono preimpostare tutti i parametri noti.

243 I costruttori di veicoli o i montatori devono procedere all'attivazione dell'apparecchio di controllo montato nel veicolo prima che questo esca dai locali in cui ha avuto luogo il montaggio.

244 L'attivazione dell'apparecchio di controllo deve avvenire automaticamente al primo inserimento di una carta del centro di controllo in una qualsiasi delle interfacce della carta.

245 Le operazioni specifiche di accoppiamento tra il sensore di movimento e l'unità elettronica di bordo, se del caso, devono avvenire automaticamente prima o durante l'attivazione.

246 Dopo l'attivazione, l'apparecchio di controllo deve essere in grado di funzionare correttamente e riconoscere tutti i diritti di accesso ai dati.

247 Dopo l'attivazione si devono poter usare tutte le funzioni di registrazione e memorizzazione dell'apparecchio di controllo.

248 A seguito del montaggio occorre procedere alla calibratura. La prima calibratura prevede l'immissione del VRN e deve essere effettuata entro 2 settimane dal montaggio o dall'attribuzione del VRN, se questa si verifica per ultima.

248a L'apparecchio di controllo deve essere posizionato a bordo del veicolo in modo tale da consentire al conducente di accedere a tutte le funzioni dal posto di guida.

2. **Targhetta di montaggio**

249 Una targhetta di montaggio chiaramente visibile viene apposta sull'apparecchio di controllo in un punto facilmente accessibile, al suo interno o in prossimità di esso, dopo la verifica in sede di primo montaggio. Dopo ogni intervento da parte di un montatore o di un'officina autorizzati deve essere apposta una nuova targhetta in sostituzione della precedente.

250 Sulla targhetta devono essere riportate almeno le indicazioni seguenti:

— nome, indirizzo o denominazione commerciale del montatore o dell'officina autorizzati,

— coefficiente caratteristico del veicolo, sotto la forma “w = … imp/km”,

— costante dell'apparecchio di controllo, sotto la forma “k = … imp/km”

— circonferenza effettiva dei pneumatici delle ruote, sotto la forma “l = … mm”,

— dimensioni dei pneumatici,

— data del rilevamento del coefficiente caratteristico del veicolo e della misurazione della circonferenza effettiva dei pneumatici delle ruote,

— numero di identificazione del veicolo.

3. **Sigilli**

251 I seguenti elementi devono essere sigillati:

— qualsiasi raccordo che, se fosse disinserito, causerebbe modifiche o perdite di dati non rilevabili;

— la targhetta di montaggio, a meno che sia apposta in modo da non poter essere tolta senza distruggere le indicazioni.

252 I sigilli summenzionati possono essere tolti:

— in casi d'emergenza,

— per installare, regolare o riparare un limitatore di velocità o qualsiasi altro dispositivo inteso a migliorare la sicurezza stradale, a condizione che l'apparecchio di controllo continui a funzionare in modo affidabile e corretto e sia risigillato da un montatore o da un'officina autorizzati (conformemente al capitolo VI) immediatamente dopo l'installazione del limitatore di velocità o di un altro dispositivo inteso a migliorare la sicurezza stradale, oppure entro sette giorni negli altri casi.

253 L'eventuale rimozione di questi sigilli deve essere l'oggetto di una giustificazione scritta, tenuta a disposizione dell'autorità competente.

VI. VERIFICHE, CONTROLLI E RIPARAZIONI

I requisiti relativi alle circostanze in cui si possono togliere i sigilli, secondo quanto indicato all'articolo 12, paragrafo 5, del regolamento (CEE) n. 3821/85, come da ultimo modificato dal regolamento (CE) n. 2135/98, sono definiti al capitolo V, punto 3, del presente allegato.

1. **Approvazione di montatori od officine**

Gli Stati membri autorizzano, sottopongono a verifiche regolari e certificano gli organismi incaricati di effettuare:

— il montaggio,

— le verifiche,

— i controlli,

— le riparazioni.

Ai sensi dell'articolo 12, paragrafo 1, di detto regolamento, le carte dell'officina sono rilasciate esclusivamente ai montatori e/o officine autorizzati ad effettuare l'attivazione e/o la calibratura dell'apparecchio di controllo in conformità del presente allegato e che, tranne caso debitamente motivato:

— non possiedono i requisiti necessari per ottenere una carta dell'azienda;

— le altre attività professionali non rappresentano un rischio potenziale per la sicurezza generale del sistema, secondo quanto previsto all'appendice 10.

2. **Verifica degli strumenti nuovi o riparati**

254 Di ogni singolo dispositivo, nuovo o riparato, vengono verificati il corretto funzionamento e l'esattezza delle indicazioni e registrazioni, nei limiti fissati al capitolo III, punti 2.1 e 2.2, mediante l'apposizione di sigilli conformemente al capitolo V, punto 3, e la calibratura.

3. **Controllo in sede di montaggio**

255 All'atto del montaggio nel veicolo, l'installazione nel suo complesso (compreso l'apparecchio di controllo) deve essere conforme alle disposizioni relative alle tolleranze massime di cui al capitolo III, punti 2.1 e 2.2.

4. **Controlli periodici**

256 I controlli periodici degli apparecchi montati nei veicoli hanno luogo dopo ogni riparazione degli apparecchi stessi, dopo ogni modifica del coefficiente caratteristico del veicolo o della circonferenza effettiva dei pneumatici, dopo un periodo di ora UTC errata di durata superiore a 20 minuti, dopo la modifica del VRN e comunque almeno ogni due anni (24 mesi) a partire dall'ultimo controllo.

257 Si devono controllare:

— lo stato di buon funzionamento dell'apparecchio di controllo, compresa la memorizzazione di dati nelle carte tachigrafiche,

— la conformità con le disposizioni del capitolo III, punti 2.1 e 2.2, relative alle tolleranze massime in sede di montaggio,

— la presenza del marchio di omologazione sull'apparecchio di controllo,

— la presenza della targhetta di montaggio,

— l'integrità dei sigilli dell'apparecchio e degli altri elementi dell'impianto,

— le dimensioni dei pneumatici e la circonferenza effettiva dei pneumatici.

258 Tali controlli devono prevedere la calibratura.

5. **Determinazione degli errori**

259 La determinazione degli errori all'atto del montaggio e durante l'uso si effettua nelle seguenti condizioni, che si devono considerare come normali condizioni di prova:

— veicolo a vuoto, in normali condizioni di marcia,

— pressione dei pneumatici conforme alle indicazioni fornite dal costruttore,

— usura dei pneumatici nei limiti ammessi dalla normativa nazionale in vigore,

— movimento del veicolo:

  — il veicolo deve spostarsi, mosso dal proprio motore, in linea retta, su terreno piatto, ad una velocità di 50 ± 5 km/h; la misurazione deve essere effettuata su una distanza di almeno 1000 m.

— a condizione che venga garantita una precisione analoga, la prova può essere effettuata con altri metodi, per esempio su un banco di prova.

6. **Riparazioni**

260 Le officine devono essere in grado di trasferire i dati dall'apparecchio di controllo al fine di fornire tali dati alle imprese di trasporto interessate.

261 Qualora il cattivo funzionamento dell'apparecchio di controllo impedisca il trasferimento dei dati registrati in precedenza, anche dopo la riparazione da parte di tali officine autorizzate, esse rilasciano alle imprese di trasporti un certificato che attesta l'impossibilità di trasferire i dati. Le officine conservano una copia di ogni certificato rilasciato per almeno un anno.

VII. RILASCIO DELLA CARTA

Le procedure di rilascio della carta definite dagli Stati membri devono conformarsi ai requisiti seguenti.

262 Al primo rilascio di una carta tachigrafica ad un richiedente, il numero della carta deve contenere un codice di serie (se applicabile), un codice di sostituzione e un codice di rinnovo uguali a "0".

263 Il numero della carta di tutte le carte tachigrafiche non personali rilasciate ad un medesimo organismo di controllo, una medesima officina o una medesima impresa di trasporti, deve avere gli stessi primi 13 caratteri ed un diverso codice di serie.

264 Una carta tachigrafica rilasciata in sostituzione di una carta tachigrafica esistente deve avere lo stesso numero della carta sostituita, eccetto per il codice di sostituzione che deve essere aumentato di un'unità (nell'ordine 0, …, 9, A, …, Z).

265 Una carta tachigrafica rilasciata in sostituzione di una carta tachigrafica esistente deve avere la stessa data di scadenza della carta sostituita.

266 Una carta tachigrafica rilasciata in rinnovo di una carta tachigrafica esistente deve avere lo stesso numero della carta rinnovata, eccetto per il codice di sostituzione che deve essere riportato a "0" e il codice di rinnovo che deve essere aumentato di un'unità (nell'ordine 0, …, 9, A, …, Z).

267 In caso di cambio di una carta tachigrafica esistente al fine di modificarne i dati amministrativi, si devono applicare le regole relative al rinnovo se il cambio è effettuato all'interno dello stesso Stato membro, oppure le regole relative al primo rilascio se tale cambio è effettuato da un altro Stato membro.

268 Alla voce "cognome del titolare della carta" per le carte dell'officina o le carte di controllo non personali deve essere riportato il nome dell'officina o dell'organismo di controllo.

VIII. OMOLOGAZIONE DELL'APPARECCHIO DI CONTROLLO E DELLE CARTE TACHIGRAFICHE

1. **Prescrizioni generali**

Agli effetti del presente capitolo, i termini "apparecchio di controllo" s'intendono come "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. I fogli di carta impiegati dall'apparecchio di controllo devono considerarsi come un componente dell'apparecchio stesso.

269 L'apparecchio di controllo deve essere presentato per l'omologazione munito di tutti i dispositivi integrati supplementari.

270 L'omologazione dell'apparecchio di controllo e delle carte tachigrafiche comprende prove riguardanti la sicurezza, prove funzionali e prove di interoperabilità. I risultati positivi di ciascuna di queste prove sono riportati su un apposito certificato.

271 Le autorità degli Stati membri competenti per l'omologazione non concedono una scheda di omologazione in conformità dell'articolo 5 del regolamento fintantoché non sia loro presentato:

— un certificato di sicurezza,

— un certificato funzionale,

— un certificato di interoperabilità,

per l'apparecchio di controllo o la carta tachigrafica che forma l'oggetto della domanda di omologazione.

272 Eventuali modifiche del software o dell'hardware dell'apparecchio o della natura dei materiali usati per la fabbricazione devono essere notificati all'autorità che ha omologato l'apparecchio prima dell'impiego. Tale autorità conferma al fabbricante l'estensione dell'omologazione oppure richiede un aggiornamento o una conferma dei certificati funzionale, di sicurezza e/o di interoperabilità pertinenti.

273 Le procedure volte ad aggiornare in situ il software dell'apparecchio di controllo devono essere approvate dall'autorità che ha omologato l'apparecchio di controllo. L'aggiornamento del software non deve modificare o cancellare i dati relativi all'attività del conducente memorizzati nell'apparecchio di controllo. Il software si può aggiornare solo sotto la responsabilità del fabbricante dell'apparecchio.

2. **Certificato di sicurezza**

274 Il certificato di sicurezza è rilasciato in conformità delle disposizioni di cui all'appendice 10 del presente allegato.

3. **Certificato funzionale**

275 Ogni richiedente di un'omologazione deve presentare all'autorità dello Stato membro competente per l'omologazione tutto il materiale e la documentazione ritenuti necessari da tale autorità.

276 Il certificato funzionale viene rilasciato al fabbricante solo se almeno tutte le prove funzionali specificate all'appendice 9 hanno dato risultati positivi.

277 L'autorità competente per l'omologazione rilascia un certificato funzionale. Tale certificato riporta, oltre al nome del beneficiario e all'identificazione del modello, un elenco dettagliato delle prove effettuate e dei risultati ottenuti.

4. **Certificato di interoperabilità**

278 Le prove di interoperabilità sono effettuate da un unico laboratorio sotto l'autorità e la responsabilità della Commissione europea.

279 Il laboratorio registra le richieste di prove di interoperabilità presentate dai fabbricanti nell'ordine cronologico di presentazione.

280 Le richieste sono registrate ufficialmente solo quando il laboratorio dispone:

— dell'intera serie di materiali e documenti necessari per le prove di interoperabilità,

— del corrispondente certificato di sicurezza,

— del corrispondente certificato funzionale.

La data di registrazione della richiesta viene notificata al fabbricante.

281 Il laboratorio non effettua le prove di interoperabilità di un apparecchio di controllo o di una carta tachigrafica che non abbia ottenuto un certificato di sicurezza e un certificato funzionale.

282 I fabbricanti che richiedono le prove di interoperabilità si impegnano a lasciare a disposizione del laboratorio incaricato di tali prove l'intera serie di materiali e documenti forniti per l'esecuzione delle prove stesse.

283 Le prove di interoperabilità sono effettuate, in conformità delle disposizioni di cui all'appendice 9, punto 5 del presente allegato, con tutti i tipi di apparecchi di controllo e di carte tachigrafiche:

— la cui omologazione è in corso di validità, o

— che sono in attesa di omologazione e hanno ottenuto un certificato valido di interoperabilità.

284 Il laboratorio rilascia al fabbricante il certificato di interoperabilità solo se tutte le prove di interoperabilità hanno dato risultati positivi.

285 Se le prove di interoperabilità non danno risultati positivi con uno o più apparecchi di controllo o carte tachigrafiche, secondo quanto previsto dal requisito 283, il certificato di interoperabilità non viene rilasciato al fabbricante finché non sono state apportate le modifiche necessarie a superare tutte le prove di interoperabilità. Il laboratorio identifica la causa del problema con l'aiuto dei fabbricanti interessati a tale mancanza di interoperabilità ed aiuta il richiedente a trovare una soluzione tecnica. Nel caso in cui il fabbricante modifichi il prodotto, spetterà al fabbricante stesso accertare presso le autorità competenti che il certificato di sicurezza e il certificato funzionale siano ancora validi.

286 Il certificato di interoperabilità ha una validità di sei mesi e viene revocato se, al termine di tale periodo, il fabbricante non ha ottenuto la corrispondente scheda di omologazione. Il certificato di interoperabilità viene trasmesso dal fabbricante all'autorità dello Stato membro competente per l'omologazione che ha rilasciato il certificato funzionale.

287 Qualsiasi elemento cui si possa ricondurre la mancanza di interoperabilità non deve essere usato a fini di lucro o per accedere ad una posizione dominante.

5. **Scheda di omologazione**

288 L'autorità competente per l'omologazione di uno Stato membro può rilasciare la scheda di omologazione non appena è in possesso dei tre certificati richiesti.

289 L'autorità competente per l'omologazione deve trasmettere una copia della scheda di omologazione al laboratorio incaricato delle prove di interoperabilità all'atto del rilascio della stessa al fabbricante.

290 Il laboratorio competente per le prove di interoperabilità gestisce un sito web pubblico nel quale mantiene aggiornato l'elenco dei modelli di apparecchio di controllo o carta tachigrafica:

— per i quali è stata registrata una richiesta di prove di interoperabilità,

— che abbiano ottenuto un certificato di interoperabilità (anche provvisorio),

— che abbiano ottenuto una scheda di omologazione.

6. **Procedura eccezionale: primo certificato di interoperabilità**

291 Per un periodo di quattro mesi successivi al rilascio del certificato di interoperabilità della prima coppia apparecchio di controllo / carte tachigrafiche (carte del conducente, dell'officina, di controllo e dell'azienda), ogni certificato di interoperabilità rilasciato (compreso il primo in assoluto), concernente le richieste presentate durante tale periodo, deve essere considerato provvisorio.

292 Se al termine di tale periodo tutti i prodotti interessati sono reciprocamente interoperabili, i rispettivi certificati di interoperabilità diventano definitivi.

293 Se durante tale periodo si riscontrano mancanze di interoperabilità, il laboratorio incaricato delle prove di interoperabilità identifica le cause dei problemi con l'aiuto di tutti i fabbricanti interessati e li invita ad apportare le modifiche necessarie.

294 Se al termine di tale periodo sussistono ancora problemi di interoperabilità, il laboratorio incaricato delle prove di interoperabilità, con la collaborazione dei fabbricanti interessati e delle autorità competenti per l'omologazione che hanno rilasciato i corrispondenti certificati funzionali, ricerca le cause della mancanza di interoperabilità e stabilisce le modifiche che ogni fabbricante deve apportare. La ricerca di soluzioni tecniche deve avvenire entro un periodo massimo di due mesi, in seguito al quale, qualora non si trovi una soluzione comune, la Commissione, dopo aver consultato il laboratorio incaricato delle prove di interoperabilità, decide quali apparecchi e quali carte ottengono un certificato definitivo di interoperabilità e ne indica i motivi.

295 Tutte le richieste di prove di interoperabilità, registrate dal laboratorio tra il termine del periodo di quattro mesi successivi al rilascio del primo certificato provvisorio di interoperabilità e la data della decisione della Commissione di cui al requisito 294, sono rinviate fino alla soluzione dei problemi iniziali di interoperabilità. Tali richieste sono quindi evase in ordine cronologico in base alla data di registrazione.

Appendice 1

DIZIONARIO DI DATI

INDICE

1. INTRODUZIONE

La presente appendice specifica i formati dei dati, gli elementi di dati e le strutture dei dati da usare nell'apparecchio di controllo e nelle carte tachigrafiche.

1.1. **Metodo di definizione dei tipi di dati**

Nella presente appendice i tipi di dati sono definiti in base al linguaggio Abstract Syntax Notation One (ASN.1). La notazione ASN.1 permette di definire dati semplici e strutturati, senza richiedere una specifica sintassi di trasmissione (regole di codifica), la quale dipende dall'applicazione e dal contesto.

La notazione convenzionale ASN.1 per l'attribuzione di nomi si basa sulla norma ISO/IEC 8824-1. Questo significa che:

— ove possibile, il significato del tipo di dati è implicitamente noto in funzione del nome attribuito,

— per i tipi di dati composti, costituiti da una combinazione di più tipi di dati, il nome è comunque un'unica sequenza di caratteri alfabetici con la lettera iniziale maiuscola, ma vengono usate lettere maiuscole anche all'interno del nome, che consentono di individuare il significato corrispondente,

— in generale, i nomi dei tipi di dati si riferiscono al nome dei tipi di dati con cui vengono costruiti, all'apparecchio in cui sono memorizzati i dati e alla funzione connessa ai dati.

Se un tipo ASN.1 è già definito nell'ambito di un'altra norma e viene usato nell'apparecchio di controllo, tale tipo ASN.1 è definito nella presente appendice.

Per tenere conto di vari tipi di regole di codifica, alcuni tipi ASN.1 compresi nella presente appendice sono limitati da identificatori del campo di valori. Gli identificatori del campo di valori sono definiti al paragrafo 3.

1.2. **Riferimenti normativi**

Nella presente appendice si rimanda alle norme seguenti.

ISO 639	Code for the representation of names of languages. First Edition: 1988. (Codice per la rappresentazione dei nomi delle lingue. Prima edizione: 1988)
EN 726-3	Identification cards systems — Telecommunications integrated circuit(s) cards and terminals — Part 3: Application independent card requirements. December 1994. (Sistemi di carte di identificazione — Carte a circuito(i) integrato(i) e terminali per telecomunicazioni — Parte 3: Requisiti validi per qualsiasi applicazione. Dicembre 1994)
ISO 3779	Road vehicles — Vehicle identification number (VIN) — Content and structure. Edition 3: 1983. (Veicoli stradali — Numero di identificazione del veicolo (VIN) — Contenuto e struttura. Edizione 3: 1983)
ISO/IEC 7816-5	Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 5: Numbering system and registration procedure for application identifiers. First edition: 1994 + Amendment 1: 1996. (Tecnologia dell'informazione — Carte di identificazione — Carte a circuito(i) integrato(i) con contatti — Parte 5: Sistemi di numerazione e procedura di registrazione per le identificazioni delle applicazioni. Prima edizione: 1994 + Modifica 1: 1996)
ISO/IEC 8824-1	Information technology — Abstract Syntax Notation 1 (ASN.1): Specification of basic notation. Edition 2: 1998. (Tecnologia dell'informazione — Abstract Syntax Notation 1 (ASN.1): Descrizione della notazione di base. Edizione 2: 1998)
ISO/IEC 8825-2	Information technology — ASN.1 encoding rules: Specification of Packed Encoding Rules (PER). Edition 2: 1998. (Tecnologia dell'informazione — Regole di codifica ASN.1: Descrizione delle regole di codifica a pacchetto (PER). Edizione 2: 1998)
ISO/IEC 8859-1	Information technology — 8 bit single-byte coded graphic character sets — Part 1: Latin alphabet No.1. First edition: 1998. (Tecnologia dell'informazione — Codifica a gruppo singolo di 8 bit di insiemi di caratteri grafici — Parte 1: Alfabeto latino n. 1. Prima edizione: 1998)
ISO/IEC 8859-7	Information technology — 8 bit single-byte coded graphic character sets — Part 7: Latin/Greek alphabet. First edition: 1987. (Tecnologia delle informazioni — Insieme di caratteri grafici codificati su un solo gruppo di 8 bit — Parte 7: Alfabeto latino/greco. Prima edizione: 1987)
ISO 16844-3	Road vehicles — Tachograph systems — Motion Sensor Interface. WD 3-20/05/99. (Veicoli stradali — Sistemi tachigrafici — Interfaccia del sensore di movimento. WD 3-20/05/99)

2. DEFINIZIONE DEI TIPI DI DATI

Per ciascuno dei seguenti tipi di dati, il valore predefinito di un contenuto "non noto" o "non applicabile" è dato dal riempimento dell'elemento di dati con byte 'FF'.

2.1. **ActivityChangeInfo**

Questo tipo di dati consente di codificare, in una parola (word) a due byte, la condizione della sede (slot) a 00h00 e/o la condizione del conducente a 00h00 e/o i cambi di attività e/o le variazioni della condizione di guida e/o le variazioni della condizione della carta riguardanti un conducente o un secondo conducente. Questo tipo di dati si riferisce ai requisiti 084, 109a, 199 e 219.

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

Assegnazione valore — Allineato all'ottetto: `'scpaatttttttttttt'B` (16 bits)

Per le registrazioni nella memoria di dati (o condizione della sede):

`'s'B` Sede (slot):

`'0'B`: CONDUCENTE,

`'1'B`: SECONDO CONDUCENTE,

`'c'B` Condizione di guida:

`'0'B`: SINGOLA,

`'1'B`: EQUIPAGGIO,

`'p'B` Condizione della carta del conducente (o dell'officina) nella relativa sede (slot):

`'0'B`: INSERITA, la carta è inserita,

`'1'B`: NON INSERITA, la carta è assente (o una carta viene estratta),

`'aa'B` Attività:

`'00'B`: INTERRUZIONE/RIPOSO,

`'01'B`: DISPONIBILITÀ,

`'10'B`: LAVORO,

`'11'B`: GUIDA,

`'ttttttttttt'B` Ora della variazione: numero di minuti a partire dalle 00h00 del giorno in questione.

Per le registrazioni nella carta del conducente (o dell'officina) (e per la condizione del conducente):

`'s'B` Sede (slot) (non pertinente se 'p' = 1, fatta salva la nota sotto):

`'0'B`: CONDUCENTE,

`'1'B`: SECONDO CONDUCENTE,

`'c'B` Condizione di guida (quando 'p' = 0) o Condizione attività successiva (quando 'p' = 1):

`'0'B`: SINGOLA, `'0'B`: NON NOTA

`'1'B`: EQUIPAGGIO, `'1'B`: NOTA (= immissione manuale)

`'p'B` Condizione carta:

`'0'B`: INSERITA, la carta è inserita in un apparecchio di controllo,

`'1'B`: NON INSERITA, la carta è assente (o la carta viene estratta),

'aa'B Attività (non pertinente se 'p' = 1 e 'c' = 0, fatta salva la nota sotto):

'00'B: INTERRUZIONE/RIPOSO,

'01'B: DISPONIBILITÀ,

'10'B: LAVORO,

'11'B: GUIDA,

'ttttttttttt'B Ora della variazione: numero di minuti a partire dalle 00h00 del giorno in questione.

Nota per il caso di "estrazione carta":

Quando la carta viene estratta:

— 's' è pertinente ed indica la sede (slot) da cui viene estratta la carta,

— 'c' deve essere impostato su 0,

— 'p' deve essere impostato su 1,

— 'aa' deve codificare l'attività selezionata in corso al momento dell'estrazione.

In seguito a un'immissione manuale, i bit 'c' e 'aa' della parola (word) (memorizzata in una carta) possono essere sovrascritti in un secondo tempo per tenere conto dell'immissione.

2.2. **Address**

Un indirizzo.

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

codePage specifica la parte della norma ISO/IEC 8859 utilizzata per codificare l'indirizzo,

address è un indirizzo codificato in conformità di ISO/IEC 8859-codePage.

2.3. **BCDString**

BCDString si usa per la rappresentazione in codice binario decimale (BCD). Questo tipo di dati è usato per rappresentare una cifra decimale in un semi-ottetto (4 bit). BCDString si basa su ISO/IEC 8824-1 'CharacterStringType'.

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

BCDString utilizza la notazione "hstring". La prima cifra esadecimale a partire da sinistra è il semi-ottetto più significativo del primo ottetto. Per ottenere un multiplo di ottetti, si devono inserire semi-ottetto a coda zero, secondo la necessità, a partire dalla prima posizione a sinistra del semi-ottetto nel primo ottetto.

Le cifre ammesse sono: 0, 1, … 9.

2.4. **CalibrationPurpose**

Codice che spiega il motivo per cui è stata registrata una serie di parametri di calibratura. Questo tipo di dati si riferisce ai requisiti 097 e 098.

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

Assegnazione valore:

'00'H valore riservato,

'01'H attivazione: registrazione dei parametri di calibratura noti al momento dell'attivazione della VU,

'02'H prima installazione: prima calibratura della VU in seguito all'attivazione,

'03'H installazione: prima calibratura della VU nel veicolo in cui è montata,

'04'H controllo periodico.

2.5. **CardActivityDailyRecord**

Informazioni, memorizzate in una carta, relative all'attività del conducente per un determinato giorno di calendario. Questo tipo di dati si riferisce ai requisiti 199 e 219.

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

activityPreviousRecordLength è la lunghezza totale in byte della registrazione giornaliera precedente. Il valore massimo è dato dalla lunghezza della OCTET STRING contenente tali registrazioni (cfr. CardActivityLengthRange, paragrafo 3). Se questa registrazione è la registrazione giornaliera meno recente, il valore di activityPreviousRecordLength dev'essere impostato su 0.

activityRecordLength è la lunghezza totale in byte di questa registrazione. Il valore massimo è dato dalla lunghezza della OCTET STRING contenente tali registrazioni.

activityRecordDate è la data della registrazione.

activityDailyPresenceCounter è il contatore di presenza giornaliera per la carta nel giorno in questione.

activityDayDistance è la distanza totale percorsa nel giorno in questione.

activityChangeInfo è la serie di dati ActivityChangeInfo per il conducente nel giorno in questione. Può contenere un massimo di 1 440 valori (un cambio di attività al minuto). La serie comprende sempre il valore ActivityChangeInfo relativo alla condizione del conducente a 00h00.

2.6. **CardActivityLengthRange**

Numero di byte in una carta del conducente o dell'officina, disponibile per memorizzare le registrazioni relative all'attività del conducente.

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

Assegnazione valore: cfr. paragrafo 3.

2.7. **CardApprovalNumber**

Numero di omologazione della carta.

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

Assegnazione valore: non specificato.

2.8. **CardCertificate**

Certificato della chiave pubblica di una carta.

```
CardCertificate ::= Certificate
```

2.9. **CardChipIdentification**

Informazioni, memorizzate in una carta, relative all'identificazione del circuito integrato (IC) della carta (requisito 191).

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

icSerialNumber è il numero di serie dell'IC, definito in EN 726-3.

icManufacturingReferences contiene l'identificazione del fabbricante dell'IC e gli elementi di fabbricazione definiti nella norma EN 726-3.

2.10. **CardConsecutiveIndex**

Il codice di serie di una carta [definizione h)].

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

Assegnazione valore: (cfr. capitolo VII del presente allegato)

Ordine di incremento: '0 , …, 9, A , … , Z , a , … , z'

2.11. **CardControlActivityDataRecord**

Informazioni, memorizzate in una carta del conducente o dell'officina, relative all'ultimo controllo cui è stato sottoposto il conducente (requisiti 210 e 225).

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

controlType è il tipo di controllo.

controlTime specifica la data e l'ora del controllo.

controlCardNumber è il FullCardNumber dell'agente che ha effettuato il controllo.

controlVehicleRegistration contiene il VRN e lo Stato membro di immatricolazione del veicolo in cui è stato effettuato il controllo.

controlDownloadPeriodBegin e **controlDownloadPeriodEnd** specificano il periodo trasferito, in caso di trasferimento.

2.12. **CardCurrentUse**

Informazioni sull'uso effettivo della carta (requisito 212).

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

sessionOpenTime è l'ora in cui viene inserita la carta per l'uso corrente. Questo elemento viene azzerato all'atto dell'estrazione della carta.

sessionOpenVehicle è l'identificazione del veicolo in uso, impostata all'atto dell'inserimento della carta. Questo elemento viene azzerato all'atto dell'estrazione della carta.

2.13. **CardDriverActivity**

Informazioni, memorizzate in una carta del conducente o dell'officina, relative all'attività del conducente (requisiti 199 e 219).

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

activityPointerOldestDayRecord specifica il punto d'inizio della memorizzazione (numero di byte a partire dall'inizio della stringa) della registrazione completa meno recente del giorno nella stringa activityDailyRecords. Il valore massimo è dato dalla lunghezza della stringa.

activityPointerNewestRecord specifica il punto d'inizio della memorizzazione (numero di byte a partire dall'inizio della stringa) della registrazione più recente del giorno nella stringa activityDailyRecords. Il valore massimo è dato dalla lunghezza della stringa.

activityDailyRecords è lo spazio disponibile per memorizzare i dati relativi all'attività del conducente (struttura dei dati: CardActivityDailyRecord) per ogni giorno di calendario in cui è stata usata la carta.

Assegnazione valore: questa stringa di ottetti viene riempita ciclicamente con le registrazioni di CardActivityDailyRecord. Al primo impiego, la memorizzazione inizia a partire dal primo byte della stringa. Tutte le nuove registrazioni vengono aggiunte in coda alla precedente. Quando la stringa è piena, la memorizzazione prosegue a partire dal primo byte della stringa, indipendentemente dalla presenza di un'interruzione all'interno di un elemento di dati. Prima di inserire nella stringa nuovi dati relativi all'attività (ingrandendo la activityDailyRecord corrente, o inserendo una nuova activityDailyRecord) per sostituire dati meno recenti, la activityPointerOldestDayRecord deve essere aggiornata per tenere conto della nuova posizione della registrazione giornaliera completa meno recente, e la activityPreviousRecordLength di questa (nuova) registrazione giornaliera completa meno recente deve essere riazzerata.

2.14. **CardDrivingLicenceInformation**

Informazioni, memorizzate in una carta del conducente, relative ai dati della patente di guida del titolare della carta (requisito 196).

```
CardDrivingLicenceInformation ::= SEQUENCE {

   drivingLicenceIssuingAuthority           Name,

   drivingLicenceIssuingNation              NationNumeric,

   drivingLicenceNumber                     IA5String(SIZE(16))

}
```

drivingLicenceIssuingAuthority è l'autorità responsabile del rilascio della patente di guida.

drivingLicenceIssuingNation è la nazionalità dell'autorità che ha rilasciato la patente di guida.

drivingLicenceNumber è il numero della patente di guida.

2.15. **CardEventData**

Informazioni, memorizzate in una carta del conducente o dell'officina, relative alle anomalie associate al titolare della carta (requisiti 204 e 223).

```
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 per le anomalie relative ai tentativi di violazione della sicurezza).

2.16. **CardEventRecord**

Informazioni, memorizzate in una carta del conducente o dell'officina, relative ad un'anomalia associata al titolare della carta (requisiti 205 e 223).

```
CardEventRecord ::= SEQUENCE {

   eventType                                EventFaultType,

   eventBeginTime                           TimeReal,

   eventEndTime                             TimeReal,

   eventVehicleRegistration                 VehicleRegistrationIdentification

}
```

eventType è il tipo di anomalia.

eventBeginTime specifica la data e l'ora d'inizio dell'anomalia.

eventEndTime specifica la data e l'ora di termine dell'anomalia.

eventVehicleRegistration contiene il VRN e lo Stato membro di immatricolazione del veicolo in cui si è verificata l'anomalia.

2.17. **CardFaultData**

Informazioni, memorizzate in una carta del conducente o dell'officina, relative ai guasti associati al titolare della carta (requisiti 207 e 223).

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

CardFaultData è una sequenza di una serie di registrazioni di guasti dell'apparecchio di controllo seguita dalla serie di registrazioni dei guasti della carta.

cardFaultRecords è una serie di registrazioni di guasti di una determinata categoria (apparecchio di controllo o carta).

2.18. **CardFaultRecord**

Informazioni, memorizzate in una carta del conducente o dell'officina, relative ad un guasto associato al titolare della carta (requisiti 208 e 223).

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

faultType è il tipo di guasto.

faultBeginTime specifica la data e l'ora d'inizio del guasto.

faultEndTime specifica la data e l'ora di termine del guasto.

faultVehicleRegistration contiene il VRN e lo Stato membro di immatricolazione del veicolo in cui si è verificato il guasto.

2.19. **CardIccIdentification**

Informazioni, memorizzate in una carta, relative all'identificazione della carta a circuito integrato (IC) (requisito 192).

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

clockStop è la modalità "Clockstop", definita nella norma EN 726-3.

cardExtendedSerialNumber contiene il numero di serie della carta IC ed i riferimenti di fabbricazione della carta IC, definiti in EN 726-3 ed ulteriormente specificati dal tipo di dati ExtendedSerialNumber.

cardApprovalNumber è il numero di omologazione della carta.

cardPersonaliserID è l'identificazione personalizzata della carta (ID), definita in EN 726-3.

embedderIcAssemblerId è l'identificazione dell'assemblatore della carta/IC, definita in EN 726-3.

icIdentifier è l'identificazione dell'IC sulla carta e del fabbricante dell'IC, definita in EN 726-3.

2.20. **CardIdentification**

Informazioni, memorizzate in una carta, relative all'identificazione della carta (requisiti 194, 215, 231, 235).

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

cardIssuingMemberState è il codice dello Stato membro che ha rilasciato la carta.

cardNumber è il numero della carta.

cardIssuingAuthorityName è il nome dell'autorità che ha rilasciato la carta.

cardIssueDate è la data di rilascio della carta all'attuale titolare.

cardValidityBegin è la data di inizio validità della carta.

cardExpiryDate è la data in cui termina la validità della carta.

2.21. **CardNumber**

Numero della carta, secondo la definizione g).

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

driverIdentification è l'identificazione univoca di un conducente in uno Stato membro.

ownerIdentification è l'identificazione univoca di un'impresa o di un'officina o di un organismo di controllo all'interno di uno Stato membro.

cardConsecutiveIndex è il codice di serie della carta.

cardReplacementIndex è il codice di sostituzione della carta.

cardRenewalIndex è il codice di rinnovo della carta.

La prima sequenza della scelta (CHOICE) è adatta a codificare il numero della carta del conducente, la seconda sequenza a codificare i numeri delle carte dell'officina, di controllo e dell'azienda.

2.22. **CardPlaceDailyWorkPeriod**

Informazioni, memorizzate in una carta del conducente o dell'officina, relative al luogo in cui inizia e/o termina il periodo di lavoro giornaliero (requisiti 202 e 221).

```
CardPlaceDailyWorkPeriod ::= SEQUENCE {

   placePointerNewestRecord                 INTEGER(0..NoOfCardPlaceRecords-1),

   placeRecords                             SET SIZE(NoOfCardPlaceRecords) OF PlaceRe-
                                            cord

}
```

placePointerNewestRecord è l'indice della registrazione più aggiornata del luogo.

Assegnazione valore: numero corrispondente al numeratore della registrazione del luogo, a partire da '0' per la prima volta in cui tale registrazione compare nella struttura.

PlaceRecords è la serie di registrazioni contenenti le informazioni relative ai luoghi inseriti.

2.23. **CardPrivateKey**

La chiave privata di una carta.

```
CardPrivateKey ::= RSAKeyPrivateExponent
```

2.24. **CardPublicKey**

La chiave pubblica di una carta.

```
CardPublicKey ::= PublicKey
```

2.25. **CardRenewalIndex**

Il codice di rinnovo di una carta [definizione i)].

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

Assegnazione valore: (cfr. capitolo VII del presente allegato).

'0' Primo rilascio.

Ordine di incremento: '0, …, 9, A, …, Z'

2.26. **CardReplacementIndex**

Il codice di sostituzione di una carta [definizione j)].

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

Assegnazione valore: (cfr. capitolo VII del presente allegato).

'0' Carta originale.

Ordine di incremento: '0, …, 9, A, …, Z'

2.27. **CardSlotNumber**

Codice usato per distinguere le due sedi (slot) di un'unità elettronica di bordo.

```
CardSlotNumber ::= INTEGER {

   driverSlot                               (0),

   co-driverSlot                            (1)

}
```

Assegnazione valore: nessun'altra specificazione.

2.28. **CardSlotsStatus**

Codice che indica il tipo di carta inserita nelle due sedi (slot) dell'unità elettronica di bordo.

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

Assegnazione valore — Allineato all'ottetto: 'ccccdddd'B:

'cccc'B Identificazione del tipo di carta inserita nella sede (slot) "secondo conducente",

'dddd'B Identificazione del tipo di carta inserita nella sede (slot) "conducente",

con i seguenti codici di identificazione:

'0000'B carta non inserita,

'0001'B carta del conducente inserita,

'0010'B carta dell'officina inserita,

'0011'B carta di controllo inserita,

'0100'B carta dell'azienda inserita.

2.29. **CardStructureVersion**

Codice che indica la versione della struttura utilizzata in una carta tachigrafica.

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

Assegnazione valore: 'aabb'H:

'aa'H Indice per le modifiche della struttura,

'bb'H Indice per le modifiche riguardanti l'impiego degli elementi di dati definiti per la struttura data dal byte più significativo.

2.30. **CardVehicleRecord**

Informazioni, memorizzate in una carta del conducente o dell'officina, relative al periodo d'impiego di un veicolo durante un giorno di calendario (requisiti 197 e 217).

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                    OdometerShort,
   vehicleOdometerEnd                      OdometerShort,
   vehicleFirstUse                         TimeReal,
   vehicleLastUse                          TimeReal,
   vehicleRegistration                     VehicleRegistrationIdentification,
   vuDataBlockCounter                      VuDataBlockCounter
}
```

vehicleOdometerBegin è il valore dell'odometro del veicolo all'inizio del periodo d'impiego del veicolo.

vehicleOdometerEnd è il valore dell'odometro del veicolo al termine del periodo d'impiego del veicolo.

vehicleFirstUse specifica la data e l'ora d'inizio del periodo d'impiego del veicolo.

vehicleLastUse specifica la data e l'ora di termine del periodo d'impiego del veicolo.

vehicleRegistration contiene il VRN e lo Stato membro di immatricolazione del veicolo.

vuDataBlockCounter è il valore del VuDataBlockCounter all'atto dell'ultima estrazione nel periodo d'impiego del veicolo.

2.31. **CardVehiclesUsed**

Informazioni, memorizzate in una carta del conducente o dell'officina, relative ai veicoli usati dal titolare della carta (requisiti 197 e 217).

```
CardVehiclesUsed := SEQUENCE {
   vehiclePointerNewestRecord              INTEGER(0..NoOfCardVehicleRecords-1),
   cardVehicleRecords                      SET SIZE(NoOfCardVehicleRecords) OF
                                           CardVehicleRecord
}
```

vehiclePointerNewestRecord è l'indice della registrazione più aggiornata del veicolo.

Assegnazione valore: numero corrispondente al numeratore della registrazione del veicolo, a partire da '0' per la prima volta in cui tale registrazione compare nella struttura.

cardVehicleRecords è la serie di registrazioni contenenti le informazioni relative ai veicoli utilizzati.

2.32. **Certificate**

Il certificato di una chiave pubblica rilasciato da un organismo di certificazione.

```
Certificate ::= OCTET STRING (SIZE(194))
```

Assegnazione valore: firma digitale con recupero parziale di un CertificateContent, secondo i meccanismi comuni di sicurezza di cui all'Appendice 11: firma (128 byte) || resto chiave pubblica (58 Byte) || riferimento dell'organismo di certificazione (8 byte).

2.33. **CertificateContent**

Il contenuto (in chiaro) del certificato di una chiave pubblica, secondo i meccanismi comuni di sicurezza di cui all'Appendice 11.

```
CertificateContent ::= SEQUENCE {
   certificateProfileIdentifier             INTEGER(0..255),
   certificationAuthorityReference          KeyIdentifier,
   certificateHolderAuthorisation           CertificateHolderAuthorisation,
   certificateEndOfValidity                 TimeReal,
   certificateHolderReference               KeyIdentifier,
   publicKey                                PublicKey
}
```

certificateProfileIdentifier è la versione del certificato corrispondente.

Assegnazione valore: '01h' per questa versione.

certificationAuthorityReference identifica l'organismo di certificazione che ha rilasciato il certificato. Fornisce inoltre il riferimento della chiave pubblica di tale organismo.

certificateHolderAuthorisation identifica i diritti del titolare del certificato.

certificateEndOfValidity è la data di scadenza amministrativa del certificato.

certificateHolderReference identifica il titolare del certificato. Fornisce inoltre il riferimento della chiave pubblica del titolare.

publicKey è la chiave pubblica per la quale è stato rilasciato il certificato in questione.

2.34. **CertificateHolderAuthorisation**

Identificazione dei diritti del titolare di un certificato.

```
CertificateHolderAuthorisation ::= SEQUENCE {
   tachographApplicationID                  OCTET STRING(SIZE(6))
   equipmentType                            EquipmentType
}
```

tachographApplicationID è l'identificazione dell'applicazione tachigrafica.

Assegnazione valore: 'FFh' '54h' '41h' '43h' '48h' '4Fh'. Si tratta di un'identificazione di applicazione di proprietà riservata, non registrata, secondo ISO/IEC 7816-5.

equipmentType è l'identificazione del tipo di apparecchio cui è destinato il certificato.

Assegnazione valore: in conformità del tipo di dati EquipmentType. 0 se si tratta del certificato di uno Stato membro.

2.35. **CertificateRequestID**

Identificazione univoca di una richiesta di certificato. Si può anche usare come identificazione della chiave pubblica di un'unità elettronica di bordo, nel caso in cui il numero di serie dell'unità elettronica di bordo cui è destinata la chiave non sia noto al momento della generazione del certificato.

```
CertificateRequestID ::= SEQUENCE {
   requestSerialNumber                    INTEGER(0..2^32-1)
   requestMonthYear                       BCDString(SIZE(2))
   crIdentifier                           OCTET STRING(SIZE(1))
   manufacturerCode                       ManufacturerCode
}
```

requestSerialNumber è un numero di serie per la richiesta di certificato, associato univocamente al fabbricante e al mese di cui sotto.

requestMonthYear è l'identificazione del mese e dell'anno di richiesta del certificato.

Assegnazione valore: codifica BCD del mese (due cifre) e dell'anno (ultime due cifre).

crIdentifier: è un'identificazione usata per distinguere una richiesta di certificato da un numero di serie completo.

Assegnazione valore: 'FFh'.

manufacturerCode: è il codice numerico del fabbricante che ha richiesto il certificato.

2.36. **CertificationAuthorityKID**

Identificazione della chiave pubblica di un organismo di certificazione (di uno Stato membro o dell'organismo europeo di certificazione).

```
CertificationAuthorityKID ::= SEQUENCE {
   nationNumeric                          NationNumeric
   nationAlpha                            NationAlpha
   keySerialNumber                        INTEGER(0..255)
   additionalInfo                         OCTET STRING(SIZE(2))
   caIdentifier                           OCTET STRING(SIZE(1))
}
```

nationNumeric è il codice numerico del paese dell'organismo di certificazione.

nationAlpha è il codice alfanumerico del paese dell'organismo di certificazione.

keySerialNumber è un numero di serie usato per distinguere le diverse chiavi dell'organismo di certificazione in caso di cambio di chiavi.

additionalInfo è un campo a due byte per codifiche supplementari (a cura dell'organismo di certificazione).

caIdentifier è un'identificazione usata per distinguere l'identificazione della chiave di un organismo di certificazione dalle identificazioni di altre chiavi.

Assegnazione valore: '01h'.

2.37. **CompanyActivityData**

Informazioni, memorizzate in una carta dell'azienda, relative alle attività eseguite con la carta (requisito 237).

```
CompanyActivityData ::= SEQUENCE {
  companyPointerNewestRecord          INTEGER(0..NoOfCompanyActivityRecords-1),
  companyActivityRecords              SET SIZE(NoOfCompanyActivityRecords) OF
    companyActivityRecord               SEQUENCE {
      companyActivityType                 CompanyActivityType,
      companyActivityTime                 TimeReal,
      cardNumberInformation               FullCardNumber,
```

```
        vehicleRegistrationInformation      VehicleRegistrationIdentification,
        downloadPeriodBegin                 TimeReal,
        downloadPeriodEnd                   TimeReal
    }
}
```

companyPointerNewestRecord è l'indice della companyActivityRecord più aggiornata.

Assegnazione valore: numero corrispondente al numeratore della registrazione delle attività dell'impresa, a partire da '0' per la prima volta in cui tale registrazione compare nella struttura.

companyActivityRecords è la serie di tutte le registrazioni delle attività dell'impresa.

companyActivityRecord è la sequenza di informazioni relative ad un'attività dell'impresa.

companyActivityType è il tipo di attività dell'impresa.

companyActivityTime specifica la data e l'ora dell'attività dell'impresa.

cardNumberInformation contiene il numero della carta e lo Stato membro che ha rilasciato la carta da cui sono stati trasferiti i dati, se pertinente.

vehicleRegistrationInformation contiene il VRN e lo Stato membro di immatricolazione del veicolo da cui sono stati trasferiti i dati o in cui è stato attivato o disattivato un blocco.

downloadPeriodBegin e **downloadPeriodEnd** specificano il periodo cui si riferisce il trasferimento dei dati della VU, se pertinente.

2.38. **CompanyActivityType**

Codice che indica un'attività eseguita da un'impresa utilizzando la propria carta dell'azienda.

```
CompanyActivityType ::= INTEGER {
    card downloading                    (1),
    VU downloading                      (2),
    VU lock-in                          (3),
    VU lock-out                         (4)
}
```

2.39. **CompanyCardApplicationIdentification**

Informazioni, memorizzate in una carta dell'azienda, relative all'identificazione dell'applicazione della carta (requisito 190).

```
CompanyCardApplicationIdentification ::= SEQUENCE {
    typeOfTachographCardId              EquipmentType,
    cardStructureVersion                CardStructureVersion,
    noOfCompanyActivityRecords          NoOfCompanyActivityRecords
}
```

typeOfTachographCardId specifica il tipo di carta.

cardStructureVersion specifica la versione della struttura utilizzata nella carta.

noOfCompanyActivityRecords è il numero di registrazioni delle attività dell'impresa che la carta è in grado di memorizzare.

2.40. **CompanyCardHolderIdentification**

Informazioni, memorizzate in una carta dell'azienda, relative all'identificazione del titolare della carta (requisito 236).

```
CompanyCardHolderIdentification ::= SEQUENCE {
    companyName                         Name,
    companyAddress                      Address,
    cardHolderPreferredLanguage         Language
}
```

companyName è il nome dell'impresa titolare.

companyAddress è l'indirizzo dell'impresa titolare.

cardHolderPreferredLanguage è la lingua abituale del titolare della carta.

2.41. **ControlCardApplicationIdentification**

Informazioni, memorizzate in una carta di controllo, relative all'identificazione dell'applicazione della carta (requisito 190).

```
ControlCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId                  EquipmentType,
   cardStructureVersion                    CardStructureVersion,
   noOfControlActivityRecords              NoOfControlActivityRecords
}
```

typeOfTachographCardId specifica il tipo di carta.

cardStructureVersion specifica la versione della struttura utilizzata nella carta.

noOfControlActivityRecords è il numero di registrazioni di attività di controllo che la carta è in grado di memorizzare.

2.42. **ControlCardControlActivityData**

Informazioni, memorizzate in una carta di controllo, relative alle attività di controllo eseguite con la carta (requisito 233).

```
ControlCardControlActivityData ::= SEQUENCE {
   controlPointerNewestRecord              INTEGER(0..NoOfControlActivityRecords-1),
   controlActivityRecords                  SET SIZE(NoOfControlActivityRecords) OF
     controlActivityRecord                   SEQUENCE {
       controlType                             ControlType,
       controlTime                             TimeReal,
       controlledCardNumber                    FullCardNumber,
       controlledVehicleRegistration           VehicleRegistrationIdentification,
       controlDownloadPeriodBegin              TimeReal,
       controlDownloadPeriodEnd                TimeReal
     }
}
```

controlPointerNewestRecord è l'indice della registrazione più aggiornata dell'attività di controllo.

Assegnazione valore: numero corrispondente al numeratore della registrazione dell'attività di controllo, a partire da '0' per la prima volta in cui tale registrazione compare nella struttura.

controlActivityRecords è la serie di tutte le registrazioni delle attività di controllo.

controlActivityRecord è la sequenza di informazioni relative ad un controllo.

controlType è il tipo di controllo.

controlTime specifica la data e l'ora del controllo.

controlledCardNumber contiene il numero della carta e lo Stato membro che ha rilasciato la carta sottoposta al controllo.

controlledVehicleRegistration contiene il VRN e lo Stato membro di immatricolazione del veicolo in cui è stato eseguito il controllo.

controlDownloadPeriodBegin e **controlDownloadPeriodEnd** specificano il periodo trasferito, in caso di trasferimento.

2.43. **ControlCardHolderIdentification**

Informazioni, memorizzate in una carta di controllo, relative all'identificazione del titolare della carta (requisito 232).

```
ControlCardHolderIdentification ::= SEQUENCE {
   controlBodyName                          Name,
   controlBodyAddress                       Address,
   cardHolderName                           HolderName,
   cardHolderPreferredLanguage              Language
}
```

controlBodyName è il nome dell'organismo di controllo del titolare della carta.

controlBodyAddress è l'indirizzo dell'organismo di controllo del titolare della carta.

cardHolderName contiene cognome e nome(i) del titolare della carta di controllo.

cardHolderPreferredLanguage è la lingua abituale del titolare della carta.

2.44. **ControlType**

Codice che indica le attività eseguite durante un controllo. Questo tipo di dati si riferisce ai requisiti 102, 210 e 225.

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

Assegnazione valore — Allineato all'ottetto: 'cvpdxxxx'B (8 Bit)

'c'B trasferimento dati carta:

'0'B: dati carta non trasferiti durante l'attività di controllo,

'1'B: dati carta trasferiti durante l'attività di controllo

'v'B trasferimento dati VU:

'0'B: dati VU non trasferiti durante l'attività di controllo,

'1'B: dati VU trasferiti durante l'attività di controllo

'p'B stampa:

'0'B: stampa non eseguita durante l'attività di controllo,

'1'B: stampa eseguita durante l'attività di controllo

'd'B visualizzazione:

'0'B: visualizzazione non utilizzata durante l'attività di controllo,

'1'B: visualizzazione utilizzata durante l'attività di controllo

'xxxx'B Non utilizzato.

2.45. **CurrentDateTime**

La data e l'ora correnti dell'apparecchio di controllo.

```
CurrentDateTime ::= TimeReal
```

Assegnazione valore: nessun'altra specificazione.

2.46. **DailyPresenceCounter**

Un contatore, memorizzato in una carta del conducente o dell'officina, incrementato di un'unità per ogni giorno di calendario in cui la carta viene inserita in una VU. Questo tipo di dati si riferisce ai requisiti 199 e 219.

```
DailyPresenceCounter ::= BCDString(SIZE(2))
```

Assegnazione valore: numero consecutivo con valore massimo 9 999, anche in questo caso a partire da 0. All'atto del primo rilascio della carta il numero è impostato su 0.

2.47. **Datef**

Data espressa in un formato numerico idoneo alla stampa.

```
Datef ::= SEQUENCE {
   anno       BCDString(SIZE(2)),
   mese       BCDString(SIZE(1)),
   giorno     BCDString(SIZE(1))
}
```

Assegnazione valore:

yyyy	anno
mm	mese
dd	giorno

'00000000'H denota esplicitamente l'assenza di data.

2.48. **Distance**

Una distanza percorsa (risultante dal calcolo della differenza tra due valori dell'odometro del veicolo espressi in chilometri).

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

Assegnazione valore: binario senza segno. Valore in km nel campo operativo 0-9 999 km.

2.49. **DriverCardApplicationIdentification**

Informazioni, memorizzate in una carta del conducente, relative all'identificazione dell'applicazione della carta (requisito 190).

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId                  EquipmentType,
   cardStructureVersion                    CardStructureVersion,
   noOfEventsPerType                       NoOfEventsPerType,
   noOfFaultsPerType                       NoOfFaultsPerType,
   activityStructureLength                 CardActivityLengthRange,
   noOfCardVehicleRecords                  NoOfCardVehicleRecords,
   noOfCardPlaceRecords                    NoOfCardPlaceRecords
}
```

typeOfTachographCardId specifica il tipo di carta.

cardStructureVersion specifica la versione della struttura utilizzata nella carta.

noOfEventsPerType è il numero di anomalie per tipo di anomalia che la carta è in grado di registrare.

noOfFaultsPerType è il numero di guasti per tipo di guasto che la carta è in grado di registrare.

activityStructureLength indica il numero di byte disponibili per memorizzare le registrazioni delle attività.

noOfCardVehicleRecords è il numero di registrazioni del veicolo che la carta è in grado di contenere.

noOfCardPlaceRecords è il numero di luoghi che la carta è in grado di registrare.

2.50. **DriverCardHolderIdentification**

Informazioni, memorizzate in una carta del conducente, relative all'identificazione del titolare della carta (requisito 195).

```
DriverCardHolderIdentification ::= SEQUENCE {
   cardHolderName                          HolderName,
   cardHolderBirthDate                     Datef,
   cardHolderPreferredLanguage             Language
}
```

cardHolderName contiene cognome e nome(i) del titolare della carta del conducente.

cardHolderBirthDate è la data di nascita del titolare della carta del conducente.

cardHolderPreferredLanguage è la lingua abituale del titolare della carta.

2.51. **EntryTypeDailyWorkPeriod**

Codice usato per distinguere inizio e termine dell'immissione del luogo di un periodo di lavoro giornaliero e la condizione dell'immissione.

```
EntryTypeDailyWorkPeriod ::= INTEGER
   Begin,  related time = card insertion time or time of entry          (0),
   End,    related time = card withdrawal time or time of entry        (1),
   Begin,  related time manually entered (start time)                   (2),
   End,    related time manually entered (end of work period)           (3),
   Begin,  related time assumed by VU                                   (4),
   End,    related time assumed by VU                                   (5)
}
```

Assegnazione valore: secondo ISO/IEC8824-1.

2.52. **EquipmentType**

Codice usato per distinguere i diversi tipi di apparecchio per l'applicazione tachigrafica.

```
EquipmentType ::= INTEGER(0..255)
- - riservato                          (0),
- - Driver Card                        (1),
- - Workshop Card                      (2),
- - Control Card                       (3),
- - Company Card                       (4),
- - Manufacturing Card                 (5),
- - Vehicle Unit                       (6),
- - Motion Sensor                      (7),
- - RFU                                (8..255)
```

Assegnazione valore: secondo ISO/IEC8824-1.

Il valore 0 è riservato, esso serve ad indicare uno Stato membro o l'Europa nel campo CHA dei certificati.

2.53. **EuropeanPublicKey**

La chiave pubblica europea.

```
EuropeanPublicKey ::= PublicKey
```

2.54. **EventFaultType**

Codice che identifica un'anomalia o un guasto.

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

Assegnazione valore:

'Ox'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 dati di marcia,
'0A'H .. '0F'H	Disponibile per uso futuro,
'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 .. '1F'H	Disponibile per uso futuro,
'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,
'26'H .. '2F'H	Disponibile per uso futuro,
'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 .. '3F'H	Disponibile per uso futuro,
'4x'H	Guasti della carta,
'40'H	Nessun'altra informazione,
'41'H .. '4F'H	Disponibile per uso futuro,
'50'H .. '7F'H	Disponibile per uso futuro,
'80'H .. 'FF'H	A cura del fabbricante.

2.55. **EventFaultRecordPurpose**

Codice che spiega il motivo per cui è stata registrata un'anomalia o un guasto.

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

Assegnazione valore:

'00'H	una delle 10 anomalie o guasti più recenti (o ultimi)
'01'H	l'anomalia più lunga per uno degli ultimi 10 giorni in cui si è verificata
'02'H	una delle 5 anomalie più lunghe nel corso degli ultimi 365 giorni
'03'H	l'ultima anomalia per uno degli ultimi 10 giorni in cui si è verificata
'04'H	l'anomalia più grave per uno degli ultimi 10 giorni in cui si è verificata
'05'H	una delle 5 anomalie più gravi nel corso degli ultimi 365 giorni
'06'H	la prima anomalia o il primo guasto che si è verificato dopo l'ultima calibratura
'07'H	un'anomalia o un guasto attivo/in atto
'08'H .. '7F'H	Disponibile per uso futuro
'80'H .. 'FF'H	a cura del fabbricante

2.56. **ExtendedSerialNumber**

Identificazione univoca di un apparecchio. Si può anche usare come identificazione della chiave pubblica di un apparecchio.

```
ExtendedSerialNumber ::= SEQUENCE {
   serialNumber                          INTEGER(0..2^32-1)
   monthYear                             BCDString(SIZE(2))
   type OCTET                            STRING(SIZE(1))
   manufacturerCode                      ManufacturerCode
}
```

serialNumber serialNumber è un numero di serie per l'apparecchio, univocamente associato al fabbricante, al tipo di apparecchio e al mese di cui sotto.

monthYear monthYear è l'identificazione del mese e dell'anno di fabbricazione (o di assegnazione del numero di serie).

Assegnazione valore: codifica BCD del mese (due cifre) e dell'anno (ultime due cifre).

type type è un'identificazione del tipo di apparecchio.

Assegnazione del valore: a cura del fabbricante, con valore riservato 'FFh'.

manufacturerCode: è il codice numerico del fabbricante dell'apparecchio.

2.57. **FullCardNumber**

Codice per l'identificazione completa di una carta tachigrafica.

```
FullCardNumber ::= SEQUENCE {
   cardType                              EquipmentType,
   cardIssuingMemberState                NationNumeric,
   cardNumber                            CardNumber
}
```

cardType è il tipo di carta tachigrafica.

cardIssuingMemberState è il codice dello Stato membro che ha rilasciato la carta.

cardNumber è il numero della carta.

2.58. **HighResOdometer**

Valore dell'odometro del veicolo: distanza cumulata percorsa dal veicolo durante il suo funzionamento.

```
HighResOdometer ::= INTEGER(0..2^32-1)
```

Assegnazione valore: binario senza segno. Valore espresso in 1/200 km nel campo operativo 0-21 055 406 km.

2.59. **HighResTripDistance**

Una distanza percorsa durante un intero viaggio o parte di esso.

```
HighResTripDistance ::= INTEGER(0..2^32-1)
```

Assegnazione valore: binario senza segno. Valore espresso in 1/200 km nel campo operativo 0-21 055 406 km.

2.60. **HolderName**

Cognome e nome(i) del titolare di una carta.

```
HolderName ::= SEQUENCE {
   holderSurname                         Name,
   holderFirstNames                      Name
}
```

holderSurname è il cognome del titolare. Il cognome non comprende titoli.

Assegnazione valore: nel caso di una carta non personale, holderSurname contiene le stesse informazioni di companyName o workshopName o controlBodyName.

holderFirstNames contiene il nome (o nomi) e le iniziali del titolare.

2.61. **K-ConstantOfRecordingEquipment**

Costante dell'apparecchio di controllo [definizione m)].

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

Assegnazione valore: impulsi per chilometro nel campo operativo 0-64255 impulsi/km.

2.62. **KeyIdentifier**

Identificazione univoca di una chiave pubblica utilizzata per codificare e selezionare la chiave. Identifica anche il titolare della 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 o di una carta tachigrafica.

La seconda scelta è adatta a codificare la chiave pubblica di un'unità elettronica di bordo (nel caso 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 Stato membro.

2.63. **L-TyreCircumference**

Circonferenza effettiva dei pneumatici delle ruote [definizione u)].

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

Assegnazione valore: binario senza segno, valore espresso in 1/8 mm nel campo operativo 0-8 031 mm.

2.64. **Language**

Codice che identifica una lingua.

```
Language ::= IA5String(SIZE(2))
```

Assegnazione valore: codifica a due lettere minuscole, secondo ISO 639.

2.65. **LastCardDownload**

Data e ora, registrati sulla carta del conducente, dell'ultimo trasferimento di dati dalla carta (a fini diversi da quelli di controllo). La data può essere aggiornata dalla VU o da qualsiasi lettore di carte.

```
LastCardDownload ::= TimeReal
```

Assegnazione valore: nessun'altra specificazione.

2.66. **ManualInputFlag**

Codice che indica se, all'atto dell'inserimento della carta, il titolare di una carta abbia o meno inserito manualmente le attività del conducente (requisito 081).

```
ManualInputFlag ::= INTEGER {
   noEntry                          (0)
   manualEntries                    (1)
}
```

Assegnazione valore: nessun'altra specificazione.

2.67. **ManufacturerCode**

Codice che identifica un fabbricante.

```
ManufacturerCode ::= INTEGER(0..255)
```

Assegnazione valore:

'00'H	Informazione non disponibile
'01'H	Valore riservato
'02'H .. '0F'H	Riservato per uso futuro
'10'H	ACTIA
'11'H .. '17'H	Riservato ai fabbricanti il cui nome comincia per 'A'
'18'H .. '1F'H	Riservato ai fabbricanti il cui nome comincia per 'B'
'20'H .. '27'H	Riservato ai fabbricanti il cui nome comincia per 'C'
'28'H .. '2F'H	Riservato ai fabbricanti il cui nome comincia per 'D'
'30'H .. '37'H	Riservato ai fabbricanti il cui nome comincia per 'E'
'38'H .. '3F'H	Riservato ai fabbricanti il cui nome comincia per 'F'
'40'H	Giesecke & Devrient GmbH
'41'H	GEM plus
'42'H .. '47'H	Riservato ai fabbricanti il cui nome comincia per 'G'
'48'H .. '4F'H	Riservato ai fabbricanti il cui nome comincia per 'H'
'50'H .. '57'H	Riservato ai fabbricanti il cui nome comincia per 'I'
'58'H .. '5F'H	Riservato ai fabbricanti il cui nome comincia per 'J'
'60'H .. '67'H	Riservato ai fabbricanti il cui nome comincia per 'K'
'68'H .. '6F'H	Riservato ai fabbricanti il cui nome comincia per 'L'
'70'H .. '77'H	Riservato ai fabbricanti il cui nome comincia per 'M'
'78'H .. '7F'H	Riservato ai fabbricanti il cui nome comincia per 'N'
'80'H	OSCARD
'81'H .. '87'H	Riservato ai fabbricanti il cui nome comincia per 'O'
'88'H .. '8F'H	Riservato ai fabbricanti il cui nome comincia per 'P'
'90'H .. '97'H	Riservato ai fabbricanti il cui nome comincia per 'Q'
'98'H .. '9F'H	Riservato ai fabbricanti il cui nome comincia per 'R'
'A0'H	SETEC
'A1'H	SIEMENS VDO
'A2'H	STONERIDGE
'A3'H .. 'A7'H	Riservato ai fabbricanti il cui nome comincia per 'S'
'AA'H	TACHOCONTROL
'AB'H .. 'AF'H	Riservato ai fabbricanti il cui nome comincia per 'T'
'B0'H .. 'B7'H	Riservato ai fabbricanti il cui nome comincia per 'U'
'B8'H .. 'BF'H	Riservato ai fabbricanti il cui nome comincia per 'V'
'C0'H .. 'C7'H	Riservato ai fabbricanti il cui nome comincia per 'W'
'C8'H .. 'CF'H	Riservato ai fabbricanti il cui nome comincia per 'X'
'D0'H .. 'D7'H	Riservato ai fabbricanti il cui nome comincia per 'Y'
'D8'H .. 'DF'H	Riservato ai fabbricanti il cui nome comincia per 'Z'

2.68. **MemberStateCertificate**

Il certificato della chiave pubblica di uno Stato membro rilasciato dall'organismo europeo di certificazione.

```
MemberStateCertificate ::= Certificate
```

2.69. **MemberStatePublicKey**

La chiave pubblica di uno Stato membro.

```
MemberStatePublicKey ::= PublicKey
```

2.70. **Name**

Un nome.

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

codePage specifica la parte della norma ISO/IEC 8859 utilizzata per codificare il nome,

name è un nome codificato in conformità di ISO/IEC 8859-codePage.

2.71. **NationAlpha**

Codice alfabetico del paese, in base alla codifica convenzionale utilizzata per gli adesivi da apporre sui paraurti dei veicoli e/o nei documenti di assicurazione armonizzati a livello internazionale (carta verde).

```
NationAlpha ::= IA5String(SIZE(3))
```

Assegnazione valore:

' '	Informazione non disponibile,
'A'	Austria,
'AL'	Albania,
'AND'	Andorra,
'ARM'	Armenia,
'AZ'	Azerbaigian,
'B'	Belgio,
'BG'	Bulgaria,
'BIH'	Bosnia Erzegovina,
'BY'	Bielorussia,
'CH'	Svizzera,
'CY'	Cipro,
'CZ'	Repubblica ceca,
'D'	Germania,
'DK'	Danimarca,
'E'	Spagna,
'EST'	Estonia,
'F'	Francia,
'FIN'	Finlandia,
'FL'	Liechtenstein,
'FR'	Isole Faer Øer,
'UK'	Regno Unito, Alderney, Guernsey, Jersey, Isola di Man, Gibilterra,
'GE'	Georgia,
'GR'	Grecia,
'H'	Ungheria,
'HR'	Croazia,
'I'	Italia,
'IRL'	Irlanda,
'IS'	Islanda,
'KZ'	Kazakstan,
'L'	Lussemburgo,
'LT'	Lituania,
'LV'	Lettonia,
'M'	Malta,
'MC'	Monaco,

'MD'	Repubblica di Moldavia,
'MK'	Macedonia,
'N'	Norvegia,
'NL'	Paesi Bassi,
'P'	Portogallo,
'PL'	Polonia,
'RO'	Romania,
'RSM'	San Marino,
'RUS'	Federazione russa,
'S'	Svezia,
'SK'	Slovacchia,
'SLO'	Slovenia,
'TM'	Turkmenistan,
'TR'	Turchia,
'UA'	Ucraina,
'V'	Città del Vaticano,
'YU'	Iugoslavia,
'UNK'	Non noto,
'EC'	Comunità europea,
'EUR'	Resto d'Europa,
'WLD'	Resto del mondo.

2.72. **NationNumeric**

Codice numerico di un paese.

```
NationNumeric ::= INTEGER(0..255)
```

Assegnazione valore:

-- Informazione non disponibile	(00)H,
-- Austria	(01)H,
-- Albania	(02)H,
-- Andorra	(03)H,
-- Armenia	(04)H,
-- Azerbaigian	(05)H,
-- Belgio	(06)H,
-- Bulgaria	(07)H,
-- Bosnia Erzegovina	(08)H,
-- Bielorussia	(09)H,
-- Svizzera	(0A)H,
-- Cipro	(0B)H,
-- Repubblica ceca	(0C)H,
-- Germania	(0D)H,
-- Danimarca	(0E)H,
-- Spagna	(0F)H,
-- Estonia	(10)H,
-- Francia	(11)H,
-- Finlandia	(12)H,
-- Liechtenstein	(13)H,
-- Isole Faer Øer	(14)H,
-- Regno Unito	(15)H,
-- Georgia	(16)H,
-- Grecia	(17)H,
-- Ungheria	(18)H,
-- Croazia	(19)H,
-- Italia	(1A)H,
-- Irlanda	(1B)H,
-- Islanda	(1C)H,

- - Kazakstan	(1D)H,
- - Lussemburgo	(1E)H,
- - Lituania	(1F)H,
- - Lettonia	(20)H,
- - Malta	(21)H,
- - Monaco	(22)H,
- - Repubblica di Moldavia	(23)H,
- - Macedonia	(24)H,
- - Norvegia	(25)H,
- - Paesi Bassi	(26)H,
- - Portogallo	(27)H,
- - Polonia	(28)H,
- - Romania	(29)H,
- - San Marino	(2A)H,
- - Federazione russa	(2B)H,
- - Svezia	(2C)H,
- - Slovacchia	(2D)H,
- - Slovenia	(2E)H,
- - Turkmenistan	(2F)H,
- - Turchia	(30)H,
- - Ucraina	(31)H,
- - Città del Vaticano	(32)H,
- - Iugoslavia	(33)H,
- - Disponibile per uso futuro	(34..FC)H,
- - Comunità europea	(FD)H,
- - Resto d'Europa	(FE)H,
- - Resto del mondo	(FF)H

2.73. **NoOfCalibrationRecords**

Numero di registrazioni di calibrature che una carta dell'officina è in grado di memorizzare.

NoOfCalibrationRecords ::= INTEGER(0..255)

Assegnazione valore: cfr. paragrafo 3.

2.74. **NoOfCalibrationsSinceDownload**

Contatore che indica il numero di calibrature effettuate con una carta dell'officina in seguito all'ultimo trasferimento dei suoi dati (requisito 230).

NoOfCalibrationsSinceDownload ::= INTEGER(0..2^{16}-1),

Assegnazione valore: nessun'altra specificazione.

2.75. **NoOfCardPlaceRecords**

Numero di registrazioni di luoghi che una carta del conducente o dell'officina è in grado di memorizzare.

NoOfCardPlaceRecords ::= INTEGER(0..255)

Assegnazione valore: cfr. paragrafo 3.

2.76. **NoOfCardVehicleRecords**

Numero di registrazioni relative ai veicoli utilizzati che una carta del conducente o dell'officina è in grado di memorizzare.

NoOfCardVehicleRecords ::= INTEGER(0..2^{16}-1)

Assegnazione valore: cfr. paragrafo 3.

2.77. **NoOfCompanyActivityRecords**

Numero di registrazioni delle attività dell'impresa che una carta dell'azienda è in grado di memorizzare.

NoOfCompanyActivityRecords ::= INTEGER(0..2^{16}-1)

Assegnazione valore: cfr. paragrafo 3.

2.78. **NoOfControlActivityRecords**

Numero di registrazioni delle attività di controllo che una carta di controllo è in grado di memorizzare.

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

Assegnazione valore: cfr. paragrafo 3.

2.79. **NoOfEventsPerType**

Numero di anomalie per tipo di anomalia che una carta è in grado di memorizzare.

```
NoOfEventsPerType ::= INTEGER(0..255)
```

Assegnazione valore: cfr. paragrafo 3.

2.80. **NoOfFaultsPerType**

Numero di guasti per tipo di guasto che una carta è in grado di memorizzare.

```
NoOfFaultsPerType ::= INTEGER(0..255)
```

Assegnazione valore: cfr. paragrafo 3.

2.81. **OdometerValueMidnight**

Il valore dell'odometro del veicolo alla mezzanotte di un determinato giorno (requisito 090).

```
OdometerValueMidnight ::= OdometerShort
```

Assegnazione valore: nessun'altra specificazione.

2.82. **OdometerShort**

Valore dell'odometro del veicolo in forma abbreviata.

```
OdometerShort ::= INTEGER(0..2^24-1)
```

Assegnazione valore: binario senza segno. Valore espresso in km nel campo operativo 0-9 999 999 km.

2.83. **OverspeedNumber**

Numero di anomalie per superamento di velocità in seguito all'ultimo controllo del superamento di velocità.

```
OverspeedNumber ::= INTEGER(0..255)
```

Assegnazione valore: 0 significa che non si è verificata alcuna anomalia per superamento di velocità in seguito all'ultimo controllo del superamento di velocità, 1 significa che si è verificata un'anomalia per superamento velocità in seguito all'ultimo controllo … 255 significa che si sono verificate 255 o più anomalie per superamento di velocità in seguito all'ultimo controllo del superamento di velocità.

2.84. **PlaceRecord**

Informazioni relative al luogo in cui inizia o termina un periodo di lavoro giornaliero (requisiti 087, 202, 221).

```
PlaceRecord ::= SEQUENCE {
   entryTime                              TimeReal,
   entryTypeDailyWorkPeriod               EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry                 NationNumeric,
   dailyWorkPeriodRegion                  RegionNumeric,
   vehicleOdometerValue                   OdometerShort
}
```

entryTime specifica la data e l'ora relativa all'immissione.

entryTypeDailyWorkPeriod è il tipo di immissione.

dailyWorkPeriodCountry è il paese inserito.

dailyWorkPeriodRegion è la regione inserita.

vehicleOdometerValue è il valore dell'odometro all'atto dell'immissione del luogo.

2.85. **PreviousVehicleInfo**

Informazioni relative al veicolo precedentemente usato da un conducente all'atto dell'inserimento della carta in un'unità elettronica di bordo (requisito 081).

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification        VehicleRegistrationIdentification,
   cardWithdrawalTime                       TimeReal
}
```

vehicleRegistrationIdentification contiene il VRN e lo Stato membro di immatricolazione del veicolo.

cardWithdrawalTime specifica la data e l'ora di estrazione della carta.

2.86. **PublicKey**

Una chiave pubblica RSA.

```
PublicKey ::= SEQUENCE {
   rsaKeyModulus                            RSAKeyModulus,
   rsaKeyPublicExponent                     RSAKeyPublicExponent
}
```

rsaKeyModulus è il modulo della coppia di chiavi.

rsaKeyPublicExponent è l'esponente pubblico della coppia di chiavi.

2.87. **RegionAlpha**

Codice numerico delle diverse regioni di un determinato paese.

```
RegionAlpha ::= IA5STRING(SIZE(3))
```

Assegnazione valore:

`' '`	Informazione non disponibile,

Spagna:

`'AN'`	Andalusia,
`'AR'`	Aragona,
`'AST'`	Asturie,
`'C'`	Cantabria,
`'CAT'`	Catalogna,
`'CL'`	Castilla-León,
`'CM'`	Castilla-La-Mancha,
`'CV'`	Valencia,
`'EXT'`	Estremadura,
`'G'`	Galizia,
`'IB'`	Baleari,
`'IC'`	Canarie,
`'LR'`	La Rioja,
`'M'`	Madrid,
`'MU'`	Murcia,
`'NA'`	Navarra,
`'PV'`	Paesi Baschi

2.88. **RegionNumeric**

Codice numerico delle diverse regioni di un determinato paese.

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

Assegnazione valore:

'00'H Informazione non disponibile,

Spagna:

'01'H Andalusia,

'02'H Aragona,

'03'H Asturie

'04'H Cantabria,

'05'H Catalogna,

'06'H Castilla-León,

'07'H Castilla-La-Mancha,

'08'H Valencia,

'09'H Estremadura,

'0A'H Galizia,

'0B'H Baleari,

'0C'H Canarie,

'0D'H La Rioja,

'0E'H Madrid,

'0F'H Murcia,

'10'H Navarra,

'11'H Paesi Baschi

2.89. **RSAKeyModulus**

Il modulo di una coppia di chiavi RSA.

```
RSAKeyModulus ::= OCTET STRING (SIZE(128))
```

Assegnazione valore: non specificato.

2.90. **RSAKeyPrivateExponent**

L'esponente privato di una coppia di chiavi RSA.

```
RSAKeyPrivateExponent ::= OCTET STRING (SIZE(128))
```

Assegnazione valore: non specificato.

2.91. **RSAKeyPublicExponent**

L'esponente pubblico di una coppia di chiavi RSA.

```
RSAKeyPublicExponent ::= OCTET STRING (SIZE(8))
```

Assegnazione valore: non specificato.

2.92. **SensorApprovalNumber**

Numero di omologazione del sensore.

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

Assegnazione valore: non specificato.

2.93. **SensorIdentification**

Informazioni, memorizzate in un sensore di movimento, relative all'identificazione del sensore stesso (requisito 077).

```
SensorIdentification ::= SEQUENCE {
   sensorSerialNumber                    SensorSerialNumber,
   sensorApprovalNumber                  SensorApprovalNumber,
   sensorSCIdentifier                    SensorSCIdentifier,
   sensorOSIdentifier                    SensorOSIdentifier
}
```

sensorSerialNumber è il numero di serie completo del sensore di movimento (comprende il codice componente e il codice del fabbricante).

sensorApprovalNumber è il numero di omologazione del sensore di movimento.

sensorSCIdentifier è l'identificativo del componente di sicurezza incorporato nel sensore di movimento.

sensorOSIdentifier è l'identificativo del sistema operativo del sensore di movimento.

2.94. **SensorInstallation**

Informazioni, memorizzate in un sensore di movimento, relative al montaggio del sensore stesso (requisito 099).

```
SensorInstallation ::= SEQUENCE {
   sensorPairingDateFirst                  SensorPairingDate,
   firstVuApprovalNumber                   VuApprovalNumber,
   firstVuSerialNumber                     VuSerialNumber,
   sensorPairingDateCurrent                SensorPairingDate,
   currentVuApprovalNumber                 VuApprovalNumber,
   currentVUSerialNumber                   VuSerialNumber
}
```

sensorPairingDateFirst è la data del primo accoppiamento del sensore di movimento con un'unità elettronica di bordo.

firstVuApprovalNumber è il numero di omologazione della prima unità elettronica di bordo accoppiata al sensore di movimento.

firstVuSerialNumber è il numero di serie della prima unità elettronica di bordo accoppiata al sensore di movimento.

sensorPairingDateCurrent è la data dell'attuale accoppiamento del sensore di movimento con l'unità elettronica di bordo.

currentVuApprovalNumber è il numero di omologazione dell'unità elettronica di bordo attualmente accoppiata al sensore di movimento.

currentVUSerialNumber è il numero di serie dell'unità elettronica di bordo attualmente accoppiata al sensore di movimento.

2.95. **SensorInstallationSecData**

Informazioni, memorizzate in una carta dell'officina, relative ai dati di sicurezza necessari per l'accoppiamento dei sensori di movimento con le unità elettroniche di bordo (requisito 214).

```
SensorInstallationSecData ::= TDesSessionKey
```

Assegnazione valore: secondo ISO 16844-3.

2.96. **SensorOSIdentifier**

Identificativo del sistema operativo del sensore di movimento.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Assegnazione valore: a cura del fabbricante.

2.97. **SensorPaired**

Informazioni, memorizzate in un'unità elettronica di bordo, relative all'identificazione del sensore di movimento accoppiato all'unità elettronica di bordo (requisito 079).

```
SensorPaired ::= SEQUENCE {
   sensorSerialNumber                      SensorSerialNumber,
   sensorApprovalNumber                    SensorApprovalNumber,
   sensorPairingDateFirst                  SensorPairingDate
}
```

sensorSerialNumber è il numero di serie del sensore di movimento attualmente accoppiato all'unità elettronica di bordo.

sensorApprovalNumber è il numero di omologazione del sensore di movimento attualmente accoppiato all'unità elettronica di bordo.

sensorPairingDateFirst è la data del primo accoppiamento con un'unità elettronica di bordo del sensore di movimento attualmente accoppiato all'unità elettronica di bordo.

2.98. **SensorPairingDate**

Data di accoppiamento del sensore di movimento con un'unità elettronica di bordo.

```
SensorPairingDate ::= TimeReal
```

Assegnazione valore: non specificato.

2.99. **SensorSerialNumber**

Numero di serie del sensore di movimento.

```
SensorSerialNumber ::= ExtendedSerialNumber
```

2.100. **SensorSCIdentifier**

Identificativo del componente di sicurezza incorporato nel sensore di movimento.

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

Assegnazione valore: a cura del fabbricante del componente.

2.101. **Signature**

Una firma digitale.

```
Signature ::= OCTET STRING (SIZE(128))
```

Assegnazione valore: secondo l'appendice 11 (Meccanismi comuni di sicurezza).

2.102. **SimilarEventsNumber**

Il numero di anomalie analoghe verificatesi in un determinato giorno (requisito 094).

```
SimilarEventsNumber ::= INTEGER(0..255)
```

Assegnazione valore: 0 non è utilizzato, 1 significa che, nel giorno in questione, si è verificata ed è stata memorizzata una sola anomalia di un dato tipo, 2 significa che si sono verificate 2 anomalie dello stesso tipo (solo una è stata memorizzata), … 255 significa che si sono verificate 255 o più anomalie dello stesso tipo.

2.103. **SpecificConditionType**

Codice che identifica una condizione particolare (requisiti 050b, 105a, 212a e 230a).

```
SpecificConditionType ::= INTEGER(0..255)
```

Assegnazione valore:

`'00'H`	Disponibile per uso futuro
`'01'H`	Escluso dal campo di applicazione — Inizio
`'02'H`	Escluso dal campo di applicazione — Fine
`'03'H`	Attraversamento mediante tragetto/treno
`'04'H .. 'FF'H`	Disponibile per uso futuro

2.104. **SpecificConditionRecord**

Informazioni, memorizzate in una carta del conducente, una carta dell'officina o un'unità elettronica di bordo, relative ad una condizione particolare (requisiti 105a, 212a e 230a).

```
SpecificConditionRecord ::= SEQUENCE {
   entryTime                                TimeReal,
   specificConditionType                    SpecificConditionType
}
```

entryTime specifica la data e l'ora di immissione.

specificConditionType è il codice che identifica la condizione particolare.

2.105. **Speed**

Velocità del veicolo (km/h).

```
Speed ::= INTEGER(0..255)
```

Assegnazione valore: chilometro all'ora nel campo operativo 0-220 km/h.

2.106. **SpeedAuthorised**

Velocità massima autorizzata del veicolo [definizione bb)].

```
SpeedAuthorised ::= Speed
```

2.107. **SpeedAverage**

Velocità media in un periodo precedentemente definito (km/h).

```
SpeedAverage ::= Speed
```

2.108. **SpeedMax**

Velocità massima misurata in un periodo precedentemente definito.

```
SpeedMax ::= Speed
```

2.109. **TDesSessionKey**

Una chiave tripla di sessione DES.

```
TDesSessionKey ::= SEQUENCE {
   tDesKeyA                                 OCTET STRING (SIZE(8))
   tDesKeyB                                 OCTET STRING (SIZE(8))
}
```

Assegnazione valore: nessun'altra specificazione.

2.110. **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 TMG.

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

Assegnazione valore — Allineato all'ottetto: numero di secondi a partire dalla mezzanotte del 1º gennaio 1970 TMG.

La data/ora massima possibile è nell'anno 2106.

2.111. **TyreSize**

Indicazione delle dimensioni dei pneumatici.

```
TyreSize ::= IA5String(SIZE(15))
```

Assegnazione valore: secondo la direttiva 92/23/CEE del 31.3.1992, GU L 129, pag. 95.

2.112. **VehicleIdentificationNumber**

Numero di identificazione del veicolo (VIN) riferito al veicolo nel suo insieme, di norma corrispondente al numero di serie del chassis o al numero di telaio.

```
VehicleIdentificationNumber ::= IA5String(SIZE(17))
```

Assegnazione valore: secondo ISO 3779.

2.113. **VehicleRegistrationIdentification**

Identificazione di un veicolo, univoca per l'Europa (VRN e Stato membro).

```
VehicleRegistrationIdentification ::= SEQUENCE {
   vehicleRegistrationNation                NationNumeric,
   vehicleRegistrationNumber                VehicleRegistrationNumber
}
```

vehicleRegistrationNation è il paese in cui è stato immatricolato il veicolo.

vehicleRegistrationNumber è il numero di immatricolazione del veicolo (VRN).

2.114. **VehicleRegistrationNumber**

Numero di immatricolazione del veicolo (VRN). Il numero di immatricolazione è assegnato dall'autorità competente.

```
VehicleRegistrationNumber ::= SEQUENCE {
   codePage                                 INTEGER (0..255),
   vehicleRegNumber                         OCTET STRING (SIZE(13))
}
```

codePage specifica la parte della norma ISO/IEC 8859 usata per codificare il vehicleRegistrationNumber,

vehicleRegNumber è un VRN codificato secondo ISO/IEC 8859-codePage.

Assegnazione valore: a cura del paese.

2.115. **VuActivityDailyData**

Informazioni, memorizzate in una VU, relative ai cambi di attività e/o alle variazioni della condizione di guida e/o alle variazioni della condizione della carta in un determinato giorno di calendario (requisito 084) e della condizione della sede (slot) a 00h00 del giorno stesso.

```
VuActivityDailyData ::= SEQUENCE {
   noOfActivityChanges                      INTEGER SIZE(0..1440),
   activityChangeInfos                      SET SIZE(noOfActivityChanges) OF
                                            ActivityChangeInfo
}
```

noOfActivityChanges è il numero di parole (word) ActivityChangeInfo nella serie activityChangeInfos.

activityChangeInfos è la serie di parole (word) ActivityChangeInfo memorizzate nella VU il giorno in questione. Essa comprende sempre due parole ActivityChangeInfo che indicano la condizione delle due sedi (slot) a 00h00 del giorno stesso.

2.116. **VuApprovalNumber**

Numero di omologazione dell'unità elettronica di bordo.

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

Assegnazione valore: non specificato.

2.117. **VuCalibrationData**

Informazioni, memorizzate in un'unità elettronica di bordo, relative alle calibrature dell'apparecchio di controllo (requisito 098).

```
VuCalibrationData ::= SEQUENCE {
   noOfVuCalibrationRecords                 INTEGER(0..255),
   vuCalibrationRecords SET                 SIZE(noOfVuCalibrationRecords) OF
                                            VuCalibrationRecord
}
```

noOfVuCalibrationRecords è il numero di registrazioni contenute nella serie vuCalibrationRecords.

vuCalibrationRecords è la serie di registrazioni di calibrature.

2.118. **VuCalibrationRecord**

Informazioni, memorizzate in un'unità elettronica di bordo, relative ad una calibratura dell'apparecchio di controllo (requisito 098).

```
VuCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                    CalibrationPurpose,
   workshopName                          Name,
   workshopAddress                       Address,
   workshopCardNumber                    FullCardNumber,
   workshopCardExpiryDate                TimeReal,
   vehicleIdentificationNumber           VehicleIdentificationNumber,
   vehicleRegistrationIdentification     VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant        W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment         K-ConstantOfRecordingEquipment,
   lTyreCircumference                    L-TyreCircumference,
   tyreSize                              TyreSize,
   authorisedSpeed                       SpeedAuthorised,
   oldOdometerValue                      OdometerShort,
   newOdometerValue                      OdometerShort,
   oldTimeValue                          TimeReal,
   newTimeValue                          TimeReal,
   nextCalibrationDate                   TimeReal
}
```

calibrationPurpose è lo scopo della calibratura.

workshopName, workshopAddress sono il nome e l'indirizzo dell'officina.

workshopCardNumber identifica la carta dell'officina usata durante la calibratura.

workshopCardExpiryDate è la data di termine validità della carta.

vehicleIdentificationNumber è il VIN.

vehicleRegistrationIdentification contiene il VRN e lo Stato membro di immatricolazione.

wVehicleCharacteristicConstant è il coefficiente caratteristico del veicolo.

kConstantOfRecordingEquipment è la costante dell'apparecchio di controllo.

lTyreCircumference è la circonferenza effettiva dei pneumatici delle ruote.

tyreSize è l'indicazione delle dimensioni dei pneumatici montati sul veicolo.

authorisedSpeed è la velocità autorizzata del veicolo.

oldOdometerValue, newOdometerValuesono i valori vecchio e nuovo dell'odometro.

oldTimeValue, newTimeValue sono i valori vecchio e nuovo di data e ora.

nextCalibrationDate è la data della prossima calibratura del tipo specificato in CalibrationPurpose che dovrà essere effettuata dall'organismo incaricato dei controlli.

2.119. **VuCardIWData**

Informazioni, memorizzate in un'unità elettronica di bordo, relative ai cicli di inserimento ed estrazione di una carta del conducente o di una carta dell'officina nell'unità elettronica di bordo (requisito 081).

```
VuCardIWData ::= SEQUENCE {
   noOfIWRecords                         INTEGER(0..216-1),
   vuCardIWRecords                       SET SIZE(noOfIWRecords) OF
                                         VuCardIWRecord
}
```

noOfIWRecords è il numero di registrazioni nella serie vuCardIWRecords.

vuCardIWRecords è una serie di registrazioni relative ai cicli di inserimento ed estrazione della carta.

2.120. **VuCardIWRecord**

Informazioni, memorizzate in un'unità elettronica di bordo, relative ad un ciclo di inserimento ed estrazione di una carta del conducente o di una carta dell'officina nell'unità elettronica di bordo (requisito 081).

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                          HolderName,
   fullCardNumber                          FullCardNumber,
   cardExpiryDate                          TimeReal,
   cardInsertionTime                       TimeReal,
   vehicleOdometerValueAtInsertion         OdometerShort,
   cardSlotNumber                          CardSlotNumber,
   cardWithdrawalTime                      TimeReal,
   vehicleOdometerValueAtWithdrawal        OdometerShort,
   previousVehicleInfo                     PreviousVehicleInfo
   manualInputFlag                         ManualInputFlag
}
```

cardHolderName contiene il cognome e il nome del titolare della carta del conducente o dell'officina memorizzati nella carta.

fullCardNumber specifica il tipo di carta, lo Stato membro di rilascio e il numero della carta memorizzati nella carta stessa.

cardExpiryDate è la data di termine validità della carta memorizzata nella carta.

cardInsertionTime specifica la data e l'ora di inserimento.

vehicleOdometerValueAtInsertion è il valore dell'odometro del veicolo all'atto dell'inserimento della carta.

cardSlotNumber è la sede (slot) in cui è inserita la carta.

cardWithdrawalTime specifica la data e l'ora di estrazione.

vehicleOdometerValueAtWithdrawal è il valore dell'odometro del veicolo all'atto dell'estrazione della carta.

previousVehicleInfo contiene informazioni, memorizzate nella carta, relative al veicolo precedentemente utilizzato dal conducente.

manualInputFlag è un indicatore (flag) che indica se, all'atto dell'inserimento della carta, il titolare della carta abbia o meno inserito manualmente le attività del conducente.

2.121. **VuCertificate**

Certificato della chiave pubblica di un'unità elettronica di bordo.

```
VuCertificate ::= Certificate
```

2.122. **VuCompanyLocksData**

Informazioni, memorizzate in un'unità elettronica di bordo, relative ai blocchi di un'impresa (requisito 104).

```
VuCompanyLocksData ::= SEQUENCE {
   noOfLocks                               INTEGER(0..20),
   vuCompanyLocksRecords                   SET SIZE(noOfLocks) OF
                                           VuCompanyLocksRecord
}
```

noOfLocks è il numero di blocchi elencati in vuCompanyLocksRecords.

vuCompanyLocksRecords è la serie di registrazioni dei blocchi di un'impresa.

2.123. **VuCompanyLocksRecord**

Informazioni, memorizzate in un'unità elettronica di bordo, relative ad un blocco di un'impresa (requisito 104).

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                          TimeReal,
   lockOutTime                         TimeReal,
   companyName                         Name,
   companyAddress                      Address,
   companyCardNumber                   FullCardNumber
}
```

lockInTime, lockOutTime specificano la data e l'ora di attivazione e di disattivazione del blocco.

companyName, companyAddress specificano il nome e l'indirizzo dell'impresa interessata all'attivazione del blocco.

companyCardNumber identifica la carta usata all'atto dell'attivazione del blocco.

2.124. **VuControlActivityData**

Informazioni, memorizzate in un'unità elettronica di bordo, relative ai controlli eseguiti utilizzando tale VU (requisito 102).

```
VuControlActivityData ::= SEQUENCE {
   noOfControls                        INTEGER(0..20),
   vuControlActivityRecords            SET SIZE(noOfControls) OF
                                       VuControlActivityRecord
}
```

noOfControls è il numero di controlli elencati in vuControlActivityRecords.

vuControlActivityRecords è la serie di registrazioni di attività di controllo.

2.125. **VuControlActivityRecord**

Informazioni, memorizzate in un'unità elettronica di bordo, relative ad un controllo eseguito utilizzando tale VU (requisito 102).

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                         ControlType,
   controlTime                         TimeReal,
   controlCardNumber                   FullCardNumber,
   downloadPeriodBeginTime             TimeReal,
   downloadPeriodEndTime               TimeReal
}
```

controlType è il tipo di controllo.

controlTime specifica la data e l'ora del controllo.

ControlCardNumber identifica la carta di controllo usata per il controllo.

downloadPeriodBeginTime è l'ora di inizio del periodo cui si riferiscono i dati trasferiti, in caso di trasferimento.

downloadPeriodEndTime è l'ora di termine del periodo cui si riferiscono i dati trasferiti, in caso di trasferimento.

2.126. **VuDataBlockCounter**

Contatore, memorizzato in una carta, che indica in ordine di sequenza i cicli di inserimento ed estrazione della carta nelle unità elettroniche di bordo.

```
VuDataBlockCounter ::= BCDString(SIZE(2))
```

Assegnazione valore: numero consecutivo con valore massimo 9 999, ricominciando la numerazione da 0.

2.127. **VuDetailedSpeedBlock**

Informazioni, memorizzate in un'unità elettronica di bordo, relative alla velocità dettagliata del veicolo per un minuto di marcia del veicolo (requisito 093).

```
VuDetailedSpeedBlock ::= SEQUENCE {
    speedBlockBeginDate                     TimeReal,
    speedsPerSecond                         SEQUENCE SIZE(60) OF Speed
}
```

speedBlockBeginDate specifica la data e l'ora del primo valore di velocità all'interno del blocco.

speedsPerSecond è la sequenza cronologica della velocità misurata ogni secondo durante il minuto che comincia da speedBlockBeginDate (inclusa).

2.128. **VuDetailedSpeedData**

Informazioni, memorizzate in un'unità elettronica di bordo, relative alla velocità dettagliata del veicolo.

```
VuDetailedSpeedData ::= SEQUENCE
    noOfSpeedBlocks                         INTEGER(0.2^16-1),
    vuDetailedSpeedBlocks                   SET SIZE(noOfSpeedBlocks) OF
                                            VuDetailedSpeedBlock
}
```

noOfSpeedBlocks è il numero di blocchi di velocità nella serie vuDetailedSpeedBlocks.

vuDetailedSpeedBlocks è la serie di blocchi di velocità dettagliata.

2.129. **VuDownloadablePeriod**

Le date meno recente e più recente per le quali un'unità elettronica di bordo conserva i dati relativi alle attività dei conducenti (requisiti 081, 084 o 087).

```
VuDownloadablePeriod ::= SEQUENCE {
    minDownloadableTime                     TimeReal
    maxDownloadableTime                     TimeReal
}
```

minDownloadableTime specifica la data e l'ora meno recenti di inserimento della carta o di cambio di attività o di immissione del luogo memorizzate nella VU.

maxDownloadableTime specifica la data e l'ora più recenti di estrazione della carta o di cambio di attività o di immissione del luogo memorizzate nella VU.

2.130. **VuDownloadActivityData**

Informazioni, memorizzate in un'unità elettronica di bordo, relative all'ultimo trasferimento dei suoi dati (requisito 105).

```
VuDownloadActivityData ::= SEQUENCE {
    downloadingTime                         TimeReal,
    fullCardNumber                          FullCardNumber,
    companyOrWorkshopName                   Name
}
```

downloadingTime specifica la data e l'ora del trasferimento di dati.

fullCardNumber identifica la carta usata per autorizzare il trasferimento di dati.

companyOrWorkshopName è il nome dell'impresa o dell'officina.

2.131. **VuEventData**

Informazioni, memorizzate in un'unità elettronica di bordo, relative alle anomalie (requisito 094 eccetto per il superamento di velocità).

```
VuEventData ::= SEQUENCE {
    noOfVuEvents                            INTEGER(0..255),
    vuEventRecords                          SET SIZE(noOfVuEvents) OF VuEventRecord
}
```

noOfVuEvents è il numero di anomalie elencate nella serie vuEventRecords.

vuEventRecords è una serie di registrazioni di anomalie.

2.132. **VuEventRecord**

Informazioni, memorizzate in un'unità elettronica di bordo, relative ad un'anomalia (requisito 094 eccetto per il superamento di velocità).

```
VuEventRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventRecordPurpose                 EventFaultRecordPurpose,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   cardNumberDriverSlotBegin          FullCardNumber,
   cardNumberCodriverSlotBegin        FullCardNumber,
   cardNumberDriverSlotEnd            FullCardNumber,
   cardNumberCodriverSlotEnd          FullCardNumber,
   similarEventsNumber                SimilarEventsNumber
}
```

eventType è il tipo di anomalia.

eventRecordPurpose è lo scopo per cui tale anomalia è stata registrata.

eventBeginTime specifica la data e l'ora di inizio dell'anomalia.

eventEndTime specifica la data e l'ora di termine dell'anomalia.

cardNumberDriverSlotBegin identifica la carta inserita nella sede (slot) "conducente" all'inizio dell'anomalia.

cardNumberCodriverSlotBegin identifica la carta inserita nella sede (slot) secondo "conducente" all'inizio dell'anomalia.

cardNumberDriverSlotEnd identifica la carta inserita nella sede (slot) "conducente" al termine dell'anomalia.

cardNumberCodriverSlotEnd identifica la carta inserita nella sede (slot) secondo "conducente" al termine dell'anomalia.

similarEventsNumber è il numero di anomalie analoghe verificatesi nel giorno in questione.

Questa sequenza si può usare per tutte le anomalie, eccetto quella relativa al superamento di velocità.

2.133. **VuFaultData**

Informazioni, memorizzate in un'unità elettronica di bordo, relative ai guasti (requisito 096).

```
VuFaultData ::= SEQUENCE {
   noOfVuFaults                       INTEGER(0..255),
   vuFaultRecords SET                 SIZE(noOfVuFaults) OF VuFaultRecord
}
```

noOfVuFaults è il numero di guasti elencati nella serie vuFaultRecords.

vuFaultRecords è una serie di registrazioni di guasti.

2.134. **VuFaultRecord**

Informazioni, memorizzate in un'unità elettronica di bordo, relative ad un guasto (requisito 096).

```
VuFaultRecord ::= SEQUENCE {
   faultType                          EventFaultType,
   faultRecordPurpose                 EventFaultRecordPurpose,
   faultBeginTime                     TimeReal,
   faultEndTime                       TimeReal,
   cardNumberDriverSlotBegin          FullCardNumber,
   cardNumberCodriverSlotBegin        FullCardNumber,
   cardNumberDriverSlotEnd            FullCardNumber,
   cardNumberCodriverSlotEnd          FullCardNumber
}
```

faultType è il tipo di guasto dell'apparecchio di controllo.

faultRecordPurpose è lo scopo per cui è stato registrato il guasto.

faultBeginTime specifica la data e l'ora di inizio del guasto.

faultEndTime specifica la data e l'ora di termine del guasto.

cardNumberDriverSlotBegin identifica la carta inserita nella sede (slot) "conducente" all'inizio del guasto.

cardNumberCodriverSlotBegin identifica la carta inserita nella sede (slot) "secondo conducente" all'inizio del guasto.

cardNumberDriverSlotEnd identifica la carta inserita nella sede (slot) "conducente" al termine del guasto.

cardNumberCodriverSlotEnd identifica la carta inserita nella sede (slot) "secondo conducente" al termine del guasto.

2.135. **VuIdentification**

Informazioni, memorizzate in un'unità elettronica di bordo, relative all'identificazione dell'unità elettronica di bordo (requisito 075).

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                    VuManufacturerName,
   vuManufacturerAddress                 VuManufacturerAddress,
   vuPartNumber                          VuPartNumber,
   vuSerialNumber                        VuSerialNumber,
   vuSoftwareIdentification              VuSoftwareIdentification,
   vuManufacturingDate                   VuManufacturingDate,
   vuApprovalNumber                      VuApprovalNumber
}
```

vuManufacturerName è il nome del fabbricante dell'unità elettronica di bordo.

vuManufacturerAddress è l'indirizzo del fabbricante dell'unità elettronica di bordo.

vuPartNumber è il codice componente dell'unità elettronica di bordo.

vuSerialNumber è il numero di serie dell'unità elettronica di bordo.

vuSoftwareIdentification identifica il software installato nell'unità elettronica di bordo.

vuManufacturingDate è la data di fabbricazione dell'unità elettronica di bordo.

vuApprovalNumber è il numero di omologazione dell'unità elettronica di bordo.

2.136. **VuManufacturerAddress**

Indirizzo del fabbricante dell'unità elettronica di bordo.

```
VuManufacturerAddress ::= Address
```

Assegnazione valore: non specificato.

2.137. **VuManufacturerName**

Nome del fabbricante dell'unità elettronica di bordo.

```
VuManufacturerName ::= Name
```

Assegnazione valore: non specificato.

2.138. **VuManufacturingDate**

Data di fabbricazione dell'unità elettronica di bordo.

```
VuManufacturingDate ::= TimeReal
```

Assegnazione valore: non specificato.

2.139. **VuOverSpeedingControlData**

Informazioni, memorizzate in un'unità elettronica di bordo, relative alle anomalie per superamento di velocità verificatesi in seguito all'ultimo controllo del superamento di velocità (requisito 095).

```
VuOverSpeedingControlData ::= SEQUENCE {
   lastOverspeedControlTime                TimeReal,
   firstOverspeedSince                     TimeReal,
   numberOfOverspeedSince                  OverspeedNumber
}
```

lastOverspeedControlTime specifica la data e l'ora dell'ultimo controllo del superamento di velocità.

firstOverspeedSince specifica la data e l'ora del primo superamento di velocità in seguito a tale controllo del superamento di velocità.

numberOfOverspeedSince è il numero di anomalie per superamento di velocità verificatesi in seguito all'ultimo controllo del superamento di velocità.

2.140. **VuOverSpeedingEventData**

Informazioni, memorizzate in un'unità elettronica di bordo, relative alle anomalie per superamento di velocità (requisito 094).

```
VuOverSpeedingEventData ::= SEQUENCE {
   noOfVuOverSpeedingEvents                INTEGER(0..255),
   vuOverSpeedingEventRecords              SET SIZE(noOfVuOverSpeedingEvents) OF
                                           VuOverSpeedingEventRecord
}
```

noOfVuOverSpeedingEvents è il numero di anomalie elencate nella serie vuOverSpeedingEventRecords.

vuOverSpeedingEventRecords è una serie di registrazioni di anomalie per superamento di velocità.

2.141. **VuOverSpeedingEventRecord**

Informazioni, memorizzate in un'unità elettronica di bordo, relative alle anomalie per superamento di velocità (requisito 094).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                               EventFaultType,
   eventRecordPurpose                      EventFaultRecordPurpose,
   eventBeginTime                          TimeReal,
   eventEndTime                            TimeReal,
   maxSpeedValue                           SpeedMax,
   averageSpeedValue                       SpeedAverage,
   cardNumberDriverSlotBegin               FullCardNumber,
   similarEventsNumber                     SimilarEventsNumber
}
```

eventType è il tipo di anomalia.

eventRecordPurpose è lo scopo per cui è stata registrata l'anomalia.

eventBeginTime specifica la data e l'ora di inizio dell'anomalia.

eventEndTime specifica la data e l'ora di termine dell'anomalia.

maxSpeedValue è la velocità massima misurata durante l'anomalia.

averageSpeedValue è la media aritmetica della velocità misurata durante l'anomalia.

cardNumberDriverSlotBegin identifica la carta inserita nella sede (slot) "conducente" all'inizio dell'anomalia.

similarEventsNumber è il numero di anomalie analoghe verificatesi nel giorno in questione.

2.142. **VuPartNumber**

Codice componente dell'unità elettronica di bordo.

```
VuPartNumber ::= IA5String(SIZE(16))
```

Assegnazione valore: a cura del fabbricante della VU.

2.143. **VuPlaceDailyWorkPeriodData**

Informazioni, memorizzate in un'unità elettronica di bordo, relative al luogo in cui un conducente inizia o termina un periodo di lavoro giornaliero (requisito 087).

```
VuPlaceDailyWorkPeriodData ::= SEQUENCE {

   noOfPlaceRecords                          INTEGER(0..255),

   vuPlaceDailyWorkPeriodRecords             SET SIZE(noOfPlaceRecords) OF
                                             VuPlaceDailyWorkPeriodRecord

}
```

noOfPlaceRecords è il numero di registrazioni elencate nella serie vuPlaceDailyWorkPeriodRecords.

vuPlaceDailyWorkPeriodRecords è una serie di registrazioni relative ai luoghi.

2.144. **VuPlaceDailyWorkPeriodRecord**

Informazioni, memorizzate in un'unità elettronica di bordo, relative al luogo in cui un conducente inizia o termina un periodo di lavoro giornaliero (requisito 087).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {

   fullCardNumber                            FullCardNumber,

   placeRecord                               PlaceRecord

}
```

fullCardNumber specifica il tipo di carta del conducente, lo Stato membro di rilascio e il numero della carta.

placeRecord contiene le informazioni relative al luogo inserito.

2.145. **VuPrivateKey**

La chiave privata di un'unità elettronica di bordo.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.146. **VuPublicKey**

La chiave pubblica di un'unità elettronica di bordo.

```
VuPublicKey ::= PublicKey
```

2.147. **VuSerialNumber**

Numero di serie dell'unità elettronica di bordo (requisito 075).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.148. **VuSoftInstallationDate**

Data di installazione del software dell'unità elettronica di bordo.

```
VuSoftInstallationDate ::= TimeReal
```

Assegnazione valore: non specificato.

2.149. **VuSoftwareIdentification**

Informazioni, memorizzate in un'unità elettronica di bordo, relative al software installato.

```
VuSoftwareIdentification ::= SEQUENCE {

   vuSoftwareVersion                         VuSoftwareVersion,

   vuSoftInstallationDate                    VuSoftInstallationDate

}
```

vuSoftwareVersion è il numero di versione del software dell'unità elettronica di bordo.

vuSoftInstallationDate è la data di installazione del software.

2.150. **VuSoftwareVersion**

Numero di versione del software dell'unità elettronica di bordo.

```
VuSoftwareVersion ::= IA5String(SIZE(4))
```

Assegnazione valore: non specificato.

2.151. **VuSpecificConditionData**

Informazioni, memorizzate in un'unità elettronica di bordo, relative a condizioni particolari.

```
VuSpecificConditionData ::= SEQUENCE {
   noOfSpecificConditionRecords              INTEGER(0..2^16-1)
   specificConditionRecords                  SET SIZE (noOfSpecificConditionRecords) OF
                                             SpecificConditionRecord
}
```

noOfSpecificConditionRecords è il numero di registrazioni elencate nella serie specificConditionRecords.

specificConditionRecords è una serie di registrazioni relative a condizioni particolari.

2.152. **VuTimeAdjustmentData**

Informazioni, memorizzate in un'unità elettronica di bordo, relative alle regolazioni dell'ora effettuate al di fuori di un ciclo ordinario di calibratura (requisito 101).

```
VuTimeAdjustmentData ::= SEQUENCE {
   noOfVuTimeAdjRecords                      INTEGER(0..6),
   vuTimeAdjustmentRecords                   SET SIZE(noOfVuTimeAdjRecords) OF
                                             VuTimeAdjustmentRecord
}
```

noOfVuTimeAdjRecords è il numero di registrazioni contenute in vuTimeAdjustmentRecords.

vuTimeAdjustmentRecords è una serie di registrazioni di regolazioni dell'ora.

2.153. **VuTimeAdjustmentRecord**

Informazioni, memorizzate in un'unità elettronica di bordo, relative ad una regolazione dell'ora effettuata al di fuori di un ciclo ordinario di calibratura (requisito 101).

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                              TimeReal,
   oldTimeValue                              TimeReal,
   newTimeValue                              TimeReal,
   workshopName                              Name,
   workshopAddress                           Address,
   workshopCardNumber                        FullCardNumber
}
```

oldTimeValue, newTimeValue sono i valori vecchio e nuovo di data e ora.

workshopName, workshopAddress sono il nome e l'indirizzo dell'officina.

workshopCardNumber identifica la carta dell'officina utilizzata per effettuare la regolazione dell'ora.

2.154. **W-VehicleCharacteristicConstant**

Coefficiente caratteristico del veicolo [definizione k)].

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

Assegnazione valore: impulsi al chilometro nel campo operativo 0-64 255 Impulsi/km.

2.155. **WorkshopCardApplicationIdentification**

Informazioni, memorizzate in una carta dell'officina, relative all'identificazione dell'applicazione della carta (requisito 190).

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId                    EquipmentType,
   cardStructureVersion                      CardStructureVersion,
   noOfEventsPerType                         NoOfEventsPerType,
   noOfFaultsPerType                         NoOfFaultsPerType,
   activityStructureLength                   CardActivityLengthRange,
   noOfCardVehicleRecords                    NoOfCardVehicleRecords,
   noOfCardPlaceRecords                      NoOfCardPlaceRecords,
   noOfCalibrationRecords                    NoOfCalibrationRecords
}
```

typeOfTachographCardId specifica il tipo di carta.

cardStructureVersion specifica la versione della struttura utilizzata nella carta.

noOfEventsPerType è il numero di anomalie per tipo di anomalia che la carta è in grado di registrare.

noOfFaultsPerType è il numero di guasti per tipo di guasto che la carta è in grado di registrare.

activityStructureLength indica il numero di byte disponibili per memorizzare le registrazioni delle attività.

noOfCardVehicleRecords è il numero di registrazioni del veicolo che la carta è in grado di contenere.

noOfCardPlaceRecords è il numero di luoghi che la carta è in grado di registrare.

noOfCalibrationRecords è il numero di registrazioni di calibrature che la carta è in grado di memorizzare.

2.156. **WorkshopCardCalibrationData**

Informazioni, memorizzate in una carta dell'officina, relative alle attività dell'officina eseguite con la carta (requisiti 227 e 229).

```
WorkshopCardCalibrationData ::= SEQUENCE {
   calibrationTotalNumber                    INTEGER(0..2^16-1),
   calibrationPointerNewestRecord            INTEGER(0..NoOfCalibrationRecords-1),
   calibrationRecords                        SET SIZE(NoOfCalibrationRecords) OF
                                             WorkshopCardCalibrationRecord
}
```

calibrationTotalNumber è il numero totale di calibrature effettuate con la carta.

calibrationPointerNewestRecord è l'indice della registrazione più aggiornata della calibratura.

Assegnazione valore: numero corrispondente al numeratore della registrazione della calibratura, a partire da '0' per la prima volta in cui tale registrazione compare nella struttura.

calibrationRecords è la serie di registrazioni contenenti le informazioni relative alle calibrature e/o regolazioni dell'ora.

2.157. **WorkshopCardCalibrationRecord**

Informazioni, memorizzate in una carta dell'officina, relative ad una calibratura effettuata con la carta (requisito 227).

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                        CalibrationPurpose,
   vehicleIdentificationNumber               VehicleIdentificationNumber,
   vehicleRegistration                       VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant            W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment             K-ConstantOfRecordingEquipment,
   lTyreCircumference                        L-TyreCircumference,
   tyreSize                                  TyreSize,
```

```
   authorisedSpeed                  SpeedAuthorised,
   oldOdometerValue                 OdometerShort,
   newOdometerValue                 OdometerShort,
   oldTimeValue                     TimeReal,
   newTimeValue                     TimeReal,
   nextCalibrationDate              TimeReal,
   vuPartNumber                     VuPartNumber,
   vuSerialNumber                   VuSerialNumber,
   sensorSerialNumber               SensorSerialNumber
}
```

calibrationPurpose è lo scopo della calibratura.

vehicleIdentificationNumber è il VIN.

vehicleRegistration contiene il VRN e lo Stato membro di immatricolazione.

wVehicleCharacteristicConstant è il coefficiente caratteristico del veicolo.

kConstantOfRecordingEquipment è la costante dell'apparecchio di controllo.

lTyreCircumference è la circonferenza effettiva dei pneumatici delle ruote.

tyreSize è l'indicazione delle dimensioni dei pneumatici montati sul veicolo.

authorisedSpeed è la velocità massima autorizzata del veicolo.

oldOdometerValue, newOdometerValue sono i valori vecchio e nuovo dell'odometro.

oldTimeValue, newTimeValue sono i valori vecchio e nuovo di data e ora.

nextCalibrationDate è la data della prossima calibratura del tipo specificato in CalibrationPurpose che dovrà essere effettuata dall'organismo incaricato dei controlli.

vuPartNumber, vuSerialNumber e **sensorSerialNumber** contengono gli elementi di dati per l'identificazione dell'apparecchio di controllo.

2.158. **WorkshopCardHolderIdentification**

Informazioni, memorizzate in una carta dell'officina, relative all'identificazione del titolare della carta (requisito 216).

```
WorkshopCardHolderIdentification ::= SEQUENCE {
   workshopName                     Name,
   workshopAddress                  Address,
   cardHolderName                   HolderName,
   cardHolderPreferredLanguage      Language
}
```

workshopName è il nome dell'officina del titolare della carta.

workshopAddress è l'indirizzo dell'officina del titolare della carta.

cardHolderName specifica il cognome e il nome del titolare (per esempio il nome del tecnico).

cardHolderPreferredLanguage è la lingua abituale del titolare della carta.

2.159. **WorkshopCardPIN**

Numero di identificazione personale (PIN) della carta dell'officina (requisito 213).

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

Assegnazione valore: il PIN noto al titolare della carta, riempito a destra con byte 'FF' fino a raggiungere 8 byte.

3. DEFINIZIONE DEI CAMPI DI VALORI E DIMENSIONI

Definición de valores variables empleados en las definiciones del apartado 2.

`TimeRealRange ::= 2^32-1`

3.1. **Definizioni relative alla carta del conducente:**

Nome del valore variabile	Min	Max
`CardActivityLengthRange`	5 544 byte (28 giorni, 93 cambi di attività al giorno)	13 776 byte (28 giorni, 240 cambi di attività al giorno)
`NoOfCardPlaceRecords`	84	112
`NoOfCardVehicleRecords`	84	200
`NoOfEventsPerType`	6	12
`NoOfFaultsPerType`	12	24

3.2. **Definizioni relative alla carta dell'officina:**

Nome del valore variabile	Min	Max
`CardActivityLengthRange`	198 byte (1 giorno, 93 cambi di attività)	492 byte (1 giorno, 240 cambi di attività)
`NoOfCardPlaceRecords`	6	8
`NoOfCardVehicleRecords`	4	8
`NoOfEventsPerType`	3	3
`NoOfFaultsPerType`	6	6
`NoOfCalibrationRecords`	88	255

3.3. **Definizioni relative alla carta di controllo:**

Nome del valore variabile	Min	Max
`NoOfControlActivityRecords`	230	520

3.4. **Definizioni relative alla carta dell'azienda:**

Nome del valore variabile	Min	Max
`NoOfCompanyActivityRecords`	230	520

4. INSIEMI DI CARATTERI

Le stringhe IA5 utilizzano i caratteri ASCII definiti nella norma ISO/IEC 8824-1. A fini di migliore leggibilità e di semplice riferimento, si riporta qui di seguito l'assegnazione dei valori. In caso di discordanza, la norma ISO/IEC 8824-1 prevale sulla presente nota informativa.

```
! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ?
@ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [ \ ] ^ _
` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~
```

Altre stringhe di caratteri (Address, Name, VehicleRegistrationNumber) utilizzano anche i caratteri definiti dai codici 192-255 della norma ISO/IEC 8859-1 (Alfabeto latino n. 1) o ISO/IEC 8859-7 (Alfabeto latino/greco).

5. CODIFICA

Se la codifica viene effettuata in base alle regole ASN.1, tutti i tipi di dati definiti devono essere codificati in conformità della norma ISO/IEC 8825-2, variante allineata.

Appendice 2

SPECIFICA DELLE CARTE TACHIGRAFICHE

INDICE

1. INTRODUZIONE

1.1. **Acronimi**

Ai fini della presente appendice, si applicano le seguenti abbreviazioni.

AC	Condizioni di accesso
AID	Identificazione dell'applicazione
ALW	Sempre
APDU	Unità dati protocollo applicazione (struttura di un comando)
ATR	Risposta al reset
AUT	Autenticato
C6, C7	Contatti nn. 6 e 7 della carta, secondo la definizione ISO/IEC 7816-2
cc	Cicli d'orologio
CHV	Informazioni di verifica del titolare della carta
CLA	Byte di classe di un comando APDU
DF	File dedicato. Un DF può contenere altri file (EF o DF)
EF	File elementare
ENC	Crittato: l'accesso è possibile solo mediante la codifica dei dati
etu	Unità di tempo elementare
IC	Circuito integrato
ICC	Carta a circuito integrato
ID	Identificazione
IFD	Interfaccia
IFS	Dimensione campo informazioni
IFSC	Dimensione campo informazioni per la carta
IFSD	Dimensione campo informazioni dispositivo (per il terminale)
INS	Byte di istruzione di un comando APDU
Lc	Lunghezza dei dati in ingresso per un comando APDU
Le	Lunghezza dei dati attesi (dati in uscita per un comando)
MF	File principale (radice DF)
P1-P2	Byte parametri
NAD	Indirizzo di nodo usato nel protocollo T=1
NEV	Mai
PIN	Numero di identificazione personale
PRO SM	Protezione con messaggistica sicura
PTS	Selezione trasmissione protocollo
RFU	Disponibile per uso futuro

RST	Reset (della carta)
SM	Messaggistica sicura
SW1-SW2	Byte di stato
TS	Carattere ATR iniziale
VPP	Tensione di programmazione
XXh	Valore XX in notazione esadecimale
||	Simbolo di concatenamento 03||04=0304

1.2. **Riferimenti normativi**

Nella presente appendice si rimanda alle seguenti norme:

EN 726-3 Identification cards systems — Telecommunications integrated circuit(s) cards and terminals — Part 3: Application independent card requirements. December 1994. (Sistemi di carte di identificazione — Carte a circuito(i) integrato(i) e terminali per telecomunicazioni — Parte 3: Requisiti della carta validi per qualsiasi applicazione. Dicembre 1994)

ISO/CEI 7816-2 Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 2: Dimensions and location of the contacts. First edition: 1999. (Tecnologie dell'informazione — Carte di identificazione — Carte a circuito/i integrato/i con contatti — Parte 2: Dimensioni e posizione dei contatti. Prima edizione: 1999)

ISO/CEI 7816-3 Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 3: Electronic signals and transmission protocol. Edition 2: 1997. (Tecnologie dell'informazione — Carte di identificazione — Carte a circuito/i integrato/i con contatti — Parte 3: Segnali elettronici e protocollo di trasmissione. Edizione 2: 1997)

ISO/CEI 7816-4 Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 4: Interindustry commands for interexchange. First edition: 1995 + Amendment 1: 1997. (Tecnologie dell'informazione — Carte di identificazione — Carte a circuito/i integrato/i con contatti — Parte 4: Comandi interindustriali per l'interscambio. Prima edizione: 1995 + Modifica 1: 1997)

ISO/CEI 7816-6 Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 6: Interindustry data elements. First Edition: 1996 + Cor 1: 1998. (Tecnologie dell'informazione — Carte di identificazione — Carte a circuito/i integrato/i con contatti — Parte 6: Elementi di dati interindustriali. Prima edizione: 1996 + Cor 1: 1998)

ISO/CEI 7816-8 Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 8: Security related interindustry commands. First Edition: 1999. (Tecnologie dell'informazione — Carte di identificazione — Carte a circuito/i integrato/i con contatti — Parte 8: Comandi interindustriali concernenti la sicurezza. Prima edizione: 1999)

ISO/CEI 9797 Information technology — Security techniques — Data integrity mechanism using a cryptographic check function employing a block cipher algorithm. Edition 2: 1994. (Tecnologie dell'informazione — Tecniche di sicurezza — Meccanismo di integrità dei dati che utilizza una funzione di controllo crittografico basata su un algoritmo di cifratura a blocchi. Edizione 2: 1994)

2. CARATTERISTICHE ELETTRICHE E FISICHE

TCS_200 Se non diversamente specificato, tutti i segnali elettronici devono essere conformi alla norma ISO/IEC 7816-3.

TCS_201 La posizione e le dimensioni dei contatti della carta devono essere conformi alla norma ISO/IEC 7816-2.

2.1. **Tensione di alimentazione ed assorbimento di corrente**

TCS_202 La carta deve funzionare in conformità delle specifiche, entro i limiti di assorbimento previsti dalla norma ISO/IEC 7816-3.

TCS_203 La carta deve funzionare con V_{cc} = 3 V (+/- 0,3 V) o con V_{cc} = 5 V (+/- 0,5 V).

La tensione è selezionata in conformità della norma ISO/IEC 7816-3.

2.2. **Tensione di programmazione V_{pp}**

TCS_204 La carta non richiede una tensione di programmazione sul pin C6. Si prevede che il pin C6 non sia collegato in un'IFD. Il contatto C6 può essere collegato alla V_{cc} nella carta, ma non va collegato a massa. Non sono ammesse altre interpretazioni della tensione di programmazione.

2.3. **Generazione e frequenza d'orologio (clock)**

TCS_205 La carta funziona entro un campo di frequenze comprese tra 1 e 5 MHz. Nell'ambito di una sessione della carta, la frequenza dell'orologio può variare di ± 2 %. La frequenza dell'orologio è generata dall'unità elettronica di bordo e non dalla carta. Il fattore di utilizzo può variare tra il 40 e il 60 %.

TCS_206 Nelle condizioni specificate nel file della carta EF_{ICC}, il clock esterno può essere arrestato. Il primo byte del file EF_{ICC} codifica le condizioni della modalità "Clockstop" (cfr. norma EN 726-3 per maggiori informazioni):

Basso	Alto		
Bit 3	Bit 2	Bit 1	
0	0	1	Clockstop ammesso, nessun livello preferito
0	1	1	Clockstop ammesso, livello alto preferito
1	0	1	Clockstop ammesso, livello basso preferito
0	0	0	Clockstop non ammesso
0	1	0	Clockstop ammesso solo al livello alto
1	0	0	Clockstop ammesso solo al livello basso

I bit da 4 a 8 non sono utilizzati.

2.4. **Contatto I/O (ingresso/uscita)**

TCS_207 Il contatto I/O C7 è utilizzato per ricevere e trasmettere dati da e verso l'IFD. Durante il funzionamento, la modalità di trasmissione deve essere attiva solo nella carta o solo nell'IFD. Se la modalità di trasmissione è attiva in entrambi i dispositivi, la carta non viene danneggiata. A condizione che non sia in fase di trasmissione, la carta passa alla modalità di ricezione.

2.5. **Condizioni della carta**

TCS_208 tensione di alimentazione inserita, la carta prevede due condizioni di funzionamento:

— condizione di funzionamento durante l'esecuzione di comandi o l'interfacciamento con l'unità digitale,

— condizione di riposo in tutti gli altri casi; in questa condizione, la carta conserva tutti i dati.

3. HARDWARE E COMUNICAZIONI

3.1. **Introduzione**

Il presente paragrafo descrive la funzionalità minima richiesta per le carte tachigrafiche e le VU al fine di garantirne il corretto funzionamento e l'interoperabilità.

Le carte tachigrafiche devono essere il più possibile conformi alle norme ISO/IEC applicabili in vigore (in particolare ISO/IEC 7816). Si fornisce comunque una descrizione completa dei comandi e dei protocolli al fine di specificare alcune limitazioni d'uso o le differenze eventualmente presenti. Se non diversamente indicato, i comandi specificati sono pienamente conformi alle norme citate.

3.2. **Protocollo di trasmissione**

TCS_300 Il protocollo di trasmissione deve essere conforme alla norma ISO/IEC 7816-3. In particolare, la VU deve riconoscere le proroghe del tempo di attesa inviate dalla carta.

3.2.1. ***Protocolli***

TCS_301 La carta deve prevedere sia il protocollo T=0 sia il protocollo T=1.

TCS_302 T=0 è il protocollo predefinito, ed è quindi necessario un comando PTS per passare al protocollo T=1.

TCS_303 I dispositivi prevedono l'impiego della convenzione diretta in entrambi i protocolli: la convenzione diretta è quindi obbligatoria per la carta.

TCS_304 Il byte di dimensione del campo di informazioni per la carta è presentato all'ATR nel carattere TA3. Questo valore è almeno pari a 'F0h' (= 240 byte).

Ai protocolli si applicano le restrizioni seguenti.

TCS_305 **T=0**

— L'interfaccia deve prevedere una risposta all'I/O dopo il fronte di salita del segnale all'RST da 400 cc.

— L'interfaccia deve essere in grado di leggere caratteri separati da 12 etu.

— L'interfaccia deve leggere un carattere errato e la sua ripetizione se separati da 13 etu. Se viene rilevato un carattere errato, il segnale di errore all'I/O può verificarsi tra 1 e 2 etu. Il dispositivo deve prevedere un ritardo di 1 etu.

— L'interfaccia deve accettare un'ATR da 33 byte (TS+32).

— In presenza di TC1 nell'ATR, deve essere previsto un tempo di protezione supplementare per i caratteri inviati dall'interfaccia, anche se i caratteri inviati dalla carta possono comunque essere separati da 12 etu. Questo vale anche per il carattere ACK inviato dalla carta dopo un carattere P3 emesso dall'interfaccia.

— L'interfaccia deve tener conto di un carattere NUL (nullo) emesso dalla carta.

— L'interfaccia deve accettare la modalità complementare per ACK.

— Il comando GET RESPONSE non può essere usato nella modalità di concatenamento per ottenere dati la cui lunghezza può superare 255 byte.

TCS_306 T=1

— Byte NAD: non utilizzato (il byte NAD è impostato a '00').

— S-block ABORT: non utilizzato.

— Errore di stato S-block VPP: non utilizzato.

— La lunghezza totale di concatenamento per un campo di dati non deve essere superiore a 255 byte (accertato dall'IFD).

— La dimensione del campo di informazioni per il dispositivo (IFSD) deve essere indicato dall'IFD immediatamente dopo l'ATR: l'IFD trasmette la richiesta dell'S-Block IFS dopo l'ATR e la carta risponde con l'S-Block IFS. Il valore consigliato per l'IFSD è 254 byte.

— La carta non chiede un riadeguamento dell'IFS.

3.2.2. ***ATR***

TCS_307 Il dispositivo controlla i byte ATR, secondo la norma ISO/IEC 7816-3. Non si devono effettuare verifiche dei caratteri storici dell'ATR.

Esempio di biprotocollo ATR di base secondo la norma ISO/IEC 7816-3

Carattere	Valore	Note
TS	'3Bh'	Indica la convenzione diretta
T0	'85h'	TD1 presente; sono presenti 5 byte storici
TD1	'80h'	TD2 presente; si deve usare T=0
TD2	'11h'	TA3 presente; si deve usare T=1
TA3	'XXh' (almeno 'F0h')	Dimensione del campo di informazioni per la carta (IFSC)
TH1 bis TH5	'XXh'	Caratteri storici
TCK	'XXh'	Carattere di controllo (OR esclusivo)

TCS_308 In seguito alla risposta al reset (ATR), il file principale (MF) è implicitamente selezionato e diventa il direttorio attivo.

3.2.3. ***PTS***

TCS_309 Il protocollo predefinito è T=0. Per impostare il protocollo T=1, il dispositivo deve inviare un PTS (anche noto come PPS) alla carta.

TCS_310 Poiché entrambi i protocolli T=0 e T=1 sono obbligatori per la carta, anche il PTS di base per il cambio di protocollo è obbligatorio per la carta.

Come indicato nella norma ISO/IEC 7816-3, il PTS si può utilizzare per passare a velocità di dati più elevate rispetto a quella predefinita, proposta dalla carta nell'ATR, se presente (TA(1) byte).

Velocità di dati più elevate per la carta sono facoltative.

TCS_311 Se non sono previste velocità di dati diverse da quella predefinita (o se la velocità di dati selezionata non è prevista), la carta risponde correttamente al PTS, secondo la norma ISO/IEC 7816-3, omettendo il byte PPS1.

Si riportano qui di seguito alcuni esempi di PTS di base per la selezione del protocollo.

Carattere	Valore	Note
PPSS	'FFh'	Carattere iniziale
PPS0	'00h' o '01h'	I caratteri da PPS1 a PPS3 non sono presenti; '00h' per selezionare T0, '01h' per selezionare T1.
PK	'XXh'	Carattere di controllo: 'XXh' = 'FFh' e PPS0 = '00h' 'XXh' = 'FEh' se PPS0 = '01h'

3.3. **Condizioni di accesso (AC)**

Le condizioni di accesso (AC) per i comandi UPDATE BINARY e READ BINARY sono definite per ogni file elementare.

TCS_312 L'AC del file corrente dev'essere soddisfatta prima di accedere al file mediante questi comandi.

Le definizioni delle condizioni di accesso disponibili sono le seguenti:

— ALW: l'azione è sempre possibile e può essere eseguita senza limitazioni.

— NEV: l'azione non è mai possibile.

— AUT: i diritti corrispondenti ad un'avvenuta autenticazione esterna devono essere aperti (eseguito dal comando EXTERNAL AUTHENTICATE).

— PRO SM: il comando dev'essere trasmesso con un totale di controllo crittografico utilizzando la messaggistica sicura (cfr. Appendice 11).

— AUT e PRO SM (combinati).

Per i comandi di elaborazione (UPDATE BINARY e READ BINARY), nella carta si possono impostare le seguenti condizioni di accesso:

	UPDATE BINARY	READ BINARY
ALW	Sì	Sì
NEV	Sì	Sì
AUT	Sì	Sì
PRO SM	Sì	No
AUT e PRO SM	Sì	No

La condizione di accesso per PRO SM non è disponibile per il comando READ BINARY. Ciò significa che la presenza di un totale di controllo crittografico per un comando READ non è mai obbligatoria. Tuttavia, utilizzando il valore 'OC' per la classe, è possibile utilizzare il comando READ BINARY con messaggistica sicura, come descritto al paragrafo 3.6.2.

3.4. **Crittazione dei dati**

Quando risulta necessario proteggere la riservatezza dei dati da leggere in un file, il file è contrassegnato come "crittato". La crittazione è effettuata utilizzando la messaggistica sicura (cfr. Appendice 11).

3.5. **Compendio di comandi e codici di errore**

I comandi e l'organizzazione dei file si desumono dalla norma ISO/IEC 7816-4, cui sono conformi.

TCS_313 La presente sezione descrive le seguenti coppie comando-risposta APDU:

Comando	INS
SELECT FILE	A4
READ BINARY	B0
UPDATE BINARY	D6
GET CHALLENGE	84
VERIFY	20
GET RESPONSE	C0
PERFORM SECURITY OPERATION: VERIFY CERTIFICATE COMPUTE DIGITAL SIGNATURE VERIFY DIGITAL SIGNATURE HASH	2A
INTERNAL AUTHENTICATE	88
EXTERNAL AUTHENTICATE	82
MANAGE SECURITY ENVIRONMENT: SETTING A KEY	22
PERFORM HASH OF FILE	2A

TCS_314 Le parole (word) di stato SW1 SW2 sono inviate in ogni messaggio di risposta ed indicano lo stato di elaborazione del comando.

SW1	SW2	Significato
90	00	Elaborazione normale
61	XX	Elaborazione normale. XX = numero di byte di risposta disponibili
62	81	Elaborazione con avvertimento. Parte dei dati rinviati potrebbero risultare danneggiati
63	CX	CHV (PIN) errato. Contatore tentativi rimasti fornito da 'X'
64	00	Errore di esecuzione — Stato della memoria non volatile immutato. Errore di integrità
65	00	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 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	00	Lunghezza errata (Lc o Le errata)
69	00	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 corrente)
69	87	Oggetti di dati previsti in messaggistica sicura mancanti
69	88	Oggetti di dati in messaggistica sicura non corretti
6A	82	File non trovato
6A	86	Parametri P1-P2 errati
6A	88	Dati indicati non trovati
6B	00	Parametri errati (scostamento al di fuori dell'EF)

SW1	SW2	Significato
6C	XX	Lunghezza errata, SW2 indica la lunghezza esatta. Non viene inviato alcun campo di dati in risposta
6D	00	Codice di istruzione non previsto o non valido
6E	00	Classe non prevista
6F	00	Altri errori di controllo

3.6. **Descrizione dei comandi**

Nel presente capitolo sono descritti i comandi obbligatori per le carte tachigrafiche.

Altri particolari di rilievo, riguardanti le operazioni crittografiche, sono forniti nell'Appendice 11 (Meccanismi comuni di sicurezza).

Tutti i comandi sono descritti a prescindere dal protocollo utilizzato (T=0 o T=1). I byte APDU CLA, INS, P1, P2, Lc e Le sono sempre indicati. Se i byte Lc o Le non sono necessari per il comando descritto, la lunghezza, il valore e la descrizione ad essi associati sono vuoti.

TCS_315 Se entrambi i byte di lunghezza (Lc e Le) sono necessari, e se l'IFD utilizza il protocollo T=0, il comando descritto dev'essere suddiviso in due parti: l'IFD invia il comando secondo quanto descritto con P3=Lc + dati e quindi invia un comando GET RESPONSE (cfr. paragrafo 3.6.6) con P3=Le.

TCS_316 Se sono necessari entrambi i byte di lunghezza e Le=0 (secure messaging):

— se si usa il protocollo T=1, la carta risponde a Le=0 inviando tutti i dati in uscita disponibili;

— se si usa il protocollo T=0, l'IFD invia il primo comando con P3=Lc + dati e la carta risponde (a questo implicito Le=0) con i byte di stato '61La', dove La è il numero di byte di risposta disponibili. L'IFD genera quindi un comando GET RESPONSE con P3=La per leggere i dati.

3.6.1. ***Select File***

Questo comando è conforme alla norma ISO/IEC 7816-4, ma ha un impiego limitato rispetto al comando definito nella norma.

Il comando SELECT FILE si usa per:

— selezionare un DF di applicazione (si deve usare la selezione per nome)

— selezionare un file elementare corrispondente all'ID del file indicato.

3.6.1.1. *Selezione in base al nome (AID)*

Questo comando consente di selezionare un DF di applicazione nella carta.

TCS_317 Il comando può essere eseguito da qualsiasi punto della struttura del file (dopo l'ATR o in qualsiasi momento).

TCS_318 La selezione di un'applicazione azzera l'ambiente di sicurezza attivo. In seguito alla selezione dell'applicazione, la chiave pubblica corrente non è più selezionata e la chiave della sessione precedente non è più disponibile per la messaggistica sicura. Si perde anche la condizione di accesso AUT.

TCS_319 Messaggio di comando

Byte	Lunghezza	Valore	Descrizione
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'04h'	Selezione in base al nome (AID)
P2	1	'0Ch'	Risposta non attesa
Lc	1	'NNh'	Numero di byte inviati alla carta (lunghezza dell'AID): '06h' per l'applicazione tachigrafica
#6-#(5+NN)	NN	'XX..XXh'	AID: 'FF 54 41 43 48 4F' per l'applicazione tachigrafica

Non è necessaria una risposta al comando SELECT FILE (Le assente in T=1, o risposta non richiesta in T=0).

TCS_320 Messaggio di risposta (risposta non richiesta)

Byte	Lunghezza	Valore	Descrizione
SW	2	'XXXXh'	Word di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde '9000'.

— Se l'applicazione corrispondente all'AID non viene trovata, lo stato di elaborazione inviato in risposta è '6A82'.

— In T=1, se il byte Le è presente, lo stato inviato in risposta è '6700'.

— In T=0, se è richiesta una risposta dopo il comando SELECT FILE, lo stato inviato in risposta è '6900'.

— 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 '6581'.

3.6.1.2. *Selezione di un file elementare utilizzando il suo identificativo*

TCS_321 Messaggio di comando

Byte	Lunghezza	Valore	Descrizione
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'02h'	Selezione di un EF sotto il DF corrente
P2	1	'0Ch'	Risposta non attesa
Lc	1	'02h'	Numero di byte inviati alla carta
#6-#7	2	'XXXXh'	Identificativo del file

Non è necessaria una risposta al comando SELECT FILE (Le assente in T=1, o risposta non richiesta in T=0).

TCS_322 Messaggio di risposta (risposta non richiesta)

Byte	Lunghezza	Valore	Descrizione
SW	2	'XXXXh'	Word di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde '9000'.

— Se il file corrispondente all'identificativo del file non viene trovato, lo stato di elaborazione inviato in risposta è '6A82'.

— In T=1, se il byte Le è presente, lo stato inviato in risposta è '6700'.

— In T=0, se è richiesta una risposta dopo il comando SELECT FILE, lo stato inviato in risposta è '6900'.

— 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 '6581'.

3.6.2. ***Read Binary***

Questo comando è conforme alla norma ISO/IEC 7816-4, ma ha un impiego limitato rispetto al comando definito nella norma.

Il comando READ BINARY è usato per leggere i dati di un file trasparente.

La risposta della carta consiste nell'invio dei dati letti, eventualmente incapsulati in una struttura di messaggistica sicura.

TCS_323 Il comando può essere eseguito solo se la condizione di sicurezza soddisfa gli attributi di sicurezza definiti per l'EF relativamente alla funzione READ.

3.6.2.1. *Comando senza messaggistica sicura*

Questo comando consente all'IFD di leggere i dati dall'EF selezionato, senza messaggistica sicura.

TCS_324 Con questo comando non è possibile la lettura di dati da un file contrassegnato come “crittato”.

TCS_325 Messaggio di comando

Byte	Lunghezza	Valore	Descrizione
CLA	1	'00h'	Messaggistica sicura non richiesta
INS	1	'B0h'	
P1	1	'XXh'	Scostamento in byte dall'inizio del file: byte più significativo
P2	1	'XXh'	Scostamento in byte dall'inizio del file: byte meno significativo
Le	1	'XXh'	Lunghezza dei dati attesi. Numero di byte da leggere

Nota: il bit 8 di P1 dev'essere impostato a 0.

TCS_326 Messaggio di risposta

Byte	Lunghezza	Valore	Descrizione
#1-#X	X	'XX..XXh'	Dati letti
SW	2	'XXXXh'	Word di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde '9000'.

— Se non è selezionato un EF, lo stato di elaborazione inviato in risposta è '6986'.

— Se il controllo dell'accesso del file selezionato non è soddisfatto, il comando viene interrotto con '6982'.

— Se lo scostamento non è compatibile con la dimensione dell'EF (scostamento > dimensione EF), lo stato di elaborazione inviato in risposta è '6B00'.

— Se la dimensione dei dati da leggere non è compatibile con la dimensione dell'EF (scostamento + Le > dimensione EF), lo stato di elaborazione inviato in risposta è '6700' o '6Cxx', ove 'xx' indica la lunghezza esatta.

— 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 '6581'.

— Se nei dati registrati è rilevato un errore di integrità, la carta deve fornire i dati richiesti e rinviare lo stato di elaborazione '6281'.

3.6.2.2. *Comando con messaggistica sicura*

Questo comando consente all'IDF di leggere i dati dall'EF selezionato con messaggistica sicura, al fine di verificare l'integrità dei dati ricevuti e di proteggere la riservatezza dei dati nel caso in cui l'EF sia contrassegnato come “crittato”.

TCS_327 Messaggio di comando

Byte	Lunghezza	Valore	Descrizione
CLA	1	'0Ch'	Richiesta messaggistica sicura
INS	1	'B0h'	INS
P1	1	'XXh'	P1 (scostamento in byte dall'inizio del file): byte più significativo
P2	1	'XXh'	P2 (scostamento in byte dall'inizio del file): byte meno significativo
Lc	1	'09h'	Lunghezza dei dati in ingresso per messaggistica sicura
#6	1	'97h'	T_{LE}: tag per la specificazione della lunghezza attesa.
#7	1	'01h'	L_{LE}: lunghezza della lunghezza attesa
#8	1	'NNh'	Specificazione della lunghezza attesa (Le originale): numero di byte da leggere

Byte	Lunghezza	Valore	Descrizione
#9	1	'8Eh'	T_{CC}: tag per il totale di controllo crittografico
#10	1	'04h'	L_{CC}: lunghezza del totale di controllo crittografico successivo
#11-#14	4	'XX..XXh'	Controllo crittografico (4 byte più significativi)
Le	1	'00h'	Secondo la norma ISO/IEC 7816-4

TCS_328 Messaggio di risposta se l'EF non è contrassegnato come "crittato" e se il formato di messaggistica sicura in ingresso è corretto:

Byte	Lunghezza	Valore	Descrizione
#1	1	'81h'	T_{PV}: tag per dati in chiaro
#2	L	'NNh' o '81 NNh'	L_{PV}: lunghezza dei dati inviati in risposta (=Le originale). L è 2 byte se L_{PV} >127 byte.
#(2+L)-#(1+L+NN)	NN	'XX..XXh'	Dati in chiaro
#(2+L+NN)	1	'8Eh'	T_{CC}: tag per il totale di controllo crittografico
#(3+L+NN)	1	'04h'	L_{CC}: lunghezza del totale di controllo crittografico successivo
#(4+L+NN)-#(7+L+NN)	4	'XX..XXh'	Totale di controllo crittografico (4 byte più significativi)
SW	2	'XXXXh'	Parole (word) di stato (SW1, SW2)

TCS_329 Messaggio di risposta se l'EF è contrassegnato come "crittato" e se il formato di messaggistica sicura in ingresso è corretto:

Byte	Lunghezza	Valore	Descrizione
#1	1	'87h'	$T_{PI\ CG}$: tag per i dati crittati (crittogramma)
#2	L	'MMh' o '81 MMh	$L_{PI\ CG}$: lunghezza dei dati crittati inviati in risposta (diversa da Le originale del comando a causa del riempimento) L è 2 byte se $L_{PI\ CG}$ > 127 byte
#(2+L)-#(1+L+MM)	MM	'01XX..XXh'	Dati crittati: indicatore di riempimento e crittogramma
#(2+L+MM)	1	'8Eh'	T_{CC}: tag per il totale di controllo crittografico
#(3+L+MM)	1	'04h'	L_{CC}: lunghezza del totale di controllo crittografico successivo
#(4+L+MM)-#(7+L+MM)	4	'XX..XXh'	Totale di controllo crittografico (4 byte più significativi)
SW	2	'XXXXh'	Word di stato (SW1, SW2)

I dati crittati inviati in risposta contengono un primo byte che indica la modalità di riempimento utilizzata. Per l'applicazione tachigrafica, l'indicatore di riempimento assume sempre il valore '01h', che indica l'impiego della modalità di riempimento specificata nella norma ISO/IEC 7816-4 (un byte con valore '80h', seguito da alcuni byte nulli: ISO/IEC 9797, metodo 2).

Gli stati di elaborazione "regolari", descritti per il comando READ BINARY senza messaggistica sicura (cfr. paragrafo 3.6.2.1), possono essere inviati in risposta utilizzando le strutture dei messaggi di risposta sopra descritte.

Si possono inoltre verificare alcuni errori che riguardano specificamente la messaggistica sicura. In tal caso, viene inviato in risposta solo lo stato di elaborazione, senza strutture di messaggistica sicura.

TCS_330 Messaggio di risposta se il formato di messaggistica sicura in ingresso è errato

Byte	Lunghezza	Valore	Descrizione
SW	2	'XXXXh'	Word di stato (SW1,SW2)

— Se non è disponibile una chiave di sessione corrente, viene inviato in risposta lo stato di elaborazione '6A88'. Questo si verifica se la chiave di sessione non è ancora stata generata o se è terminato il corso di validità della chiave di sessione (in questo caso l'IFD deve rieseguire un processo di autenticazione reciproca per impostare una nuova chiave di sessione).

— Se nel formato di messaggistica sicura mancano alcuni oggetti di dati attesi (secondo quanto sopra specificato), viene inviato in risposta lo stato di elaborazione '6987': questo errore si verifica se manca un tag atteso o se il comando non è costruito in modo corretto.

— Se alcuni oggetti di dati non sono corretti, lo stato di elaborazione inviato in risposta è '6988': questo errore si verifica se tutti i tag richiesti sono presenti, ma alcune lunghezze sono diverse da quelle attese.

— Se la verifica del totale di controllo crittografico ha esito negativo, lo stato di elaborazione inviato in risposta è '6688'.

3.6.3. ***Update Binary***

Questo comando è conforme alla norma ISO/IEC 7816-4, ma ha un impiego limitato rispetto al comando definito nella norma.

Il messaggio di comando UPDATE BINARY avvia l'aggiornamento (cancellazione + scrittura) dei bit già presenti in un EF binario con i bit indicati nel comando APDU.

TCS_331 Il comando può essere eseguito solo se la condizione di sicurezza soddisfa gli attributi di sicurezza definiti per l'EF per la funzione UPDATE (se il controllo di accesso della funzione UPDATE comprende la PRO SM, si deve aggiungere la messaggistica sicura nel comando).

3.6.3.1. *Comando senza messaggistica sicura*

Questo comando consente all'IFD di scrivere dati nell'EF selezionato, senza che la carta verifichi l'integrità dei dati ricevuti. Questa modalità in chiaro è consentita solo se il file in questione non è contrassegnato come "crittato".

TCS_332 Messaggio di comando

Byte	Lunghezza	Valore	Descrizione
CLA	1	'00h'	Messaggistica sicura non richiesta
INS	1	'D6h'	
P1	1	'XXh'	Scostamento in byte dall'inizio del file: byte più significativo
P2	1	'XXh'	Scostamento in byte dall'inizio del file: byte meno significativo
Lc	1	'NNh'	Lc Lunghezza dei dati da aggiornare. Numero di byte da scrivere
#6-#(5+NN)	NN	'XX..XXh'	Dati da scrivere

Nota: il bit 8 di P1 dev'essere impostato a 0.

TCS_333 Messaggio di risposta

Byte	Lunghezza	Valore	Descrizione
SW	2	'XXXXh'	Word di stato (SW1,SW2)

— Se il comando ha esito positivo, la carta risponde '9000'.

— Se non è selezionato un EF, lo stato di elaborazione inviato in risposta è '6986'.

— Se il controllo di accesso del file selezionato non è soddisfatto, il comando viene interrotto con '6982'.

— Se lo scostamento non è compatibile con la dimensione dell'EF (scostamento > dimensione EF), lo stato di elaborazione inviato in risposta è '6B00'.

— Se la dimensione dei dati da scrivere non è compatibile con la dimensione dell'EF (scostamento + Le > dimensione EF), lo stato di elaborazione inviato in risposta è '6700'.

— 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'.

— Se l'operazione di scrittura fallisce, lo stato di elaborazione inviato in risposta è '6581'.

3.6.3.2. *Comando con messaggistica sicura*

Questo comando consente all'IFD di scrivere dati nell'EF selezionato, con verifica dell'integrità dei dati ricevuti da parte della carta. Poiché non è richiesta la riservatezza, i dati non sono crittati.

TCS_334 Mensaje de comando

Byte	Lunghezza	Valore	Descrizione
CLA	1	'0Ch'	Messaggistica sicura richiesta
INS	1	'D6h'	INS
P1	1	'XXh'	Scostamento in byte dall'inizio del file: byte più significativo
P2	1	'XXh'	Scostamento in byte dall'inizio del file: byte meno significativo
Lc	1	'XXh'	Lunghezza del campo di dati sicuri
#6	1	'81h'	T_{PV}: tag per i dati in chiaro
#7	L	'NNh' o '81 NNh'	L_{PV}: lunghezza dei dati trasmessi L è 2 byte se L_{PV} > 127 byte
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Dati in chiaro (dati da scrivere)
#(7+L+NN)	1	'8Eh'	T_{CC}: tag per il totale di controllo crittografico
#(8+L+NN)	1	'04h'	L_{CC}: lunghezza del totale di controllo crittografico successivo
#(9+L+NN)-#(12+L+NN)	4	'XX..XXh'	Totale di controllo crittografico (4 byte più significativi)
Le	1	'00h'	Secondo la norma ISO/IEC 7816-4

TCS_335 Messaggio di risposta se il formato di messaggistica sicura in ingresso è corretto

Byte	Lunghezza	Valore	Descrizione
#1	1	'99h'	T_{SW}: tag per le word di stato (protetto da CC)
#2	1	'02h'	L_{SW}: lunghezza delle word di stato inviate in risposta
#3-#4	2	'XXXXh'	Word di stato (SW1, SW2)
#5	1	'8Eh'	T_{CC}: tag per il totale di controllo crittografico
#6	1	'04h'	L_{CC}: lunghezza del totale di controllo crittografico successivo
#7-#10	4	'XX..XXh'	Totale di controllo crittografico (4 byte più significativi)
SW	2	'XXXXh'	Word di stato (SW1, SW2)

Gli stati di elaborazione "regolari", descritti per il comando UPDATE BINARY senza messaggistica sicura (cfr. paragrafo 3.6.3.1), possono essere inviati in risposta utilizzando la struttura del messaggio di risposta sopra descritta.

Si possono inoltre verificare alcuni errori che riguardano specificamente la messaggistica sicura. In tal caso, viene inviato in risposta solo lo stato di elaborazione, senza strutture di messaggistica sicura:

TCS_336 Messaggio di risposta in caso di errore di messaggistica sicura

Byte	Lunghezza	Valore	Descrizione
SW	2	'XXXXh'	Word di stato (SW1, SW2)

— Se non è disponibile una chiave di sessione corrente, viene inviato in risposta lo stato di elaborazione '6A88'.

— Se nel formato di messaggistica sicura mancano alcuni oggetti di dati attesi (secondo quanto sopra specificato), viene inviato in risposta lo stato di elaborazione '6987' questo errore si verifica se manca un tag atteso o se il comando non è costruito in modo corretto.

— Se alcuni oggetti di dati non sono corretti, lo stato di elaborazione inviato in risposta è '6988': questo errore si verifica se tutti i tag richiesti sono presenti, ma alcune lunghezze sono diverse da quelle attese.

— Se la verifica del totale di controllo crittografico ha esito negativo, lo stato di elaborazione inviato in risposta è '6688'.

3.6.4. ***Get Challenge***

Questo comando è conforme alla norma ISO/IEC 7816-4, ma ha un impiego limitato rispetto al comando definito nella norma.

Il comando GET CHALLENGE chiede alla carta di generare una Challenge da utilizzare in una procedura di sicurezza, in cui un crittogramma o alcuni dati cifrati vengono inviati alla carta.

TCS_337 La Challenge generata dalla carta è valida solo per il comando successivo, che utilizza una Challenge, inviato alla carta.

TCS_338 Messaggio di comando

Byte	Lunghezza	Valore	Descrizione
CLA	1	'00h'	CLA
INS	1	'84h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Le	1	'08h'	Le (lunghezza della Challenge attesa).

TCS_339 Messaggio di risposta

Byte	Lunghezza	Valore	Descrizione
#1-#8	8	'XX..XXh'	Challenge
SW	2	'XXXXh'	Word di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde '9000'.

— Se Le è diversa da '08h', lo stato di elaborazione è '6700'.

— Se i parametri P1-P2 sono scorretti, lo stato di elaborazione è '6A86'.

3.6.5. ***Verify***

Questo comando è conforme alla norma ISO/IEC 7816-4, ma ha un impiego limitato rispetto al comando definito nella norma.

Il comando VERIFY avvia il confronto nella carta dei dati CHV (PIN) inviati dal comando con il CHV di riferimento memorizzato nella carta.

Nota: il PIN inserito dall'utente dev'essere riempito a destra con byte 'FFh' dall'IFD, fino a raggiungere la lunghezza di 8 byte.

TCS_340 Se il comando ha esito positivo, i diritti corrispondenti al CHV presentato vengono aperti e il contatore dei tentativi rimasti per il CHV viene riportato al valore iniziale.

TCS_341 Se il confronto ha esito negativo, l'informazione viene registrata nella carta al fine di limitare il numero di ulteriori tentativi d'impiego del CHV di riferimento.

TCS_342 Messaggio di comando

Byte	Lunghezza	Valore	Descrizione
CLA	1	'00h'	CLA
INS	1	'20h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (il CHV di riferimento verificato è implicitamente noto)
Lc	1	'08h'	Lunghezza del codice CHV trasmesso
#6-#13	8	'XX..XXh'	CHV

TCS_343 Messaggio di risposta

Byte	Lunghezza	Valore	Descrizione
SW	2	'XXXXh'	Word di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde '9000'.

— Se il CHV di riferimento non viene trovato, lo stato di elaborazione inviato in risposta è '6A88'.

— Se il CHV è bloccato (il contatore dei tentativi rimasti per il CHV è nullo), lo stato di elaborazione inviato in risposta è '6983'. In presenza di tale stato, il CHV non può più essere presentato con esito positivo.

— Se il confronto ha esito negativo, il contatore dei tentativi rimasti diminuisce e viene inviato in risposta lo stato '63CX' (X > 0 e X è uguale al contatore dei tentativi rimasti per il CHV. Se X = 'F', il contatore dei tentativi per il CHV è maggiore di 'F').

— Se il CHV di riferimento è considerato danneggiato, lo stato di elaborazione inviato in risposta è '6400' o '6581'.

3.6.6. ***Get Response***

Questo comando è conforme alla norma ISO/IEC 7816-4.

Il comando (necessario e disponibile solo per il protocollo T=0) è utilizzato per trasmettere i dati preparati dalla carta all'interfaccia (caso in cui un comando include sia Lc che Le).

Il comando GET_RESPONSE dev'essere inviato immediatamente dopo il comando di preparazione dei dati, altrimenti i dati in questione vanno perduti. Dopo l'esecuzione del comando GET_RESPONSE (eccetto per il caso in cui si verifichi l'errore '61xx' o '6Cxx', cfr. sotto), i dati precedentemente preparati non sono più disponibili.

TCS_344 Messaggio di comando

Byte	Lunghezza	Valore	Descrizione
CLA	1	'00h'	
INS	1	'C0h'	
P1	1	'00h'	
P2	1	'00h'	
Le	1	'XXh'	Numero di byte attesi

TCS_345 Messaggio di risposta

Byte	Lunghezza	Valore	Descrizione
#1-#X	X	'XX..XXh'	Dati
SW	2	'XXXXh'	Word di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde '9000'.

— Se i dati non sono stati preparati dalla carta, lo stato di elaborazione inviato in risposta è '6900' o '6F00'.

— Se Le supera il numero di byte disponibili o se Le è nullo, lo stato di elaborazione inviato in risposta è '6Cxx', dove 'xx' indica il numero esatto di byte disponibili. In tal caso, i dati preparati restano disponibili per un successivo comando GET_RESPONSE.

— Se Le non è nullo ed è inferiore al numero di byte disponibili, i dati richiesti vengono normalmente inviati dalla carta, e lo stato di elaborazione inviato in risposta è '61xx', dove 'xx' indica il numero di byte ancora disponibili per un ulteriore comando GET_RESPONSE.

— Se il comando non è previsto (protocollo T=1), la carta risponde '6D00'.

3.6.7. ***PSO: Verify Certificate***

Questo comando è conforme alla norma ISO/IEC 7816-8, ma ha un impiego limitato rispetto al comando definito nella norma.

Il comando VERIFY CERTIFICATE è utilizzato dalla carta per ottenere una chiave pubblica dall'esterno e per verificarne la validità.

TCS_346 Se il comando VERIFY CERTIFICATE ha esito positivo, la chiave pubblica viene memorizzata per uso futuro nell'ambiente di sicurezza. Questa chiave viene esplicitamente impostata da parte del comando MSE (cfr. paragrafo 3.6.10), utilizzando il suo identificativo di chiave, per impiego con comandi relativi alla sicurezza (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE o VERIFY CERTIFICATE).

TCS_347 In ogni caso, il comando VERIFY CERTIFICATE utilizza la chiave pubblica precedentemente selezionata dal comando MSE per aprire il certificato. Tale chiave pubblica deve essere quella di uno degli Stati membri o quella d'Europa.

TCS_348 Messaggio di comando

Byte	Lunghezza	Valore	Descrizione
CLA	1	'00h'	CLA
INS	1	'2Ah'	Esecuzione operazione di sicurezza
P1	1	'00h'	P1
P2	1	'AEh'	P2: dati non codificati BER-TLV (concatenamento di elementi di dati)
Lc	1	'CEh'	Lc: lunghezza del certificato, 194 byte
#6-#199	194	'XX..XXh'	Certificato: concatenamento di elementi di dati (secondo la descrizione di cui all'Appendice 11)

TCS_349 Messaggio di risposta

Byte	Lunghezza	Valore	Descrizione
SW	2	'XXXXh'	Word di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde '9000'.

— Se la verifica del certificato fallisce, lo stato di elaborazione inviato in risposta è '6688'. Il processo di verifica ed apertura del certificato è descritto nell'Appendice 11.

— Se nell'ambiente di sicurezza non è presente una chiave pubblica, viene inviato in risposta '6A88'.

— Se la chiave pubblica selezionata (usata per aprire il certificato) è considerata danneggiata, lo stato di elaborazione inviato in risposta è '6400' o '6581'.

— Se la chiave pubblica selezionata (usata per aprire il certificato) ha una CHA.LSB (`CertificateHolderAuthorisation.equipmentType`) diversa da '00' (ovvero non è quella di uno delgi Stati membri o quella d'Europa) lo stato di elaborazione inviato in risposta è '6985'.

3.6.8. ***Internal Authenticate***

Questo comando è conforme alla norma ISO/IEC 7816-4.

Utilizzando il comando INTERNAL AUTHENTICATE, l'IFD può autenticare la carta.

Il processo di autenticazione è descritto nell'Appendice 11. Esso prevede le seguenti dichiarazioni.

TCS_350 Il comando INTERNAL AUTHENTICATE utilizza la chiave privata della carta (selezionata implicitamente) per firmare dati di autenticazione, compreso K1 (primo elemento per l'accordo sulla chiave di sessione) e RND1, ed utilizza la chiave pubblica attualmente selezionata (mediante l'ultimo comando MSE) per crittare la firma e formare il token di autenticazione (cfr. Appendice 11 per maggiori particolari).

TCS_351 Messaggio di comando

Byte	Lunghezza	Valore	Descrizione
CLA	1	'00h'	CLA
INS	1	'88h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Lc	1	'10h'	Lunghezza dei dati inviati alla carta
#6-#13	8	'XX..XXh'	Challenge usata per autenticare la carta
#14-#21	8	'XX..XXh'	VU.CHR (cfr. Appendice 11)
Le	1	'80h'	Lunghezza dei dati attesi dalla carta

TCS_352 Messaggio di risposta

Byte	Lunghezza	Valore	Descrizione
#1-#128	128	'XX..XXh'	Token di autenticazione carta (cfr. Appendice 11)
SW	2	'XXXXh'	Word di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde '9000'.

— Se nell'ambiente di sicurezza non è presente una chiave pubblica, lo stato di elaborazione inviato in risposta è '6A88'.

— Se nell'ambiente di sicurezza non è presente una chiave privata, lo stato di elaborazione inviato in risposta è '6A88'.

— Se VU.CHR non corrisponde all'identificativo della chiave pubblica corrente, lo stato di elaborazione inviato in risposta è '6A88'.

— Se la chiave privata selezionata è considerata danneggiata, lo stato di elaborazione inviato in risposta è '6400' o '6581'.

TCS_353 Se il comando INTERNAL AUTHENTICATE ha esito positivo, la chiave di sessione corrente, se presente, viene cancellata e non è più disponibile. Per avere a disposizione una nuova chiave di sessione, il comando EXTERNAL AUTHENTICATE dev'essere eseguito con esito positivo.

3.6.9. ***External Authenticate***

Questo comando è conforme alla norma ISO/IEC 7816-4.

Utilizzando il comando EXTERNAL AUTHENTICATE, la carta può autenticare l'IFD.

Il processo di autenticazione è descritto nell'Appendice 11. Esso prevede le dichiarazioni seguenti.

TCS_354 Il comando EXTERNAL AUTHENTICATE dev'essere immediatamente preceduto da un comando GET CHALLENGE. La carta genera una Challenge all'esterno (RND3).

TCS_355 La verifica del crittogramma utilizza RND3 (Challenge generata dalla carta), la chiave privata della carta (selezionata implicitamente) e la chiave pubblica precedentemente selezionata dal comando MSE.

TCS_356 La carta verifica il crittogramma e, se è corretto, viene aperta la condizione di accesso AUT.

TCS_357 Il crittogramma in ingresso porta il secondo elemento per l'accordo sulla chiave di sessione K2.

TCS_358 Messaggio di comando

Byte	Lunghezza	Valore	Descrizione
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (la chiave pubblica da usare è implicitamente nota ed è stata precedentemente impostata dal comando MSE)
Lc	1	'80h'	Lc (lunghezza dei dati inviati alla carta)
#6-#133	128	'XX..XXh'	Crittogramma (cfr. Appendice 11)

TCS_359 Messaggio di risposta

Byte	Lunghezza	Valore	Descrizione
SW	2	'XXXXh'	Word di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde '9000'.

— Se nell'ambiente di sicurezza non è presente una chiave pubblica, viene inviato in risposta '6A88'.

— Se il CHA della chiave pubblica impostata non è il concatenamento dell'AID dell'applicazione tachigrafica e di un tipo di apparecchio VU, lo stato di elaborazione inviato in risposta è '6F00' (cfr. Appendice 11).

— Se nell'ambiente di sicurezza non è presente una chiave privata, lo stato di elaborazione inviato in risposta è '6A88'.

— Se la verifica del crittogramma è errata, lo stato di elaborazione inviato in risposta è '6688'.

— Se il comando non è immediatamente preceduto da un comando GET CHALLENGE, lo stato di elaborazione inviato in risposta è '6985'.

— Se la chiave privata selezionata è considerata danneggiata, lo stato di elaborazione inviato in risposta è '6400' o '6581'.

TCS_360 Se il comando EXTERNAL AUTHENTICATE ha esito positivo, e se la prima parte della chiave di sessione è resa disponibile da un comando INTERNAL AUTHENTICATE recentemente eseguito con esito positivo, la chiave di sessione viene impostata per i comandi futuri che utilizzano la messaggistica sicura.

TCS_361 Se la prima parte della chiave di sessione non è resa disponibile da un precedente comando INTERNAL AUTHENTICATE, la seconda parte della chiave di sessione, inviata dall'IFD, non viene memorizzata nella carta. Questo meccanismo garantisce che il processo di autenticazione reciproca sia eseguito nell'ordine specificato nell'Appendice 11.

3.6.10. ***Manage Security Environment***

Questo comando è usato per impostare una chiave pubblica a scopo di autenticazione.

Questo comando è conforme alla norma ISO/IEC 7816-8. L'uso del comando è limitato rispetto a quello previsto dalla norma.

TCS_362 La chiave indicata nel campo di dati MSE è valida per ogni file del DF Tachograph.

TCS_363 La chiave indicata nel campo di dati MSE rimane la chiave pubblica corrente fino al successivo comando MSE corretto.

TCS_364 Se la chiave indicata non è (già) presente nella carta, l'ambiente di sicurezza resta invariato.

TCS_365 Messaggio di comando

Byte	Lunghezza	Valore	Descrizione
CLA	1	'00h'	CLA
INS	1	'22h'	INS
P1	1	'C1h'	P1: chiave indicata valida per tutte le operazioni crittografiche
P2	1	'B6h'	P2 (dati indicati riguardanti la firma digitale)
Lc	1	'0Ah'	Lc: lunghezza del campo dati successivo
#6	1	'83h'	Tag per indicare una chiave pubblica in casi asimmetrici
#7	1	'08h'	Lunghezza del riferimento della chiave (identificativo chiave)
#8-#15	08h	'XX..XXh'	Identificativo chiave, secondo quanto specificato nell'Appendice 11

TCS_366 Messaggio di risposta

Byte	Lunghezza	Valore	Descrizione
SW	2	'XXXXh'	Word di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde '9000'.

— Se la chiave indicata non è presente nella carta, lo stato di elaborazione inviato in risposta è '6A88'.

— Se mancano alcuni oggetti di dati attesi nel formato di messaggistica sicura, viene inviato in risposta lo stato di elaborazione '6987'. Ciò si può verificare se manca il tag '83h'.

— Se alcuni oggetti di dati non sono corretti, lo stato di elaborazione inviato in risposta è '6988'. Ciò si può verificare se la lunghezza dell'identificativo della chiave è diversa da '08h'.

— Se la chiave selezionata è considerata danneggiata, lo stato di elaborazione inviato in risposta è '6400' o '6581'.

3.6.11. ***PSO: Hash***

Questo comando si usa per trasferire alla carta il risultato del calcolo di una funzione hash di alcuni dati. Questo comando è usato per verificare le firme digitali. Il valore hash è memorizzato in EEPROM per il successivo comando di verifica di una firma digitale.

Questo comando è conforme alla norma ISO/IEC 7816-8. L'uso del comando è limitato rispetto a quello previsto dalla norma.

TCS_367 Messaggio di comando

Byte	Lunghezza	Valore	Descrizione
CLA	1	'00h'	CLA
INS	1	'2Ah'	Esecuzione operazione di sicurezza
P1	1	'90h'	Risposta codice hash
P2	1	'A0h'	Tag: il campo dati contiene DO interessati alla funzione hash
Lc	1	'16h'	Lc lunghezza del campo di dati successivo
#6	1	'90h'	Tag per il codice hash
#7	1	'14h'	Lunghezza del codice hash
#8-#27	20	'XX..XXh'	Codice hash

TCS_368 Messaggio di risposta

Byte	Lunghezza	Valore	Descrizione
SW	2	'XXXXh'	Word di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde '9000'.

— Se mancano alcuni oggetti di dati attesi (secondo quanto sopra specificato), viene inviato in risposta lo stato di elaborazione '6987'. Ciò si può verificare se manca uno dei tag '90h'.

— Se alcuni oggetti di dati non sono corretti, lo stato di elaborazione inviato in risposta è '6988'. Questo errore si verifica se il tag richiesto è presente, ma con una lunghezza diversa da '14h'.

3.6.12. ***Perform Hash of File***

Questo comando non è conforme alla norma ISO/IEC 7816-8. Pertanto il byte CLA di questo comando indica che il comando PERFORM SECURITY OPERATION/HASH viene utilizzato in modo esclusivo e riservato.

TCS_369 Il comando PERFORM HASH OF FILE è usato per eseguire la funzione hash dell'area di dati dell'EF trasparente selezionato.

TCS_370 Il risultato dell'operazione hash è memorizzato nella carta. Può poi essere utilizzato per ottenere una firma digitale del file, utilizzando il comando PSO: COMPUTE DIGITAL SIGNATURE. Questo risultato resta disponibile per il comando COMPUTE DIGITAL SIGNATURE fino al successivo comando PERFORM HASH OF FILE eseguito con esito positivo.

TCS_371 Messaggio di comando

Byte	Lunghezza	Valore	Descrizione
CLA	1	'80h'	CLA
INS	1	'2Ah'	Esecuzione operazione di sicurezza
P1	1	'90h'	Tag: Hash
P2	1	'00h'	P2: esecuzione della funzione hash dei dati del file trasparente selezionato

TCS_372 Messaggio di risposta

Byte	Lunghezza	Valore	Descrizione
SW	2	'XXXXh'	Word di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde '9000'.

— Se non è selezionata un'applicazione, viene inviato in risposta lo stato di elaborazione '6985'.

— Se l'EF selezionato è considerato danneggiato (errori d'integrità negli attributi del file o nei dati registrati), lo stato di elaborazione inviato in risposta è '6400' o '6581'.

— Se il file selezionato non è un file trasparente, lo stato di elaborazione inviato in risposta è '6986'.

3.6.13. ***PSO: Compute Digital Signature***

Questo comando è usato per calcolare la firma digitale del codice hash precedentemente calcolato (cfr. PERFORM HASH OF FILE, paragrafo 3.6.12).

Questo comando è conforme alla norma ISO/IEC 7816-8. L'uso del comando è limitato rispetto a quello previsto dalla norma.

TCS_373 La chiave privata della carta è usata per calcolare la firma digitale ed è implicitamente nota alla carta.

TCS_374 La carta esegue una firma digitale utilizzando un metodo di riempimento conforme a PKCS1 (cfr. Appendice 11 per ulteriori particolari).

TCS_375 Messaggio di comando

Byte	Lunghezza	Valore	Descrizione
CLA	1	'00h'	CLA
INS	1	'2Ah'	Esecuzione operazione di sicurezza
P1	1	'9Eh'	Firma digitale da inviare in risposta
P2	1	'9Ah'	Tag: il campo di dati contiene dati da firmare. Poiché non è incluso un campo di dati, i dati sono considerati già presenti nella carta (hash del file)
Le	1	'80h'	Lunghezza della firma attesa

TCS_376 Messaggio di risposta

Byte	Lunghezza	Valore	Descrizione
#1-#128	128	'XX..XXh'	Firma dell'hash precedentemente calcolato
SW	2	'XXXXh'	Word di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde '9000'.

— Se la chiave privata implicitamente selezionata è considerata danneggiata, lo stato di elaborazione inviato in risposta è '6400' o '6581'.

3.6.14. ***PSO: Verify Digital Signature***

Questo comando si usa per verificare la firma digitale, fornita come un ingresso, conformemente al PKCS1 di un messaggio, il cui hash è noto alla carta. L'algoritmo della firma è implicitamente noto alla carta.

Questo comando è conforme alla norma ISO/IEC 7816-8. L'uso del comando è limitato rispetto a quello previsto dalla norma.

TCS_377 Il comando VERIFY DIGITAL SIGNATURE usa sempre la chiave pubblica selezionata dal precedente comando MANAGE SECURITY ENVIRONMENT e il codice hash precedente inserito da un comando PSO: HASH.

TCS_378 Messaggio di comando

Byte	Lunghezza	Valore	Descrizione
CLA	1	'00h'	CLA
INS	1	'2Ah'	Esecuzione operazione di sicurezza
P1	1	'00h'	
P2	1	'A8h'	Tag: il campo dati contiene DO interessati alla verifica
Lc	1	'83h'	Lunghezza Lc del campo di dati successivo
#28	1	'9Eh'	Tag per la firma digitale
#29-#30	2	'8180h'	Lunghezza della firma digitale (128 byte, codificati secondo la norma ISO/IEC 7816-6)
#31-#158	128	'XX..XXh'	Contenuto della firma digitale

TCS_379 Messaggio di risposta

Byte	Lunghezza	Valore	Descrizione
SW	2	'XXXXh'	Word di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde '9000'.

— Se la verifica della firma fallisce, lo stato di elaborazione inviato in risposta è '6688'. Il processo di verifica è descritto nell'Appendice 11.

— Se non è selezionata una chiave pubblica, lo stato di elaborazione inviato in risposta è '6A88'.

— Se mancano alcuni oggetti di dati attesi (secondo quanto sopra specificato), viene inviato in risposta lo stato di elaborazione '6987'. Ciò si può verificare se manca uno dei tag richiesti.

— Se non è disponibile un codice hash per elaborare il comando (in conseguenza di un comando PSO: HASH precedente), lo stato di elaborazione inviato in risposta è '6985'.

— Se alcuni oggetti di dati non sono corretti, lo stato di elaborazione inviato in risposta è '6988'. Ciò si può verificare se la lunghezza di uno degli oggetti di dati richiesti non è corretta.

— Se la chiave pubblica selezionata è considerata danneggiata, lo stato di elaborazione inviato in risposta è '6400' o '6581'.

4. STRUTTURA DELLE CARTE TACHIGRAFICHE

Il presente paragrafo specifica le strutture dei file delle carte tachigrafiche per la memorizzazione di dati accessibili.

Non specifica le strutture interne, che dipendono dal fabbricante della carta, come per esempio le intestazioni dei file, né la memorizzazione e la gestione degli elementi di dati necessari solo per l'uso interno, quali `EuropeanPublicKey`, `CardPrivateKey`, `TDesSessionKey` o `WorkshopCardPin`.

La capacità utile di memorizzazione delle carte tachigrafiche è di 11 kbytes minimo. Si possono usare capacità maggiori. In tal caso, la struttura della carta rimane invariata, ma aumenta il numero di registrazioni di alcuni elementi della struttura. Questo paragrafo specifica i valori minimi e massimi di tale numero di registrazioni.

4.1. **Struttura della carta del conducente**

TCS_400 Dopo la personalizzazione, la carta del conducente deve presentare la struttura dei file e le condizioni di accesso permanenti indicate qui di seguito.

File	File ID	Condizioni di accesso		
		Lettura	Aggiornamento	Crittato
MF	3F00			
├─EF ICC	0002	ALW	NEV	No
├─EF IC	0005	ALW	NEV	No
└─DF Tachograph	0500			
├─EF Application_Identification	0501	ALW	NEV	No
├─EF Card_Certificate	C100	ALW	NEV	No
├─EF CA_Certificate	C108	ALW	NEV	No
├─EF Identification	0520	ALW	NEV	No
├─EF Card_Download	050E	ALW	ALW	No
├─EF Driving_Licence_Info	0521	ALW	NEV	No
├─EF Events_Data	0502	ALW	PRO SM / AUT	No
├─EF Faults_Data	0503	ALW	PRO SM / AUT	No
├─EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	No
├─EF Vehicles_Used	0505	ALW	PRO SM / AUT	No
├─EF Places	0506	ALW	PRO SM / AUT	No
├─EF Current_Usage	0507	ALW	PRO SM / AUT	No
├─EF Control_Activity_Data	0508	ALW	PRO SM / AUT	No
└─EF Specific_Conditions	0522	ALW	PRO SM / AUT	No

TCS_401 Le strutture di tutti gli EF devono essere trasparenti.

TCS_402 La lettura con messaggistica sicura deve essere possibile per tutti i file sotto il DF Tachograph.

TCS_403 La carta del conducente deve presentare la seguente struttura dei dati:

File/Elemento di dati	N. di registrazioni	Dimensione (byte) Min	Dimensione (byte) Max	Valori predefiniti
MF		*11411*	*24959*	
╠═EF ICC		*25*	*25*	
╚═CardIccIdentification		*25*	*25*	
├─clockStop		1	1	{00}
├─cardExtendedSerialNumber		8	8	{00..00}
├─cardApprovalNumber		8	8	{20..20}
├─cardPersonaliserID		1	1	{00}
├─embedderIcAssemblerId		5	5	{00..00}
└─icIdentifier		2	2	{00 00}
╠═EF IC		*8*	*8*	
╚═CardChipIdentification		*8*	*8*	
├─icSerialNumber		4	4	{00..00}
└─icManufacturingReferences		4	4	{00..00}
╚═DF Tachograph		*11378*	*24926*	
╠═EF Application_Identification		*10*	*10*	
╚═DriverCardApplicationIdentification		*10*	*10*	
├─typeOfTachographCardId		1	1	{00}
├─cardStructureVersion		2	2	{00 00}
├─noOfEventsPerType		1	1	{00}
├─noOfFaultsPerType		1	1	{00}
├─activityStructureLength		2	2	{00 00}
├─noOfCardVehicleRecords		2	2	{00 00}
└─noOfCardPlaceRecords		1	1	{00}
╠═EF Card_Certificate		*194*	*194*	
╚═CardCertificate		194	194	{00..00}
╠═EF CA_Certificate		*194*	*194*	
╚═MemberStateCertificate		194	194	{00..00}
╠═EF Identification		*143*	*143*	
├─CardIdentification		*65*	*65*	
├─cardIssuingMemberState		1	1	{00}
├─cardNumber		16	16	{20..20}
├─cardIssuingAuthorityName		36	36	{20..20}
├─cardIssueDate		4	4	{00..00}
├─cardValidityBegin		4	4	{00..00}
└─cardExpiryDate		4	4	{00..00}
└─DriverCardHolderIdentification		*78*	*78*	
├─cardHolderName		*72*	*72*	
├─holderSurname		36	36	{00, 20..20}
└─holderFirstNames		36	36	{00, 20..20}
├─cardHolderBirthDate		4	4	{00..00}
└─cardHolderPreferredLanguage		2	2	{20 20}

EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*864*	*1728*	
CardEventData		*864*	*1728*	
cardEventRecords	6	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
CardDriverActivity		*5548*	*13780*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*2606*	*6202*	
CardVehiclesUsed		*2606*	*6202*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*2604*	*6200*	
CardVehicleRecord	n_3	*31*	*31*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
EF Places		*841*	*1121*	
CardPlaceDailyWorkPeriod		*841*	*1121*	
placePointerNewestRecord		1	1	{00}
placeRecords		*840*	*1120*	
PlaceRecord	n_4	*10*	*10*	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
CardCurrentUse		*19*	*19*	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*280*	*280*	
SpecificConditionRecord	56	*5*	*5*	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

TCS_404 I valori sotto indicati, usati per fornire le dimensioni nella tabella precedente, sono i valori minimo e massimo del numero di registrazioni che la struttura dei dati della carta del conducente deve utilizzare:

		Min	Max
n_1	NoOfEventsPerType	**6**	12
n_2	NoOfFaultsPerType	**12**	24
n_3	NoOfCardVehicleRecords	**84**	200
n_4	NoOfCardPlaceRecords	**84**	112
n_6	CardActivityLengthRange	5544 byte (28 giorni * 93 cambi di attività)	13776 byte (28 giorni * 240 cambi di attività)

4.2. **Struttura della carta dell'officina**

TCS_405 Dopo la personalizzazione, la carta dell'officina deve presentare la struttura dei file e le condizioni di accesso permanenti indicate qui di seguito.

		Condizioni di accesso		
File	ID file	Lettura	Aggiornamento	Crittato
MF	3F00			
├─EF ICC	0002	ALW	NEV	No
├─EF IC	0005	ALW	NEV	No
└─DF Tachograph	0500			
├─EF Application_Identification	0501	ALW	NEV	No
├─EF Card_Certificate	C100	ALW	NEV	No
├─EF CA_Certificate	C108	ALW	NEV	No
├─EF Identification	0520	ALW	NEV	No
├─EF Card_Download	0509	ALW	ALW	No
├─EF Calibration	050A	ALW	PRO SM / AUT	No
├─EF Sensor_Installation_Data	050B	ALW	NEV	Sì
├─EF Events_Data	0502	ALW	PRO SM / AUT	No
├─EF Faults_Data	0503	ALW	PRO SM / AUT	No
├─EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	No
├─EF Vehicles_Used	0505	ALW	PRO SM / AUT	No
├─EF Places	0506	ALW	PRO SM / AUT	No
├─EF Current_Usage	0507	ALW	PRO SM / AUT	No
├─EF Control_Activity_Data	0508	ALW	PRO SM / AUT	No
└─EF Specific_Conditions	0522	ALW	PRO SM / AUT	No

TCS_406 Le strutture di tutti gli EF devono essere trasparenti.

TCS_407 La lettura con messaggistica sicura deve essere possibile per tutti i file sotto il DF Tachograph.

TCS_408 La carta dell'officina deve presentare la seguente struttura dei dati:

File/Elemento di dati	N. di registrazioni	Dimensioni (byte) Min	Dimensioni (byte) Max	Valori predefiniti
MF		*11088*	*29061*	
├─EF ICC		*25*	*25*	
│ └─CardIccIdentification		*25*	*25*	
│ ├─clockStop		1	1	{00}
│ ├─cardExtendedSerialNumber		8	8	{00..00}
│ ├─cardApprovalNumber		8	8	{20..20}
│ ├─cardPersonaliserID		1	1	{00}
│ ├─embedderIcAssemblerId		5	5	{00..00}
│ └─icIdentifier		2	2	{00 00}
├─EF IC		*8*	*8*	
│ └─CardChipIdentification		*8*	*8*	
│ ├─icSerialNumber		4	4	{00..00}
│ └─icManufacturingReferences		4	4	{00..00}
└─DF Tachograph		*11055*	*29028*	
├─EF Application_Identification		*11*	*11*	
│ └─WorkshopCardApplicationIdentification		*11*	*11*	
│ ├─typeOfTachographCardId		1	1	{00}
│ ├─cardStructureVersion		2	2	{00 00}
│ ├─noOfEventsPerType		1	1	{00}
│ ├─noOfFaultsPerType		1	1	{00}
│ ├─activityStructureLength		2	2	{00 00}
│ ├─noOfCardVehicleRecords		2	2	{00 00}
│ ├─noOfCardPlaceRecords		1	1	{00}
│ └─noOfCalibrationRecords		1	1	{00}

═EF Card_Certificate		*194*	*194*	
└CardCertificate		194	194	{00..00}
═EF CA_Certificate		*194*	*194*	
└MemberStateCertificate		194	194	{00..00}
═EF Identification		*211*	*211*	
├CardIdentification		*65*	*65*	
├cardIssuingMemberState		1	1	{00}
├cardNumber		16	16	{20..20}
├cardIssuingAuthorityName		36	36	{00, 20..20}
├cardIssueDate		4	4	{00..00}
├cardValidityBegin		4	4	{00..00}
└cardExpiryDate		4	4	{00..00}
└WorkshopCardHolderIdentification		*146*	*146*	
├workshopName		36	36	{00, 20..20}
├workshopAddress		36	36	{00, 20..20}
├cardHolderName				
├holderSurname		36	36	{00, 20..20}
└holderFirstNames		36	36	{00, 20..20}
└cardHolderPreferredLanguage		2	2	{20 20}
═EF Card_Download		*2*	*2*	
└NoOfCalibrationsSinceDownload		2	2	{00 00}
═EF Calibration		*9243*	*26778*	
└WorkshopCardCalibrationData		*9243*	*26778*	
├calibrationTotalNumber		2	2	{00 00}
├calibrationPointerNewestRecord		1	1	{00}
└calibrationRecords		*9240*	*26775*	
└WorkshopCardCalibrationRecord	n_5	*105*	*105*	
├calibrationPurpose		1	1	{00}
├vehicleIdentificationNumber		17	17	{20..20}
├vehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├wVehicleCharacteristicConstant		2	2	{00 00}
├kConstantOfRecordingEquipment		2	2	{00 00}
├lTyreCircumference		2	2	{00 00}
├tyreSize		15	15	{20..20}
├authorisedSpeed		1	1	{00}
├oldOdometerValue		3	3	{00..00}
├newOdometerValue		3	3	{00..00}
├oldTimeValue		4	4	{00..00}
├newTimeValue		4	4	{00..00}
├nextCalibrationDate		4	4	{00..00}
├vuPartNumber		16	16	{20..20}
├vuSerialNumber		8	8	{00..00}
└sensorSerialNumber		8	8	{00..00}
═EF Sensor_Installation_Data		*16*	*16*	
└SensorInstallationSecData		16	16	{00..00}
═EF Events_Data		*432*	*432*	
└CardEventData		*432*	*432*	
└cardEventRecords	6	*72*	*72*	
└CardEventRecord	n_1	*24*	*24*	
├eventType		1	1	{00}
├eventBeginTime		4	4	{00..00}
├eventEndTime		4	4	{00..00}
└eventVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
═EF Faults_Data		*288*	*288*	
└CardFaultData		*288*	*288*	
└cardFaultRecords	2	*144*	*144*	
└CardFaultRecord	n_2	*24*	*24*	
├faultType		1	1	{00}
├faultBeginTime		4	4	{00..00}
├faultEndTime		4	4	{00..00}
└faultVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
═EF Driver_Activity_Data		*202*	*496*	
└CardDriverActivity		*202*	*496*	
├activityPointerOldestDayRecord		2	2	{00 00}
├activityPointerNewestRecord		2	2	{00 00}
└activityDailyRecords	n_6	198	492	{00..00}
═EF Vehicles_Used		*126*	*250*	
└CardVehiclesUsed		*126*	*250*	
├vehiclePointerNewestRecord		2	2	{00 00}
└cardVehicleRecords		*124*	*248*	
├CardVehicleRecord	n_3	*31*	*31*	
├vehicleOdometerBegin		3	3	{00..00}

├─vehicleOdometerEnd		3	3	{00..00}
├─vehicleFirstUse		4	4	{00..00}
├─vehicleLastUse		4	4	{00..00}
├─vehicleRegistration				
│ ├─vehicleRegistrationNation		1	1	{00}
│ └─vehicleRegistrationNumber		14	14	{00, 20..20}
└─vuDataBlockCounter		2	2	{00 00}
═EF Places		*61*	*81*	
└─CardPlaceDailyWorkPeriod		*61*	*81*	
├─placePointerNewestRecord		1	1	{00}
└─placeRecords		*60*	*80*	
└─PlaceRecord	n_4	*10*	*10*	
├─entryTime		4	4	{00..00}
├─entryTypeDailyWorkPeriod		1	1	{00}
├─dailyWorkPeriodCountry		1	1	{00}
├─dailyWorkPeriodRegion		1	1	{00}
└─vehicleOdometerValue		3	3	{00..00}
═EF Current_Usage		*19*	*19*	
└─CardCurrentUse		*19*	*19*	
├─sessionOpenTime		4	4	{00..00}
└─sessionOpenVehicle				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
═EF Control_Activity_Data		*46*	*46*	
└─CardControlActivityDataRecord		*46*	*46*	
├─controlType		1	1	{00}
├─controlTime		4	4	{00..00}
├─controlCardNumber				
│ ├─cardType		1	1	{00}
│ ├─cardIssuingMemberState		1	1	{00}
│ └─cardNumber		16	16	{20..20}
├─controlVehicleRegistration				
│ ├─vehicleRegistrationNation		1	1	{00}
│ └─vehicleRegistrationNumber		14	14	{00, 20..20}
├─controlDownloadPeriodBegin		4	4	{00..00}
└─controlDownloadPeriodEnd		4	4	{00..00}
═EF Specific_Conditions		*10*	*10*	
└─SpecificConditionRecord	2	*5*	*5*	
├─entryTime		4	4	{00..00}
└─SpecificConditionType		1	1	{00}

TCS_409 I valori sotto indicati, usati per fornire le dimensioni nella tabella precedente, sono i valori minimo e massimo del numero di registrazioni che la struttura dei dati della carta dell'officina deve utilizzare:

		Min	Max
n_1	NoOfEventsPerType	**3**	3
n_2	NoOfFaultsPerType	**6**	6
n_3	NoOfCardVehicleRecords	**4**	8
n_4	NoOfCardPlaceRecords	**6**	8
n_6	CardActivityLengthRange	88	255
n_5	NoOfCalibrationRecords	198 byte (1 giorno * 93 cambi di attività)	492 byte (1 giorno * 240 cambi di attività)

4.3. **Struttura della carta di controllo**

TCS_410 Dopo la personalizzazione, la carta di controllo deve presentare la struttura dei file e le condizioni di accesso permanenti indicate qui di seguito.

		Condizioni di accesso		
File	ID file	Lettura	Aggiornamento	Crittato
MF	3F00			
├─EF ICC	0002	ALW	NEV	No
├─EF IC	0005	ALW	NEV	No
└─DF Tachograph	0500			
├─EF Application_Identification	0501	ALW	NEV	No
├─EF Card_Certificate	C100	ALW	NEV	No
├─EF CA_Certificate	C108	ALW	NEV	No
├─EF Identification	0520	AUT	NEV	No
└─EF Controller_Activity_Data	050C	ALW	PRO SM / AUT	No

TCS_411 Le strutture di tutti gli EF devono essere trasparenti.

TCS_412 La lettura con messaggistica sicura deve essere possibile per tutti i file sotto il DF Tachograph.

TCS_413 La carta di controllo deve presentare la struttura dei dati seguente:

File/Elemento di dati	N. di registrazioni	Dimensioni (byte) Min	Dimensioni (byte) Max	Valori predefiniti
MF		*11219*	*24559*	
╠═EF ICC		*25*	*25*	
╠═└─CardIccIdentification		*25*	*25*	
╠═├─clockStop		1	1	{00}
╠═├─cardExtendedSerialNumber		8	8	{00..00}
╠═├─cardApprovalNumber		8	8	{20..20}
╠═├─cardPersonaliserID		1	1	{00}
╠═├─embedderIcAssemblerId		5	5	{00..00}
╠═└─icIdentifier		2	2	{00 00}
╠═EF IC		*8*	*8*	
╠═└─CardChipIdentification		*8*	*8*	
╠═├─icSerialNumber		4	4	{00..00}
╠═└─icManufacturingReferences		4	4	{00..00}
╚═DF Tachograph		*11186*	*24526*	
═══╠═EF Application_Identification		*5*	*5*	
═══╠═└─ControlCardApplicationIdentification		*5*	*5*	
═══╠═├─typeOfTachographCardId		1	1	{00}
═══╠═├─cardStructureVersion		2	2	{00 00}
═══╠═└─noOfControlActivityRecords		2	2	{00 00}
═══╠═EF Card_Certificate		*194*	*194*	
═══╠═└─CardCertificate		194	194	{00..00}
═══╠═EF CA_Certificate		*194*	*104*	
═══╠═└─MemberStateCertificate		194	104	{00..00}
═══╠═EF Identification		*211*	*211*	
═══╠═├─CardIdentification		*65*	*65*	
═══╠═│ ├─cardIssuingMemberState		1	1	{00}
═══╠═│ ├─cardNumber		16	16	{20..20}
═══╠═│ ├─cardIssuingAuthorityName		36	36	{00, 20..20}
═══╠═│ ├─cardIssueDate		4	4	{00..00}
═══╠═│ ├─cardValidityBegin		4	4	{00..00}
═══╠═│ └─cardExpiryDate		4	4	{00..00}
═══╠═└─ControlCardHolderIdentification		*146*	*146*	
═══╠═ ├─controlBodyName		36	36	{00, 20..20}
═══╠═ ├─controlBodyAddress		36	36	{00, 20..20}
═══╠═ ├─cardHolderName				
═══╠═ │ ├─holderSurname		36	36	{00, 20..20}
═══╠═ │ └─holderFirstNames		36	36	{00, 20..20}
═══╠═ └─cardHolderPreferredLanguage		2	2	{20 20}
═══╚═EF Controller_Activity_Data		*10582*	*23922*	
═══════└─ControlCardControlActivityData		*10582*	*23922*	
═══════ ├─controlPointerNewestRecord		2	2	{00 00}
═══════ └─controlActivityRecords		*10580*	*23920*	
═══════ └─controlActivityRecord	n_7	*46*	*46*	
═══════ ├─controlType		1	1	{00}
═══════ ├─controlTime		4	4	{00..00}
═══════ ├─controlledCardNumber				
═══════ │ ├─cardType		1	1	{00}
═══════ │ ├─cardIssuingMemberState		1	1	{00}
═══════ │ └─cardNumber		16	16	{20..20}
═══════ ├─controlledVehicleRegistration				
═══════ │ ├─vehicleRegistrationNation		1	1	{00}
═══════ │ └─vehicleRegistrationNumber		14	14	{00, 20..20}
═══════ ├─controlDownloadPeriodBegin		4	4	{00..00}
═══════ └─controlDownloadPeriodEnd		4	4	{00..00}

TCS_414 I valori sotto indicati, usati per fornire le dimensioni nella tabella precedente, sono i valori minimo e massimo del numero di registrazioni che la struttura dei dati della carta di controllo deve utilizzare:

		Min	Max
n_7	NoOfControlActivityRecords	230	520

4.4. **Struttura della carta dell'azienda**

TCS_415 Dopo la personalizzazione, la carta dell'azienda deve presentare la struttura dei file e le condizioni di accesso permanenti indicate qui di seguito.

File	ID file	Condizioni di accesso		
		Lettura	Aggiornamento	Crittato
MF	3F00			
├─EF ICC	0002	ALW	NEV	No
├─EF IC	0005	ALW	NEV	No
└─DF Tachograph	0500			
├─EF Application_Identification	0501	ALW	NEV	No
├─EF Card_Certificate	C100	ALW	NEV	No
├─EF CA_Certificate	C108	ALW	NEV	No
├─EF Identification	0520	AUT	NEV	No
└─EF Company_Activity_Data	050D	ALW	PRO SM / AUT	No

TCS_416 Le strutture di tutti gli EF devono essere trasparenti.

TCS_417 La lettura con messaggistica sicura deve essere possibile per tutti i file sotto il DF Tachograph.

TCS_418 La carta dell'azienda deve presentare la struttura dei dati seguente:

File/Elemento di dati	N. di registrazioni	Dimensioni (byte) Min	Dimensioni (byte) Max	Valori predefiniti
MF		*11147*	*24487*	
├═EF ICC		*25*	*25*	
│ └─CardIccIdentification		*25*	*25*	
│ ├─clockStop		1	1	{00}
│ ├─cardExtendedSerialNumber		8	8	{00..00}
│ ├─cardApprovalNumber		8	8	{20..20}
│ ├─cardPersonaliserID		1	1	{00}
│ ├─embedderIcAssemblerId		5	5	{00..00}
│ └─icIdentifier		2	2	{00 00}
├═EF IC		*8*	*8*	
│ └─CardChipIdentification		*8*	*8*	
│ ├─icSerialNumber		4	4	{00..00}
│ └─icManufacturingReferences		4	4	{00..00}
└═DF Tachograph		*11114*	*24454*	
├═EF Application_Identification		*5*	*5*	
│ └─CompanyCardApplicationIdentification		*5*	*5*	
│ ├─typeOfTachographCardId		1	1	{00}
│ ├─cardStructureVersion		2	2	{00 00}
│ └─noOfCompanyActivityRecords		2	2	{00 00}
├═EF Card_Certificate		*194*	*194*	
│ └─CardCertificate		194	194	{00..00}
├═EF CA_Certificate		*194*	*194*	
│ └─MemberStateCertificate		194	194	{00..00}
├═EF Identification		*139*	*139*	
│ ├─CardIdentification		*65*	*65*	
│ ├─cardIssuingMemberState		1	1	{00}
│ ├─cardNumber		16	16	{20..20}
│ ├─cardIssuingAuthorityName		36	36	{00, 20..20}
│ ├─cardIssueDate		4	4	{00..00}
│ ├─cardValidityBegin		4	4	{00..00}
│ └─cardExpiryDate		4	4	{00..00}
│ └─CompanyCardHolderIdentification		*74*	*74*	
│ ├─companyName		36	36	{00, 20..20}
│ ├─companyAddress		36	36	{00, 20..20}
│ └─cardHolderPreferredLanguage		2	2	{20 20}
└═EF Company_Activity_Data		*10582*	*23922*	
└─CompanyActivityData		*10582*	*23922*	
├─companyPointerNewestRecord		2	2	{00 00}
└─companyActivityRecords		*10580*	*23920*	
└─companyActivityRecord	n_8	46	46	
├─companyActivityType		1	1	{00}
├─companyActivityTime		4	4	{00..00}
├─cardNumberInformation				
├─cardType		1	1	{00}
├─cardIssuingMemberState		1	1	{00}
└─cardNumber		16	16	{20..20}
├─vehicleRegistrationInformation				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}

├─cardNumberInformation			
│ ├─cardType	1	1	{00}
│ ├─cardIssuingMemberState	1	1	{00}
│ └─cardNumber	16	16	{20..20}
├─downloadPeriodBegin	4	4	{00..00}
└─downloadPeriodEnd	4	4	{00..00}

I valori sotto indicati, usati per fornire le dimensioni nella tabella precedente, sono i valori minimo e massimo del numero di registrazioni che la struttura dei dati della carta dell'azienda deve utilizzare:

		Min	Max
n_8	NoOfCompanyActivityRecords	230	520

Appendice 3

PITTOGRAMMI

PIC_001 L'apparecchio di controllo può usare i pittogrammi e le combinazioni di pittogrammi seguenti:

1. PITTOGRAMMI DI BASE

	Persone	**Interventi**	**Modalità di funzionamento**
	Azienda		Modo azienda
	Controllo	Controllo	Modo controllo
	Conducente	Guida	Modo funzionamento
	Officina/Centro di prova	Controllo/Calibratura	Modo calibratura
	Fabbricante		

	Attività	**Durata**
	Disponibile	Periodo di disponibilità in corso
	Guida	Periodo di guida continuo
	Riposo	Periodo di riposo in corso
	Lavoro	Periodo di lavoro in corso
	Interruzione	Periodo cumulato di interruzione
?	Non noto	

	Apparecchio	**Funzioni**
1	Sede (slot) «conducente»	
2	Sede (slot) «secondo conducente»	
	Carta	
	Orologio	
	Dispositivo di visualizzazione	Visualizzazione
	Memorizzazione esterna	Trasferimento dati
	Alimentazione di energia	
	Stampante/Documento stampato	Stampa
	Sensore	
	Dimensioni dei pneumatici	
	Veicolo/Unità elettronica di bordo	

	Condizioni particolari
OUT	Escluso dal campo di applicazione
	Attraversamento mediante traghetto/treno

	Varie		
!	Anomalie		Guasti
	Inizio del periodo di lavoro giornaliero		Temine del periodo di lavoro giornaliero
	Località	M	Immissione manuale delle attività del conducente
	Sicurezza		Velocità
	Ora	Σ	Totale / Riepilogo

	Indicatori
24h	Giornaliero
|	Settimanale
||	Quindicinale
	Da/A

2. COMBINAZIONI DI PITTOGRAMMI

	Varie		
	Luogo di controllo		
	Luogo in cui termina il periodo di lavoro		Luogo in cui inizia il periodo di lavoro giornaliero
	Dalle ore		Alle ore
	Dal veicolo		
OUT	Inizio «Escluso dal campo di applicazione»	OUT	Termine «Escluso dal campo di applicazione»

Carte

Carta del conducente
Carta dell'azienda
Carta di controllo
Carta dell'officina
Carta assente

Guida

Guida con equipaggio
Periodo di guida per una settimana
Periodo di guida per due settimane

Documenti stampati

Stampa giornaliera delle attività del conducente contenute nella carta
Stampa giornaliera delle attività del conducente contenute nella VU
Stampa di anomalie e guasti contenuti nella carta
Stampa di anomalie e guasti contenuti nella VU
Stampa dei dati tecnici
Stampa dei superamenti di velocità

Anomalie

Inserimento di una carta non valida
Conflitto di carte
Sovrapposizione di orari
Guida in assenza di una carta adeguata
Inserimento carta durante la guida
Chiusura errata ultima sessione carta
Superamento di velocità
Interruzione dell'alimentazione di energia
Errore dati di movimento
Violazione della sicurezza
Regolazione dell'ora (in officina)
Controllo superamento di velocità

Guasti

Guasto della carta [sede (slot) «conducente»]
Guasto della carta [sede (slot) «secondo conducente»]
Guasto del dispositivo di visualizzazione
Guasto nel trasferimento di dati
Guasto della stampante
Guasto del sensore
Guasto all'interno della VU

Procedura di immissione manuale

Stesso periodo di lavoro giornaliero?
Termine del periodo di lavoro precedente?
Conferma o immissione del luogo in cui termina il periodo di lavoro
Immissione ora di inizio
Immissione del luogo in cui inizia il periodo di lavoro

Nota: All'appendice 4 sono definite alcune combinazioni di pittogrammi supplementari per creare blocchi di stampa o identificazioni delle registrazioni.

Appendice 4

DOCUMENTI STAMPATI

INDICE

1. PRESCRIZIONI GENERALI

Ogni documento stampato è realizzato mediante il concatenamento di diversi blocchi di dati, possibilmente identificati da un'identificazione di blocco.

Un blocco di dati contiene una o più registrazioni, possibilmente identificate da un'identificazione di registrazione.

PRT_001 Se un'identificazione di blocco precede direttamente un'identificazione di registrazione, quest'ultima non viene stampata.

PRT_002 Nel caso in cui un elemento dei dati non sia noto, o non debba essere stampato per motivi riguardanti i diritti di accesso ai dati, al suo posto vengono stampati degli spazi.

PRT_003 Se il contenuto di un'intera riga non è noto, o non deve essere stampato, la riga viene omessa.

PRT_004 I campi contenenti dati numerici sono stampati con l'allineamento a destra, con le migliaia e i milioni separati da uno spazio e senza zeri iniziali.

PRT_005 I campi contenenti dati in sequenza sono stampati con l'allineamento a sinistra e riempiti da spazi fino a coprire l'intera lunghezza dell'elemento di dati o, se necessario, troncati in corrispondenza di tale lunghezza (nomi e indirizzi).

2. SPECIFICHE DEI BLOCCHI DI DATI

Nel presente capitolo sono stati usati i seguenti segni grafici convenzionali:

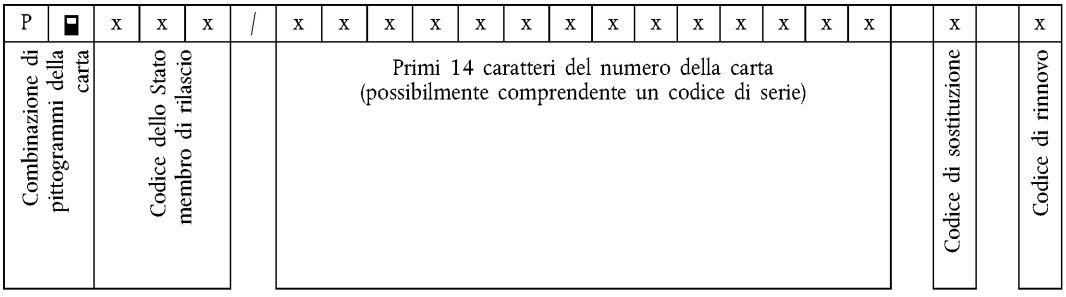
— i caratteri in *grassetto* indicano il testo normale da stampare (la stampa produce caratteri normali),

— i caratteri normali indicano le variabili (pittogrammi o dati), da sostituire con i rispettivi valori nella stampa,

— i nomi delle variabili sono integrati da caratteri di sottolineatura per indicare la lunghezza dell'elemento di dati disponibile per la variabile,

— le date sono indicate nel formato "gg/mm/aaaa" (giorno, mese, anno); si può anche usare il formato "gg.mm.aaaa",

— con l'espressione "identificazione della carta" s'intende un elemento così composto: tipo di carta dato da una combinazione di pittogrammi della carta, il codice dello Stato membro che ha rilasciato la carta, una barra e il numero della carta con i codici di sostituzione e di rinnovo separati da uno spazio:



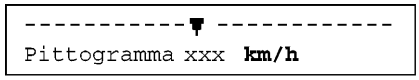
PRT_006 I documenti stampati usano i blocchi di dati e/o le registrazioni di dati sotto riportati, in base ai significati e formati seguenti:

Numero del blocco o della registrazione Significato	Formato dei dati
1 **Data e ora di stampa del documento**	gg/mm/aaaa hh:mm **(UTC)**

2 **Tipo di documento stampato**

Identificazione del blocco

Combinazione di pittogrammi del documento stampato (cfr. appendice 3), Regolazione del limitatore di velocità (solo per la stampa dei superamenti di velocità)



3 **Identificazione del titolare della carta**

Identificazione del blocco P = pittogramma persone

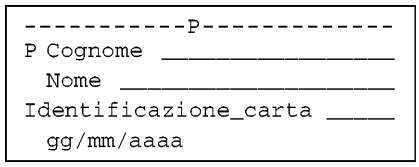
Cognome del titolare

Nome/i del titolare (se presente)

Identificazione della carta

Data di scadenza della carta (se presente)

Nel caso di una carta non personale, che non contiene il cognome del titolare, viene invece stampato il nome dell'impresa, dell'officina o dell'organismo di controllo

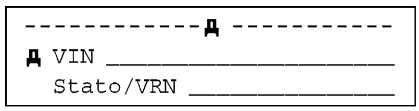


4 **Identificazione del veicolo**

Identificazione del blocco

VIN

Stato membro di immatricolazione e VRN

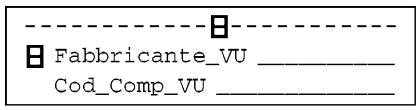


5 **Identificazione della VU**

Identificazione del blocco

Nome del fabbricante della VU

Codice componente della VU



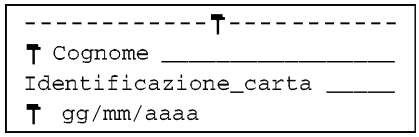
6 **Ultima calibratura dell'apparecchio di controllo**

Identificazione del blocco

Nome dell'officina

Identificazione della carta dell'officina

Data della calibratura



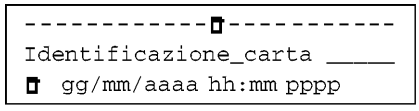
7 **Ultimo controllo (da parte di un agente incaricato del controllo)**

Identificazione del blocco

Identificazione della carta di controllo

Data, ora e tipo di controllo

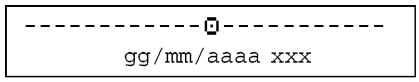
Tipo di controllo: max. quattro pittogrammi. Il tipo di controllo può essere (una combinazione di):
: Trasferimento dati carta, : Trasferimento dati VU, : Stampa, : Visualizzazione



8 **Attività del conducente memorizzate in una carta in ordine cronologico**

Identificazione del blocco

Data della richiesta (giorno di calendario cui si riferisce la stampa) + Contatore giornaliero presenza carta



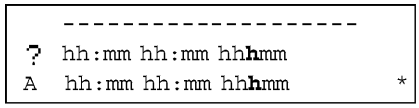
8.1 *Periodo durante il quale la carta non era inserita*

8.1a Identificazione della registrazione (inizio periodo)

8.1b *Periodo non noto*. Ora di inizio e termine, durata

8.1c *Attività immessa manualmente*

Pittogramma dell'attività, ora di inizio e termine (compresi), durata, i periodi di riposo di almeno un'ora sono contrassegnati da un asterisco.

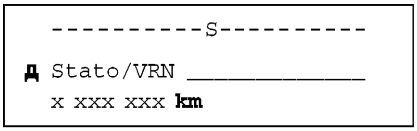


8.2 *Inserimento carta nella sede (slot) S*

Identificazione della registrazione; S = Pittogramma sede (slot)

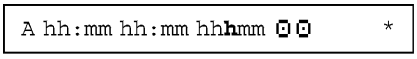
Stato membro di immatricolazione del veicolo e VRN

Odometro del veicolo all'inserimento della carta

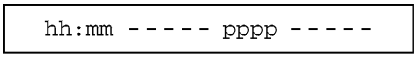


8.3 *Attività (a carta inserita)*

Pittogramma dell'attività, ora di inizio e termine (compresi), durata, condizione di guida (pittogramma equipaggio se EQUIPAGGIO, spazio vuoto se SINGOLA), i periodi di riposo di almeno un'ora sono contrassegnati da un asterisco.

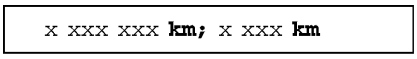


8.3a *Condizioni particolari.* Ora di immissione, pittogramma della condizione particolare (o combinazione di pittogrammi).



8.4 *Estrazione della carta*

Odometro del veicolo e distanza percorsa a partire dall'ultimo inserimento per cui è noto l'odometro.

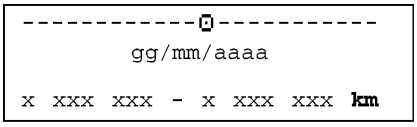


9 **Attività del conducente memorizzate in una VU per sede (slot) e in ordine cronologico**

Identificazione del blocco

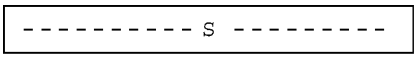
Data della richiesta (giorno di calendario cui si riferisce il documento stampato)

Odometro del veicolo alle ore 00:00 e 24:00



10 **Attività trattate nella sede (slot) S**

Identificazione del blocco

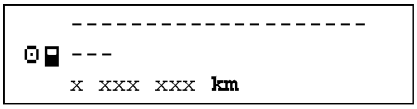


10.1 *Periodo durante il quale non è inserita una carta nella sede (slot) S*

Identificazione della registrazione

Carta assente

Odometro del veicolo all'inizio del periodo



10.2 *Inserimento della carta*

Identificazione registrazione dell'inserimento carta

Cognome del conducente

Nome del conducente

Identificazione della carta del conducente

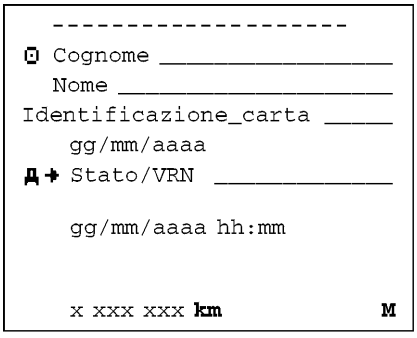
Data di scadenza della carta del conducente

Stato membro di immatricolazione e VRN del veicolo usato in precedenza

Data e ora di estrazione della carta dal veicolo precedente

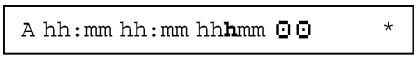
Riga vuota

Odometro del veicolo all'atto dell'inserimento della carta, flag dell'immissione manuale delle attività del conducente (M = sì, spazio vuoto = no)



10.3 *Attività*

Pittogramma dell'attività, ora di inizio e termine (compresi), durata, condizione di guida (pittogramma equipaggio se EQUIPAGGIO, spazio vuoto se SINGOLA), i periodi di riposo di almeno un'ora sono contrassegnati da un asterisco.



10.3a *Condizioni particolari*. Ora di immissione, pittogramma della condizione particolare (o combinazione di pittogrammi)

```
hh:mm ----- pppp -----
```

10.4 *Estrazione della carta o termine del periodo "carta assente"*

Odometro del veicolo all'atto dell'estrazione della carta o al termine del periodo "carta assente" e distanza percorsa a partire dall'inserimento o dall'inizio del periodo "carta assente".

```
x xxx xxx km; x xxx km
```

11 **Riepilogo giornaliero**

Identificazione blocco

```
----------Σ ---------
```

11.1 *Riepilogo della VU dei periodi senza carta nella sede (slot) "conducente"*

Identificazione del blocco

```
10■ - - -
```

11.2 *Riepilogo della VU dei periodi senza carta nella sede (slot) "secondo conducente"*

Identificazione del blocco

```
20■ - - -
```

11.3 *Riepilogo giornaliero della VU per conducente*

Identificazione della registrazione

Cognome del conducente

Nome/i del conducente

Identificazione della carta del conducente

```
  --------------------
0 Cognome ____________________
  Nome _____________________
Identificazione_carta _____
```

11.4 *Immissione del luogo in cui inizia e/o termina un periodo di lavoro giornaliero*

pi = pittogramma luogo inizio/termine, ora, paese, regione

Odometro

```
pihh:mm  Pae  Reg
  x xxx  xxx  km
```

11.5 *Totali attività (contenute in una carta)*

Durata totale guida, distanza percorsa

Durata totale lavoro e disponibilità

Durata totale riposo e periodi non noti

Durata totale delle attività dell'equipaggio

```
  0 hhhmm x xxx km
  ⚒ hhhmm ⧈ hhhmm
  ⊢ hhhmm ? hhhmm
00 hhhmm
```

11.6 *Totali attività [periodi senza carta nella sede (slot) "conducente"]*

Durata totale guida, distanza percorsa

Durata totale lavoro e disponibilità

Durata totale riposo

```
  0 hhhmm x xxx km
  ⚒ hhhmm ⧈ hhhmm
  ⊢ hhhmm
```

11.7 *Totali attività [periodi senza carta nella sede (slot) "secondo conducente"]*

Durata totale lavoro e disponibilità

Durata totale riposo

```
  ⚒ hhhmm ⧈ hhhmm
  ⊢ hhhmm
```

11.8 *Totali attività (per conducente, comprese entrambe le sedi)*

Durata totale guida, distanza percorsa

Durata totale lavoro e disponibilità

Durata totale riposo

Durata totale delle attività dell'equipaggio

Se si richiede un documento stampato giornaliero per il giorno in corso, le informazioni sul riepilogo giornaliero sono calcolate in base ai dati disponibili al momento della stampa.

```
hhhmm x xxx km
hhhmm hhhmm
hhhmm
hhhmm
```

12 **Anomalie e/o guasti memorizzati in una carta**

12.1 Identificazione del blocco ultimi 5 “anomalie e guasti” registrati in una carta

```
-------- !x --------
```

12.2 Identificazione del blocco di tutte le “anomalie” registrate in una carta

```
--------- ! ---------
```

12.3 Identificazione del blocco di tutti i “guasti” registrati in una carta

```
--------- x ---------
```

12.4 *Registrazione anomalie e/o guasti*

Identificazione della registrazione

Pittogramma anomalia/guasto, scopo della registrazione, data e ora di inizio

Codice aggiuntivo anomalia/guasto (se presente), durata

Stato membro di immatricolazione e VRN del veicolo in cui si è verificata l'anomalia o il guasto

```
----------------------
Pit (p)     gg/mm/aaaa hh:mm

!xxx                   hhhmm
 Stato/VRN _____
```

13 **Anomalie e/o guasti memorizzati o in corso in una VU**

13.1 Identificazione del blocco ultimi 5 “anomalie e guasti” registrati nella VU

```
--------- !x --------
```

13.2 Identificazione del blocco di tutte le “anomalie” registrate o in corso in una VU

```
--------- ! ---------
```

13.3 Identificazione del blocco di tutti i “guasti” registrati o in corso in una VU

```
--------- x ---------
```

13.4 *Registrazione anomalia e/o guasto*

Identificazione della registrazione

Pittogramma anomalia/guasto, scopo della registrazione, data e ora di inizio

Codice aggiuntivo anomalia/guasto (se presente), numero di anomalie analoghe nel giorno in questione, durata

Identificazione delle carte inserite all'inizio o al termine dell'anomalia o guasto (max 4 righe senza ripetere gli stessi numeri di carta)

Caso in cui non è stata inserita alcuna carta

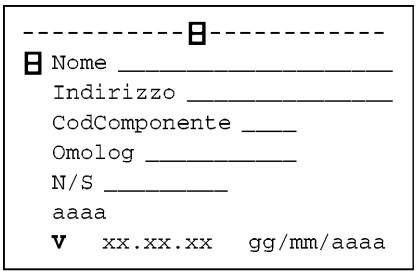
Lo scopo della registrazione (p) è un codice numerico che spiega il motivo della registrazione dell'anomalia o del guasto, codificato in base all'elemento di dati `EventFaultRecordPurpose`.

```
----------------------
Pit  (p)  gg/mm/aaaa  hh:mm
!xxx      (xxx)       hhhmm

Identificazione_carta _____
Identificazione_carta _____
Identificazione_carta _____
Identificazione_carta _____
 ---
```

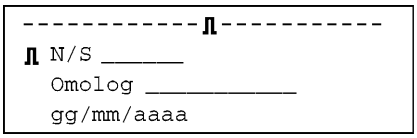
14 **Identificazione della VU**

Identificazione del blocco
Nome del fabbricante della VU
Indirizzo del fabbricante della VU
Codice componente della VU
Numero di omologazione della VU
Numero di serie della VU
Anno di fabbricazione della VU
Versione software della VU e data di installazione



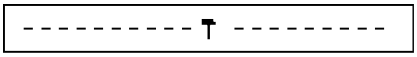
15 **Identificazione del sensore**

Identificazione del blocco
Numero di serie del sensore
Numero di omologazione del sensore
Data del primo montaggio del sensore



16 **Dati relativi alla calibratura**

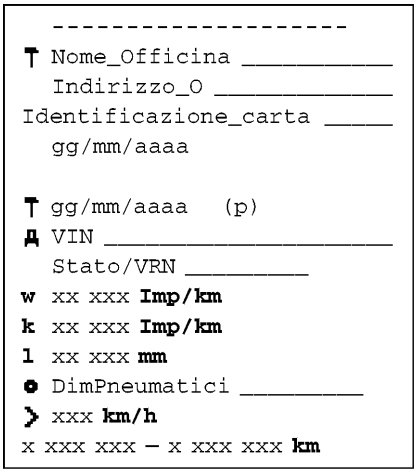
Identificazione del blocco



16.1 *Registrazione della calibratura*

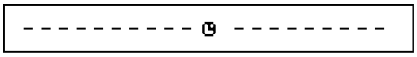
Identificazione della registrazione
Officina che ha effettuato la calibratura
Indirizzo dell'officina
Identificazione della carta dell'officina
Data di scadenza della carta dell'officina
Riga vuota
Data della calibratura + scopo della calibratura
VIN
Stato membro di immatricolazione e VRN
Coefficiente caratteristico del veicolo
Costante dell'apparecchio di controllo
Circonferenza effettiva dei pneumatici delle ruote
Dimensione dei pneumatici montati
Regolazione del limitatore di velocità
Valori vecchio e nuovo dell'odometro

Lo scopo della calibratura (p) è un codice numerico che spiega il motivo della registrazione di questi parametri di calibratura, codificato in base all'elemento di dati `CalibrationPurpose`.



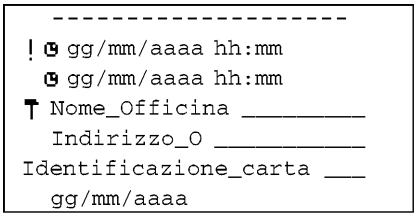
17 **Regolazione dell'ora**

Identificazione del blocco



17.1 *Registrazione della regolazione dell'ora*

Identificazione della registrazione
Data e ora vecchia
Data e ora nuova
Officina che ha effettuato la regolazione dell'ora
Indirizzo dell'officina
Identificazione della carta dell'officina
Data di scadenza della carta dell'officina



18 **Anomalia e guasto più recenti registrati nella VU**

Identificazione del blocco

Data e ora dell'anomalia più recente

Data e ora del guasto più recente

```
---------- !×  ----------
!  gg/mm/aaaa  hh:mm
×  gg/mm/aaaa  hh:mm
```

19 **Informazioni relative al controllo superamento di velocità**

Identificazione del blocco

Data e ora dell'ultimo CONTROLLO SUPERAMENTO DI VELOCITÀ

Data/ora del primo superamento di velocità e numero di superamenti di velocità a partire da tale data

```
------------>>  -----------
>  gg/mm/aaaa  hh:mm
>> gg/mm/aaaa  hh:mm (nnn)
```

20 **Registrazione superamento di velocità**

20.1 Identificazione del blocco "primo superamento di velocità dopo l'ultima calibratura"

```
--------  >>  --------
```

20.2 Identificazione del blocco "5 superamenti più gravi nel corso degli ultimi 365 giorni"

```
-------  >>(365) -------
```

20.3 Identificazione del blocco "superamento più grave per ciascuno degli ultimi 10 giorni in cui si è verificato"

```
-------  >>(10)  -------
```

20.4 Identificazione della registrazione

Data, ora e durata

Velocità massima e media, numero di anomalie analoghe nel giorno in questione

Cognome del conducente

Nome/i del conducente

Identificazione della carta del conducente

```
    ------------------
>> gg/mm/aaaa hh:mm hhhmm
   xxx km/h xxx km/h (xxx)
   Cognome _____________
   Nome ________________
Identificazione_carta _____
```

20.5 Se in un blocco non sono stati registrati superamenti di velocità

```
>> - - -
```

21 **Informazioni da inserire manualmente**

Identificazione del blocco

21.1 Luogo di controllo

21.2 Firma dell'agente incaricato del controllo

21.3 Dalle ore

21.4 Alle ore

21.5 Firma del conducente

"Informazioni da inserire manualmente": inserire un numero sufficiente di righe vuote sopra una voce da compilare a mano, per consentire la trascrizione effettiva delle informazioni richieste o per apporre una firma.

```
------------------------
  ..........................
  ..........................
  ..........................
  ..........................
  ..........................
```

3. SPECIFICHE DEI DOCUMENTI STAMPATI

Nel presente capitolo sono stati usati i seguenti segni grafici convenzionali:

N

Blocco di stampa o numero di registrazione N

N

Blocco di stampa o numero di registrazione N ripetuto tante volte quante necessario

X/Y

Blocchi di stampa o registrazioni X e/o Y, a seconda della necessità, ripetuti tante volte quante necessario

3.1. **Stampa giornaliera delle attività del conducente contenute nella carta**

PRT_007 Il documento stampato giornaliero delle attività del conducente contenute nella carta deve rispettare il formato seguente:

1	Data e ora di stampa del documento
2	Tipo di documento
3	Identificazione dell'agente incaricato del controllo (se nella VU è inserita una carta di controllo)
3	Identificazione del conducente (dalla carta cui si riferisce il documento stampato)
4	Identificazione del veicolo (veicolo da cui si ottiene il documento stampato)
5	Identificazione della VU (VU da cui si ottiene il documento stampato)
6	Ultima calibratura di questa VU
7	Ultimo controllo cui è stato sottoposto il conducente
8	Delimitatore delle attività del conducente
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Attività del conducente in ordine cronologico
11	Delimitatore riepilogo giornaliero
11.4	Luoghi immessi in ordine cronologico
11.5	Totali delle attività
12.1	Anomalie o guasti dal delimitatore della carta
12.4	Registrazioni di anomalie/guasti (ultime 5 anomalie o guasti memorizzati nella carta)
13.1	Anomalie o guasti dal delimitatore della VU
13.4	Registrazioni di anomalie/guasti (ultime 5 anomalie o guasti memorizzati o in corso nella VU)
21.1	Luogo di controllo
21.2	Firma dell'agente incaricato del controllo
21.5	Firma del conducente

3.2. **Stampa giornaliera delle attività del conducente contenute nella VU**

PRT_008 Il documento stampato giornaliero delle attività del conducente contenute nella VU deve rispettare il formato seguente:

1	Data e ora di stampa del documento
2	Tipo di documento
3	Identificazione del titolare della carta (per tutte le carte inserite nella VU)
4	Identificazione del veicolo (veicolo da cui si ottiene il documento stampato)
5	Identificazione della VU (VU da cui si ottiene il documento stampato)
6	Ultima calibratura di questa VU
7	Ultimo controllo di questo apparecchio di controllo
9	Delimitatore delle attività del conducente
10	Delimitatore della sede “conducente” (slot 1)
10.1 / 10.2 / 10.3 /10.3a / 10.4	Attività in ordine cronologico (sede “conducente”)
10	Delimitatore della sede “secondo conducente” (slot 2)
10.1 / 10.2 / 10.3 /10.3a / 10.4	Attività in ordine cronologico (sede “secondo conducente”)
11	Delimitatore del riepilogo giornaliero
11.1	Riepilogo dei periodi senza carta nella sede (slot) “conducente”
11.4	Luoghi inseriti in ordine cronologico
11.6	Totali delle attività

11.2	Riepilogo dei periodi senza carta nella sede (slot) “secondo conducente”	
11.4	Luoghi immessi in ordine cronologico	
11.7	Totali delle attività	
11.3	Riepilogo delle attività per un conducente, comprese entrambe le sedi	
11.4	Luoghi immessi da tale conducente in ordine cronologico	
11.7	Totali delle attività per questo conducente	
13.1	Delimitatore di anomalie e guasti	
13.4	Registrazioni di anomalie/guasti (ultime 5 anomalie o guasti memorizzati o in corso nella VU)	
21.1	Luogo di controllo	
21.2	Firma dell'agente incaricato del controllo	
21.3	Dalle ore	(spazio disponibile per consentire a un conducente senza carta di indicare i periodi pertinenti)
21.4	Alle ore	
21.5	Firma del conducente	

3.3. **Stampa di anomalie e guasti contenuti nella carta**

PRT_009 Il documento stampato di anomalie e guasti contenuti nella carta deve rispettare il formato seguente:

1	Data e ora di stampa del documento
2	Tipo di documento
3	Identificazione dell'agente incaricato del controllo (se nella VU è inserita una carta di controllo)
3	Identificazione del conducente (dalla carta cui si riferisce il documento stampato)
4	Identificazione del veicolo (veicolo da cui si ottiene il documento stampato)
12.2	Delimitatore delle anomalie
12.4	Registrazioni delle anomalie (tutte le anomalie memorizzate nella carta)
12.3	Delimitatore dei guasti
12.4	Registrazioni dei guasti (tutti i guasti memorizzati nella carta)
21.1	Luogo di controllo
21.2	Firma dell'agente incaricato del controllo
21.5	Firma del conducente

3.4. **Stampa di anomalie e guasti contenuti nella VU**

PRT_010 Il documento stampato di anomalie e guasti contenuti nella VU deve rispettare il formato seguente:

1	Data e ora di stampa del documento
2	Tipo di documento
3	Identificazione del titolare della carta (per tutte le carte inserite nella VU)
4	Identificazione del veicolo (veicolo da cui si ottiene il documento stampato)
13.2	Delimitatore delle anomalie
13.4	Registrazioni delle anomalie (tutte le anomalie memorizzate o in corso nella VU)
13.3	Delimitatore dei guasti
13.4	Registrazioni dei guasti (tutti i guasti memorizzati o in corso nella VU)
21.1	Luogo del controllo
21.2	Firma dell'agente incaricato del controllo
21.5	Firma del conducente

3.5. **Stampa dei dati tecnici**

PRT_011 Il documento stampato dei dati tecnici deve rispettare il formato seguente:

1	Data e ora di stampa del documento
2	Tipo di documento
3	Identificazione del titolare della carta (per tutte le carte inserite nella VU)
4	Identificazione del veicolo (veicolo da cui si ottiene il documento stampato)
14	Identificazione della VU
15	Identificazione del sensore
16	Delimitatore dei dati di calibratura
16.1	Registrazioni delle calibrature (tutte le registrazioni disponibili in ordine cronologico)
17	Delimitatore delle regolazioni dell'ora
17.1	Registrazioni delle regolazioni dell'ora (tutte le registrazioni disponibili per le regolazioni dell'ora e i dati di calibratura)
18	Anomalia e guasto più recenti registrati nella VU

3.6. **Stampa dei superamenti di velocità**

PRT_012 Il documento stampato dei superamenti di velocità deve rispettare il formato seguente:

1	Data e ora di stampa del documento
2	Tipo di documento
3	Identificazione del titolare della carta (per tutte le carte inserite nella VU)
4	Identificazione del veicolo (veicolo da cui si ottiene il documento stampato)
19	Informazioni relative ai superamenti di velocità
20.1	Identificazione dei dati relativi ai superamenti di velocità
20.4 / 20.5	Primo superamento di velocità successivo all'ultima calibratura
20.2	Identificazione dei dati relativi al superamento di velocità
20.4 / 20.5	I 5 superamenti di velocità più gravi nel corso degli ultimi 365 giorni
20.3	Identificazione dei dati relativi al superamento di velocità
20.4 / 20.5	Il superamento di velocità più grave per ciascuno degli ultimi 10 giorni in cui si è verificato
21.1	Luogo del controllo
21.2	Firma dell'agente incaricato del controllo
21.5	Firma del conducente

Appendice 5

DISPOSITIVO DI VISUALIZZAZIONE

Nella presente appendice sono stati usati i seguenti segni grafici convenzionali:

— i caratteri in **grassetto** indicano il testo normale da visualizzare (la visualizzazione rimane in caratteri normali),

— i caratteri normali indicano le variabili (pittogrammi o dati) da sostituire con i rispettivi valori nella visualizzazione:

gg mm aaaa: giorno, mese, anno,

hh: ore,

mm: minuti,

D: pittogramma di durata,

EF: combinazione di pittogrammi relativi ad anomalie o guasti,

O: pittogramma della modalità di funzionamento.

DIS_001 L'apparecchio di controllo deve visualizzare i dati nei formati seguenti:

Dati	Formato
Visualizzazione predefinita	
Ora locale	Hh:mm
Modalità di funzionamento	O
Informazioni relative al conducente	1 Dhh**h**mm ▮▮hh**h**mm
Informazioni relative al secondo conducente	2 Dhh**h**mm
Condizione "Escluso dal campo di applicazione" aperta	OUT
Visualizzazione degli avvisi	
Superamento del periodo di guida continuo	10 hh**h**mm ▮▮hh**h**mm
Anomalia o guasto	EF
Visualizzazione di altre informazioni	
Data UTC Ora	UTC gg/mm/aaaa o UTC gg.mm.aaaa Hh:mm
Periodo di guida continuo e periodo cumulato di interruzione del conducente	10 hh**h**mm ▮▮hh**h**mm
Periodo di guida continuo e periodo cumulato di interruzione del secondo conducente	20 hh**h**mm ▮▮hh**h**mm
Periodo cumulato di guida del conducente per la settimana in corso e quella precedente	10 ‖ hhh**h**mm
Periodo cumulato di guida del secondo conducente per la settimana in corso e quella precedente	20 ‖ hhh**h**mm

Appendice 6

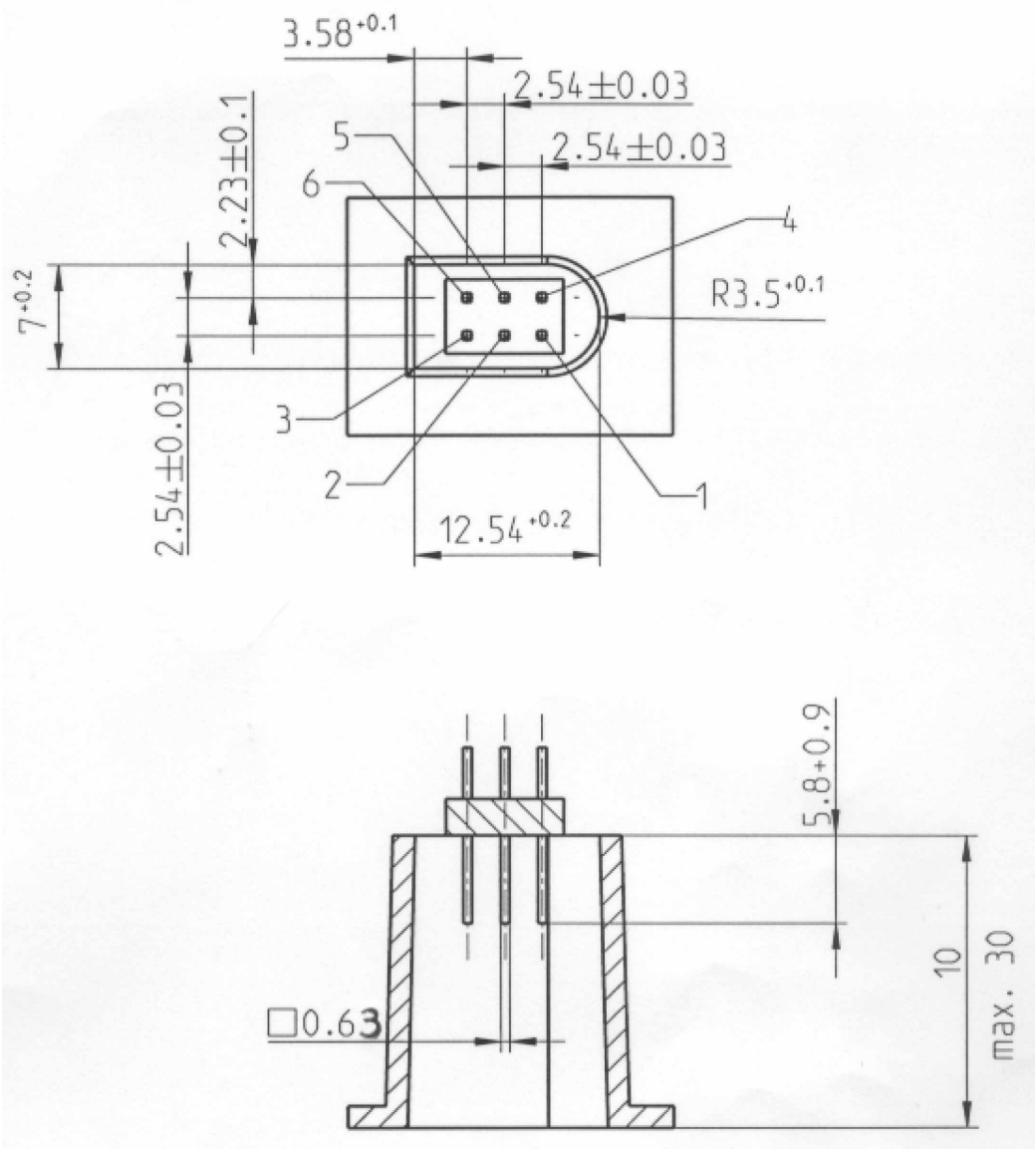
INTERFACCE ESTERNE

INDICE

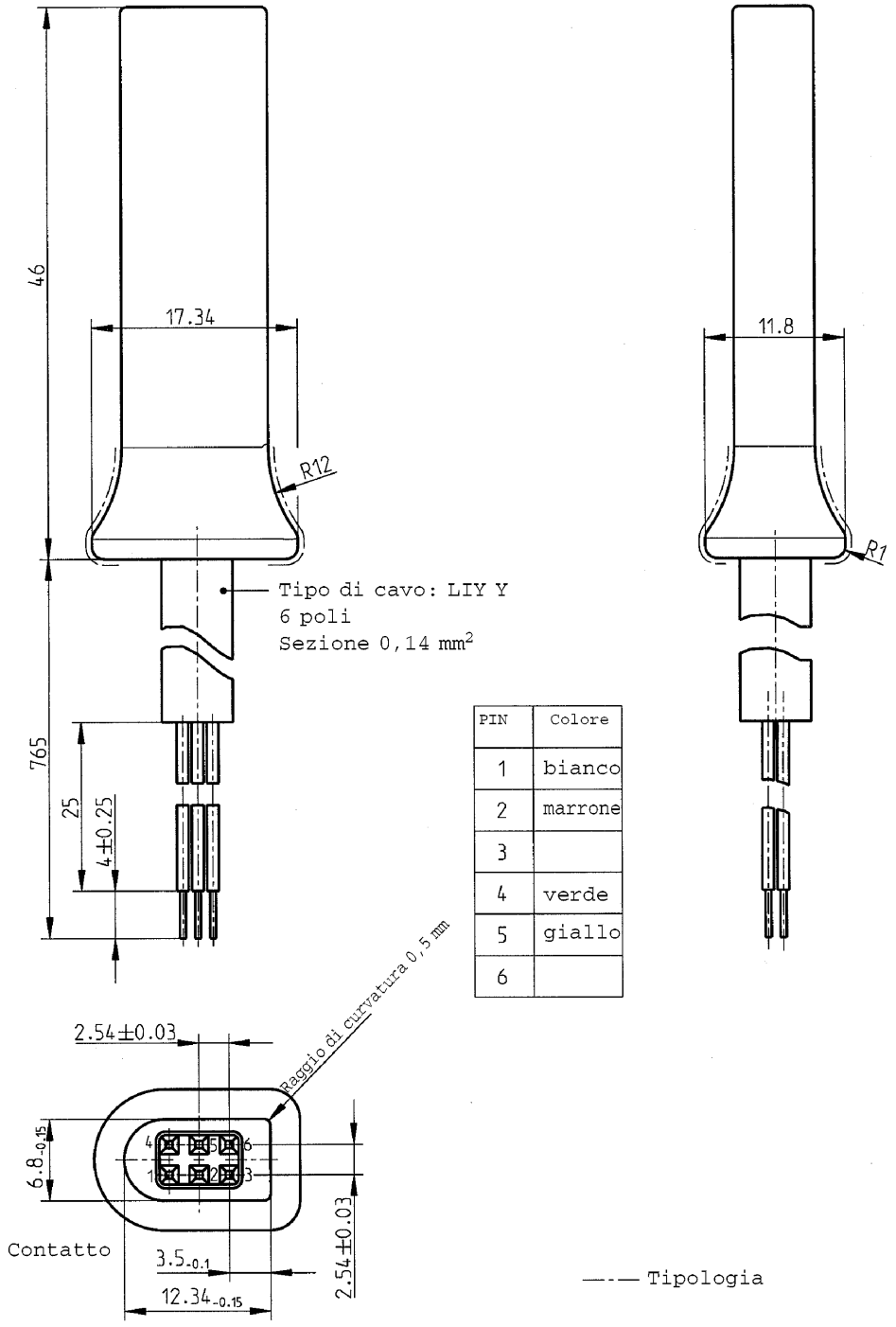
1. HARDWARE

1.1. **Connettore**

INT_001 Il connettore di trasferimento/calibratura deve essere un connettore a 6 pin, cui poter accedere sul pannello anteriore senza necessità di smontare alcun elemento dell'apparecchio di controllo, e deve essere conforme al disegno sotto riportato (tutte le dimensioni sono indicate in millimetri).



Il disegno sotto riportato illustra un tipico connettore volante a 6 pin.



PIN	Colore
1	bianco
2	marrone
3	
4	verde
5	giallo
6	

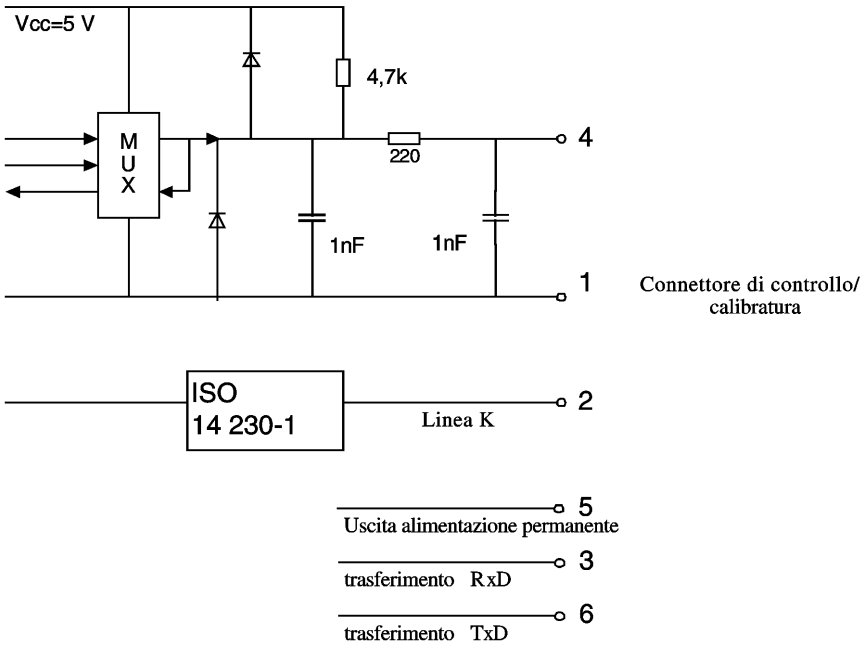
1.2. **Distribuzione dei contatti**

INT_002 I contatti devono essere distribuiti in base alla tabella seguente:

Pin	Descrizione	Note
1	Polo negativo batteria	Collegato al polo negativo della batteria del veicolo
2	Comunicazione dati	Linea K (ISO 14230-1)
3	RxD — Trasferimento	Ingresso di dati all'apparecchio di controllo
4	Segnale ingresso/uscita	Calibratura
5	Uscita alimentazione permanente	Il campo di tensione deve essere quello dell'alimentazione elettrica del veicolo meno 3V per tenere conto della caduta di tensione nel circuito di protezione Uscita 40 mA
6	TxD — Trasferimento	Uscita di dati dall'apparecchio di controllo

1.3. **Schema elettrico**

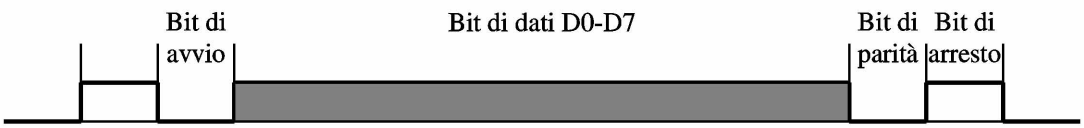
INT_003 Lo schema elettrico deve essere conforme a quello sotto riportato.



2. INTERFACCIA DI TRASFERIMENTO

INT_004 L'interfaccia di trasferimento deve essere conforme alle specifiche RS232.

INT_005 L'interfaccia di trasferimento deve utilizzare un bit di avvio, 8 bit di dati con il bit meno significativo (LSB) per primo, un bit di parità pari e 1 bit di arresto.



Organizzazione dei byte di datiBit di avvio un bit con livello logico 0

Bit di dati: trasmessi con LSB per primo

Bit di parità: parità pari

Bit di arresto: un bit con livello logico 1

In caso di trasmissione di dati numerici costituiti da più di un byte, il byte più significativo viene trasmesso per primo ed il byte meno significativo viene trasmesso per ultimo.

INT_006 La velocità di trasmissione deve avere un campo di regolazione compreso tra 9 600 bps e 115 200 bps. La trasmissione deve avvenire alla velocità di trasmissione più elevata possibile, con la velocità iniziale impostata su 9 600 bps dopo l'avvio della comunicazione.

3. INTERFACCIA DI CALIBRATURA

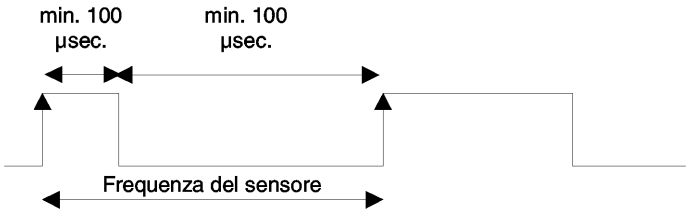
INT_007 La comunicazione dati deve essere conforme alla norma ISO 14230-1, Veicoli stradali — Sistemi diagnostici — Keyword Protocol 2000 — Parte 1: Livello fisico, Prima edizione: 1999.

INT_008 Il segnale in ingresso/uscita deve essere conforme alle seguenti specifiche elettriche:

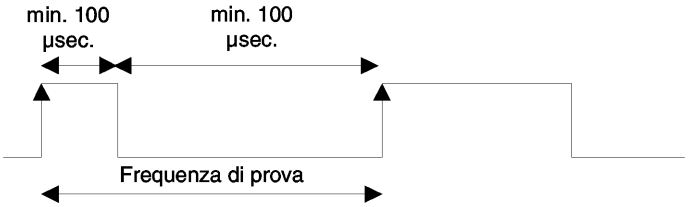
Parametro	Minimo	Tipico	Massimo	Note
U_{low} (ingresso)			1,0 V	I = 750 µA
U_{high} (ingresso)	4 V			I = 200 µA
Frequenza			4 kHz	
U_{low} (uscita)			1,0 V	I = 1 mA
U_{high} (uscita)	4 V			I = 1 mA

INT_009 Il segnale in ingresso/uscita deve essere conforme alle seguenti temporizzazioni:

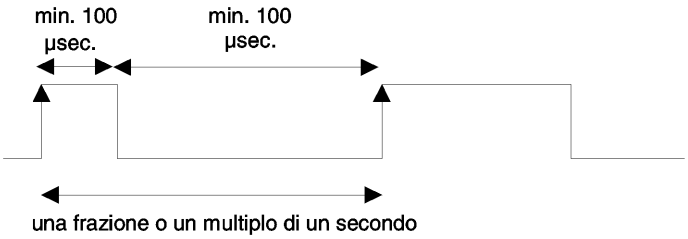
Segnale del sensore (uscita)



Segnale di prova (ingresso)



Segnale d'orologio UTC (uscita)



Appendice 7

PROTOCOLLI DI TRASFERIMENTO DEI DATI

INDICE

1. INTRODUZIONE

La presente appendice stabilisce le procedure per l'esecuzione delle differenti modalità di trasferimento dei dati ad un dispositivo di memorizzazione esterno (ESM), insieme ai protocolli da attuare per garantire il corretto trasferimento dei dati e la piena compatibilità del formato dei dati trasferiti, in modo da consentire a qualsiasi agente incaricato del controllo di ispezionare i dati in questione e verificarne l'autenticità e integrità prima di procedere alla loro analisi.

1.1. **Campo di applicazione**

Il trasferimento di dati ad 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.

DDP_001 I dati trasferiti nel corso di un'unica sessione devono essere memorizzati all'interno dell'ESM in uno stesso file.

1.2. **Acronimi e simboli**

Nella presente appendice sono utilizzati i seguenti acronimi:

AID	Application identifier — Identificazione dell'applicazione
ATR	Answer to reset — Risposta all'operazione di azzeramento
CS	Checksum byte — Byte di totale di controllo
DF	Dedicated file — File dedicato
DS	Diagnostic Session — Sessione diagnostica
EF	Elementary file — File elementare
ESM	External storage medium — Dispositivo di memorizzazione esterno
FID	File identifier (file ID) — Identificativo del file
FMT	Format byte — Byte di formato (primo byte dell'intestazione del messaggio)
ICC	Integrated circuit card — Carta a circuito integrato
IDE	Intelligent dedicated equipment — Apparecchio intelligente dedicato: apparecchio utilizzato per effettuare il trasferimento di dati nell'ESM (ad esempio: un personal computer)
IFD	Interface device — Interfaccia
KWP	Keyword protocol 2000
LEN	Length byte — Byte di lunghezza (ultimo byte nell'intestazione messaggio)
PPS	Protocol parameter selection — Selezione dei parametri di protocollo
PSO	Perform Security Operation — Esecuzione operazione di sicurezza
SID	Service identifier — Identificativo del servizio
SRC	Source byte — Byte sorgente
TGT	Target byte — Byte di destinazione
TLV	Tag length value — Valore lunghezza tag
TREP	Transfer Response Parameter — Parametro di risposta di trasferimento
TRTP	Transfer Request Parameter — Parametro di richiesta di trasferimento
VU	Vehicle unit — Unità elettronica di bordo

2. TRASFERIMENTO DEI DATI DA UNA VU

2.1. **Procedura di trasferimento dei dati**

Per effettuare un trasferimento di dati da una VU, l'operatore deve eseguire le seguenti operazioni:

— inserire la propria carta tachigrafica in una sede (slot) della VU ([1]);

— collegare l'IDE al connettore di trasferimento dati della VU;

— stabilire il collegamento tra l'IDE e la VU;

— selezionare sull'IDE i dati da trasferire e inviare la richiesta alla VU;

— terminare la sessione di trasferimento dati.

2.2. **Protocollo di trasferimento dei dati**

Il protocollo è strutturato sulla base di una configurazione di tipo "master-slave", in cui all'IDE è assegnato il ruolo principale (master) e alla VU quello secondario (slave).

La struttura, i tipi e il flusso dei messaggi si basano principalmente sul Keyword Protocol 2000 (KWP) (ISO 14230-2 Road vehicles — Diagnostic systems — Keyword protocol 2000 — Part 2: Data link layer) (ISO 14230-2 Veicoli stradali — Sistemi di diagnosi — Keyword Protocol 2000 — Parte 2: Livello di collegamento di trasmissione dati).

Il livello dell'applicazione è basato in gran parte sull'attuale versione della norma ISO 14229-1 (Veicoli stradali — Sistemi di diagnosi — Parte 1: Servizi di diagnosi, versione 6 del 22 febbraio 2001).

2.2.1. ***Struttura dei messaggi***

DDP_002 Tutti i messaggi scambiati tra l'IDE e la VU sono formattati secondo una struttura composta da tre sezioni:

— intestazione, costituita da un byte di formato (FMT), un byte di destinazione (TGT), un byte sorgente (SRC) e eventualmente un byte di lunghezza (LEN),

— campo di dati, costituito da un byte identificativo del servizio (SID), che può comprendere un byte facoltativo relativo alla sessione diagnostica (DS_) o un byte facoltativo relativo al parametro di trasferimento (TRIP o TREP),

— totale di controllo, costituito da un byte di totale di controllo (CS).

Intestazione				Campo di dati					Totale di controllo
FMT	TGT	SRC	LEN	SID	DATA	…	…	…	CS
4 byte				Lunghezza massima: 255 byte					1 byte

I byte di TGT e di SRC rappresentano l'indirizzo fisico del destinatario e del mittente del messaggio. I valori esadecimali sono rispettivamente F0 per l'IDE e EE per la VU.

Il byte di LEN è la lunghezza della sezione riservata al campo di dati.

Il byte del totale di controllo è dato dalla somma su 8 bit, modulo 256, di tutti i byte del messaggio escluso lo stesso CS.

I byte relativi a FMT, DS_, TRTP e TREP sono definiti più avanti nel presente documento.

([1]) L'inserimento della carta provoca l'abilitazione degli opportuni diritti di accesso alla funzione di trasferimento e ai dati in questione.

DDP_003 Nel caso in cui i dati da inviare nel messaggio eccedano lo spazio disponibile nella sezione riservata al campo di dati, il messaggio viene suddiviso in diversi sottomessaggi. Ciascun sottomessaggio ha un'intestazione, gli stessi SID, TREP e un contatore a 2 byte che indica il numero sequenziale del sottomessaggio all'interno del messaggio totale. Per abilitare la verifica degli errori e interrompere la trasmissione di dati, l'IDE conferma tutti i sottomessaggi. L'IDE può accettare un sottomessaggio, chiedere che sia ritrasmesso, richiedere alla VU di ricominciare o interrompere la trasmissione.

DDP_004 Se l'ultimo sottomessaggio contiene esattamente 255 byte nel campo di dati, è necessario allegare un sottomessaggio finale con un campo di dati vuoto (salvo SID, TREP e il contatore sottomessaggi) per indicare la fine del messaggio.

Esempio:

Intesta-zione	SID	REP	Messaggio	CS
4 byte	Lunghezza superiore a 255 byte			

è inviato nella seguente forma:

Intesta-zione	SID	REP	00	01	Sottomessaggio 1	CS
4 byte	255 byte					

Intesta-zione	SID	REP	00	02	Sottomessaggio 2	CS
4 byte	255 byte					

…

Intesta-zione	SID	REP	xx	yy	Sottomessaggio n	CS
4 byte	Lunghezza inferiore a 255 byte					

o nella forma:

Intesta-zione	SID	REP	00	01	Sottomessaggio 1	CS
4 byte	255 byte					

Intesta-zione	SID	REP	00	02	Sottomessaggio 2	CS
4 byte	255 byte					

…

Intesta-zione	SID	REP	xx	yy	Sottomessaggio n	CS
4 byte	255 byte					

Intesta-zione	SID	REP	xx	yy+1	CS
4 byte	4 byte				

2.2.2. ***Tipi di messaggi***

Il protocollo di comunicazione per il trasferimento di dati tra la VU e l'IDE richiede lo scambio di 8 differenti tipi di messaggi.

La tabella che segue riepiloga questi messaggi.

Struttura del messaggio	Dimensione massima: 4 byte Intestazione				Dimensione massima: 255 byte Dati			1 byte Totale di controllo
IDE -> <- VU	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATI	CS
Richiesta di inizio comunicazione	81	EE	F0		81			E0
Risposta positiva di inizio comunicazione	80	F0	EE	03	C1		8F,EA	9B
Richiesta di inizio sessione diagnostica	80	EE	F0	02	10	81		F1
Risposta positiva di inizio sessione diagnostica	80	F0	EE	02	50	81		31
Servizi di controllo del collegamento								
Verifica della frequenza di baud (fase 1)								
9 600 Bd	80	EE	F0	04	87		01,01,01	EC
19 200 Bd	80	EE	F0	04	87		01,01,02	ED
38 400 Bd	80	EE	F0	04	87		01,01,03	ED
57 600 Bd	80	EE	F0	04	87		01,01,04	EF
115 200 Bd	80	EE	F0	04	87		01,01,05	F0
Risposta positiva verifica della frequenza di baud	80	F0	EE	02	C7		01	28
Frequenza di baud di transizione (fase 2)	80	EE	F0	03	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	03	75		00,FF	D5
Richiesta di trasferimento dati								
Ispezione	80	EE	F0	02	36	01		97
Attività	80	EE	F0	06	36	02	Data	CS
Anomalie e guasti	80	EE	F0	02	36	03		99
Dati dettagliati relativi alla velocità	80	EE	F0	02	36	04		9A
Dati tecnici	80	EE	F0	02	36	05		9B
Trasferimento dati carta	80	EE	F0	02	36	06		9C
Risposta positiva di trasferimento dati	80	F0	EE	Len	76	TREP	Dati	CS
Richiesta di chiusura trasferimento	80	EE	F0	01	37			96
Risposta positiva richiesta di chiusura trasferimento	80	F0	EE	01	77			D6
Richiesta di termine comunicazione	80	EE	F0	01	82			E1
Risposta positiva di termine comunicazione	80	F0	EE	01	C2			21
Riconoscimento sottomessaggio	80	EE	F0	Len	83		Dati	CS
Risposte negative								
Rifiuto generico	80	F0	EE	03	7F	Sid rich.	10	CS
Servizio non supportato	80	F0	EE	03	7F	Sid rich.	11	CS
Sottofunzione non supportata	80	F0	EE	03	7F	Sid rich.	12	CS
Lunghezza del messaggio non corretta	80	F0	EE	03	7F	Sid rich.	13	CS
Condizioni non soddisfatte o errore nella sequenza di richiesta	80	F0	EE	03	7F	Sid rich.	22	CS
Richiesta fuori valori limite	80	F0	EE	03	7F	Sid rich.	31	CS
Invio dati rifiutato	80	F0	EE	03	7F	Sid rich.	50	CS
Risposta pendente	80	F0	EE	03	7F	Sid rich.	78	CS
Dati non disponibili	80	F0	EE	03	7F	Sid rich.	FA	CS

Note:
— Sid rich. = il Sid della richiesta corrispondente.
— TREP = il TRTP della richiesta corrispondente.
— Le celle scure indicano l'assenza di trasmissione.
— Il termine "invio dati" (upload) (riferito all'IDE) è utilizzato per compatibilità con la norma ISO 14229 e ha lo stesso significato di "trasferimento" (riferito alla VU).
— La tabella non riporta i potenziali contatori a 2 byte di sottomessaggi.

2.2.2.1. *Richiesta di inizio comunicazione (SID 81)*

DDP_005 Tale messaggio è inviato dall'IDE per stabilire il collegamento nelle comunicazioni con la VU. Le comunicazioni sono in un primo tempo sempre effettuate a 9 600 baud (la frequenza di baud può eventualmente essere cambiata in un secondo tempo, ricorrendo agli opportuni servizi di controllo del collegamento).

2.2.2.2. *Risposta positiva di inizio comunicazione (SID C1)*

DDP_006 Questo messaggio è inviato dalla VU per rispondere positivamente alla richiesta di inizio comunicazione e comprende i 2 byte chiave '8F' e 'EA', i quali indicano che l'unità supporta il protocollo con intestazione, comprendente le informazioni su destinazione, sorgente e lunghezza.

2.2.2.3. *Richiesta di inizio sessione diagnostica (SID 10)*

DDP_007 Questo messaggio è inviato dall'IDE allo scopo di chiedere una nuova sessione diagnostica della VU. La sotto funzione 'sessione per difetto' (81 esadecimale) indica che deve essere avvita una sessione diagnostica standard.

2.2.2.4. *Risposta positiva di inizio sessione diagnostica (SID 50)*

DDP_008 Questo messaggio è inviato dalla VU per rispondere positivamente alla richiesta di sessione diagnostica.

2.2.2.5. *Servizio di controllo del collegamento (SID 87)*

DDP_052 Il servizio di controllo del collegamento è utilizzato dall'IDE per cambiare la frequenza di baud. Il cambiamento avviene in due fasi. Nella fase 1 l'IDE propone il cambiamento, indicando la nuova frequenza. Ricevuta la risposta positiva della VU, l'IDE conferma il cambiamento di frequenza di Baud alla VU (fase 2). L'IDE passa quindi alla nuova frequenza di baud. Ricevuta la conferma, anche la VU passa alla nuova frequenza.

2.2.2.6. *Risposta positiva di controllo del collegamento (SID C7)*

DDP_053 La risposta positiva di controllo di collegamento è inviata dalla VU rispondere positivamente alla richiesta di controllo del collegamento (fase 1). Nessuna risposta è invece inviata alla richiesta di conferma (fase 2).

2.2.2.7. *Richiesta di invio dati (upload) (SID 35)*

DDP_009 Questo messaggio è inviato dall'IDE per specificare alla VU che si richiede un'operazione di trasferimento dati. Per soddisfare i requisiti della norma ISO 14229 vengono anche inviati dati relativi alla collocazione, alla dimensione ed al formato dei dati richiesti. Poiché tali informazioni non sono note all'IDE prima dell'invio, l'indirizzo di memoria è impostato su 0, il formato non è né criptato né compresso e la dimensione della memoria è impostata sul valore massimo.

2.2.2.8. *Risposta positiva di invio dati (upload) (SID 75)*

DDP_010 Questo messaggio è inviato dalla VU per segnalare all'IDE che la VU è pronta ad eseguire il trasferimento dei dati. Per soddisfare i requisiti della norma ISO 14229 nel messaggio di risposta positiva sono contenuti anche dati che indicano all'IDE che i successivi messaggi di risposta positiva di trasferimento dati comprenderanno al massimo 00FF bytes esadecimali.

2.2.2.9. *Richiesta di trasferimento dati (SID 36)*

DDP_011 Questo messaggio è inviato dall'IDE per specificare alla VU il tipo di dati da trasferire. Un parametro di richiesta di trasferimento (TRTP) indica il tipo di trasferimento.

Vi sono sei tipi di trasferimento dati:

— Ispezione (TRTP 01),

— Attività relative ad una data specifica (TRTP 02),

— Anomalie e guasti (TRTP 03),

— Dati dettagliati relativi alla velocità (TRTP 04),

— Dati tecnici (TRTP 05),

— Trasferimento dati carta (TRTP 06).

DDP_054 La IDE deve obbligatoriamente richiedere il trasferimento dati in modalità ispezione (TRTP 01) durante una sessione di trasferimento, solo in tal modo i certificati della VU sono infatti registrati nei file trasferiti (e permettono così la verifica della firma digitale).

Nel secondo caso (TRTP 02) il messaggio Richiesta di trasferimento dati comprende l'indicazione del giorno di calendario (formato `TimeReal`) da trasferire.

2.2.2.10. *Risposta positiva di trasferimento dati (SID 76)*

DDP_012 Questo messaggio è inviato dalla VU in risposta alla Richiesta di trasferimento dati e contiene i dati richiesti, con il parametro di risposta di trasferimento (TRTP) corrispondente al TRTP della richiesta.

DDP_055 Nel primo caso (TRTP 01), la VU invia le informazioni 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 ad un'impresa,

— blocchi di un'impresa,

— controlli precedenti.

2.2.2.11. *Richiesta di chiusura trasferimento (SID 37)*

DDP_013 Questo messaggio è inviato dall'IDE per informare la VU che la sessione di trasferimento è terminata.

2.2.2.12. *Risposta positiva di richiesta chiusura trasferimento (SID 77)*

DDP_014 Questo messaggio è inviato dalla VU per confermare la ricezione della Richiesta di chiusura trasferimento.

2.2.2.13. *Richiesta di termine comunicazione (SID 82)*

DDP_015 Questo messaggio è inviato dall'IDE per disattivare il collegamento di comunicazione con la VU.

2.2.2.14. *Richiesta di risposta positiva di termine comunicazione (SID C2)*

DDP_016 Questo messaggio è inviato dalla VU per confermare la ricezione della Richiesta di termine comunicazione.

2.2.2.15. *Conferma di ricezione sottomessaggio (SID 83)*

DDP_017 Questo messaggio è inviato dall'IDE per confermare l'avvenuta ricezione di ciascuna parte di un messaggio trasmesso sotto forma di differenti sottomessaggi. Il campo di dati contiene il SID ricevuto dalla VU e un codice a 2 byte, come descritto qui di seguito:

— MsgC + 1 conferma la corretta ricezione del sottomessaggio MsgC.

Richiesta da parte dell'IDE alla VU di inviare il sottomessaggio successivo.

— MsgC indica un problema nella ricezione del sottomessaggio MsgC.

Richiesta da parte dell'IDE alla VU di inviare di nuovo il sottomessaggio.

— FFFF richiede la conclusione del messaggio.

Può essere utilizzato dall'IDE per terminare la trasmissione del messaggio della VU per qualsiasi ragione.

La ricezione dell'ultimo sottomessaggio di un messaggio (byte di LEN < 255) può essere confermata utilizzando uno qualsiasi di questi codici oppure non essere confermata.

Le risposte della VU, composte da diversi sottomessaggi, sono:

— Risposta positiva di trasferimento dati (SID 76).

2.2.2.16. *Risposta negativa (SID 7F)*

DDP_018 Questo messaggio è inviato dalla VU in risposta ai messaggi di richiesta sopra menzionati nel caso in cui la VU non sia in grado di soddisfare la richiesta in questione. I campi di dati del messaggio comprendono il SID della risposta (7F), il SID della richiesta, e un codice che specifica la ragione della risposta negativa. Sono disponibili i seguenti codici:

— 10 rifiuto generico

L'azione non può essere eseguita per una ragione diversa da quelle sotto esposte.

— 11 Servizio non supportato

Mancata comprensione del SID relativo alla richiesta.

— 12 sottofunzione non supportata

Mancata comprensione del DS_ o TRTP relativo alla richiesta, o assenza di ulteriori sottomessaggi da trasmettere.

— 13 lunghezza del messaggio non corretta

Il messagio ricevuto non ha la giusta lunghezza.

— 22 condizioni non corrette o errore nella sequenza di richiesta

Il servizio richiesto non è attivo o la sequenza dei messaggi di richiesta non è corretta.

— 31 richiesta fuori valori limite

Il parametro indicato (specifico campo dei dati) non è valido.

— 50 invio dati (upload) rifiutato

La richiesta non può essere eseguita (errata modalità di funzionamento della VU o guasto interno della VU).

— 78 risposta pendente

L'azione richiesta non può essere completata nel tempo previsto e la VU non è pronta per accettare un'altra richiesta.

— FA dati non disponibili

I dati oggetto di una richiesta di trasferimento non sono disponibili nella VU (ad esempio, non vi è alcuna carta inserita, ecc.).

2.2.3. ***Flusso di messaggi***

Qui di seguito è illustrato un tipico flusso di messaggi nel corso di una normale procedura di trasferimento dati:

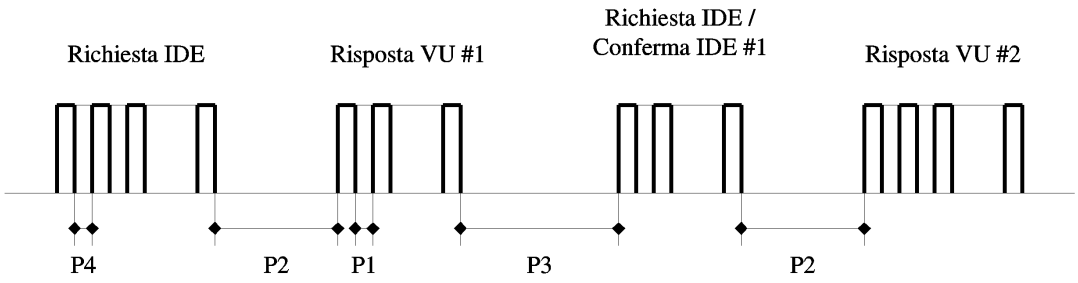
IDE		VU
Richiesta di inizio comunicazione	⇨	
	⇦	Risposta positiva
Richiesta di inizio sessione diagnostica	⇨	
	⇦	Risposta positiva
Richiesta di invio dati (upload)	⇨	
	⇦	Risposta positiva
Richiesta di trasferimento dati ispezione	⇨	
	⇦	Risposta positiva
Richiesta di trasferimento dati #2	⇨	
	⇦	Risposta positiva #1
Conferma ricezione sottomessaggio #1	⇨	
	⇦	Risposta positiva #2
Conferma ricezione sottomessaggio #2	⇨	
	⇦	Risposta positiva #m
Conferma ricezione sottomessaggio #m	⇨	
	⇦	Risposta positiva (campo di dati < 255 byte)
Conferma ricezione sottomessaggio (facoltativo)	⇨	
	…	
Richiesta di trasferimento dati #n	⇨	
	⇦	Risposta positiva
Richiesta di chiusura trasferimento	⇨	
	⇦	Risposta positiva
Richiesta di termine comunicazione	⇨	
	⇦	Risposta positiva

2.2.4. ***Temporizzazione***

DDP_019 La figura di seguito riportata illustra i parametri di temporizzazione importanti durante il normale funzionamento:

Figura 1

Flusso di messaggi, temporizzazione



Dove:

P1 = Intervallo di tempo tra byte per la risposta della VU.

P2 = Intervallo di tempo tra la fine della richiesta dell'IDE e l'inizio della risposta della VU, o tra la fine della conferma di ricezione da parte dell'IDE e l'inizio della successiva risposta della VU.

P3 = Intervallo di tempo tra la fine della risposta della VU e l'inizio della nuova richiesta dell'IDE, o tra la fine della risposta della VU e l'inizio della conferma di ricezione da parte dell'IDE, o tra la fine della richiesta dell'IDE e l'inizio della nuova richiesta dell'IDE in caso di mancata risposta da parte della VU.

P4 = Intervallo di tempo tra byte per la richiesta da parte dell'IDE.

P5 = Valore ampliato di P3 per il trasferimento dei dati della carta.

I valori consentiti per i parametri di temporizzazione sono illustrati nella tabella successiva (impostazione dei parametri di temporizzazione supplementari relativi al KWP, utilizzata in caso di indirizzamento fisico per una comunicazione più veloce).

Parametri di temporizzazione	Valore limite inferiore (ms)	Valore limite superiore (ms)
T1	0	20
T2	20	1 000 (*)
T3	10	5 000
T4	5	20
T5	10	20 minuti

(*) in caso di risposta negativa da parte della VU contenente un codice che indichi "richiesta correttamente ricevuta, risposta pendente", il valore è esteso allo stesso valore limite superiore di P3.

2.2.5. ***Gestione degli errori***

In caso di errore durante lo scambio di messaggi, lo schema del flusso dei messaggi è modificato a seconda di quale apparecchio abbia rilevato l'errore e del messaggio che l'ha generato.

Le figure 2 e 3 indicano le procedure di gestione degli errori rispettivamente per la VU e per l'IDE.

2.2.5.1. *Fase di inizio della comunicazione*

DDP_020 Se durante la fase di avvio delle comunicazioni l'IDE rileva un errore, nella temporizzazione o nel flusso di bit, esso attende per un intervallo di tempo pari al valore minimo di P3 prima di riproporre la richiesta.

DDP_021 Se la VU rileva un errore nella sequenza inviata dall'IDE, essa non invia risposta e attende un altro messaggio di Richiesta di inizio comunicazione, che deve pervenire entro un limite di tempo pari al valore massimo di P3.

2.2.5.2. *Fase di comunicazione*

Si possono individuare due distinti ambiti di gestione degli errori:

1. Rilevamento da parte della VU di un errore di trasmissione dell'IDE

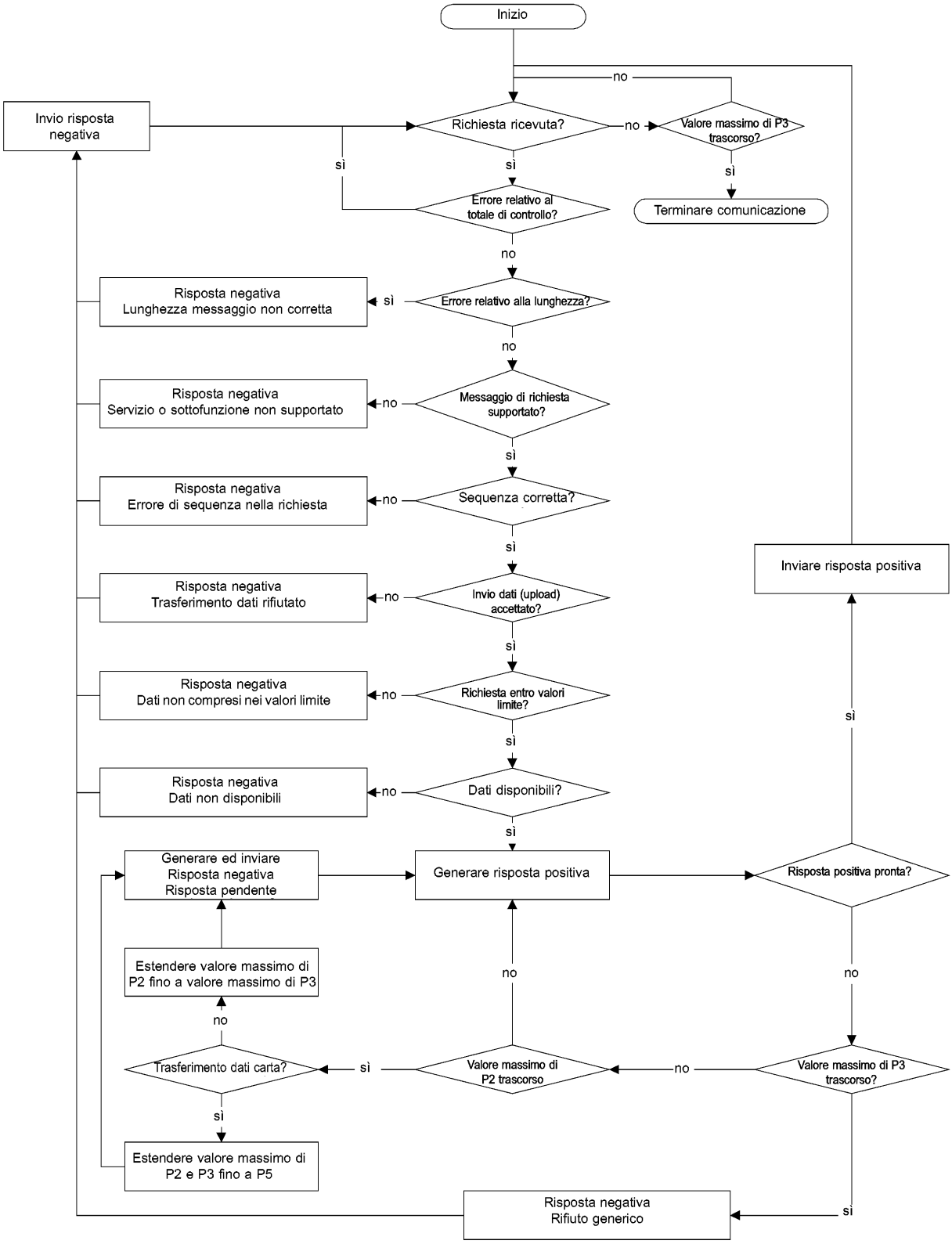
DDP_022 Per ogni messaggio ricevuto la VU rileva l'eventuale presenza di errori di temporizzazione, di formato dei byte (ad esempio: violazione dei bit di avvio e di arresto) e di struttura (numero errato dei byte ricevuti, byte errato relativo al totale di controllo).

DDP_023 In caso di rilevamento di uno degli errori sopra menzionati da parte della VU, quest'ultima non invia alcuna risposta e ignora il messaggio ricevuto.

DDP_024 È possibile che la VU rilevi altri errori relativi al formato o al contenuto del messaggio ricevuto (ad esempio, messaggio non supportato) anche se questo soddisfa i requisiti previsti di lunghezza e totale di controllo; in tal caso, la VU invia all'IDE un messaggio di Risposta negativa che specifica la natura dell'errore in questione.

Figura 2

Gestione degli errori da parte della VU



2. Rilevamento da parte dell'IDE di un errore di trasmissione della VU

DDP_025 Per ogni messaggio ricevuto l'IDE rileva l'eventuale presenza di errori di temporizzazione, di formato dei byte (ad esempio: violazione dei bit di avvio e di arresto) e di struttura (numero errato dei byte ricevuti, byte errato relativo al totale di controllo).

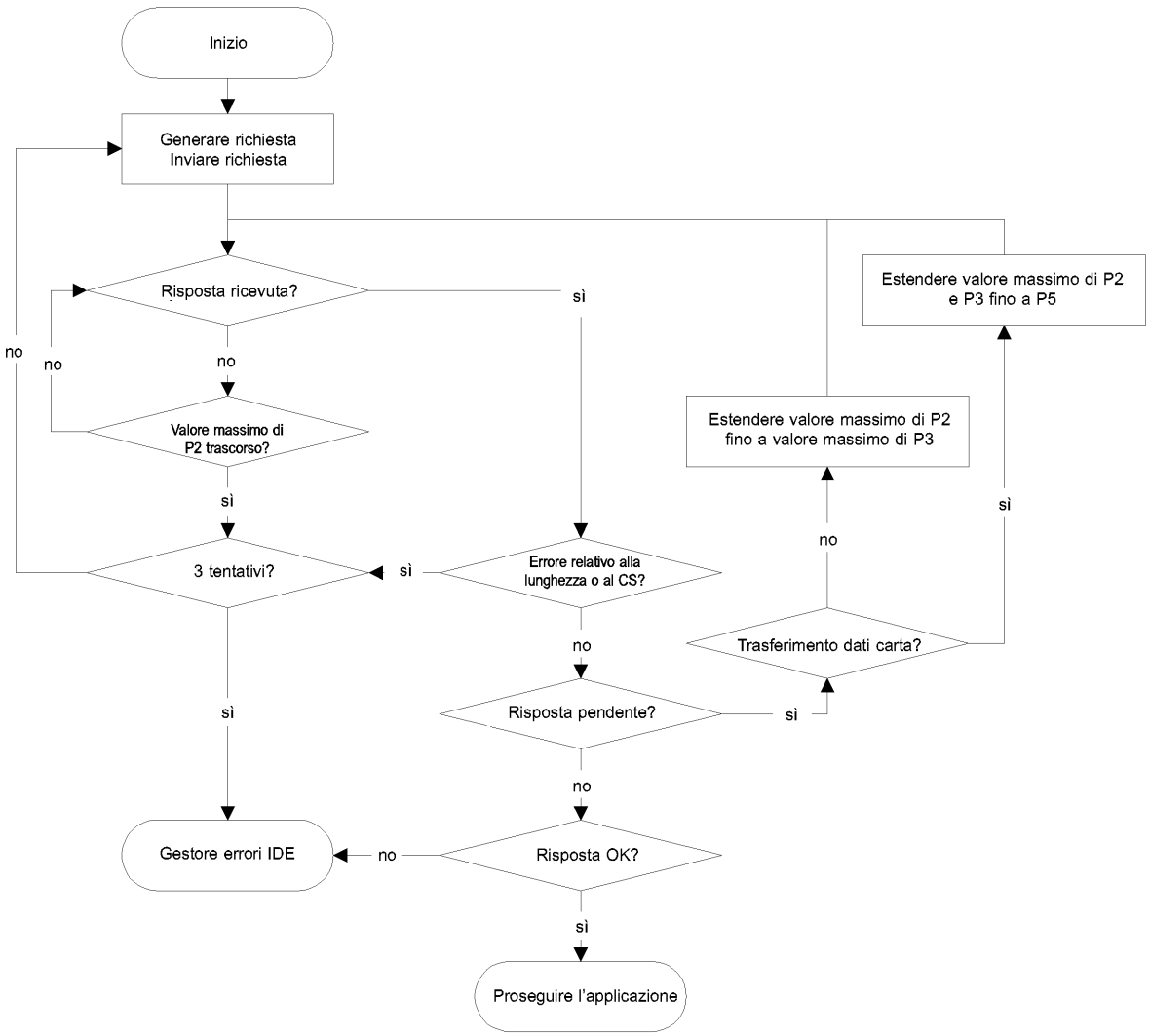
DDP_026 L'IDE rileva errori di sequenza, ad esempio messaggi successivi con incrementi non corretti del contatore di sottomessaggi.

DDP_027 In caso di rilevamento di un errore da parte dell'IDE o in assenza di risposta da parte della VU entro un periodo di tempo pari al valore massimo di P2, il messaggio di richiesta viene nuovamente inviato per un numero massimo complessivo di tre trasmissioni. Ai fini di tale rilevamento di errori, la conferma di ricezione di un sottomessaggio è considerata come una richiesta inviata alla VU.

DDP_028 L'IDE attende un intervallo di tempo pari almeno al valore minimo di P3 prima dell'inizio di ciascuna trasmissione; il periodo di attesa viene misurato a partire dall'ultimo intervento calcolato di un bit di arresto dopo il rilevamento dell'errore.

Figura 3

Gestione degli errori da parte dell'IDE



2.2.6. ***Contenuto del messaggio di risposta***

Il presente punto definisce il contenuto dei campi di dati dei vari messaggi di risposta positiva.

Gli elementi di dati sono definiti nell'Appendice 1 (Dizionario di dati).

2.2.6.1. *Risposta positiva di trasferimento dati ispezione*

DDP_029 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 75 e TREP 01, nonchè alla suddivisione e al conteggio appropriati dei sottomessaggi:

Elementi di dati	Lunghezza (byte)	Commento
MemberStateCertificate	194	Certificati di sicurezza della VU
VUCertificate	194	
VehicleIdentificationNumber	17	Identificazione del veicolo
VehicleRegistrationIdentification		
vehicleRegistrationNation	1	
vehicleRegistrationNumber	14	
CurrentDateTime	4	Data e ora correnti della VU
VuDownloadablePeriod		Periodo temporale disponibile per il trasferimento
minDownloadableTime	4	
maxDownloadableTime	4	
CardSlotsStatus	1	Tipo di carte inserite nella VU
VuDownloadActivityData		Precedente trasferimento dati della VU
downloadingTime	4	
fullCardNumber	18	
companyOrWorkshopName	36	
VuCompanyLocksData		Tutti i blocchi di impresa memorizzati. Se la sezione è vuota, viene inviato soltanto il dato noOfLocks = 0
noOfLocks	1	
...	(98)	
VuCompanyLocksRecord		
lockInTime	4	
lockOutTime	4	
companyName	36	
companyAddress	36	
companyCardNumber	18	
...		
VuControlActivityData		Tutte le registrazioni di controllo memorizzate nella VU. Se la sezione è vuota, viene inviato soltanto il dato noOfControls = 0
noOfControls	1	
...	(31)	
VuControlActivityRecord		
controlType	1	
controlTime	4	
controlCardNumber	18	
downloadPeriodBeginTime	4	
downloadPeriodEndTime	4	
...		
Signature	128	Firma RSA di tutti i dati (eccetto i certificati) a partire dal VehicleIdentificationNumber fino all'ultimo byte dell'ultimo VuControlActivityRecord

2.2.6.2. *Risposta positiva di trasferimento dati relativi alle attività*

DDP_030 Il campo contenente 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 e TREP 02, nonchè alla suddivisione e al conteggio appropriati dei sottomessaggi:

Elemento di dati	Lunghezza (byte)	Commento
TimeReal	4	Data del giorno oggetto del trasferimento
OdometerValueMidnight	3	Odometro al termine del giorno oggetto del trasferimento
VuCardIWData		Dati relativi ai cicli di estrazione/inserimento carte. — Se la presente sezione non contiene dati disponibili, viene inviato soltanto il dato noOfVuCardIWRecords = 0 — Se il periodo relativo a VuCardIWRecord comprende il superamento dell'ora 00.00 (inserimento carta nel giorno precedente) o 24.00 (estrazione carta nel giorno successivo), il dato compare per esteso all'interno dei due giorni interessati
noOfVuCardIWRecords	2	
...	(129)	
VuCardIWRecord: cardHolderName		
holderSurname	36	
holderFirstNames	36	
fullCardNumber	18	
cardExpiryDate	4	
cardInsertionTime	4	
vehicleOdometerValueAtInsertion	3	
cardSlotNumber	1	
cardWithdrawalTime	4	
vehicleOdometerValueAtWithdrawal	3	
previousVehicleInfo		
vehicleRegistrationIdentification		
vehicleRegistrationNation	1	
vehicleRegistrationNumber	14	
cardWithdrawalTime	4	
manualInputFlag	1	
...		
VuActivityDailyData		Condizione della sede (slot) a 00h00 e cambi di attività registrati relativi al giorno oggetto del trasferimento.
noOfActivityChanges	2	
...		
ActivityChangeInfo	2	
...		
VuPlaceDailyWorkPeriodData		Dati sui luoghi registrati relativi al giorno oggetto del trasferimento. Se la sezione è vuota, viene inviato soltanto il dato noOfPlaceRecords = 0
noOfPlaceRecords	1	
...	(28)	
VuPlaceDailyWorkPeriodRecord: fullCardNumber	18	
placeRecord		
entryTime	4	
entryTypeDailyWorkPeriod	1	
dailyWorkPeriodCountry	1	
dailyWorkPeriodRegion	1	
vehicleOdometerValue	3	
...		
VuSpecificConditionData		Dati su condizioni particolari registrate relative al giorno oggetto del trasferimento. Se la sezione è vuota, viene inviato soltanto il dato noOfSpecificConditionRecords = 0
noOfSpecificConditionRecords	2	
...	(5)	
SpecificConditionRecord		
EntryTime	4	
specificConditionType	1	
...		
Signature	128	Firma RSA di tutti i dati a partire da TimeReal fino all'ultimo byte dell'ultima registrazione di condizioni particolari

2.2.6.3. *Risposta positiva di trasferimento dati relativi ad anomalie e guasti*

DDP_031 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 e TREP 03, nonchè alla suddivisione e al conteggio appropriati dei sottomessaggi:

Elemento di dati	Lunghezza (byte)	Commento
VuFaultData		Tutti i guasti memorizzati o in corso nella VU. Se la sezione è vuota, viene inviato soltanto il dato noOfVuFaults = 0
NoOfVuFaults	1	
...	(82)	
VuFaultRecord: FaultType	1	
VuFaultRecord: FaultRecordPurpose	1	
VuFaultRecord: FaultBeginTime	4	
VuFaultRecord: FaultEndTime	4	
VuFaultRecord: CardNumberDriverSlotBegin	18	
VuFaultRecord: cardNumberCodriverSlotBegin	18	
VuFaultRecord: CardNumberDriverSlotEnd	18	
VuFaultRecord: CardNumberCodriverSlotEnd	18	
...		
VuEventData		Tutte le anomalie (eccetto il superamento di velocità) memorizzate o in corso nella VU. Se la sezione è vuota, viene inviato soltanto il dato noOfVuEvents = 0
NoOfVuEvents	1	
...	(83)	
VuEventRecord: EventType	1	
VuEventRecord: EventRecordPurpose	1	
VuEventRecord: EventBeginTime	4	
VuEventRecord: EventEndTime	4	
VuEventRecord: CardNumberDriverSlotBegin	18	
VuEventRecord: cardNumberCodriverSlotBegin	18	
VuEventRecord: CardNumberDriverSlotEnd	18	
VuEventRecord: CardNumberCodriverSlotEnd	18	
VuEventRecord: SimilarEventsNumber	1	
...		
VuOverSpeedingControlData		Dati relativi all'ultimo controllo del superamento di velocità (valore predefinito in assenza di dati)
LastOverspeedControlTime	4	
FirstOverspeedSince	4	
NumberOfOverspeedSince	1	
VuOverSpeedingEventData		Tutte le anomalie relative al superamento di velocità memorizzate nella VU. Se la sezione è vuota, viene inviato soltanto il dato noOfVuOverSpeedingEvents = 0
NoOfVuOverSpeedingEvents	1	
...	(31)	
VuOverSpeedingEventRecord: EventType	1	
VuOverSpeedingEventRecord: EventRecordPurpose	1	
VuOverSpeedingEventRecord: EventBeginTime	4	
VuOverSpeedingEventRecord: EventEndTime	4	
VuOverSpeedingEventRecord: MaxSpeedValue	1	
VuOverSpeedingEventRecord: AverageSpeedValue	1	
VuOverSpeedingEventRecord: CardNumberDriverSlotBegin	18	
VuOverSpeedingEventRecord: SimilarEventsNumber	1	
...		
VuTimeAdjustmentData		Tutte le anomalie relative alla regolazione dell'ora memorizzate nella VU (al di fuori di un ciclo completo di calibratura). Se la sezione è vuota, viene inviato soltanto il dato noOfVuTimeAdjRecords = 0
NoOfVuTimeAdjRecords	1	
...	(98)	
VuTimeAdjustmentRecord: OldTimeValue	4	
VuTimeAdjustmentRecord: NewTimeValue	4	
VuTimeAdjustmentRecord: WorkshopName	36	
VuTimeAdjustmentRecord: WorkshopAddress	36	
VuTimeAdjustmentRecord: WorkshopCardNumber	18	
...		
Signature	128	Firma RSA di tutti i dati a partire da noOfVuFaults fino all'ultimo byte dell'ultima registrazione relativa alla regolazione dell'ora

2.2.6.4. *Risposta positiva di trasferimento dati dettagliati relativi alla velocità*

DDP_032 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 e TREP 04, nonchè alla suddivisione e al conteggio appropriati dei sottomessaggi:

Elemento di dati	Lunghezza (byte)	Commento
VuDetailedSpeedData		Tutti i dati dettagliati relativi alla velocità memorizzati nella VU (un blocco velocità al minuto a veicolo in movimento) 60 valori di velocità al minuto (uno al secondo)
NoOfSpeedBlocks	2	
...	(64)	
VuDetailedSpeedBlock: SpeedBlockBeginDate	4	
VuDetailedSpeedBlock: speedsPerSecond	60	
...		
Signature	128	Firma RSA di tutti i dati a partire da noOfSpeedBlocks fino all'ultimo byte relativo all'ultimo blocco di velocità

2.2.6.5. *Risposta positiva di trasferimento dati tecnici*

DDP_033 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 e TREP 05, nonchè alla suddivisione e al conteggio appropriati dei sottomessaggi:

Elemento di dati	Lunghezza (byte)	Commento
VuIdentification		
vuManufacturerName	36	
vuManufacturerAddress	36	
vuPartNumber	16	
vuSerialNumber	8	
vuSoftwareIdentification		
vuSoftwareVersion	4	
vuSoftInstallationDate	4	
vuManufacturingDate	4	
vuApprovalNumber	8	
SensorPaired		
sensorSerialNumber	8	
sensorApprovalNumber	8	
sensorPairingDateFirst	4	
VuCalibrationData		Tutte le registrazioni relative alla calibratura memorizzate nella VU
noOfVuCalibrationRecords	1	
...	(164)	
VuCalibrationRecord: calibrationPurpose	1	
VuCalibrationRecord: workshopName	36	
VuCalibrationRecord: workshopAddress	36	
VuCalibrationRecord: workshopCardNumber	18	
VuCalibrationRecord: workshopCardExpiryDate	4	
VuCalibrationRecord: vehicleIdentificationNumber	17	
VuCalibrationRecord: vehicleRegistrationIdentification		
VuCalibrationRecord: vehicleRegistrationNation	1	
VuCalibrationRecord: vehicleRegistrationNumber	14	
VuCalibrationRecord: wVehicleCharacteristicConstant	2	
VuCalibrationRecord: kConstantOfRecordingEquipment	2	
VuCalibrationRecord: lTyreCircumference	2	
VuCalibrationRecord: tyreSize	15	
VuCalibrationRecord: authorisedSpeed	1	
VuCalibrationRecord: oldOdometerValue	3	
VuCalibrationRecord: newOdometerValue	3	
VuCalibrationRecord: oldTimeValue	4	
VuCalibrationRecord: newTimeValue	4	
VuCalibrationRecord: nextCalibrationDate	4	
...		
Signature	128	Firma RSA di tutti i dati a partire da vuManufactuerName fino all'ultimo byte dell'ultimo dato relativo a VuCalibrationRecord

2.3. **Memorizzazione dei file ESM**

DDP_034 Se una sessione di trasferimento comprende dati relativi alla VU, l'IDE memorizza in un unico file fisico tutti i dati ricevuti dalla VU nel corso della sessione nell'ambito dei messaggi di risposta positiva di trasferimento dati. I dati memorizzati non comprendono le intestazioni dei messaggi, i contatori dei sottomessaggi, i sottomessaggi vuoti e i totali di controllo, ma comprendono SID e TREP (relativi soltanto al primo sottomessaggio nel caso di più sottomessaggi).

3. PROTOCOLLO DI TRASFERIMENTO DEI DATI DELLE CARTE TACHIGRAFICHE

3.1. **Campo di applicazione**

Il presente punto descrive il trasferimento diretto dei dati relativi alla carta tachigrafica ad un IDE. Poiché quest'ultimo non è parte dell'ambiente sicuro, non viene effettuata alcuna autenticazione tra la carta e l'IDE.

3.2. **Definizioni**

Sessione di trasferimento: Ogni trasferimento di dati dell'ICC. La sessione comprende la procedura completa, dalla reinizializzazione dell'ICC da parte di un IFD fino alla disattivazione dell'ICC (estrazione della carta o reinizializzazione successiva).

File di dati con firma: Un file proveniente dall'ICC. Il file è trasferito all'IFD con testo in chiaro. Nell'ICC il file viene "frammentato" (con la funzione di hash) e firmato, quindi la firma è trasferita all'IFD.

3.3. **Trasferimento dei dati della carta**

DDP_035 Il trasferimento dei dati di una carta tachigrafica comprende le seguenti fasi:

— Trasferimento negli EF `ICC` e `IC` dell'informazione comune relativa alla carta. Questa informazione è facoltativa e non è resa sicura mediante firma digitale.

— Trasferimento degli EF `Card_Certificate` e . 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 DF `Tachograph`) ad eccezione di EF `Card_Download`. Questa informazione è resa sicura mediante firma digitale.

  — Per ogni sessione di trasferimento è obbligatorio il trasferimento almeno degli EF `Application_Identification` e `ID`.

  — Nel trasferire i dati relativi alla carta del conducente è obbligatorio trasferire anche i seguenti EF:

    — `Events_Data`,

    — `Faults_Data`,

    — `Driver_Activity_Data`,

    — `Vehicles_Used`,

    — `Places`,

    — `Control_Activity_Data`,

    — `Specific_Conditions`.

— Nel trasferimento dei dati relativi alla carte del conducente, aggiomare il dato `LastCard_Download` nell'EF `Card_Download`,

— Nel trasferimento dei dati relativi alla carta dell'officina, azzerare il contatore di calibratura nell'EF `Card_Download`.

3.3.1. ***Sequenza di inizializzazione***

DDP_036 L'IDE avvia la sequenza nel modo seguente:

Carta	Direzione	IDE/IFD	Significato/Osservazioni
	⇦	Reinizializzazione Hardware	
ATR	⇨		

È facoltativo utilizzare la PPS per passare ad una velocità di trasmissione maggiore fintanto che l'ICC sia in grado di supportarla.

3.3.2. ***Sequenza dei file di dati non firmati***

DDP_037 La sequenza per il trasferimento degli EF `ICC`, `IC`, `Card_Certificate` e `CA_Certificate` è la seguente:

Carta	Direzione	IDE/IFD	Significato/Osservazioni
	⇦	SELECT FILE	Selezione mediante identificativi di file
OK	⇨		
	⇦	READ BINARY	Se il file contiene un numero di dati superiore alle dimensioni della memoria di transito del lettore o della carta, è necessario ripetere il comando fino all'avvenuta lettura del file completo
File Data OK	⇨	Invio dati in memoria a ESM	Conformemente al punto 3.4, Formato di memorizzazione dei dati

Nota: prima di selezionare l'EF `Card_Certificate`, è necessario selezionare l'applicazione del tachigrafo (selezione mediante AID).

3.3.3. ***Sequenza dei file di dati firmati***

DDP_038 Per ciascuno dei seguenti file che devono essere trasferiti insieme alla rispettiva firma è necessario utilizzare la successiva sequenza:

Carta	Direzione	IDE/IFD	Significato/Osservazioni
	⇦	SELECT FILE	
OK	⇨		
	⇦	PERFORM HASH OF FILE	Calcola il valore di hash sul contenuto dei dati del file selezionato, mediante l'algoritmo di hash conformemente all'Appendice 11. Il comando in questione non è del tipo ISO
Calcolo del valore di hash relativo al file e memorizzazione temporanea di tale valore			
OK	⇨		
	⇦	READ BINARY	Se il file contiene un numero di dati superiore alle dimensioni della memoria di transito 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	Conformemente al punto 3.4, Formato di memorizzazione dei dati
	⇦	PSO: COMPUTE DIGITAL SIGNATURE	
Esecuzione dell'operazione di sicurezza "Calcolo firma digitale" mediante il valore di hash temporaneamente memorizzato			
Firma OK	⇨	Aggiunta dei dati a quelli precedentemente memorizzati nell'ESM	Conformemente al punto 3.4, Formato di memorizzazione dei dati

3.3.4. ***Sequenza di azzeramento del contatore di calibratura***

DDP_039 La sequenza di azzeramento del contatore `NoOfCalibrationsSinceDownload` nell'EF `Card_Download` in una carta dell'officina è il seguente:

Carta	Direzione	IDE/IFD	Significato/Osservazioni
OK	⇦ ⇨	SELECT FILE EF `Card_Download`	Selezione mediante identificativi di file
	⇦	UPDATE BINARY `NoOfCalibrationsSinceDownload` = '00 00'	
Azzeramento numero di trasferimenti dati carta			
OK	⇨		

3.4. **Formato di memorizzazione dei dati**

3.4.1. ***Introduzione***

DDP_040 La memorizzazione dei dati trasferiti deve avvenire nel rispetto delle seguenti condizioni:

— I dati devono essere memorizzati in modo trasparente. Ciò significa che durante la memorizzazione è necessario rispettare l'ordine dei byte, così come quello dei bit all'interno dei byte trasferiti dalla carta.

— Tutti i file relativi alla carta trasferiti nell'ambito di una stessa sessione sono memorizzati nell'ESM in un unico file.

3.4.2. ***Formato dei file***

DDP_041 Il formato dei file è costituito da una concatenazione di diversi oggetti TLV.

DDP_042 Il tag di un EF deve essere costituito dal FID seguito dall'appendice "00".

DDP_043 Il tag di una firma relativa ad un EF deve essere costituito dal FID del file stesso seguito dall'appendice "01".

DDP_044 La lunghezza è rappresentata da un valore di due byte. Tale valore definisce il numero di byte che costituiscono il campo valori. Il valore "FF FF" nel campo relativo alla lunghezza è disponibile per un uso futuro.

DDP_045 In caso di mancato trasferimento di un file, non viene memorizzato alcun dato ad esso relativo (nessun tag né valore zero relativo alla lunghezza).

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)	3 byte
FID (2 byte) || "01"	Tag per firma di EF (FID)	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`
05 05 01	00 80	Firma dell'EF `Vehicles_Used`

4. TRASFERIMENTO DEI DATI RELATIVI AD UNA CARTA TACHIGRAFICA ATTRAVERSO L'UNITÀ ELETTRONICA DI BORDO.

DDP_047 La VU deve consentire di trasferire il contenuto della carta del conducente inserita ad un IDE ad essa collegata.

DDP_048 Per avviare la modalità in questione (cfr. 2.2.2.9) l'IDE invia alla VU un messaggio "Richiesta di trasferimento dati relativi a carta tachigrafica".

DDP_049 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".

DDP_050 L'IDE deve ricuperare i dati relativi alla carta dal messaggio "Risposta positiva di trasferimento dati" (eliminando tutte le intestazioni, i SID, i TREP, i contatori di sottomessaggi, e i totali di controllo) e memorizzarli all'interno di un unico file fisico secondo quanto descritto al punto 2.3.

DDP_051 La VU deve quindi, se del caso, aggiornare il file `ControlActivityData` o il file `Card_Download` della carta del conducente.

Appendice 8

PROTOCOLLO DI CALIBRATURA

INDICE

1. INTRODUZIONE

La presente appendice descrive come avviene lo scambio di dati tra l'unità elettronica di bordo e un tester (apparecchio di prova) attraverso la linea K, che costituisce parte dell'interfaccia di calibratura illustrata nell'appendice 6; descrive inoltre il controllo della linea dei segnali di entrata/uscita sul connettore di calibratura.

La procedura per stabilire le comunicazioni sulla linea K è descritta nella sezione 4 "Servizi di comunicazione".

La presente appendice si avvale del concetto di "sessioni" diagnostiche per stabilire la finalità del controllo sulla linea K in diverse condizioni. L'impostazione predefinita è la "sessione diagnostica standard", che consente la lettura di tutti i dati dell'unità elettronica di bordo ma non la scrittura di dati nell'unità stessa.

Il prospetto delle sessioni diagnostiche è riportato nella sezione 5 "Servizi di gestione".

CPR_001 La "sessione di programmazione ECU" consente l'inserimento dei dati nell'unità elettronica di bordo. In caso di inserimento dei dati di calibratura (requisiti 097 e 098), l'unità elettronica di bordo deve inoltre essere in modalità CALIBRATURA.

La procedura di trasferimento dati sulla linea K è descritta nella sezione 4 "Servizi di comunicazione". Il formato dei dati trasferiti è descritto in dettaglio nella sezione 8 "formato delle registrazioni".

CPR_002 La "sessione di regolazione ECU" consente di selezionare la modalità I/O della linea dei segnali di entrata/uscita di calibratura attraverso l'interfaccia della linea K. Il controllo della linea dei segnali di entrata/uscita è descritto nella sezione 7 "Controllo degli impulsi di prova — Unità funzionale di controllo dei segnali di entrata/uscita".

CPR_003 Nel presente documento l'indirizzo del tester è indicato come 'tt'. Nonostante vi possano essere indirizzi preferenziali, la VU deve rispondere correttamente a qualsiasi indirizzo di tester. L'indirizzo fisico della VU è 0xEE.

2. TERMINI, DEFINIZIONI E RIFERIMENTI

I protocolli, i messaggi ed i codici di errore si basano in gran parte sulla versione più aggiornata del progetto di norma ISO14299-1 (Road vehicles — Diagnostic systems — Part 1: Diagnostic services, version 6 of 22 February 2001).

Per gli identificativi di servizio, le richieste di servizio e le relative risposte e per i parametri standard si utilizzano la codifica a byte e valori esadecimali.

Il termine "tester" si riferisce all'apparecchio utilizzato per l'inserimento dei dati di programmazione/calibratura nella VU.

I termini "client" e "server" si riferiscono rispettivamente al tester e alla VU.

Il termine ECU (Electronic Control Unit — Unita elettronica di controllo) si riferisce alla VU.

Riferimenti normativi:

ISO 14230-2: Road Vehicles -Diagnostic Systems — Keyword Protocol 2000 — Part 2: Data Link Layer. First edition: 1999. (Veicoli — Sistemi diagnostici)

3. PROSPETTO DEI SERVIZI

3.1. **Servizi disponibili**

La seguente tabella fornisce il prospetto dei servizi disponibili nell'apparecchio di controllo e definiti nell'ambito del presente documento.

CPR_004 La tabella indica i servizi disponibili in una sessione diagnostica abilitata.

— La 1a colonna elenca i servizi disponibili.

— La 2a colonna indica il numero della sezione all'interno della presente appendice in cui il servizio è ulteriormente definito.

— La 3a colonna assegna i valori dell'identificativo servizio per i messaggi di richiesta.

— La 4a colonna specifica i servizi di "StandardDiagnosticSession" (SD) che devono essere attuati in ogni VU.

— La 5a colonna specifica i servizi di "ECUAdjustmentSession" (ECUAS) che devono essere attuati per consentire il controllo della linea dei segnali I/O nel connettore di calibratura situato sul pannello frontale della VU.

— La 6a colonna specifica i servizi di "ECUProgrammingSession" (ECUPS) che devono essere attuati per consentire la programmazione dei parametri all'interno della VU.

Tabella 1

Tabella riassuntiva dei valori di identificativo servizio

			Sessioni diagnostiche		
Nome del servizio diagnostico	N. sezione	Val. Rich. SID	SD	ECUAS	ECUPS
StartCommunication	4.1	81	■	■	■
StopCommunication	4.2	82	■		
Testerpresent	4.3	3E	■	■	■
StartDiagnosticSession	5.1	10	■	■	■
SecurityAccess	5.2	27	■	■	■
ReadDataByIdentifier	6.1	22	■	■	■
WriteDataByIdentifier	6.2	2E			■
InputOutputControlByIdentifier	7.1	2F		■	

■ Questo simbolo indica che il servizio è obbligatorio nella corrispondente sessione diagnostica.
L'assenza di simboli indica che il servizio in questione non è consentito nella corrispondente sessione diagnostica.

3.2. **Codici di risposta**

Per ogni servizio sono definiti appositi codici di risposta.

4. SERVIZI DI COMUNICAZIONE

Determinati servizi sono necessari per stabilire e mantenere le comunicazioni e non compaiono al livello di applicazione. I servizi disponibili sono descritti nella seguente tabella:

Tabella 2

Servizi di comunicazione

Nome del servizio	Descrizione
StartCommunication	Il client richiede l'inizio di una sessione di comunicazione con il/i server.
StopCommunication	Il client richiede il termine della sessione di comunicazione corrente.
TesterPresent	Il client segnala al server di essere ancora in contatto.

CPR_005 Il servizio StartCommunication è utilizzato per iniziare una comunicazione. Per poter eseguire qualsiasi servizio è necessario inizializzare la comunicazione in oggetto ed i parametri di comunicazione devono essere quelli adatti alla modalità richiesta.

4.1. **Servizio StartCommunication**

CPR_006 Alla ricezione di una primitiva di indicazione di StartCommunication, la VU verifica se nelle condizioni correnti sia possibile inizializzare il collegamento della comunicazione richiesta. La condizioni valide per l'inizializzazione del collegamento sono descritte nel documento della norma ISO 14230-2.

CPR_007 Quindi la VU compie tutte le azioni necessarie a inizializzare il collegamento ed invia una primitiva di risposta di StartCommunication con i parametri di Risposta positiva selezionati.

CPR_008 Se una VU già inizializzata (con qualsiasi sessione diagnostica in corso) riceve un nuovo messaggio StartCommunication Request (ad esempio a causa del recupero dell'errore nel tester) la richiesta viene accettata e la VU deve essere nuovamente inizializzata.

CPR_009 Se per qualsiasi motivo non è possibile procedere all'inizializzazione del collegamento, la VU continua a funzionare nelle condizioni immediatamente precedenti al tentativo di inizializzazione.

CPR_010 Il messaggio StartCommunication Request deve essere indirizzato fisicamente.

CPR_011 L'inizializzazione della VU per i servizi è effettuato con un metodo di "inizializzazione veloce", che prevede:

— un tempo di inattività del bus prima di qualsiasi attività,

— il susseguente invio da parte del tester di una configurazione di inizializzazione,

— la presenza nella risposta della VU di tutte le informazioni necessarie a stabilire la comunicazione.

CPR_012 Una volta completata l'inizializzazione:

— tutti i parametri di comunicazione sono impostati sui valori predefiniti nella tabella 4, conformemente ai byte chiave,

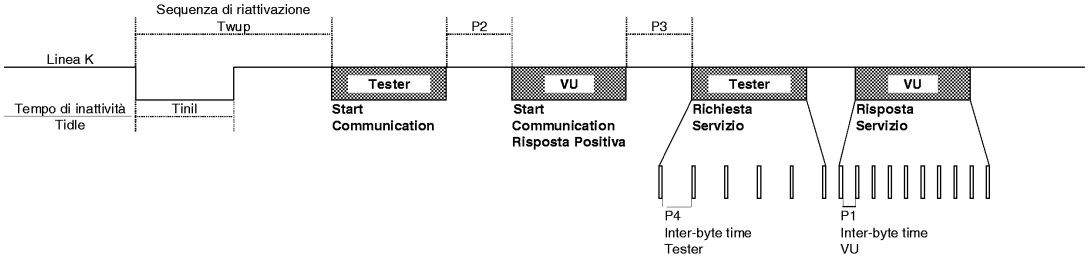
— la VU resta in attesa della prima richiesta da parte del tester,

— la VU risulta in modalità di diagnosi predefinita, ovvero impostata su StandardDiagnosticSession,

— linea dei segnali I/O di calibratura è nell'impostazione predefinita, ovvero disabilitata.

CPR_014 La frequenza dei dati sulla linea K deve essere di 10 400 baud.

CPR_016 L'inizializzazione veloce è avviata dal tester con la trasmissione della sequenza di riattivazione (Wup) sulla linea K. La sequenza inizia con un tempo breve di Tinil dopo il tempo di inattività sulla linea K. Il tester trasmette quindi il primo bit del servizio StartCommunication dopo un tempo di Twup successivo al primo fronte di discesa.



CPR_017 I valori di temporizzazione per l'inizializzazione veloce e le comunicazioni in generale sono illustrati nelle seguenti tabelle. Vi sono differenti possibilità per ciò che riguarda il tempo di inattività:

— prima trasmissione seguente l'accensione, tempo di inattività = 300 ms,

— dopo il completamento di un servizio StopCommunication, tempo di inattività = P3min,

— dopo il termine della comunicazione a causa del superamento del tempo limite P3max, tempo di inattività = 0.

Tabella 3

Valori di temporizzazione per l'inizializzazione veloce

Parametro		Valore minimo	Valore massimo
Tinil	25 ± 1 ms	24 ms	26 ms
Twup	50 ± 1 ms	49 ms	51 ms

Tabella 4

Valori di temporizzazione della comunicazione

Parametro di temporizzazione	Descrizione parametro	Valore minimo [ms]	Valore massimo [ms]
		min.	max.
P1	Intervallo di tempo tra byte per la risposta della VU	0	20
P2	Tempo intercorrente tra la richiesta del tester e la risposta della VU o tra due risposte della VU	25	250
P3	Tempo intercorrente tra la conclusione delle risposte della VU e l'inizio di una nuova richiesta del tester	55	5000
P4	Intervallo di tempo tra byte per la richiesta del tester	5	20

CPR_018 Il formato del messaggio per l'inizializzazione veloce è descritto nelle tabelle seguenti.

Tabella 5

Messaggio StartCommunication Request

Byte n.	Denominazione del parametro	Valore esadecimale	Mnemonico
n. 1	Byte di formato — indirizzamento fisico	81	FMT
n. 2	Byte dell'indirizzo di destinazione	EE	TGT
n. 3	Byte dell'indirizzo di provenienza	tt	SRC
n. 4	Identificativo StartCommunication Request Service	81	SCR
n. 5	Totale di controllo	00-FF	CS

Tabella 6

Messaggio StartCommunication Positive Response

Byte n.	Denominazione del parametro	Valore esadecimale	Mnemonico
n. 1	Byte di formato — indirizzamento fisico	80	FMT
n. 2	Byte dell'indirizzo di destinazione	tt	TGT
n. 3	Byte dell'indirizzo di provenienza	EE	SRC
n. 4	Byte di lunghezza aggiuntivo	03	LEN
n. 5	Identificativo StartCommunication Positive Response Service	C1	SCRPR
n. 6	Byte-chiave 1	EA	KB1
n. 7	Byte-chiave 2	8F	KB2
n. 8	Totale di controllo	00-FF	CS

CPR_019 Non vi è alcuna risposta negativa al messaggio StartCommunication Request; in assenza di messaggi di risposta positiva da trasmettere, la VU non è inizializzata, rimane in modalità di funzionamento normale e non vi è trasmissione.

4.2. **Servizio StopCommunication**

4.2.1. ***Descrizione del messaggio***

Lo scopo di questo servizio è la conclusione di una sessione di comunicazione.

CPR_020 Al ricevimento di una primitiva di indicazione di StopCommunication, la VU verifica se nelle condizioni correnti sia possibile concludere la comunicazione in atto. In tal caso la VU compie tutte le azioni necessarie allo scopo.

CPR_021 Se la conclusione della comunicazione risulta attuabile, prima di procedere la VU invia una primitiva di risposta di StopCommunication con i parametri di Risposta positiva selezionati.

CPR_022 Se invece per qualsiasi motivo non è possibile procedere alla conclusione della comunicazione, la VU invia una primitiva di risposta di StopCommunication con il parametro di Risposta negativa selezionato.

CPR_023 In caso di riscontro da parte della VU di un tempo di superamento del tempo limite P3max, la comunicazione viene terminata senza invio di alcuna primitiva di risposta.

4.2.2. ***Formato del messaggio***

CPR_024 I formati dei messaggi per le primitive di StopCommunication sono descritti nelle seguenti tabelle.

Tabella 7

Messaggio StopCommunication Request

Byte n.	Denominazione del parametro	Valore esadecimale	Mnemonico
n. 1	Byte di formato — indirizzamento fisico	80	FMT
n. 2	Byte dell'indirizzo di destinazione	EE	TGT
n. 3	Byte dell'indirizzo di provenienza	tt	SRC
n.4	Byte di lunghezza aggiuntivo	01	LEN
n. 5	Identificativo StopCommunication Request Service	82	SPR
n. 6	Totale di controllo	00-FF	CS

Tabella 8

Messaggio StopCommunication Positive Response

Byte n.	Denominazione del parametro	Valore esadecimale	Mnemonico
n. 1	Byte di formato — indirizzamento fisico	80	FMT
n. 2	Byte dell'indirizzo di destinazione	tt	TGT
n. 3	Byte dell'indirizzo di provenienza	EE	SRC
n. 4	Byte di lunghezza aggiuntivo	01	LEN
n. 5	Identificativo StopCommunication Positive Response Service	C2	SPRPR
n. 6	Totale di controllo	00-FF	CS

Tabella 9

Messaggio StopCommunication Negative Response

Byte n.	Denominazione del parametro	Valore esadecimale	Mnemonico
n. 1	Byte di formato — indirizzamento fisico	80	FMT
n. 2	Byte dell'indirizzo di destinazione	tt	TGT
n. 3	Byte dell'indirizzo di provenienza	EE	SRC
n. 4	Byte di lunghezza aggiuntivo	03	LEN
n. 5	Identificativo negative Response Service	7F	NR
n. 6	StopCommunication Request Service Identification	82	SPR
n. 7	responseCode = generalReject	10	RC_GR
n. 8	Totale di controllo	00-FF	CS

4.2.3. **Definizione dei parametri**

Questo servizio non richiede la definizione dei parametri.

4.3. Servizio TesterPresent

4.3.1. **Descrizione del messaggio**

Il servizio TesterPresent è impiegato dal tester per indicare al server di essere ancora in collegamento, in modo che il server non torni automaticamente alla modalità di funzionamento normale, interrompendo così l'eventuale comunicazione. Tale servizio, attivato periodicamente, mantiene attiva la sessione diagnostica/di comunicazione reimpostando il timer P3 ogni volta che il servizio stesso viene richiesto.

4.3.2. **Formato del messaggio**

CPR_079 I formati dei messaggi per le primitive di TesterPresent sono descritti nelle seguenti tabelle.

Tabella 10

Messaggio TesterPresent Request

Byte n.	Denominazione del parametro	Valore esadecimale	Mnemonico
n. 1	Byte di formato — indirizzamento fisico	80	FMT
n. 2	Byte dell'indirizzo di destinazione	EE	TGT
n. 3	Byte dell'indirizzo di provenienza	tt	SRC
n. 4	Byte di lunghezza aggiuntivo	02	LEN
n. 5	Identificativo della richiesta di TesterPresent	3E	TP
n. 6	Sottofunzione = risposta richiesta = [si	01	RESPREQ_Y
	no]	02	RESPREQ_NO
n. 7	Totale di controllo	00-FF	CS

CPR_080 Se il parametro risposta richiesta è impostato su "sì" il server deve rispondere con il presente messaggio di risposta positiva. Se è impostato su "no" il server non invia alcuna risposta.

Tabella 11

Messaggio TesterPresent Positive Response

Byte n.	Denominazione del parametro	Valore esadecimale	Mnemonico
n. 1	Byte di formato — indirizzamento fisico	80	FMT
n. 2	Byte dell'indirizzo di destinazione	tt	TGT
n. 3	Byte dell'indirizzo di provenienza	EE	SRC
n. 4	Byte di lunghezza aggiuntivo	01	LEN
n. 5	Identificativo TesterPresent Positive Response Service	7E	TPPR
n. 6	Totale di controllo	00-FF	CS

CPR_081 Il presente servizio utilizza i seguenti codici di risposta negativa:

Tabella 12

Messaggio TesterPresent Negative Response

Byte n.	Denominazione del parametro	Valore esadecimale	Mnemonico
n. 1	Byte di formato — indirizzamento fisico	80	FMT
n. 2	Byte dell'indirizzo di destinazione	tt	TGT
n. 3	Byte dell'indirizzo di provenienza	EE	SRC
n. 4	Byte di lunghezza aggiuntivo	03	LEN
n. 5	Identificativo negative Response Service	7F	NR
n. 6	Identificativo TesterPresent Request Service	3E	TP
n. 7	codice di risposta = [SubFunctionNotSupported-InvalidFormat	12	RC_SFNS_IF
	incorrectMessageLength]	13	RC_IML
n. 8	Totale di controllo	00-FF	CS

5. SERVIZI DI GESTIONE

I servizi disponibili sono descritti nella seguente tabella:

Tabella 13

Servizi di gestione

Nome del servizio	Descrizione
StartDiagnosticSession	Il client richiede l'avvio della sessione diagnostica con una VU.
SecurityAccess	Il client richiede l'accesso a funzioni riservate ad utenti autorizzati.

5.1. **Servizio StartDiagnosticSession**

5.1.1. ***Descrizione del messaggio***

CPR_025 Il servizio StartDiagnosticSession serve ad abilitare nel server sessioni diagnostiche differenti. Una sessione diagnostica abilita una serie specifica di servizi secondo quanto illustrato nella Tabella 17. Nel corso di una sessione possono essere attivati servizi specificamente legati alle necessità del fabbricante del veicolo non previsti nel presente documento. Le regole di attuazione devono soddisfare i seguenti requisiti:

— nella VU deve essere sempre attiva una ed una sola sessione diagnostica,

— all'accensione, la Vu deve sempre attivare la StandardDiagnosticSession, se non viene attivata nessun'altra sessione diagnostica, la StandardDiagnosticSession deve continuare a funzionare fintantoché la VU è accesa,

— se il tester richiede una sessione diagnostica già attiva, la VU deve inviare un messaggio di risposta positivo,

— quando il tester richiede una nuova sessione diagnostica, la VU deve innanzitutto inviare un messaggio di risposta positiva di StartDiagnosticSession prima di attivare la nuova sessione. Se non è in grado di avviare la nuova sessione diagnostica richiesta, la VU invia un messaggio di risposta negativa di StartDiagnosticSession e mantiene attiva la sessione corrente.

CPR_026 L'avvio di una sessione diagnostica avviene soltanto in presenza di comunicazioni già stabilite tra il client e la VU.

CPR_027 I parametri di temporizzazione definiti nella tabella 4 si attivano in seguito all'invio completato con successo del messaggio StartDiagnosticSession, con parametro diagnosticSession impostato su “StandardDiagnosticSession” nel messaggio di richiesta nel caso in cui in precedenza sia già stata attivata un'altra sessione diagnostica.

5.1.2. ***Formato del messaggio***

CPR_028 I formati dei messaggi per le primitive di StartDiagnosticSession sono descritti nelle seguenti tabelle.

Tabella 14

Messaggio StartDiagnosticSession Request

Byte n.	Denominazione del parametro	Valore esadecimale	Mnemonico
n. 1	Byte di formato — indirizzamento fisico	80	FMT
n. 2	Byte dell'indirizzo di destinazione	EE	TGT
n. 3	Byte dell'indirizzo di provenienza	tt	SRC
n. 4	Byte di lunghezza aggiuntivo	02	LEN
n. 5	Identificativo StartDiagnosticSession Request Service	10	STDS
n. 6	diagnosticSession = [valore contenuto nella Tabella 17]	xx	DS_…
n. 7	Totale di controllo	00-FF	CS

Tabella 15

Messaggio StartDiagnosticSession Positive Response

Byte n.	Denominazione del parametro	Valore esadecimale	Mnemonico
n. 1	Byte di formato — indirizzamento fisico	80	FMT
n. 2	Byte dell'indirizzo di destinazione	tt	TGT
n. 3	Byte dell'indirizzo di provenienza	EE	SRC
n. 4	Byte di lunghezza aggiuntivo	02	LEN
n. 5	Identificativo StartDiagnosticSession Positive Response Service	50	STDSPR
n. 6	DiagnosticSession = [stesso valore del byte n. 6, Tabella 14]	xx	DS_…
n. 7	Totale di controllo	00-FF	CS

Tabella 16

Messaggio StartDiagnosticSession Negative Response

Byte n.	Denominazione del parametro	Valore esadecimale	Mnemonico
n. 1	Byte di formato — indirizzamento fisico	80	FMT
n. 2	Byte dell'indirizzo di destinazione	tt	TGT
n. 3	Byte dell'indirizzo di provenienza	EE	SRC
n. 4	Byte di lunghezza aggiuntivo	03	LEN
n. 5	Identificativo Negative Response Service	7F	NR
n. 6	Identificativo StartDiagnosticSession Request Service	10	STDS
n. 7	codice di risposta = [subFunctionNotSupported ([a])	12	RC_SFNS
	incorrectMessageLength ([b])	13	RC_IML
	conditionsNotCorrect ([c])]	22	RC_CNC
n. 8	Totale di controllo	00-FF	CS

([a]) Il valore inserito nel byte n. 6 del messaggio di richiesta non è supportato, ovvero non è presente nella Tabella 17;
([b]) La lunghezza del messaggio è errata;
([c]) Non sono soddisfatti i criteri di richiesta di StartDiagnosticSession.

5.1.3. ***Definizione dei parametri***

CPR_029 Il parametro diagnosticSession (DS_) è utilizzato nell'ambito del servizio StartDiagnosticSession per selezionare il ruolo specifico del/i server. Nel presente documento sono descritte le seguenti sessioni diagnostiche:

Tabella 17

Definizione dei valori del parametro diagnosticSession

Valore esadecimale	Descrizione	Mnemonico
81	StandardDiagnosticSession Tale sessione diagnostica abilita tutti i servizi riportati nella Tabella 1, colonna 4 "SD". Tali servizi consentono la lettura dei dati inviati dal server (VU). Questa sessione diagnostica si attiva in seguito all'inizializzazione completata con successo tra client (tester) e server (VU) e può essere soprascritta dalle altre sessioni diagnostiche descritte nella presente sezione.	SD
85	ECUProgrammingSession Tale sessione diagnostica abilita tutti i servizi riportati nella Tabella 1, colonna 6 "ECUPS". Tali servizi supportano la programmazione della memoria del server (VU). Questa sessione diagnostica può essere soprascritta dalle altre sessioni diagnostiche descritte nella presente sezione.	ECUPS
87	ECUAdjustmentSession Tale sessione diagnostica abilita tutti i servizi riportati nella Tabella 1, colonna 5 "ECUAS". Tali servizi supportano il controllo messaggi in entrata/uscita del server (VU). Questa sessione diagnostica può essere soprascritta dalle altre sessioni diagnostiche descritte nella presente sezione.	ECUAS

5.2. **Servizio SecurityAccess**

La scrittura dei dati di calibratura o l'accesso alla relativa linea dei segnali di entrata/uscita non sono consentiti a meno che la VU si trovi nella modalità CALIBRATURA. Oltre all'inserimento di una carta dell'officina valida all'interno della VU, prima che sia consentito l'accesso alla modalità CALIBRATURA è altresì necessario inserire nella VU il codice PIN appropriato.

Il servizio SecurityAccess fornisce un mezzo per l'inserimento del codice PIN e per segnalare al tester se la VU si trovi in modalità CALIBRATURA.

È possibile inserire il codice PIN anche con procedure alternative.

5.2.1. ***Descrizione del messaggio***

Il servizio SecurityAccess consiste nell'invio del messaggio SecurityAccess "requestSeed", seguito dal messaggio SecurityAccess "sendKey". È necessario eseguire il servizio in questione successivamente al servizio StartDiagnosticSession.

CPR_033 Il tester utilizza il messaggio SecurityAccess "requestSeed" per verificare se l'unità elettronica di bordo sia pronta a ricevere il codice PIN.

CPR_034 Nel caso in cui l'unità elettronica di bordo si trovi già in modalità CALIBRATURA, risponde alla richiesta inviando un vettore di inizializzazione ("seed") del valore di 0x0000 utilizzando il servizio SecurityAccess Positive Response.

CPR_035 Se l'unità elettronica di bordo è predisposta alla ricezione del codice PIN proveniente da una carta dell'officina per effettuarne la verifica, risponde alla richiesta inviando un vettore di inizializzazione ("seed") superiore a 0x0000 mediante il servizio SecurityAccess Positive Response.

CPR_036 In caso invece di unità elettronica di bordo non predisposta alla ricezione del codice PIN da parte del tester, a causa dell'inserimento di una carta dell'officina non valida, del mancato inserimento di una carta dell'officina o della predisposizione dell'unità elettronica di bordo alla ricezione del codice PIN attraverso altre procedure, la stessa VU risponde alla richiesta con un messaggio di Risposta Negativa contenente un codice di risposta impostato su conditionsNotCorrectOrRequestSequenceError.

CPR_037 Il tester utilizza infine il messaggio SecurityAccess "sendKey" per inviare il codice PIN all'unità elettronica di bordo. Al fine di garantire il tempo necessario per l'esecuzione della procedura di autenticazione della carta, la VU impiega il codice di risposta negativa requestCorrectlyReceived-ResponsePending per prolungare il tempo di risposta. Il tempo massimo di risposta non deve comunque superare i 5 minuti. Quando il servizio richiesto è stato completato, la VU invia un messaggio di risposta positivo o negativo, con un codice di risposta diverso dal precedente. Il codice negativo di risposta requestCorrectlyReceived-ResponsePending può essere ripetuto dalla VU fintantoché il servizio richiesto non è stato completato ed il messaggio di risposta conclusivo non è stato inviato.

CPR_038 L'unità elettronica di bordo risponde a tale richiesta attraverso il servizio SecurityAccess Positive Response soltanto quando si trova in modalità CALIBRATURA.

CPR_039 Nei casi seguenti, l'unità elettronica di bordo risponde alla richiesta in questione con un messaggio di Risposta negativa contenente un codice di risposta impostato su:

— subFunctionNot supported: formato non valido del parametro della sottofunzione (accessType),

— conditionsNotCorrectOrRequestSequenceError: VU non predisposta a ricevere l'inserimento del codice PIN,

— invalidKey: codice PIN non valido e numero massimo di tentativi di verifica del codice PIN non superato,

— exceededNumberOfAttempts: codice PIN non valido e numero massimo di tentativi di verifica del codice PIN superato,

— generalReject: codice PIN corretto ma reciproca autenticazione con la carta dell'officina fallita.

5.2.2. ***Formato del messaggio — SecurityAccess — requestSeed***

CPR_040 I formati dei messaggi per le primitive di SecurityAccess "requestSeed" sono descritti nelle seguenti tabelle.

Tabella 18

Messaggio SecurityAccess Request — requestSeed

Byte n.	Denominazione del parametro	Valore esadecimale	Mnemonico
n. 1	Byte di formato — indirizzamento fisico	80	FMT
n. 2	Byte dell'indirizzo di destinazione	EE	TGT
n. 3	Byte dell'indirizzo di provenienza	tt	SRC
n. 4	Byte di lunghezza aggiuntivo	02	LEN
n. 5	Identificativo StopCommunication Request Service	27	SA
n. 6	accessType — requestSeed	7D	AT_RSD
n. 7	Totale di controllo	00-FF	CS

Tabella 19

Messaggio SecurityAccess — requestSeed Positive Response

Byte n.	Denominazione del parametro	Valore esadecimale	Mnemonico
n. 1	Byte di formato — indirizzamento fisico	80	FMT
n. 2	Byte dell'indirizzo di destinazione	tt	TGT
n. 3	Byte dell'indirizzo di provenienza	EE	SRC
n. 4	Byte di lunghezza aggiuntivo	04	LEN
n. 5	Identificativo SecurityAccess Positive Response Service	67	SAPR
n. 6	accessType — requestSeed	7D	AT_RSD
n. 7	Vettore di inizializzazione (seed) byte alto	00-FF	SEEDH
n. 8	Vettore di inizializzazione (seed) byte basso	00-FF	SEEDL
n. 9	Totale di controllo	00-FF	CS

Tabella 20

Messaggio SecurityAccess Negative Response

Byte n.	Denominazione del parametro	Valore esadecimale	Mnemonico
n. 1	Byte di formato — indirizzamento fisico	80	FMT
n. 2	Byte dell'indirizzo di destinazione	tt	TGT
n. 3	Byte dell'indirizzo di provenienza	EE	SRC
n. 4	Byte di lunghezza aggiuntivo	03	LEN
n. 5	Identificativo negativeResponse Service	7F	NR
n. 6	Identificativo SecurityAccess Request Service	27	SA
n. 7	codice di risposta = [conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
	incorrectMessageLength]	13	RC_IML
n. 8	Totale di controllo	00-FF	CS

5.2.3. ***Formato del messaggio — SecurityAccess — sendKey***

CPR_041 I formati dei messaggi per le primitive di SecurityAccess "sendKey" sono descritti nelle seguenti tabelle.

Tabella 21

Messaggio SecurityAccess Request — sendKey

Byte n.	Denominazione del parametro	Valore esadecimale	Mnemonico
n. 1	Byte di formato — indirizzamento fisico	80	FMT
n. 2	Byte dell'indirizzo di destinazione	EE	TGT
n. 3	Byte dell'indirizzo di provenienza	tt	SRC
n. 4	Byte di lunghezza aggiuntivo	m+2	LEN
n. 5	Identificativo SecurityAccess Request Service	27	SA
n. 6	accessType — sendKey	7E	AT_SK
Dal n. 7 al n. m+6	Chiave n. 1 (byte alto)	xx	KEY
	…	…	
	Chiave n. m (byte basso, m deve essere compreso tra 4 e 8 incluso)	xx	
n. m+7	Totale di controllo	00-FF	CS

Tabella 22

Messaggio SecurityAccess — sendKey Positive Response

Byte n.	Denominazione del parametro	Valore esadecimale	Mnemonico
n. 1	Byte di formato — indirizzamento fisico	80	FMT
n. 2	Byte dell'indirizzo di destinazione	tt	TGT
n. 3	Byte dell'indirizzo di provenienza	EE	SRC
n. 4	Byte di lunghezza aggiuntivo	02	LEN
n. 5	Identificativo SecurityAccess Positive Response Service	67	SAPR
n. 6	accessType — sendKey	7E	AT_SK
n. 7	Totale di controllo	00-FF	CS

Tabella 23

Messaggio SecurityAccess Negative Response

Byte n.	Denominazione del parametro	Valore esadecimale	Mnemonico
n. 1	Byte di formato — indirizzamento fisico	80	FMT
n. 2	Byte dell'indirizzo di destinazione	tt	TGT
n. 3	Byte dell'indirizzo di provenienza	EE	SRC
n. 4	Byte di lunghezza aggiuntivo	03	LEN
n. 5	Identificativo NegativeResponse Service	7F	NR
n. 6	Identificativo SecurityAccess Request Service	27	SA
n. 7	codice di risposta = [generalReject	10	RC_GR
	subFunctionNotSupported	12	RC_SFNS
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
	invalidKey	35	RC_IK
	exceededNumberOfAttempts	36	RC_ENA
	requestCorrectlyReceived-ResponsePending]	78	RC_RCR_RP
n. 8	Totale di controllo	00-FF	CS

6. SERVIZI DI TRASMISSIONE DATI

I servizi disponibili sono descritti nella seguente tabella:

Tabella 24

Servizi di trasmissione dati

Nome del servizio	Descrizione
ReadDataByIdentifier	Il client richiede la trasmissione del valore corrente di un record con accesso mediante recordDataIdentifier.
WriteDataByIdentifier	Il client richiede la scrittura di un record con accesso mediante recordDataIdentifier.

6.1. **Servizio ReadDataByIdentifier**

6.1.1. ***Descrizione del messaggio***

CPR_050 Il servizio ReadDataByIdentifier è utilizzato dal client per richiedere valori dei dati registrati al server. I dati sono identificati mediante parametro recordDataIdentifier. È responsabilità del fabbricante della VU assicurare che quando si utilizza questo servizio lo stato del server sia quello prescritto.

6.1.2. ***Formato del messaggio***

CPR_051 I formati dei messaggi per le primitive di ReadDataByIdentifier sono descritti nelle seguenti tabelle.

Tabella 25

Messaggio ReadDataByIdentifier Request

Byte n.	Denominazione del parametro	Valore esadecimale	Mnemonico
n. 1	Byte di formato — indirizzamento fisico	80	FMT
n. 2	Byte dell'indirizzo di destinazione	EE	TGT
n. 3	Byte dell'indirizzo di provenienza	tt	SRC
n. 4	Byte di lunghezza aggiuntivo	03	LEN
n. 5	Identificativo ReadDataByIdentifier Request Service	22	RDBI
Dal n. 6 al n. 8	recordDataIdentifier = [valore contenuto nella Tabella 28]	xxxx	RDI_…
n. 8	Totale di controllo	00-FF	CS

Tabella 26

Messaggio ReadDataByIdentifier Positive Response

Byte n.	Denominazione del parametro	Valore esadecimale	Mnemonico
n. 1	Byte di formato — indirizzamento fisico	80	FMT
n. 2	Byte dell'indirizzo di destinazione	tt	TGT
n. 3	Byte dell'indirizzo di provenienza	EE	SRC
n. 4	Byte di lunghezza aggiuntivo	m+3	LEN
n. 5	Identificativo ReadDataByIdentifier Positive Response Service	62	RDBIPR
Dal n. 6 al n. 7	recordDataIdentifier = [stesso valore dei byte n. 6 e n. 7, Tabella 25]	xxxx	RDI_…
Dal n. 8 al n. m+7	dataRecord[] = [dato n. 1 : dato n. m]	xx : xx	DREC_DATA1 : DREC_DATAm
n. m+8	Totale di controllo	00-FF	CS

Tabella 27

Messaggio ReadDataByIdentifier Negative Response

Byte n.	Denominazione del parametro	Valore esadecimale	Mnemonico
n. 1	Byte di formato — indirizzamento fisico	80	FMT
n. 2	Byte dell'indirizzo di destinazione	tt	TGT
n. 3	Byte dell'indirizzo di provenienza	EE	SRC
n. 4	Byte di lunghezza aggiuntivo	03	LEN
n. 5	Identificativo NegativeResponse Service	7F	NR
n. 6	Identificativo ReadDataByIdentifier Request Service	22	RDBI
n. 7	codice di risposta = [requestOutOfRange incorrectMessageLength conditionsNotCorrect]	31 13 22	RC_ROOR RC_IML RC_CNC
n. 8	Totale di controllo	00-FF	CS

6.1.3. ***Definizione dei parametri***

CPR_052 Il parametro recordDataIdentifier (RDI_) nel messaggio ReadDataByIdentifier Request identifica un record di dati.

CPR_053 I valori di recordDataIdentifier definiti dal presente documento sono illustrati nella tabella seguente.

La tabella relativa a recordDataIdentifier è costituita da quattro colonne e da più righe.

— La 1a colonna (Valore esadecimale) comprende il “valore esadecimale” assegnato al parametro recordDataIdentifier specificato nella 3a colonna.

— La 2a colonna (Elemento di dati) specifica l'elemento di dati dell'appendice 1 riferito a recordDataIdentifier (in alcuni casi è necessario transcodificare).

— La 3a colonna (Descrizione) indica il nome dello specifico recordDataIdentifier.

— La 4a colonna (Mnemonico) specifica l'identificativo mnemonico del parametro recordDataIdentifier in questione.

Tabella 28

Definizione dei valori del parametro recordDataIdentifier

Valore esadecimale	Elemento di dati	Nome del recordDataIdentifier (vedi formato nella sezione 8.2)	Mnemonico
F90B	CurrentDateTime	TimeDate	RDI_TD
F912	HighResOdometer	HighResolutionTotalVehicleDistance	RDI_HRTVD
F918	K-ConstantOfRecordingEquipment	Kfactor	RDI_KF
F91C	L-TyreCircumference	LfactorTyreCircumference	RDI_LF
F91D	W-VehicleCharacteristicConstant	WvehicleCharacteristicFactor	RDI_WVCF
F921	TyreSize	TyreSize	RDI_TS
F922	nextCalibrationDate	NextCalibrationDate	RDI_NCD
F92C	SpeedAuthorised	SpeedAuthorised	RDI_SA
F97D	vehicleRegistrationNation	RegisteringMemberState	RDI_RMS
F97E	VehicleRegistrationNumber	VehicleRegistrationNumber	RDI_VRN
F190	VehicleIdentificationNumber	VIN	RDI_VIN

CPR_054 Il parametro dataRecord (DREC_) è utilizzato nell'ambito del messaggio ReadDataByIdentifier Positive Response per fornire al client (tester) il record dei dati identificato dal parametro recordDataIdentifier. Il formato dei dati è indicato nella sezione 8. Ulteriori dataRecords, impiegati a discrezione dell'utilizzatore, devono comprendere i dati specifici in entrata, quelli interni e quelli in uscita della VU; essi sono permessi, benché non definiti nel presente documento.

6.2. **Servizio WriteDataByIdentifier**

6.2.1. ***Descrizione del messaggio***

CPR_056 Il servizio WriteDataByIdentifier è utilizzato dal client per registrare valori dei dati nel server. I dati sono identificati mediante parametro recordDataIdentifier. È responsabilità del fabbricante della VU assicurare che quando si utilizza questo servizio lo stato del server sia quello prescritto. Per aggiornare i parametri elencati nella Tabella 28 la VU deve trovarsi in modalità CALIBRATURA.

6.2.2. ***Formato del messaggio***

CPR_057 I formati dei messaggi per le primitive di WriteDataByIdentifier sono descritti nelle seguenti tabelle.

Tabella 29

Messaggio WriteDataByIdentifier Request

Byte n.	Denominazione del parametro	Valore esadecimale	Mnemonico
n. 1	Byte di formato — indirizzamento fisico	80	FMT
n. 2	Byte dell'indirizzo di destinazione	EE	TGT
n. 3	Byte dell'indirizzo di provenienza	tt	SRC
n. 4	Byte di lunghezza aggiuntivo	m+3	LEN
n. 5	Identificativo WriteDataByIdentifier Request Service	2E	WDBI
Dal n. 6 al n. 7	recordDataIdentifier = [valore contenuto nella Tabella 28]	xxxx	RDI_…
Dal n. 8 al m+7	dataRecord[] = [dato n. 1 : dato n. m]	xx : xx	DREC_DATA1 : DREC_DATAm
n. m+8	Totale di controllo	00-FF	CS

Tabella 30

Messaggio WriteDataByIdentifier Positive Response

Byte n.	Denominazione del parametro	Valore esadecimale	Mnemonico
n. 1	Byte di formato — indirizzamento fisico	80	FMT
n. 2	Byte dell'indirizzo di destinazione	tt	TGT
n. 3	Byte dell'indirizzo di provenienza	EE	SRC
n. 4	Byte di lunghezza aggiuntivo	03	LEN
n. 5	Identificativo WriteDataByIdentifier Positive Response Service	6E	WDBIPR
Dal n. 6 al n. 7	recordDataIdentifier = [stesso valore dei byte n. 6 e n. 7, Tabella 29]	xxxx	RDI_…
n. 8	Totale di controllo	00-FF	CS

Tabella 31

Messaggio WriteDataByIdentifier Negative Response

Byte n.	Denominazione del parametro	Valore esadecimale	Mnemonico
n. 1	Byte di formato — indirizzamento fisico	80	FMT
n. 2	Byte dell'indirizzo di destinazione	tt	TGT
n. 3	Byte dell'indirizzo di provenienza	EE	SRC
n. 4	Byte di lunghezza aggiuntivo	03	LEN
n. 5	Identificativo NegativeResponse Service	7F	NR
n. 6	Identificativo WriteDataByIdentifier Request Service	2E	WDBI
n. 7	codice di risposta = [requestOutOfRange	31	RC_ROOR
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect]	22	RC_CNC
n. 8	Totale di controllo	00-FF	CS

6.2.3. ***Definizione dei parametri***

Il parametro recordDataIdentifier (RDI_) è definito nella tabella 28.

Il parametro dataRecord (DREC_) è utilizzato nell'ambito del messaggio WriteDataByIdentifier Request per fornire al server (VU) il record dei dati identificato dal parametro recordDataIdentifier. Il formato dei dati è indicato nella sezione 8.

7. CONTROLLO DEGLI IMPULSI DI PROVA — UNITÀ FUNZIONALE DI CONTROLLO DEI SEGNALI DI I/O

I servizi disponibili sono descritti nella seguente tabella:

Tabella 32

Unità funzionale di controllo dei segnali di entrata/uscita

Nome del servizio	Descrizione
InputOutputControlByIdentifier	Il client richiede il controllo di uno specifico segnale di entrata/uscita al server.

7.1. **Servizio InputOutputControlByIdentifier**

7.1.1. ***Descrizione del messaggio***

Attraverso il connettore anteriore deve essere possibile effettuare un collegamento che consenta il controllo degli impulsi di prova o la loro verifica costante mediante tester adatto.

CPR_058 È possibile configurare tale linea dei segnali I/O di calibratura mediante comando della linea K, utilizzando il servizio InputOutputControlByIdentifier per selezionare la funzione di entrata o di uscita richiesta per la linea in questione. La linea può assumere i diversi stati indicati di seguito:

— disabled (disabilitata),

— speedSignalInput, in cui la linea dei segnali I/O di calibratura è utilizzata per inviare un segnale di prova (speed signal) al posto del segnale di velocità inviato dal sensore di movimento,

— realTimeSpeedSignalOutputSensor, in cui la linea dei segnali I/O di calibratura è utilizzata per inviare il segnale di velocità del sensore di movimento,

— RTCOutput, in cui la linea dei segnali I/O di calibratura è utilizzata per inviare il segnale dell'orologio UTC.

CPR_059 L'operazione di configurazione dello stato della linea richiede che l'unità elettronica di bordo abbia iniziato una sessione di regolazione e che sia in modalità CALIBRATURA. Al termine della sessione di regolazione o della modalità CALIBRATURA, l'unità elettronica di bordo deve verificare che lo stato della linea dei segnali I/O di calibratura sia nuovamente 'disabilitata' (impostazione predefinita).

CPR_060 Se sulla linea del segnale velocità in tempo reale in entrata alla VU vengono ricevuti degli impulsi di velocità mentre la linea dei segnali I/O di calibratura è impostata come ingresso, è necessario impostare la linea dei segnali I/O di calibratura come uscita o riportarla alla condizione di disabilitazione.

CPR_061 Le diverse fasi sono così articolate:

— stabilire la comunicazione mediante il servizio StartCommunication,

— iniziare una sessione di regolazione mediante il servizio StartDiagnosticSession e adottare la modalità di funzionamento CALIBRATURA (l'ordine di queste due operazioni non è rilevante),

— modificare lo stato del segnale di uscita mediante l'operazione InputOutputControlByIdentifier Service.

7.1.2. ***Formato del messaggio***

CPR_062 I formati dei messaggi per le primitive di InputOutputControlByIdentifier sono descritti nelle seguenti tabelle.

Tabella 33

Messaggio InputOutputControlByIdentifier Request

Byte n.	Denominazione del parametro	Valore esadecimale	Mnemonico
n. 1	Byte di formato — indirizzamento fisico	80	FMT
n. 2	Byte dell'indirizzo di destinazione	EE	TGT
n. 3	Byte dell'indirizzo di provenienza	tt	SRC
n. 4	Byte di lunghezza aggiuntivo	xx	LEN
n. 5	InputOutputControlByIdentifier Request Sid	2F	IOCBI
Dal n. 6 al n. 7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
n. 8 oppure dal n. 8 al n. 9	ControlOptionRecord = [		COR_…
	inputOutputControlParameter — uno dei valori della Tabella 36	xx	IOCP_…
	controlState — uno dei valori della Tabella 38 (cfr. nota)]	xx	CS_…
n. 9 oppure n. 10	Totale di controllo	00-FF	CS

Nota: Il parametro controlState è presente soltanto in alcuni casi (cfr. punto 7.1.3).

Tabella 34

Messaggio InputOutputControlByIdentifier Positive Response

Byte n.	Denominazione del parametro	Valore esadecimale	Mnemonico
n. 1	Byte di formato — indirizzamento fisico	80	FMT
n. 2	Byte dell'indirizzo di destinazione	tt	TGT
n. 3	Byte dell'indirizzo di provenienza	EE	SRC
n. 4	Byte di lunghezza aggiuntivo	xx	LEN
n. 5	inputOutputControlByIdentifier Positive Response SId	6F	IOCBIPR
Dal n. 6 al n. 7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
n. 8 oppure dal n. 8 al n. 9	controlStatusRecord = [		CSR_
	inputOutputControlParameter (stesso valore del byte n. 8, Tabella 33)	xx	IOCP_…
	inputOutputControlParameter (stesso valore del byte n. 9, Tabella 33)] (se del caso)	xx	CS_…
n. 9 oppure n. 10	Totale di controllo	00-FF	CS

Tabella 35

Messaggio InputOutputControlByIdentifier Negative Response

Byte n.	Denominazione del parametro	Valore esadecimale	Mnemonico
n. 1	Byte di formato — indirizzamento fisico	80	FMT
n. 2	Byte dell'indirizzo di destinazione	tt	TGT
n. 3	Byte dell'indirizzo di provenienza	EE	SRC
n. 4	Byte di lunghezza aggiuntivo	03	LEN
n. 5	Identificativo negativeResponse Service	7F	NR
n. 6	inputOutputControlByIdentifier Request SId	2F	IOCBI
n. 7	responseCode = [		
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect	22	RC_CNC
	requestOutOfRange	31	RC_ROOR
	deviceControlLimitsExceeded]	7A	RC_DCLE
n. 8	Totale di controllo	00-FF	CS

7.1.3. ***Definizione dei parametri***

CPR_064 Il parametro inputOutputControlParameter (IOCP_) è definito nella seguente tabella.

Tabella 36

Definizione dei valori del parametro inputOutputControlParameter

Valore esadecimale	Descrizione	Mnemonico
01	ReturnControlToECU Tale valore indica al server (VU) che il tester non ha più il controllo della linea dei segnali I/O di calibratura.	RCTECU
01	ResetToDefault Tale valore indica al server (VU) che si richiede di riportare alla propria impostazione predefinita la linea dei segnali I/O di calibratura.	RTD
03	ShortTermAdjustment Tale valore indica al server (VU) che si richiede di adeguare la linea dei segnali I/O di calibratura al valore indicato nel parametro controlState.	STA

CPR_065 Il parametro controlState è presente soltanto quando il parametro inputOutputControlParameter è impostato su ShortTermAdjustment ed è definito nella seguente tabella:

Tabella 37

Definizione dei valori del parametro controlState

Modalità	Valore esadecimale	Descrizione
Disable	00	La linea I/O è disabilitata (impostazione predefinita)
Enable	01	La linea I/O di calibrazione è abilitata come speedSignalInput
Enable	02	La linea I/O di calibrazione è abilitata come realTimeSpeedSignalOutputSensor
Enable	03	La linea I/O di calibrazione è abilitata come RTCOutput

8. FORMATO DELLE REGISTRAZIONI

La presente sezione contiene informazioni in merito a:

— regole generali da applicare a serie di parametri trasmessi dalla VU al tester,

— formati da impiegare nelle operazioni di trasferimento attuate tramite i servizi di trasmissione dati di cui alla sezione 6.

CPR_067 Tutti i parametri indicati devono essere supportati dalla VU.

CPR_068 I dati trasmessi dalla VU al tester in risposta ad un messaggio di richiesta devono essere di tipo misurato (ovvero valore corrente del parametro richiesto, secondo quanto misurato o osservato dalla VU).

8.1. **Valori limite dei parametri trasmessi**

CPR_069 La Tabella 38 definisce i limiti adottati per determinare la validità dei parametri trasmessi.

CPR_070 I valori della serie "indicatore di errore" permettono alla VU di indicare immediatamente che non sono al momento disponibili dati parametrici validi, in seguito ad errori intervenuti nell'apparecchio di controllo.

CPR_071 I valori della serie "non disponibile" permettono alla VU di trasmettere un messaggio che contiene un parametro non disponibile o non supportato dal modulo in questione. I valori della serie "non richiesto" permettono di trasmettere messaggi di comando e di identificare i parametri per i quali non ci si deve attendere alcuna risposta dall'apparecchio cui sono inviati.

CPR_072 Se il malfunzionamento di un componente non permette la trasmissione di dati validi per un determinato parametro, al loro posto devono essere trasmessi i codici di errore contenuti nella Tabella 38. Se tuttavia il dato misurato o calcolato risulta valido, benché superi i valori limite stabiliti per lo specifico parametro, non deve essere impiegato alcun codice d'errore: il dato deve essere trasmesso utilizzando, a seconda del caso, il valore parametrico massimo o minimo.

Tabella 38

Possibili valori del parametro dataRecords

Nome della serie	1 byte (Valore esadecimale)	2 byte (Valore esadecimale)	4 byte (Valore esadecimale)	ASCII
Segnale valido	da 00 a FA	da 0000 a FAFF	da 00000000 a FAFFFFFF	da 1 a 254
Codice specifico del parametro	FB	da FB00 a FBFF	da FB000000 a FBFFFFFF	nessuno
Serie riservata per futuri indicatori (in bit)	da FC a FD	da FC00 a FDFF	da FC000000 a FDFFFFFF	nessuno
Codice di errore	FE	da FE00 a FEFF	da FE000000 a FEFFFFFF	0
Non disponibile o non richiesto	FF	da FF00 a FFFF	da FF000000 a FFFFFFFF	FF

CPR_073 Se i parametri sono codificati in ASCII, il carattere ASCII "*" è riservato quale limitatore.

8.2. **Formato del parametro dataRecords**

Le Tabelle da 39 a 42 indicano i formati da impiegare utilizzando i servizi ReadDataByIdentifier e WriteDataByIdentifier.

CPR_074 La tabella 39 indica lunghezza, risoluzione e limiti operativi della serie, per ogni parametro identificato da un recordDataIdentifier:

Tabella 39

Formato del parametro dataRecords

Denominazione del parametro	Lunghezza dato (in bytes)	Risoluzione	Limiti operativi
TimeDate	8	Cfr. informazioni dettagliate nella Tabella 40	
HighResolutionTotalVehicleDistance	4	5 m/bit gain, 0 m offset	0 a + da 0 a + 21 055 406 km km
Kfactor	2	0,001 impulsi/m /bit gain, 0 offset	da 0 a 64,255 impulsi/m
LfactorTyreCircumference	2	0,125 10^{-3} m /bit gain, 0 offset	da 0 a 8 031 m
WvehicleCharacteristicFactor	2	0,001 impulsi/m /bit gain, 0 offset	da 0 a 64,255impulsi/m
TyreSize	15	ASCII	ASCII
NextCalibrationDate	3	Cfr. informazioni dettagliate nella Tabella 41	
SpeedAuthorised	2	1/256 km/h/bit gain, 0 offset	0 a da 0 a 250 996 km/h km/h
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	Cfr. informazioni dettagliate nella Tabella 44	
VIN	17	ASCII	ASCII

CPR_075 La Tabella 40 indica i formati dei diversi tipi di byte impiegati dal parametro TimeDate:

Tabella 40

Formato dettagliato del parametro TimeDate (recordDataIdentifier value n. F00B)

Byte	Definizione dei parametri	Risoluzione	Limiti operativi
1	Secondi	0,25 s/bit gain, 0 s offset	da 0 a 59 sec.
2	Minuti	1 min/bit gain, 0 min offset	da 0 a 59 min.
3	Ore	1 h/bit gain, 0 h offset	da 0 a 23 ore
4	Mese	1 mese/bit gain, 0 mese offset	da 1 a 12 mesi
5	Giorno	0,25 giorni/bit gain, 0 giorni offset (cfr. la nota alla Tabella 41)	da 0,25 a 31,75 giorni
6	Anno	1 anno/bit gain, + 1985 anno offset (cfr. la nota alla Tabella 41)	Dall'anno 1985 al 2235
7	Local Minute Offset	1 min/bit gain, – 125 min offset	da – 59 a 59 min.
8	Local Hour Offset	1 ora/bit gain, – 125 ore offset	da – 23 a + 23 ore

CPR_076 La Tabella 41 indica i formati dei diversi tipi di byte impiegati dal parametro NextCalibrationDate:

Tabella 41

Formato dettagliato del parametro NextCalibrationDate (recordDataIdentifier value n. F022)

Byte	Definizione dei parametri	Risoluzione	Limiti operativi
1	Mese	1 mese/bit gain, 0 mesi offset	da 1 a 12 mesi
2	Giorno	0.25 giorni/bit gain, 0 giorni offset (cfr. la nota alla Tabella 41)	da 0,25 a 31,75 giorni
3	Anno	1 anno/bit gain, +1985 anni offset (cfr. la nota seguente)	Dall'anno 1985 al 2235

Nota: relativa all'impiego del parametro "Giorno":
1. Nella data, il valore 0 non è un valore valido. I valori 1, 2, 3 e 4 sono utilizzati per identificare il primo giorno del mese, 5, 6, 7 e 8 per identificare il secondo e così via.
2. Tale parametro non influenza né modifica il parametro relativo all'ora.

Nota: relativa all'impiego del parametro "Anno":
Il valore 0 corrisponde all'anno 1985, il valore 1 corrisponde al 1986 e così via.

CPR_078 La Tabella 42 indica i formati dei diversi tipi di byte impiegati dal parametro VehicleRegistrationNumber:

Tabella 42

Formato dettagliato del parametro VehicleRegistrationNumber (recordDataIdentifier value n. F07E)

Byte	Definizione dei parametri	Risoluzione	Limiti operativi
1	Code Page (definito nell'appendice 1)	ASCII	da 01 a 0A
2-14	Vehicle Registration Number (definito nell'appendice 1)	ASCII	ASCII

Appendice 9

OMOLOGAZIONE ELENCO DELLE PROVE MINIME PRESCRITTE

INDICE

1. INTRODUZIONE

1.1. **Omologazione**

L'omologazione CE di un apparecchio di controllo (o suo componente) o una carta tachigrafica si basa su:

— una certificazione di sicurezza, effettuata da un organismo ITSEC, rispetto ad un obiettivo di sicurezza pienamente conforme all'appendice 10 del presente allegato,

— una certificazione funzionale, effettuata dalle autorità competenti degli Stati membri, che attesta la conformità dell'elemento sottoposto alle prove ai requisiti del presente allegato in termini di funzioni eseguite, precisione delle misurazioni e caratteristiche ambientali,

— una certificazione di interoperabilità, effettuata dall'organismo competente, che attesta la piena interoperabilità dell'apparecchio di controllo (o carta tachigrafica) con i modelli di carta tachigrafica (o apparecchio di controllo) necessari (cfr. capitolo VIII del presente allegato).

La presente appendice specifica le prove minime che le autorità competenti degli Stati membri devono eseguire nell'ambito delle prove funzionali, nonché le prove minime che l'organismo competente deve eseguire nell'ambito delle prove di interoperabilità. Le procedure da seguire per l'esecuzione delle prove e il tipo di prove non sono ulteriormente specificati.

Gli aspetti concernenti la certificazione della sicurezza non sono contemplati dalla presente appendice. Se alcune prove richieste per l'omologazione vengono effettuate nell'ambito delle procedure di valutazione e certificazione della sicurezza, non è necessario che tali prove vengano ripetute. In quest'ultimo caso, solo i risultati delle prove della sicurezza possono essere oggetto di controlli. A titolo d'informazione, nella presente appendice i requisiti che devono essere sottoposti a prova (o che sono strettamente collegati alle prove previste) nell'ambito della certificazione della sicurezza sono segnalati con un asterisco ("*").

La presente appendice esamina separatamente l'omologazione del sensore di movimento e dell'unità elettronica di bordo come componenti dell'apparecchio di controllo. Non è prescritta l'interoperabilità tra ogni modello di sensore di movimento e ogni modello di unità elettronica di bordo, pertanto l'omologazione di un sensore di movimento può essere accordata solo se abbinata all'omologazione di una unità elettronica di bordo (e viceversa).

1.2. **Riferimenti normativi**

Nella presente appendice si rimanda alle norme seguenti:

IEC 68-2-1	Environmental testing — Part 2: Tests — Tests A: Cold. 1990 + Amendment 2: 1994. (Prove ambientali — Parte 2: Prove — Prova A: Freddo. 1990 + Modifica 2: 1994)
IEC 68-2-2	Environmental testing — Part 2: Tests — Tests B: Dry heat. 1974 + Amendment 2: 1994. (Prove ambientali — Parte 2: Prove — Prova B: Calore secco. 1974 + Modifica 2: 1994)
IEC 68-2-6	Basic environmental testing procedures — Test methods — Test Fc and guidance: Vibrations (sinusoidal). 6th edition: 1985. [Procedure di prove ambientali di base — Metodi di prova — Prova Fc e guida: Vibrazioni (sinusoidali). 6ª edizione: 1985]
IEC 68-2-14	Basic environmental testing procedures — Test methods — Test N: Change of temperature. Modification 1: 1986. (Procedure di prove ambientali di base — Metodi di prova — Prova N: Variazione di temperatura. Modifica 1: 1986)
IEC 68-2-27	Basic environmental testing procedures — Test methods — Test Ea and guidance: Shock. Edition 3: 1987. (Procedure di prove ambientali di base — Metodi di prova — Prova Ea e guida: Urti. Edizione 3: 1987)
IEC 68-2-30	Basic environmental testing procedures — Test methods — Test Db and guidance: Damp heat, cyclic (12 + 12 — hour cycle). Modification 1: 1985. [Procedure di prove ambientali di base — Metodi di prova — Prova Db e guida: Calore umido, ciclico (ciclo di 12 + 12 ore). Modifica 1: 1985]
IEC 68-2-35	Basic environmental testing procedure — Test methods — Test Fda: Random Vibrations wide band — Reproducibility High. Modification 1: 1983. (Procedure di prove ambientali di base — Metodi di prova — Prova Fda: Vibrazioni casuali, banda larga — Riproducibilità alta. Modifica 1: 1983)
IEC 529	Degrees of protection provided by enclosures (IP code). Edition 2: 1989. [Gradi di protezione degli involucri (Codice IP). Edizione 2: 1989]
IEC 61000-4-2	Electromagnetic Compatibility (EMC) — Testing and measurement techniques — Electrostatic discharge immunity test: 1995/Amendment 1: 1998 [Compatibilità elettromagnetica (CEM) — Tecniche di prova e di misura — Prove di immunità a scarica elettrostatica: 1995/Modifica 1: 1998]
ISO 7637-1	Road vehicles — Electrical disturbance by conduction and coupling — Part 1: Passenger cars and light commercial vehicles with nominal 12 V supply voltage — Electrical transient conduction along supply lines only. Edition 2: 1990. (Veicoli stradali — Disturbi elettrici da conduzione e accoppiamento — Parte 1: Autovetture e veicoli commerciali leggeri con tensione di alimentazione nominale di 12 V — Conduzione dei transitori elettrici solo sulle linee di alimentazione. Edizione 2: 1990)

ISO 7637-2 Road vehicles — Electrical disturbance by conduction and coupling — Part 2: Commercial vehicles with nominal 24 V supply voltage — Electrical transient conduction along supply lines only. First edition: 1990. (Veicoli stradali — Disturbi elettrici da conduzione e accoppiamento — Parte 2: Veicoli commerciali con tensione di alimentazione nominale di 24 V — Conduzione dei transitori elettrici solo sulle linee di alimentazione. Prima edizione: 1990)

ISO 7637-3 Road vehicles — Electrical disturbance by conduction and coupling — Part 3: Vehicles with 12 V or 24 V supply voltage — Electrical transient transmission by capacitive and inductive coupling via lines other than supply lines. First Edition: 1995 + Cor 1: 1995. (Veicoli stradali — Disturbi elettrici da conduzione e accoppiamento — Parte 3: Veicoli con tensione di alimentazione nominale di 12 V o 24 V — Trasmissione di transitori elettrici mediante accoppiamento capacitivo e induttivo attraverso linee diverse da quelle di alimentazione. Prima edizione: 1995 + Cor 1: 1995)

ISO/IEC 7816-1 Identification cards — Integrated circuit(s) cards with contacts — Part 1: Physical characteristics. First edition: 1998. (Carte di identificazione — Carte a circuito integrato con contatti — Parte 1: Caratteristiche fisiche. Prima edizione: 1998)

ISO/IEC 7816-2 Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 2: Dimensions and location of the contacts. First edition: 1999. (Tecnologie dell'informazione — Carte di identificazione — Carte a circuito/i integrato/i con contatti — Parte 2: Dimensioni e posizione dei contatti. Prima edizione: 1999)

ISO/IEC 7816-3 Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 3: Electronic signals and transmission protocol. Edition 2: 1997. (Tecnologie dell'informazione — Carte di identificazione — Carte a circuito/i integrato/i con contatti — Parte 3: Segnali elettronici e protocollo di trasmissione. Edizione 2: 1997)

ISO/IEC 10373 Identification cards — Test methods. First edition: 1993. (Carte di identificazione — Metodi di prova. Prima edizione: 1993)

2. PROVE FUNZIONALI PER L'UNITÀ ELETTRONICA DI BORDO

N.	Prova	Descrizione	Requisiti applicabili
1.	**Esame amministrativo**		
1.1.	Documentazione	Correttezza della documentazione	
1.2.	Risultati prove fabbricante	Risultati delle prove effettuate dal fabbricante durante l'integrazione. Attestati cartacei.	070, 071, 073
2.	**Controllo visivo**		
2.1.	Conformità con la documentazione		
2.2.	Identificazione/Iscrizioni		168, 169
2.3.	Materiali		163-167
2.4	Sigilli		251
2.5.	Interfacce esterne		
3.	**Prove funzionali**		
3.1.	Funzioni		002, 004, 244
3.2.	Modalità di funzionamento		006*, 007*, 008*, 009*, 106, 107
3.3.	Funzioni e diritti di accesso ai dati		010*, 011*, 240, 246, 247
3.4.	Controllo inserimento ed estrazione carte		013, 014, 015*, 016*, 106
3.5.	Misurazione di velocità e distanza		017-026
3.6.	Misurazione del tempo (prova effettuata a 20 °C)		027-032
3.7.	Controllo delle attività del conducente		033-043, 106
3.8.	Controllo delle condizioni di guida		044, 045, 106
3.9.	Immissioni manuali		046-050b
3.10.	Gestione dei blocchi di un'impresa		051-055
3.11.	Verifica delle attività di controllo		056, 057
3.12.	Rilevamento di anomalie e/o guasti		059-069, 106

N.	Prova	Descrizione	Requisiti applicabili
3.13.	Dati di identificazione dell'apparecchio		075*, 076*, 079
3.14.	Dati relativi all'inserimento e all'estrazione della carta del conducente		081*-083*
3.15.	Dati relativi all'attività del conducente		084*-086*
3.16.	Dati relativi alle località		087*-089*
3.17.	Dati relativi all'odometro		090*-092*
3.18.	Dati dettagliati relativi alla velocità		093*
3.19.	Dati relativi alle anomalie		094*, 095
3.20.	Dati relativi ai guasti		096*
3.21.	Dati relativi alla calibratura		097*, 098*
3.22.	Dati relativi alla regolazione dell'ora		100*, 101*
3.23.	Dati relativi alle attività di controllo		102*, 103*
3.24.	Dati relativi ai blocchi di un'impresa		104*
3.25.	Dati relativi al trasferimento		105*
3.26.	Dati relativi a condizioni particolari		105a*, 105b*
3.27.	Registrazione e memorizzazione nelle carte tachigrafiche		108, 109*, 109a*, 110*, 111, 112
3.28.	Visualizzazione		072, 106, 113 a 128, PIC_001, DIS_001
3.29.	Stampa		072, 106, 129-138, PIC_001, PRT_001-PRT_0-12
3.30.	Avvisi		106, 139-148, PIC_001
3.31.	Trasferimento di dati verso un dispositivo esterno		072, 106, 149-151
3.32.	Trasmissione di dati ad altri dispositivi esterni		152, 153
3.33.	Calibratura		154*, 155*, 156*, 245
3.34.	Regolazione dell'ora		157*, 158*
3.35.	Non interferenza di funzioni supplementari		003, 269

N.	Prova	Descrizione	Requisiti applicabili
4.	**Prove ambientali**		
4.1.	Temperatura	Verificare la funzionalità mediante: — prova Ad, IEC 68-2-1, per una durata di 72 ore alla temperatura più bassa (−20 °C) e alternando 1 ora in funzione/1 ora di riposo, — prova Bd, IEC 68-2-2, per una durata di 72 ore alla temperatura più alta (+ 70 °C) e alternando 1 ora in funzione/1 ora di riposo Cicli di temperature: verificare che l'unità elettronica di bordo possa sopportare variazioni rapide della temperatura ambientale, mediante prova Na, IEC 68-2-14, 20 cicli, ciascuno con temperature che variano da quella più bassa (−20 °C) a quella più alta (+ 70 °C) e una permanenza di 2 ore sia alla temperatura più bassa che a quella più alta 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	159
4.2.	Umidità	Verificare che l'unità elettronica di bordo possa sopportare un'umidità ciclica (prova termica), mediante prova Db, IEC 68-2-30, sei cicli di 24 ore, ciascuno con temperature che variano da + 25 °C a + 55 °C ed un'umidità relativa del 97 % a + 25 °C e del 93 % a + 55 °C	160
4.3.	Vibrazioni	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: 5 g Questo requisito si verifica mediante prova Fc, IEC 68-2-6, con una durata minima della prova di 3 × 12 ore (12 ore per asse) 2. Vibrazioni casuali: Verificare che l'unità elettronica di bordo possa sopportare vibrazioni casuali aventi le seguenti caratteristiche: frequenza 5-150 Hz, livello 0,02 g^2/Hz Questo requisito si verifica mediante prova Ffda, IEC 68-2-35, con una durata minima della prova di 3 × 12 ore (12 ore per asse) e alternando 1 ora in funzione/1 ora di riposo Le due prove sopra descritte sono effettuate su due campioni diversi del modello di apparecchio sottoposto alle prove	163
4.4.	Protezione contro l'acqua e i corpi estranei	Verificare che l'indice di protezione dell'unità elettronica di bordo, secondo IEC 529, sia almeno IP 40, quando montata in un veicolo, in condizioni di funzionamento	164, 165
4.5.	Protezione contro sovratensione	Verificare che l'unità elettronica di bordo possa sopportare un'alimentazione di: Versioni a 24 V: 34 V a + 40 °C per 1 ora versioni a 12 V: 17 V a + 40 °C per 1 ora	161
4.6.	Protezione contro polarità inversa	Verificare che l'unità elettronica di bordo possa sopportare un'inversione dell'alimentazione	161

N.	Prova	Descrizione	Requisiti applicabili
4.7.	Protezione contro cortocircuiti	Verificare che i segnali in ingresso e in uscita siano protetti contro i cortocircuiti rispetto ad alimentazione e massa	161
5.	**Prove della compatibilità elettromagnetica**		
5.1.	Emissioni irradiate e sensibilità ai disturbi	Conformità con la direttiva 95/54/CE	162
5.2.	Scariche elettrostatiche	Conformità con la norma IEC 61000-4-2, ± 2 kV (livello 1)	162
5.3.	Sensibilità ai transitori condotti nell'alimentazione	Per le versioni a 24 V, conformità con la norma ISO 7637-2: impulso 1a: Vs = − 100 V, Ri = 10 ohm impulso 2: Vs = + 100 V, Ri = 10 ohm impulso 3a: Vs = − 100 V, Ri = 50 ohm impulso 3b: Vs = + 100 V, Ri = 50 ohm impulso 4: Vs = − 16 V, Va = − 12 V, t6=100 ms impulso 5: Vs = + 120 V, Ri = 2,2 ohm, td = 250 ms Per le versioni a 12V, conformità con la norma ISO 7637-1: impulso 1: Vs = − 100 V, Ri = 10 ohm impulso 2: Vs = + 100 V, Ri = 10 ohm impulso 3a: Vs = − 100 V, Ri = 50 ohm impulso 3b: Vs = + 100 V, Ri = 50 ohm impulso 4: Vs = − 6 V, Va = − 5 V, t6 = 15 ms impulso 5: Vs = + 65 V, Ri = 3 ohm, td = 100 ms 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	162

3. PROVE FUNZIONALI PER IL SENSORE DI MOVIMENTO

N.	Prova	Descrizione	Requisiti applicabili
1.	**Esame amministrativo**		
1.1.	Documentazione	Correttezza della documentazione	
2.	**Controllo visivo**		
2.1.	Conformità con la documentazione		
2.2.	Identificazione/Iscrizioni		169, 170
2.3.	Materiali		163-167
2.4.	Sigilli		251
3.	**Prove funzionali**		
3.1.	Dati di identificazione del sensore		077*
3.2.	Accoppiamento sensore di movimento — unità elettronica di bordo		099*, 155
3.3.	Rilevamento del movimento		
	Precisione della misurazione del movimento		022-026

N.	Prova	Descrizione	Requisiti applicabili
4.	**Prove ambientali**		
4.1.	Temperatura di esercizio	Verificare la funzionalità (secondo quanto definito alla prova n. 3.3) nel campo di temperatura [- 40 °C; + 135 °C], mediante: — prova Ad, IEC 68-2-1, per una durata di 96 ore alla temperatura più bassa To_{min}, — prova Bd, IEC 68-2-2, per una durata di 96 ore alla temperatura più alta To_{max}	159
4.2.	Cicli di temperature	Verificare la funzionalità (secondo quanto definito alla prova n. 3.3) mediante: prova Na, IEC 68-2-14, 20 cicli, ciascuno con temperature che variano da quella più bassa (− 40 °C) a quella più alta (+135 °C) e una permanenza di 2 ore sia alla temperatura più bassa che a quella più alta Si può effettuare una serie ridotta di prove (fra quelle definite alla prova 3.3) alla temperatura più bassa, alla temperatura più alta e durante i cicli di temperature	159
4.3.	Cicli di umidità	Verificare la funzionalità (secondo quanto definito alla prova n. 3.3), mediante prova Db, IEC 68-2-30, 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	160
4.4.	Vibrazioni	Verificare la funzionalità (secondo quanto definito alla prova n. 3.3), mediante prova Fc, IEC 68-2-6, con una durata di 100 cicli di frequenza: Spostamento costante tra 10 e 57 Hz: picco di 1,5 mm accelerazione costante tra 57 e 500 Hz: 20 g	163
4.5.	Urto meccanico	Verificare la funzionalità (secondo quanto definito alla prova n. 3.3), mediante prova Ea, IEC 68-2-27, 3 urti in entrambe le direzioni dei 3 assi perpendicolari	163
4.6.	Protezione contro l'acqua e i corpi estranei	Verificare che l'indice di protezione del sensore di movimento, secondo IEC 529, sia almeno IP 64, quando montato in un veicolo, in condizioni di funzionamento	165
4.7.	Protezione contro polarità inversa	Verificare che il sensore di movimento possa sopportare un'inversione dell'alimentazione	161
4.8.	Protezione contro cortocircuiti	Verificare che i segnali in ingresso e in uscita siano protetti contro i cortocircuiti rispetto ad alimentazione e massa	161
5.	**Compatibilità elettromagnetica**		
5.1.	Emissioni irradiate e sensibilità ai disturbi	Verificare la conformità con la direttiva 95/54/CE	162
5.2.	Scariche elettrostatiche	Conformità con la norma IEC 61000-4-2, ± 2 kV (livello 1)	162
5.3.	Sensibilità ai transitori condotti nelle linee dati	Conformità con la norma ISO7637-3 (livello III)	162

4. PROVE FUNZIONALI PER LE CARTE TACHIGRAFICHE

N.	Prova	Descrizione	Requisiti applicabili
1.	**Esame amministrativo**		
1.1.	Documentazione	Correttezza della documentazione	
2.	**Controllo visivo**		
2.1.		Accertare che tutte le caratteristiche di protezione e i dati visibili siano stampati correttamente sulla carta e siano conformi	171-181
3.	**Prove fisiche**		
3.1.	Verificare le dimensioni della carta e la posizione dei contatti		184 ISO/IEC 7816-1 ISO/IEC 7816-2
4.	**Prove dei protocolli**		
4.1.	ATR	Verificare la conformità dell'ATR	ISO/IEC 7816-3 TCS 304, 307, 308
4.2.	T=0	Verificare la conformità del protocollo T=0	ISO/IEC 7816-3 TCS 302, 303, 305
4.3.	PTS	Verificare la conformità del comando PTS passando all'impostazione T=1 da T=0	ISO/IEC 7816-3 TCS 309-311
4.4.	T=1	Verificare la conformità del protocollo T=1	ISO/IEC 7816-3 TCS 303, / 306
5.	**Struttura della carta**		
5.1.		Controllare la conformità della struttura dei file della carta, verificando la presenza dei file obbligatori nella carta e le relative condizioni di accesso	TCS 312 TCS 400*, 401, 402, 403*, 404, 405*, 406, 407, 408*, 409, 410*, 411, 412, 413*, 414, 415*, 416, 417, 418*, 419
6.	**Prove funzionali**		
6.1.	Elaborazione normale	Verificare almeno una volta ogni uso ammesso di ciascun comando (per es.: verificare il comando UPDATE BINARY con CLA = '00', CLA = '0C' e con parametri P1,P2 e Lc diversi). Verificare che le operazioni siano state effettivamente eseguite nella carta (per es.: leggendo il file su cui è stato eseguito il comando)	da TCS 313 a TCS 379
6.2.	Messaggi di errore	Verificare almeno una volta ogni messaggio di errore (secondo quanto specificato all'appendice 2) per ciascun comando. Verificare almeno una volta ogni errore generico (eccetto per gli errori di integrità '6400', verificati nell'ambito della certificazione della sicurezza)	
7.	**Prove ambientali**		
7.1.		Accertare che le carte funzionino entro i limiti delle condizioni definite in conformità della norma ISO/IEC 10373	185-188 ISO/IEC 7816-1

5. PROVE DI INTEROPERABILITÀ

N.	Prova	Descrizione
1.	Autenticazione reciproca	Verificare che l'autenticazione reciproca tra l'unità del veicolo 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 della carta, che tutte le registrazioni corrispondenti siano state effettuate correttamente Verificare, mediante la stampa giornaliera della carta, che tutte le registrazioni corrispondenti si possano leggere correttamente

Appendice 10

OBIETTIVI GENERALI DI SICUREZZA

La presente appendice specifica il contenuto minimo richiesto per gli obiettivi di sicurezza del sensore di movimento, dell'unità elettronica di bordo e delle carte tachigrafiche.

Al fine di formulare gli obiettivi di sicurezza rispetto ai quali richiedere la certificazione della sicurezza, i fabbricanti devono perfezionare e completare i documenti a seconda della necessità, senza modificare né cancellare le specifiche relative alle minacce, agli obiettivi, alle procedure e alle funzioni di sicurezza in essi contenute.

INDICE

Obiettivi generali di sicurezza per i senori di movimento

Obiettivi generali di sicurezza per l'unità elettronica di bordo

Obiettivi generali di sicurezza per le carte tachigrafiche

OBIETTIVI GENERALI DI SICUREZZA PER I SENSORI DI MOVIMENTO

1. **Introduzione**

Il presente documento contiene una descrizione del sensore di movimento, delle minacce che deve essere in grado di neutralizzare e degli obiettivi di sicurezza che deve conseguire. Specifica le funzioni di sicurezza richieste e indica la robustezza minima dichiarata dei meccanismi di sicurezza e il grado di garanzia richiesto per lo sviluppo e la valutazione.

I requisiti cui fa riferimento il presente documento sono quelli contemplati nel corpo dell'allegato I B. A fini di chiarezza, sono talvolta presenti ripetizioni tra i requisiti di cui all'allegato I B e quelli degli obiettivi di sicurezza. In caso di ambiguità tra un requisito di sicurezza e un requisito di cui all'allegato I B cui il requisito di sicurezza si riferisce, fa fede il requisito indicato nel corpo dell'allegato I B.

I requisiti di cui all'allegato I B cui non fanno riferimento gli obiettivi di sicurezza non sono oggetto di funzioni di sicurezza.

A fini di rintracciabilità nella documentazione relativa allo sviluppo e alla valutazione, alle specifiche di ogni minaccia, obiettivo, procedura e funzione di sicurezza è stata assegnata un'apposita etichetta.

2. **Acronimi, definizioni e riferimenti normativi**

2.1. ***Acronimi***

ROM	(Read Only Memory) — Memoria a sola lettura
SEF	Security enforcing function — Funzione di sicurezza
TBD	To be defined — Da definire
TOE	Target of evaluation — Obiettivo di valutazione
VU	Vehicle unit — Unità elettronica di bordo

2.2. ***Definizioni***

Tachigrafo digitale	L'apparecchio di controllo
Entità	Un dispositivo collegato al sensore di movimento
Dati di movimento	I dati scambiati con la VU, che rappresentano la velocità e la distanza percorsa
Elementi fisicamente separati	Componenti fisici del sensore di movimento distribuiti nel veicolo in contrapposizione ai componenti fisici contenuti nell'involucro del sensore di movimento
Dati di sicurezza	I dati specifici necessari per l'esecuzione delle funzioni di sicurezza (per es., chiavi crittocrafiche)
Sistema	Apparecchiature, persone o organismi interessati in qualsiasi modo all'apparecchio di controllo
Utente	Una persona che utilizza il sensore di movimento (se non usato nell'espressione “dati dell'utente”)
Dati dell'utente	Qualsiasi dato, diverso dai dati di movimento e di sicurezza, registrato o memorizzato dal sensore di movimento

2.3. ***Riferimenti normativi***

ITSEC ITSEC — Criteri per la valutazione della sicurezza delle tecnologie dell'informazione, 1991

3. **Descrizione del prodotto**

3.1. ***Descrizione del sensore di movimento e metodo d'impiego***

Il sensore di movimento è destinato al montaggio in veicoli adibiti al trasporto stradale ed ha lo scopo di fornire ad una VU dati di movimento attendibili che rappresentano la velocità del veicolo e la distanza percorsa.

Il sensore di movimento è collegato meccanicamente ad un elemento mobile del veicolo, il cui movimento può rappresentare la velocità del veicolo o la distanza percorsa. Può essere installato nella scatola del cambio o in qualsiasi altra parte del veicolo.

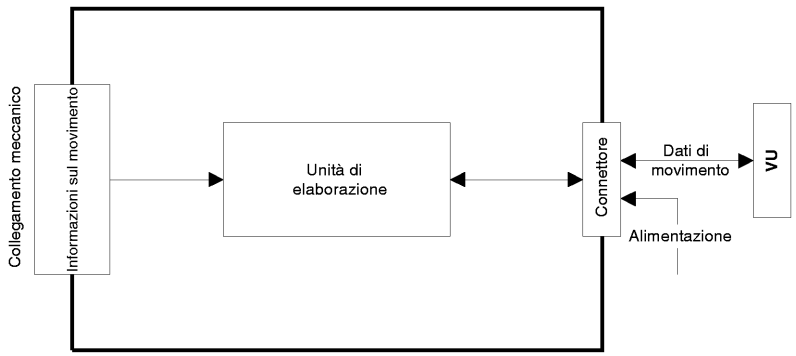
Nel modo operativo, il sensore di movimento è collegato a una VU.

Può anche essere collegato ad apparecchiature specifiche a fini di gestione (TBD dal fabbricante)

Il sensore di movimento tipico è illustrato nella figura seguente:

Figura 1

Sensore di movimento tipico

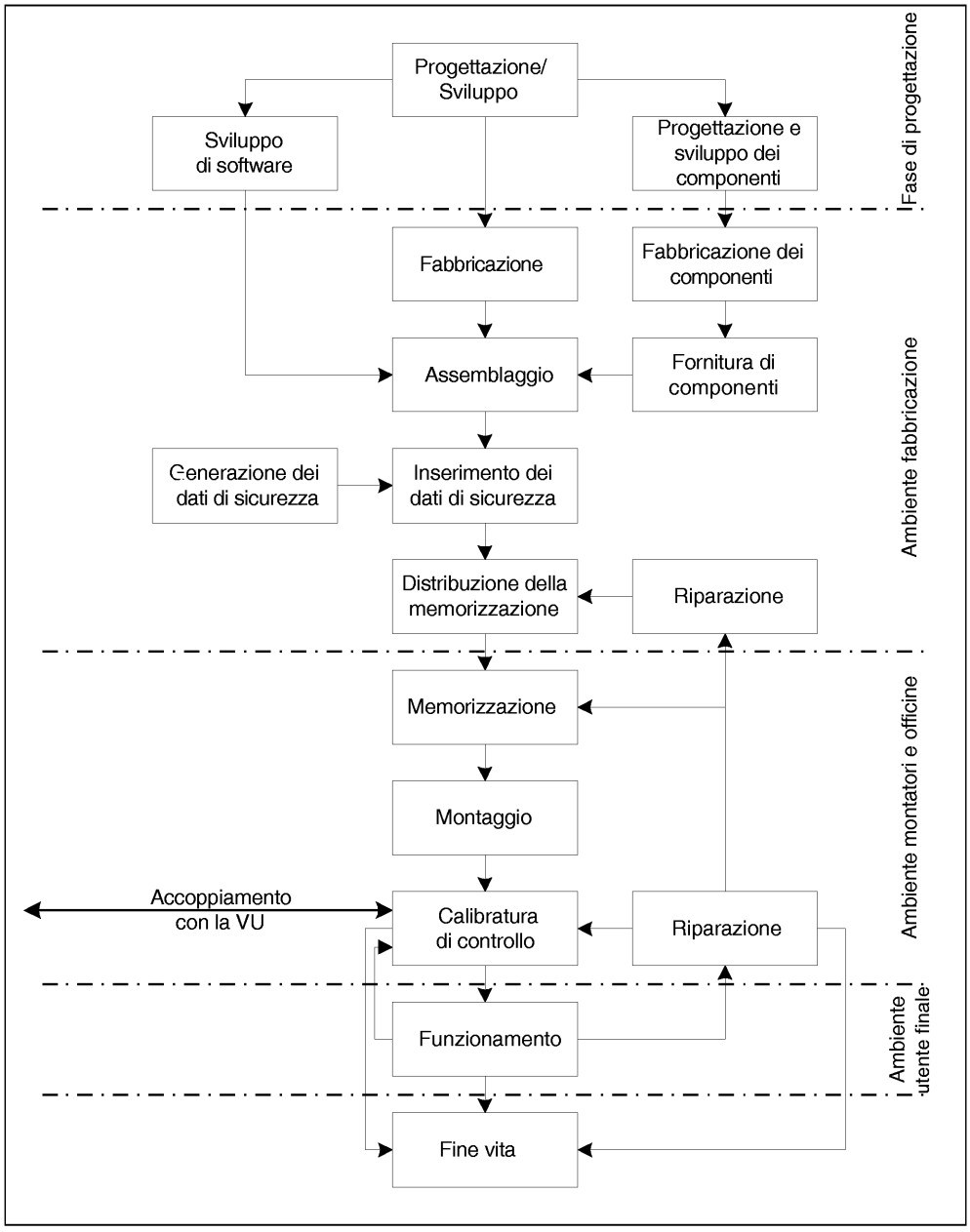


3.2. ***Ciclo di vita del sensore di movimento***

Il ciclo di vita tipico del sensore di movimento è illustrato nella figura seguente:

Figura 2

Ciclo di vita tipico del sensore di movimento



3.3. ***Minacce***

Il presente paragrafo descrive le minacce che possono riguardare il sensore di movimento.

3.3.1. *Minacce per le strategie di controllo dell'accesso*

T.Access Gli utenti potrebbero tentare di accedere a funzioni che non sono autorizzati ad usare

3.3.2. *Minacce concernenti il modello*

T.Faults	Difetti dei prodotti hardware e software e delle procedure di comunicazione potrebbero porre il sensore di movimento in condizioni impreviste tali da pregiudicarne la sicurezza
T.Tests	L'uso di modalità di prova che non siano state disabilitate o di vulnerabilità presenti nel sistema potrebbe pregiudicare la sicurezza del sensore di movimento
T.Design	Gli utenti potrebbero tentare di ottenere illecitamente informazioni sul modello sia partendo dal materiale del fabbricante (mediante furto, corruzione, ecc.) sia con tecniche di retroanalisi (reverse engineering)

3.3.3. *Minacce concernenti il funzionamento*

T.Environment	Gli utenti potrebbero compromettere la sicurezza del sensore di movimento con attacchi di carattere ambientale (termici, elettromagnetici, ottici, chimici, meccanici, ecc.)
T.Hardware	Gli utenti potrebbero tentare di modificare gli elementi hardware del sensore di movimento
T.Mechanical_Origin	Gli utenti potrebbero tentare di manipolare l'input del sensore di movimento (per es. allentando le viti nella scatola del cambio, ecc.)
T.Motion_Data	Gli utenti potrebbero tentare di modificare i dati di movimento del veicolo (aggiunte, modifiche, cancellazione, riproduzione del segnale)
T.Power_Supply	Gli utenti potrebbero tentare di vanificare gli obiettivi di sicurezza del sensore di movimento modificandone (interrompendo, riducendo, aumentando) l'alimentazione
T.Security_Data	Gli utenti potrebbero tentare di ottenere illecitamente informazioni sui dati di sicurezza durante la generazione o il trasferimento o la memorizzazione di tali dati nell'apparecchio
T.Software	Gli utenti potrebbero tentare di modificare il software del sensore di movimento
T.Stored_Data	Gli utenti potrebbero tentare di modificare i dati memorizzati (dati di sicurezza o dell'utente)

3.4. ***Obiettivi di sicurezza***

L'obiettivo di sicurezza principale del sistema a tachigrafo digitale è il seguente:

O.Main	I dati soggetti al controllo delle autorità competenti devono essere disponibili e rispecchiare interamente ed accuratamente le attività dei conducenti e dei veicoli sottoposti al controllo per quanto riguarda i periodi di guida, lavoro, disponibilità e riposo e la velocità del veicolo

L'obiettivo di sicurezza del sensore di movimento, che contribuisce a realizzare l'obiettivo di sicurezza generale, è quindi:

O.Sensor_Main	I dati trasmessi dal sensore di movimento devono essere resi disponibili alla VU in modo tale che la VU sia in grado di determinare interamente ed accuratamente il movimento del veicolo in termini di velocità e distanza percorsa

3.5. ***Obiettivi di sicurezza relativi alle tecnologie dell'informazione (IT)***

Gli obiettivi di sicurezza IT specifici del sensore di movimento, che contribuiscono a realizzare il suo obiettivo di sicurezza principale, sono i seguenti:

O.Access	Il sensore di movimento deve controllare l'accesso delle entità collegate alle funzioni e ai dati
O.Audit	Il sensore di movimento deve verificare i tentativi di compromettere la sua sicurezza e risalire alle entità ad essi associate
O.Authentication	Il sensore di movimento deve autenticare le entità collegate

O.Processing	Il sensore di movimento deve garantire l'elaborazione accurata degli input da cui vengono ricavati i dati di movimento
O.Reliability	Il sensore di movimento deve fornire un servizio affidabile
O.Secured_Data_Exchange	Il sensore di movimento deve garantire la sicurezza degli scambi di dati con la VU

3.6. ***Mezzi fisici, procedure e personale***

Il presente punto descrive i requisiti fisici e relativi alle procedure o al personale che contribuiscono alla sicurezza del sensore di movimento.

3.6.1. *Progettazione dell'apparecchio*

M.Development	I responsabili dello sviluppo del sensore di movimento devono garantire che l'attribuzione delle responsabilità durante lo sviluppo sia tale da salvaguardare la sicurezza IT
M.Manufacturing	I fabbricanti del sensore di movimento devono garantire che l'attribuzione delle responsabilità durante la fabbricazione sia tale da salvaguardare la sicurezza IT e che durante il processo di fabbricazione il sensore di movimento sia protetto contro attacchi fisici che possono compromettere la sicurezza IT

3.6.2. *Consegna dell'apparecchio*

M.Delivery	I fabbricanti di sensori di movimento, i costruttori di veicoli e i montatori o le officine devono garantire che la movimentazione del sensore di movimento avvenga in modo tale da salvaguardare la sicurezza IT

3.6.3. *Generazione e consegna dei dati di sicurezza*

M.Sec_Data_Generation	Agli algoritmi di generazione dei dati di sicurezza devono poter accedere soltanto persone autorizzate e fidate
M.Sec_Data_Transport	I dati di sicurezza devono essere generati, trasferiti ed inseriti nel sensore di movimento in modo tale da preservarne la riservatezza e l'integrità appropriate

3.6.4. *Montaggio, calibratura e controllo dell'apparecchio*

M.Approved_Workshops	Il montaggio, la calibratura e la riparazione dell'apparecchio di controllo devono essere effettuati da officine o da montatori autorizzati e fidati
M.Mechanical_Interface	Si devono prevedere misure atte a rilevare manomissioni fisiche del collegamento meccanico (per es. sigilli)
M.Regular_Inspections	L'apparecchio di controllo deve essere sottoposto a calibrature e controlli periodici

3.6.5. *Controllo dell'applicazione della legislazione*

M.Controls	I controlli dell'applicazione della legislazione devono essere eseguiti regolarmente e in modo casuale, e devono prevedere verifiche della sicurezza

3.6.6. *Aggiornamenti del software*

M.Software_Upgrade	Prima di poter essere installate in un sensore di movimento, le nuove versioni del software devono ottenere la certificazione di sicurezza

4. **Funzioni di sicurezza**

4.1. ***Identificazione e autenticazione***

UIA_101	Il sensore di movimento deve essere in grado di stabilire, per ogni interazione, l'identità di ogni entità cui è collegato.

UIA_102 L'identità di un'entità collegata consiste in:

— un gruppo entità:

— VU,

— dispositivo di gestione,

— altro,

una ID entità (solo VU).

UIA_103 L'ID entità di una VU collegata è costituita dal numero di omologazione della VU e dal numero di serie della VU.

UIA_104 Il sensore di movimento deve essere in grado di autenticare ogni VU o dispositivo di gestione cui è collegato:

— all'atto del collegamento dell'entità,

— all'atto del ripristino dell'alimentazione.

UIA_105 Il sensore di movimento deve essere in grado di riautenticare periodicamente la VU cui è collegato.

UIA_106 Il sensore di movimento rileva ed impedisce l'uso di dati di autenticazione copiati e riprodotti.

UIA_107 Dopo aver rilevato (TBD dal fabbricante e non più di 20) tentativi consecutivi falliti di autenticazione, la SEF:

— genera una registrazione di verifica dell'anomalia,

— avvisa l'entità,

— continua ad esportare i dati di movimento in una modalità non sicura.

4.2. ***Controllo dell'accesso***

I controlli dell'accesso garantiscono che le informazioni vengano lette, create o modificate nel TOE soltanto da persone autorizzate.

4.2.1. *Strategia di controllo dell'accesso*

ACC_101 Il sensore di movimento controlla i diritti di accesso alle funzioni e ai dati.

4.2.2. *Diritti di accesso ai dati*

ACC_102 Il sensore di movimento garantisce che i dati di identificazione del sensore possano essere scritti una sola volta (requisito 078).

ACC_103 Il sensore di movimento accetta e/o memorizza i dati dell'utente solo se provengono da entità autenticate.

ACC_104 Il sensore di movimento applica diritti appropriati di lettura e scrittura ai dati di sicurezza.

4.2.3. *Struttura dei file e condizioni di accesso*

ACC_105 La struttura dei file delle applicazioni e dei file di dati e le condizioni di accesso vengono create durante la fabbricazione e quindi bloccate contro eventuali modifiche o cancellazioni future.

4.3. ***Responsabilità***

ACT_101 Il sensore di movimento conserva nella sua memoria i dati di identificazione del sensore di movimento (requisito 077).

ACT_102 Il sensore di movimento memorizza nella sua memoria i dati di montaggio (requisito 099).

ACT_103 Il sensore di movimento è in grado di trasmettere alle entità autenticate, su loro richiesta, i dati relativi alla responsabilità.

4.4. ***Verifica***

AUD_101 Per le anomalie che compromettono la sua sicurezza, il sensore di movimento genera registrazioni di verifica delle anomalie.

AUD_102 Le anomalie che pregiudicano la sicurezza del sensore di movimento sono le seguenti:

— tentativi di violazione della sicurezza:

  — autenticazione fallita,

  — errore di integrità dei dati memorizzati,

  — errore nel trasferimento interno di dati,

  — apertura non autorizzata dell'involucro,

  — sabotaggio di elementi hardware,

— guasto del sensore.

AUD_103 Le registrazioni di verifica comprendono i dati seguenti:

— data e ora dell'anomalia,

— tipo di anomalia,

— identità dell'entità collegata,

se i dati richiesti non sono disponibili viene fornita un'adeguata indicazione predefinita (TBD dal fabbricante).

AUD_104 Il sensore di movimento invia alla VU le registrazioni di verifica all'atto della loro generazione e può anche memorizzarle nella sua memoria.

AUD_105 Nel caso in cui il sensore di movimento memorizzi le registrazioni di verifica, esso deve garantire la conservazione di 20 registrazioni di verifica indipendentemente dall'esaurimento della capacità di memorizzazione delle verifiche ed essere in grado di trasmettere alle entità autenticate, su loro richiesta, le registrazioni di verifica memorizzate.

4.5. ***Accuratezza***

4.5.1. *Strategia di controllo del flusso di informazioni*

ACR_101 Il sensore di movimento garantisce che i dati di movimento possano essere elaborati e ricavati soltanto in base all'input meccanico del sensore.

4.5.2. *Trasferimenti interni di dati*

I requisiti del presente paragrafo si applicano solo se il sensore di movimento utilizza elementi fisicamente separati.

ACR_102 Se i dati vengono trasferiti tra elementi fisicamente separati del sensore di movimento, tali dati devono essere protetti contro eventuali modifiche.

ACR_103 Al rilevamento di un errore nel trasferimento di dati durante un trasferimento interno, la trasmissione viene ripetuta e la SEF genera una registrazione di verifica dell'anomalia.

4.5.3. *Integrità dei dati memorizzati*

ACR_104 Il sensore di movimento controlla i dati dell'utente memorizzati nella sua memoria per verificare l'assenza di errori di integrità.

ACR_105 Al rilevamento di un errore di integrità dei dati dell'utente memorizzati, la SEF genera una registrazione di verifica.

4.6. ***Affidabilità del servizio***

4.6.1. *Prove*

RLB_101 Tutti i comandi, le azioni o i punti di prova specifici per le esigenze di prova nella fase di fabbricazione vengono disabilitati o eliminati prima del termine della fase di fabbricazione. Non deve essere possibile ripristinarli per impiego successivo.

RLB_102 Durante l'avviamento iniziale e durante il normale funzionamento, il sensore di movimento esegue prove automatiche per verificare il suo funzionamento corretto. Le prove automatiche del sensore di movimento comprendono una verifica dell'integrità dei dati di sicurezza e una verifica dell'integrità del codice eseguibile memorizzato (se non in ROM).

RLB_103 Al rilevamento di un guasto interno durante la prova automatica, la SEF genera una registrazione di verifica (guasto del sensore).

4.6.2. *Software*

RLB_104 Deve essere impedita l'analisi e la ricerca e correzione di errori del software del sensore di movimento sul campo.

RLB_105 Non devono essere accettati input da fonti esterne come codici eseguibili.

4.6.3. *Protezione fisica*

RLB_106 Se il modello del sensore di movimento ne consente l'apertura, il sensore deve rilevare ogni apertura dell'involucro, anche in assenza di alimentazione esterna per un minimo di 6 mesi. In tal caso, la SEF genera una registrazione di verifica dell'anomalia. (È ammesso che la registrazione di verifica sia generata e memorizzata in seguito al ripristino dell'alimentazione).

Se il modello del sensore di movimento non ne consente l'apertura, esso deve essere tale da consentire di individuare facilmente eventuali tentativi di manomissione (per es., mediante controllo visivo).

RLB_107 Il sensore di movimento rileva i sabotaggi specificati (TBD dal fabbricante) degli elementi hardware.

RLB_108 Nel caso sopra descritto, la SEF genera una registrazione di verifica e il sensore di movimento: (TBD dal fabbricante).

4.6.4. *Interruzioni dell'alimentazione*

RLB_109 Il sensore di movimento rimane in condizione di sicurezza durante l'interruzione o le variazioni di alimentazione.

4.6.5. *Condizioni di azzeramento*

RLB_110 In caso di interruzione dell'alimentazione, o qualora un'operazione venga interrotta prima del completamento, o in qualsiasi altra condizione di azzeramento, il sensore di movimento deve essere completamente azzerato.

4.6.6. *Disponibilità dei dati*

RLB_111 Il sensore di movimento garantisce la possibilità di accedere alle risorse quando necessario e che le risorse non siano richieste né trattenute senza necessità.

4.6.7. *Applicazioni multiple*

RLB_112 Se il sensore di movimento prevede applicazioni diverse da quella tachigrafica, tutte le applicazioni devono essere fisicamente e/o logicamente separate le une dalle altre. Tali applicazioni non devono condividere dati di sicurezza. In ogni dato momento può essere attivo un solo compito.

4.7. ***Scambio di dati***

DEX_101 Il sensore di movimento esporta i dati di movimento verso la VU con attributi di sicurezza associati, in modo da consentire alla VU di verificarne l'integrità e l'autenticità.

4.8. ***Crittografia***

I requisiti del presente punto si applicano solo se necessario, a seconda dei meccanismi di sicurezza utilizzati e delle soluzioni adottate dal fabbricante.

CSP_101 Ogni operazione crittografica effettuata dal sensore di movimento si deve basare su un algoritmo specificato e su dimensioni di chiave specificate.

CSP_102 Se il sensore di movimento genera chiavi crittografiche, tale operazione si deve basare su algoritmi di generazione di chiavi crittografiche specificati e su dimensioni di chiavi crittografiche specificate.

CSP_103 Se il sensore di movimento distribuisce chiavi crittografiche, tale operazione si deve basare su metodi di distribuzione di chiavi specificati.

CSP_104 Se il sensore di movimento accede a chiavi crittografiche, tale operazione si deve basare su metodi di accesso a chiavi crittografiche specificati.

CSP_105 Se il sensore di movimento distrugge chiavi crittografiche, tale operazione si deve basare su metodi di distruzione di chiavi crittografiche specificati.

5. **Definizione dei meccanismi di sicurezza**

I meccanismi di sicurezza che realizzano le funzioni di sicurezza del sensore di movimento sono definiti dai fabbricanti del sensore.

6. **Robustezza minima dei meccanismi di sicurezza**

La robustezza minima dei meccanismi di sicurezza del sensore di movimento è Elevata, secondo quanto stabilito nella norma ITSEC.

7. **Grado di garanzia**

Il grado di garanzia che deve fornire il sensore di movimento è il livello ITSEC E3, secondo quanto stabilito nella norma ITSEC.

8. **Fondamento logico**

Le matrici riportate di seguito forniscono una spiegazione logica delle SEF, indicando:

— quale SEF o misura neutralizza la minaccia indicata,

— quale SEF realizza gli obiettivi di sicurezza IT.

	Minacce											Obiettivi IT					
	T.Access	T.Faults	T.Test	T.Design	T.Environment	A.Hardware	T.Mechanical_Origin	T.Motion_Data	T.Power_Supply	T.Security_Data	T.Software	T.Stored_Data	O.Access	O.Audit	O.Authentication	O.Processing	O.Reliability	O.Secured_Data_Exchange
Mezzi fisici, procedure e personale																		
Sviluppo		x	x	x														
Fabbricazione			x	x														
Consegna						x					x	x						
Generazione dati sicurezza										x								
Trasferimento dati sicurezza										x								
Officine autorizzate							x											
Collegamento meccanico							x											
Controllo regolare						x	x		x		x							
Controlli applicazione legislazione					x	x	x		x	x	x							
Aggiornamenti software											x							
Funzioni di sicurezza																		
Identificazione e autenticazione																		
UIA_101 Identificazione entità	x							x					x		x			x
UIA_102 Identità entità	x												x		x			
UIA_103 Identità VU														x				
UIA_104 Autenticazione entità	x							x					x		x			x
UIA_105 Riautenticazione	x							x					x		x			x
UIA_106 Autenticazione impossibile	x							x					x		x			
UIA_107 Autenticazione fallita								x						x			x	
Controllo dell'accesso																		
ACC_101 Strategia di controllo dell'accesso	x									x		x	x					
ACC_102 ID sensore di movimento												x	x					

	Minacce												Obiettivi IT					
	T.Access	T.Faults	T.Test	T.Design	T.Environment	A.Hardware	T.Mechanical_Origin	T.Motion_Data	T.Power_Supply	T.Security_Data	T.Software	T.Stored_Data	O.Access	O.Audit	O.Authentication	O.Processing	O.Reliability	O.Secured_Data_Exchange
ACC_103 Dati utente												x	x					
ACC_104 Dati sicurezza										x		x	x					
ACC_105 Struttura dei file e condizioni di accesso	x									x		x	x					
Responsabilità																		
ACT_101 Dati ID sensore di movimento														x				
ACT_102 Dati accoppiamento														x				
ACT_103 Dati responsabilità														x				
Verifica																		
AUD_101 Registrazioni di verifica														x				
AUD_102 Elenco verifica anomalie	x				x	x						x		x				
AUD_103 Dati verifica														x				
AUD_104 Strumenti verifica														x				
AUD_105 Memorizzazione registrazioni di verifica														x				
Accuratezza																		
ACR_101 Strategia di controllo flusso informazioni								x								x	x	
ACR_102 Trasferimenti interni																x	x	
ACR_103 Trasferimenti interni														x				
ACR_104 Integrità dati memorizzati												x					x	
ACR_105 Integrità dati memorizzati												x		x				
Affidabilità																		
RLB_101 Prove di fabbricazione			x	x													x	
RLB_102 Prove automatiche		x				x			x		x						x	
RLB_103 Prove automatiche						x			x		x			x				
RLB_104 Analisi software				x							x						x	
RLB_105 Input software											x					x	x	
RLB_106 Apertura involucro				x	x	x				x	x	x					x	
RLB_107 Sabotaggio hardware						x											x	
RLB_108 Sabotaggio hardware						x								x				
RLB_109 Interruzioni alimentazione									x								x	
RLB_110 Azzeramento		x															x	
RLB_111 Disponibilità dati																x	x	
RLB_112 Applicazioni multiple																	x	
Scambio di dati																		
DEX_101 Esportazione sicura dati di movimento								x										x
Crittografia																		
CSP_101 Algoritmi																	x	x
CSP_102 Generazione chiavi																	x	x
CSP_103 Distribuzione chiavi																	x	x
CSP_104 Accesso chiavi																	x	x
CSP_105 Distruzione chiavi																	x	x

OBIETTIVI GENERALI DI SICUREZZA PER L'UNITÀ ELETTRONICA DI BORDO

1. **Introduzione**

Il presente documento contiene una descrizione dell'unità elettronica di bordo, delle minacce che deve essere in grado di neutralizzare e degli obiettivi di sicurezza che deve conseguire. Specifica le funzioni di sicurezza richieste e indica la robustezza minima dichiarata dei meccanismi di sicurezza e il grado di garanzia richiesto per lo sviluppo e la valutazione.

I requisiti cui fa riferimento il presente documento sono quelli indicati nel corpo dell'allegato I B. A fini di chiarezza, sono talvolta presenti ripetizioni tra i requisiti di cui all'allegato I B e quelli degli obiettivi di sicurezza. In caso di ambiguità tra un requisito di sicurezza ed un requisito di cui all'allegato I B cui il requisito di sicurezza si riferisce, fa fede il requisito indicato nel corpo dell'allegato I B.

I requisiti di cui all'allegato I B cui non fanno riferimento gli obiettivi di sicurezza non sono oggetto di funzioni di sicurezza.

A fini di rintracciabilità nella documentazione relativa allo sviluppo e alla valutazione, alle specifiche di ogni minaccia, obiettivo, procedura e funzione di sicurezza è stata assegnata un'apposita etichetta.

2. **Acronimi, definizioni e riferimenti normativi**

2.1. ***Acronimi***

PIN	Personal identification number — Numero di identificazione personale
ROM	Read only memory — Memoria a sola lettura
SEF	Security enforcing function — Funzione di sicurezza
TBD	To be defined — Da definire
TOE	Target of evaluation — Target di valutazione
VU	Vehicle unit — Unità elettronica di bordo

2.2. ***Definizioni***

Tachigrafo digitale	L'apparecchio di controllo
Dati di movimento	I dati scambiati con il sensore di movimento, che rappresentano la velocità e la distanza percorsa
Elementi fisicamente separati	Componenti fisici della VU distribuiti nel veicolo in contrapposizione ai componenti fisici contenuti nell'involucro della VU
Dati di sicurezza	I dati specifici necessari per l'esecuzione delle funzioni di sicurezza (per es., chiavi crittografiche)
Sistema	Apparecchiature, persone o organismi interessati in qualsiasi modo all'apparecchio di controllo
Utente	Gli utenti sono intesi come le persone che utilizzano l'apparecchio. Di norma gli utenti della VU sono i conducenti, gli agenti incaricati dei controlli, le officine e le imprese
Dati dell'utente	Qualsiasi dato, diverso dai dati di sicurezza, registrato o memorizzato dalla VU, prescritto al punto 12 del capitolo III

2.3. ***Riferimenti normativi***

ITSEC	ITSEC — Criteri per la valutazione della sicurezza delle tecnologie dell'informazione, 1991

3. **Descrizione del prodotto**

3.1. ***Descrizione dell'unità elettronica di bordo e metodo d'impiego***

La VU è destinata al montaggio in veicoli per i trasporti stradali ed ha lo scopo di registrare, memorizzare, visualizzare, stampare e trasmettere dati relativi alle attività del conducente.

È collegata a un sensore di movimento con il quale scambia i dati di movimento del veicolo.

Gli utenti si identificano con la VU mediante carte tachigrafiche.

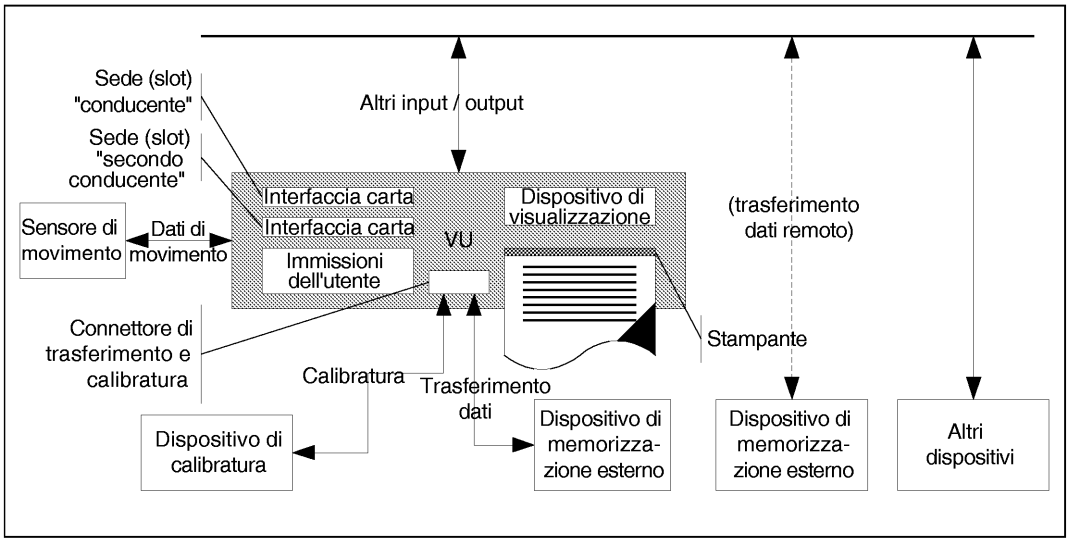
La VU registra e memorizza i dati relativi alle attività dell'utente nella sua memoria di dati e registra inoltre tali dati nelle carte tachigrafiche.

La VU trasmette dati al dispositivo di visualizzazione, alla stampante e a dispositivi esterni.

L'ambiente operativo dell'unità elettronica di bordo, quando è montata in un veicolo, è illustrato nella figura seguente:

Figura 2

Ambiente operativo della VU



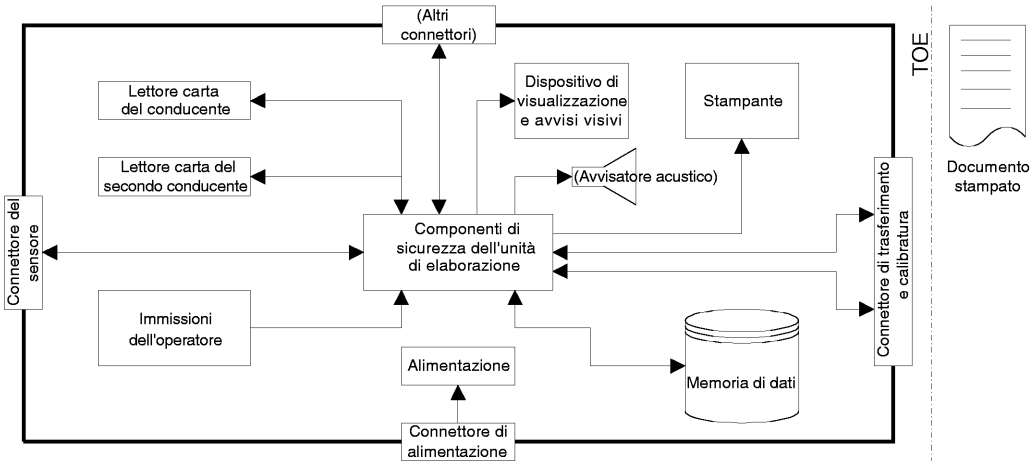
Le caratteristiche generali, le funzioni e le modalità di funzionamento della VU sono descritti nel capitolo II dell'allegato I B.

I requisiti funzionali della VU sono specificati nel capitolo III dell'allegato I B.

La VU tipica è illustrata nella figura seguente:

Figura 3

VU tipica (…) facoltativo



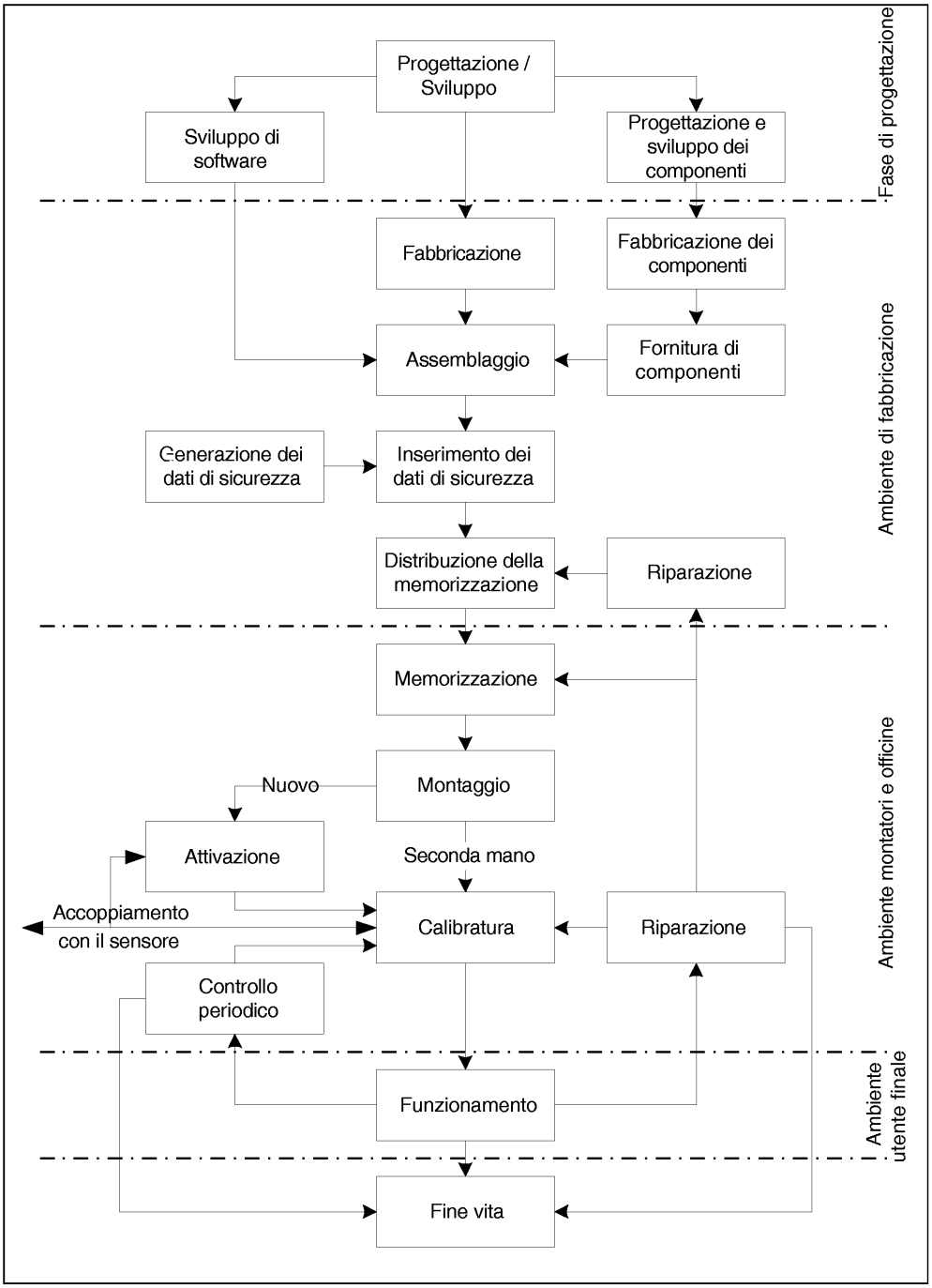
Va rilevato che sebbene il meccanismo della stampante faccia parte del TOE, il documento cartaceo, una volta prodotto, non vi rientra.

3.2. ***Ciclo di vita dell'unità elettronica di bordo***

Il ciclo di vita tipico della VU è illustrato nella figura seguente:

Figura 4

Ciclo di vita tipico della VU



3.3. ***Minacce***

Il presente paragrafo descrive le minacce che possono riguardare la VU.

3.3.1. *Minacce per l'identificazione e le strategie di controllo dell'accesso*

T.Access	Gli utenti potrebbero tentare di accedere a funzioni che non sono autorizzati ad usare (per es., accesso alla funzione di calibratura da parte dei conducenti)
T.Identification	Gli utenti potrebbero tentare di usare varie identificazioni oppure nessuna identificazione

3.3.2. *Minacce concernenti il modello*

T.Faults	Difetti dei prodotti hardware e software e delle procedure di comunicazione potrebbero porre la VU in condizioni impreviste tali da pregiudicarne la sicurezza
T.Tests	L'uso di modalità di prova che non siano state disabilitate o di vulnerabilità presenti nel sistema potrebbe pregiudicare la sicurezza della VU
T.Design	Gli utenti potrebbero tentare di ottenere illecitamente informazioni sul modello sia partendo dal materiale del fabbricante (mediante furto, corruzione, ecc.) sia con tecniche di retroanalisi (reverse engineering)

3.3.3. *Minacce concernenti il funzionamento*

T.Calibration_Parameters	Gli utenti potrebbero tentare di usare apparecchi mal tarati (mediante la modifica dei dati di calibratura o vulnerabilità organizzative)
T.Card_Data_Exchange	Gli utenti potrebbero tentare di modificare i dati durante gli scambi tra VU e carte tachigrafiche (aggiunte, modifiche, cancellazioni, riproduzione del segnale)
T.Clock	Gli utenti potrebbero tentare di modificare l'orologio interno
T.Environment	Gli utenti potrebbero compromettere la sicurezza della VU con attacchi di carattere ambientale (termici, elettromagnetici, ottici, chimici, meccanici, ecc.)
T.Fake_Devices	Gli utenti potrebbero tentare di collegare alla VU dispositivi contraffatti (sensori di movimento, carte intelligenti)
T.Hardware	Gli utenti potrebbero tentare di modificare gli elementi hardware della VU
T.Motion_Data	Gli utenti potrebbero tentare di modificare i dati di movimento del veicolo (aggiunte, modifiche, cancellazioni, riproduzione del segnale)
T.Non_Activated	Gli utenti potrebbero usare apparecchi non attivati
T.Output_Data	Gli utenti potrebbero tentare di modificare i dati trasmessi (stampa, visualizzazione o trasferimento)
T.Power_Supply	Gli utenti potrebbero tentare di vanificare gli obiettivi di sicurezza della VU modificandone (interrompendo, riducendo, aumentando) l'alimentazione
T.Security_Data	Gli utenti potrebbero tentare di ottenere illecitamente informazioni sui dati di sicurezza durante la generazione o il trasferimento o la memorizzazione di tali dati nell'apparecchio
T.Software	Gli utenti potrebbero tentare di modificare il software della VU
T.Stored_Data	Gli utenti potrebbero tentare di modificare i dati memorizzati (dati di sicurezza o dell'utente)

3.4. ***Obiettivi di sicurezza***

L'obiettivo di sicurezza principale del sistema a tachigrafo digitale è il seguente:

O.Main	I dati soggetti al controllo delle autorità competenti devono essere disponibili e rispecchiare interamente ed accuratamente le attività dei conducenti e dei veicoli sottoposti al controllo per quanto riguarda i periodi di guida, lavoro, disponibilità e riposo e la velocità del veicolo

Gli obiettivi di sicurezza della VU, che contribuiscono a realizzare l'obiettivo di sicurezza principale, sono quindi:

O.VU_Main	I dati da misurare e registrare e quindi da sottoporre al controllo delle autorità competenti devono essere disponibili e rispecchiare accuratamente le attività dei conducenti e dei veicoli sottoposti al controllo per quanto riguarda i periodi di guida, lavoro, disponibilità e riposo e la velocità del veicolo
O.VU_Export	La VU deve essere in grado di esportare i dati verso strumenti di memorizzazione esterni in modo tale da permettere di verificare l'integrità e l'autenticità di tali dati

3.5. ***Obiettivi di sicurezza relativi alle tecnologie dell'informazione (IT)***

Gli obiettivi di sicurezza IT specifici della VU, che contribuiscono a realizzare i suoi obiettivi di sicurezza principali, sono i seguenti:

O.Access	La VU deve controllare l'accesso degli utenti alle funzioni e ai dati
O.Accountability	La VU deve raccogliere dati accurati relativi alla responsabilità
O.Audit	La VU deve verificare i tentativi di compromettere la sicurezza del sistema e risalire agli utenti ad essi associati
O.Authentication	La VU autentica gli utenti e le entità collegate (quando è necessario stabilire un percorso fidato tra entità)
O.Integrity	La VU deve preservare l'integrità dei dati memorizzati
O.Output	La VU deve garantire che i dati trasmessi rispecchino accuratamente i dati misurati o memorizzati
O.Processing	La VU deve garantire l'elaborazione accurata degli input da cui vengono ricavati i dati dell'utente
O.Reliability	La VU deve fornire un servizio affidabile
O.Secured_Data_Exchange	La VU deve garantire la sicurezza degli scambi di dati con il sensore di movimento e con le carte tachigrafiche.

3.6. ***Mezzi fisici, procedure e personale***

Il presente punto descrive i requisiti fisici e relativi alle procedure o al personale che contribuiscono alla sicurezza della VU.

3.6.1. *Progettazione dell'apparecchio*

M.Development	I responsabili dello sviluppo della VU devono garantire che l'attribuzione delle responsabilità durante lo sviluppo sia tale da salvaguardare la sicurezza IT
M.Manufacturing	I fabbricanti delle VU devono garantire che l'attribuzione delle responsabilità durante la fabbricazione sia tale da salvaguardare la sicurezza IT e che durante il processo di fabbricazione la VU sia protetta contro attacchi fisici che possono compromettere la sicurezza IT

3.6.2. *Consegna e attivazione dell'apparecchio*

M.Delivery	I fabbricanti di VU, i costruttori di veicoli e i montatori o le officine devono garantire che la movimentazione delle VU non attivate avvenga in modo tale da salvaguardare la sicurezza della VU
M.Activation	Dopo il montaggio, i costruttori di veicoli e i montatori o le officine devono attivare la VU prima che il veicolo lasci i locali in cui è stato effettuato il montaggio

3.6.3. *Generazione e consegna dei dati di sicurezza*

M.Sec_Data_Generation	Agli algoritmi di generazione dei dati di sicurezza devono poter accedere soltanto persone autorizzate e fidate
M.Sec_Data_Transport	I dati di sicurezza devono essere generati, trasferiti ed inseriti nella VU in modo tale da preservarne la riservatezza e l'integrità appropriate

3.6.4. *Consegna delle carte*

M.Card_Availability	Le carte tachigrafiche devono essere rese disponibili e consegnate soltanto a persone autorizzate
M.Driver_Card_Uniqueness	I conducenti possono possedere **una** sola carta del conducente valida
M.Card_Traceability	Deve essere possibile risalire alla consegna della carta (liste bianche, liste nere) e si devono usare liste nere durante le verifiche della sicurezza

3.6.5. *Montaggio, calibratura e controllo dell'apparecchio*

M.Approved_Workshops	Il montaggio, la calibratura e la riparazione dell'apparecchio di controllo devono essere effettuati da officine o da montatori autorizzati e fidati
M.Regular_Inpections	L'apparecchio di controllo deve essere sottoposto a calibrature e controlli periodici
M.Faithful_Calibration	Durante la calibratura i montatori e le officine autorizzati devono inserire nell'apparecchio di controllo i parametri del veicolo corretti

3.6.6. *Funzionamento dell'apparecchio*

M.Faithful_Drivers	I conducenti devono rispettare le norme e tenere un comportamento responsabile (per es., usare la propria carta del conducente, selezionare correttamente l'attività in caso di selezione manuale, ecc.)

3.6.7. *Controllo dell'applicazione della legislazione*

M.Controls	I controlli dell'applicazione della legislazione devono essere eseguiti regolarmente e in modo casuale, e devono prevedere verifiche della sicurezza

3.6.8. *Aggiornamenti del software*

M.Software_Upgrade	Prima di poter essere installate in una VU, le nuove versioni del software devono ottenere la certificazione di sicurezza

4. **Funzioni di sicurezza**

4.1. ***Identificazione e autenticazione***

4.1.1. *Identificazione e autenticazione del sensore di movimento*

UIA_201 La VU deve essere in grado di stabilire, per ogni interazione, l'identità del sensore di movimento cui è collegata.

UIA_202 L'identità del sensore di movimento è costituita dal numero di omologazione del sensore e dal numero di serie del sensore.

UIA_203 La VU autentica il sensore di movimento cui è collegata:

— all'atto del collegamento del sensore di movimento,

— all'atto di ogni calibratura dell'apparecchio di controllo,

— all'atto del ripristino dell'alimentazione.

L'autenticazione è reciproca ed è attivata dalla VU.

UIA_204 La VU deve reidentificare e riautenticare periodicamente (TBD dal fabbricante, ma più di una volta all'ora) il sensore di movimento cui è collegata e garantire che il sensore di movimento identificato durante l'ultima calibratura dell'apparecchio di controllo non sia cambiato.

UIA_205 La VU rileva ed impedisce l'uso di dati di autenticazione copiati e riprodotti.

UIA_206 Dopo aver rilevato (TBD dal fabbricante, ma non più di 20) tentativi consecutivi falliti di autenticazione e/o dopo aver rilevato un cambiamento non autorizzato (cioè non durante una calibratura dell'apparecchio di controllo) dell'identità del sensore di movimento, la SEF:

— genera una registrazione di verifica dell'anomalia,

— avvisa l'utente,

— continua ad accettare ed utilizzare i dati di movimento non sicuri inviati dal sensore di movimento.

4.1.2. *Identificazione e autenticazione dell'utente*

UIA_207 La VU deve verificare costantemente e in modo selettivo l'identità di due utenti, controllando le carte tachigrafiche inserite rispettivamente nella sede (slot) "conducente" e nella sede (slot) "secondo conducente" dell'apparecchio di controllo.

UIA_208 L'identità dell'utente è costituita da:

— un gruppo utente:

  — CONDUCENTE (carta del conducente),

  — AGENTE INCARICATO DEL CONTROLLO (carta di controllo),

  — OFFICINA (carta dell'officina),

  — IMPRESA (carta dell'azienda),

  — NON NOTO (carta non inserita),

— una ID utente, composta di:

  — codice dello Stato membro che ha rilasciato la carta e numero della carta,

  — NON NOTO se il gruppo di utenti è NON NOTO.

Le identità NON NOTE possono essere implicitamente o esplicitamente note.

UIA_209 La VU provvede all'autenticazione degli utenti all'atto dell'inserimento della carta.

UIA_210 La VU provvede alla riautenticazione degli utenti:

— all'atto del ripristino dell'alimentazione,

— periodicamente o in seguito ad anomalie specifiche (TBD dal fabbricante, ma più di una volta al giorno).

UIA_211 L'autenticazione è eseguita comprovando che la carta inserita è una carta tachigrafica valida, in possesso di dati di sicurezza che solo il sistema può attribuire. L'autenticazione è reciproca ed è attivata dalla VU.

UIA_212 Inoltre, le officine devono essere autenticate positivamente mediante un controllo del PIN. La lunghezza dei PIN è di almeno 4 caratteri.

Nota: Nel caso in cui il PIN sia trasferito alla VU da un apparecchio esterno collocato in prossimità della VU, non è necessario proteggere la riservatezza del PIN durante il trasferimento.

UIA_213 La VU rileva ed impedisce l'uso di dati di autenticazione copiati e riprodotti.

UIA_214 Dopo aver rilevato 5 tentativi consecutivi falliti di autenticazione, la SEF:

— genera una registrazione di verifica dell'anomalia,

— avvisa l'utente,

— considera l'utente come NON NOTO, e la carta come non valida (definizione z) e requisito 007).

4.1.3. *Identificazione e autenticazione di un'impresa con collegamento remoto*

La possibilità di collegamento remoto di un'impresa è facoltativa. Il presente punto si applica quindi solo nel caso in cui tale funzione sia prevista.

UIA_215 Per ogni interazione con un'impresa con collegamento remoto, la VU deve essere in grado di stabilire l'identità dell'impresa.

UIA_216 L'identità dell'impresa con collegamento remoto è costituita dal codice dello Stato membro che ha rilasciato la carta dell'azienda e dal numero della carta dell'azienda.

UIA_217 La VU deve autenticare correttamente l'impresa con collegamento remoto prima di consentire l'esportazione di dati verso tale impresa.

UIA_218 L'autenticazione viene effettuata verificando che l'impresa sia in possesso di una carta dell'azienda in corso di validità, contenente dati di sicurezza che solo il sistema può distribuire.

UIA_219 La VU rileva e impedisce l'uso di dati di autenticazione copiati e riprodotti.

UIA_220 Dopo il rilevamento di 5 tentativi consecutivi falliti di autenticazione, la VU:

— avvisa l'impresa con collegamento remoto.

4.1.4. *Identificazione e autenticazione di dispositivi di gestione*

I fabbricanti di VU possono prevedere dispositivi dedicati per introdurre ulteriori funzioni di gestione della VU (per es., aggiornamenti del software, ricaricamento dei dati di sicurezza, ecc.). Il presente punto si applica quindi solo nel caso in cui siano previste tali funzioni.

UIA_221 Per ogni interazione con un dispositivo di gestione, la VU deve essere in grado di stabilire l'identità del dispositivo.

UIA_222 Prima di consentire ulteriori interazioni, la VU autentica correttamente il dispositivo di gestione.

UIA_223 La VU rileva e impedisce l'uso di dati di autenticazione copiati e riprodotti.

4.2. ***Controllo dell'accesso***

I controlli dell'accesso garantiscono che le informazioni vengano lette, create o modificate nel TOE soltanto da persone autorizzate.

Va rilevato che i dati dell'utente registrati dalla VU, sebbene presentino aspetti sensibili riguardanti la riservatezza o i segreti commerciali, non sono di natura riservata. Pertanto, i requisiti funzionali relativi ai diritti di accesso ai dati (requisito 011) non formano oggetto di una funzione di sicurezza.

4.2.1. *Strategia di controllo dell'accesso*

ACC_201 La VU gestisce e verifica i diritti di controllo dell'accesso alle funzioni e ai dati.

4.2.2. *Diritti di accesso alle funzioni*

ACC_202 La VU applica le regole riguardanti la selezione della modalità di funzionamento (requisiti da 006 a 009).

ACC_203 La VU utilizza la modalità di funzionamento per applicare le regole riguardanti il controllo dell'accesso alle funzioni (requisito 010).

4.2.3. *Diritti di accesso ai dati*

ACC_204 La VU applica le regole riguardanti l'accesso alla scrittura dei dati di identificazione della VU (requisito 076).

ACC_205 La VU applica le regole di accesso alla scrittura dei dati di identificazione del sensore di movimento cui è accoppiata (requisiti 079 e 155).

ACC_206 Dopo l'attivazione della VU, la VU garantisce che i dati di calibratura si possano inserire e memorizzare nella memoria di dati della VU solo nel modo calibratura (requisiti 154 e 156).

ACC_207 Dopo l'attivazione della VU, la VU applica le regole di accesso alla scrittura e alla cancellazione dei dati di calibratura (requisito 097).

ACC_208 Dopo l'attivazione della VU, la VU garantisce che le regolazioni dell'ora si possano inserire e memorizzare nella memoria della VU solo nel modo calibratura. (Questo requisito non si applica a piccole regolazioni dell'ora consentite dai requisiti 157 e 158).

ACC_209 Dopo l'attivazione della VU, la VU applica le regole di accesso alla scrittura e alla cancellazione dei dati di regolazione dell'ora (requisito 100).

ACC_210 La VU applica i diritti appropriati di accesso alla lettura e scrittura dei dati di sicurezza (requisito 080).

4.2.4. *Struttura dei file e condizioni di accesso*

ACC_211 La struttura dei file delle applicazioni e dei file di dati e le condizioni di accesso vengono create durante la fabbricazione e quindi bloccate contro eventuali modifiche o cancellazioni future.

4.3. ***Responsabilità***

ACT_201 La VU garantisce che le attività siano correttamente imputate ai conducenti (requisiti 081, 084, 087, 105a, 105b, 109 e 109a).

ACT_202 La VU conserva dati di identificazione permanenti (requisito 075).

ACT_203 La VU garantisce che le attività siano correttamente imputate alle officine (requisiti 098, 101 e 109).

ACT_204 La VU garantisce che le attività siano correttamente imputate agli agenti incaricati dei controlli (requisiti 102, 103 e 109).

ACT_205 La VU registra i dati dell'odometro (requisito 090) e i dati precisi sulla velocità (requisito 093).

ACT_206 La VU garantisce che i dati dell'utente di cui ai requisiti da 081 a 093 e da 102 a 105b compresi non vengano modificati in seguito alla registrazione, eccetto quando diventano i dati memorizzati meno recenti da sostituire con dati nuovi.

ACT_207 La VU garantisce che i dati già memorizzati in una carta tachigrafica (requisiti 109 e 109a) non vengano modificati dalla VU stessa, eccetto per sostituire i dati meno recenti con dati nuovi (requisito 110) o nel caso descritto nella nota al punto 2.1 dell'appendice 1.

4.4. ***Verifica***

Le funzioni di verifica sono richieste solo per le anomalie che possono indicare una manipolazione o un tentativo di violazione della sicurezza. Non sono richieste per il normale esercizio dei diritti, anche se riguardanti la sicurezza.

AUD_201 Per le anomalie che compromettono la sua sicurezza, la VU registra tali anomalie con i relativi dati (requisiti 094, 096 e 109).

AUD_202 Le anomalie che pregiudicano la sicurezza della VU sono le seguenti:

— tentativi di violazione della sicurezza:

  — mancata autenticazione del sensore di movimento,

  — mancata autenticazione della carta tachigrafica,

  — cambiamento non autorizzato del sensore di movimento,

  — errore di integrità nell'immissione dei dati della carta,

  — errore di integrità dei dati dell'utente memorizzati,

  — errore nel trasferimento interno di dati,

  — apertura non autorizzata dell'involucro,

  — sabotaggio di elementi hardware,

— chiusura errata dell'ultima sessione della carta,

— anomalia relativa ad errore dei dati di movimento,

— anomalia relativa ad interruzione dell'alimentazione,

— guasto all'interno della VU.

AUD_203 La VU applica le regole di memorizzazione delle registrazioni di verifica (requisiti 094 e 096).

AUD_204 La VU memorizza le registrazioni di verifica generate dal sensore di movimento nella sua memoria di dati.

AUD_205 Si devono poter stampare, visualizzare e trasferire le registrazioni di verifica.

4.5. ***Riutilizzo degli oggetti***

REU_201 La VU garantisce la possibilità di riutilizzare gli oggetti memorizzati in modo temporaneo, senza che ciò comporti un flusso inammissibile di informazioni.

4.6. ***Accuratezza***

4.6.1. *Strategie di controllo del flusso di informazioni*

ACR_201 La VU garantisce che i dati dell'utente relativi ai requisiti 081, 084, 087, 090, 093, 102, 104, 105, 105a e 109 possano essere elaborati solo dalle fonti di immissione corrette:

— dati di movimento del veicolo,

— orologio in tempo reale della VU,

— parametri di calibratura dell'apparecchio di controllo,

— carte tachigrafiche,

— immissioni dell'utente.

ACR_201a La VU garantisce che i dati dell'utente relativi al requisito 109a possano essere inseriti solo per il periodo compreso tra l'ultima estrazione della carta e l'inserimento in atto (requisito 050a).

4.6.2. *Trasferimento interno di dati*

I requisiti del presente paragrafo si applicano solo se la VU utilizza elementi fisicamente separati.

ACR_202 Se i dati vengono trasferiti tra elementi fisicamente separati della VU, tali dati devono essere protetti contro eventuali modifiche.

ACR_203 Al rilevamento di un errore di trasferimento di dati durante un trasferimento interno, la trasmissione viene ripetuta e la SEF genera una registrazione di verifica dell'anomalia.

4.6.3. *Integrità dei dati memorizzati*

ACR_204 La VU controlla i dati dell'utente memorizzati nella memoria di dati per verificare eventuali errori di integrità.

ACR_205 Al rilevamento di un errore di integrità dei dati dell'utente memorizzati, la SEF genera una registrazione di verifica.

4.7. ***Affidabilità del servizio***

4.7.1. *Prove*

RLB_201 Tutti i comandi, le azioni o i punti di prova specifici per le esigenze di prova nella fase di fabbricazione della VU vengono disabilitati o eliminati prima dell'attivazione della VU. Non deve essere possibile ripristinarli per impiego successivo.

RLB_202 Durante l'avviamento iniziale e durante il funzionamento normale la VU esegue prove automatiche per verificare il suo funzionamento corretto. Le prove automatiche della VU comprendono una verifica dell'integrità dei dati di sicurezza e una verifica dell'integrità del codice eseguibile memorizzato (se non in ROM).

RLB_203 Al rilevamento di un guasto interno durante la prova automatica, la SEF:

— genera una registrazione di verifica (eccetto per il modo calibratura) (guasto all'interno della VU),

— preserva l'integrità dei dati memorizzati.

4.7.2. *Software*

RLB_204 In seguito all'attivazione della VU, deve essere impedita l'analisi e la ricerca e correzione di errori del software sul campo.

RLB_205 Non devono essere accettati input da fonti esterne come codici eseguibili.

4.7.3. *Protezione fisica*

RLB_206 Se il modello della VU ne consente l'apertura, la VU deve rilevare ogni apertura dell'involucro, eccetto per il modo calibratura, anche in assenza di alimentazione esterna per un minimo di 6 mesi. In tal caso, la SEF genera una registrazione di verifica. (È ammesso che la registrazione di verifica sia generata e memorizzata in seguito al ripristino dell'alimentazione.)

Se il modello della VU non ne consente l'apertura, esso deve essere tale da consentire di individuare facilmente eventuali tentativi di manomissione (per es., mediante controllo visivo).

RLB_207 Dopo l'attivazione, la VU rileva i sabotaggi specificati (TBD dal fabbricante) degli elementi hardware.

RLB_208 Nel caso sopra descritto, la SEF genera una registrazione di verifica e la VU: (TBD dal fabbricante).

4.7.4. *Interruzioni dell'alimentazione*

RLB_209 La VU rileva le variazioni dell'alimentazione rispetto ai valori specificati, comprese le interruzioni.

RLB_210 Nel caso suindicato, la SEF:

— genera una registrazione di verifica (eccetto per il modo calibratura),

— preserva la condizione di sicurezza della VU,

— salvaguarda le funzioni di sicurezza relative a componenti o processi ancora in funzione,

— preserva l'integrità dei dati memorizzati.

4.7.5. *Condizioni di azzeramento*

RLB_211 In caso di interruzione dell'alimentazione, o qualora un'operazione venga interrotta prima del completamento, o in qualsiasi altra condizione di azzeramento, la VU deve essere completamente azzerata.

4.7.6. *Disponibilità dei dati*

RLB_212 La VU garantisce la possibilità di accedere alle risorse quando necessario e che le risorse non siano richieste né trattenute senza necessità.

RLB_213 La VU deve garantire che le carte non possano essere estratte prima della memorizzazione dei dati pertinenti nelle carte stesse (requisiti 015 e 016).

RLB_214 Nel caso suindicato, la SEF genera una registrazione di verifica dell'anomalia.

4.7.7. *Applicazioni multiple*

RLB_215 Se la VU prevede applicazioni diverse da quella tachigrafica, tutte le applicazioni devono essere fisicamente e/o logicamente separate le une dalle altre. Tali applicazioni non devono condividere dati di sicurezza. In ogni dato momento può essere attivo un solo compito.

4.8. ***Scambio di dati***

Il presente punto riguarda lo scambio di dati tra la VU e i dispositivi ad essa collegati.

4.8.1. *Scambio di dati con il sensore di movimento*

DEX_201 La VU verifica l'integrità e l'autenticità dei dati di movimento importati dal sensore di movimento.

DEX_202 Al rilevamento di un errore di integrità o di autenticità dei dati di movimento, la SEF:

— genera una registrazione di verifica,

— continua ad usare i dati importati.

4.8.2. *Scambio di dati con le carte tachigrafiche*

DEX_203 La VU verifica l'integrità e l'autenticità dei dati importati dalle carte tachigrafiche.

DEX_204 Al rilevamento di un errore di integrità o di autenticità dei dati della carta, la VU:

— genera una registrazione di verifica,

— non usa i dati.

DEX_205 La VU esporta i dati verso le carte tachigrafiche intelligenti con i relativi attributi di sicurezza, in modo da consentire alle carte di verificarne l'integrità e l'autenticità.

4.8.3. *Scambio di dati con dispositivi di memorizzazione esterni (funzione di trasferimento)*

DEX_206 La VU genera una prova d'origine per i dati trasferiti ad un dispositivo esterno.

DEX_207 La VU fornisce al destinatario la possibilità di verificare la prova d'origine dei dati trasferiti.

DEX_208 La VU trasferisce i dati al dispositivo di memorizzazione esterno con i relativi attributi di sicurezza, in modo da consentire la verifica dell'integrità e dell'autenticità dei dati trasferiti.

4.9. ***Crittografia***

I requisiti del presente punto si applicano solo se necessario, a seconda dei meccanismi di sicurezza utilizzati e delle soluzioni adottate dal fabbricante.

CSP_201 Qualsiasi operazione crittografica effettuata dalla VU si deve basare su un algoritmo specificato e su dimensioni di chiavi specificate.

CSP_202 Se la VU genera chiavi crittografiche, tale operazione si deve basare su algoritmi di generazione di chiavi crittografiche specificati e su dimensioni di chiavi crittografiche specificate.

CSP_203 Se la VU distribuisce chiavi crittografiche, tale operazione si deve basare su metodi di distribuzione di chiavi specificati.

CSP_204 Se la VU accede a chiavi crittografiche, tale operazione si deve basare su metodi di accesso a chiavi crittografiche specificati.

CSP_205 Se la VU distrugge chiavi crittografiche, tale operazione si deve basare su metodi di distruzione di chiavi crittografiche specificati.

5. **Definizione dei meccanismi di sicurezza**

I meccanismi di sicurezza prescritti sono specificati all'appendice 11.

Tutti gli altri meccanismi di sicurezza sono definiti dai fabbricanti.

6. **Robustezza minima dei meccanismi di sicurezza**

La robustezza minima dei meccanismi di sicurezza dell'unità elettronica di bordo è Elevata, secondo quanto stabilito nella norma ITSEC.

7. **Grado di garanzia**

Il grado di garanzia che deve fornire l'unità elettronica di bordo è il livello ITSEC E3, secondo quanto stabilito nella norma ITSEC.

8. **Fondamento logico**

Le matrici riportate di seguito forniscono una spiegazione logica delle SEF, indicando:

— quale SEF o misura neutralizza la minaccia indicata,

— quale SEF realizza l'obiettivo di sicurezza IT indicato.

	Minacce																		Obiettivi IT								
	T.Access	T.Identification	T.Faults	T.Tests	T.Design	T.Calibration_Parameters	T.Card_Data_Exchange	T.Clock	T.Environment	T.Fake_Device	T.Hardware	T.Motion_Data	T.Non_Activated	T.Output_Data	T.Power_Supply		T.Security_Data	T.Software	T.Stored_Data	O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secured_Data_Exchange
Mezzi fisici, procedure e personale																												
Sviluppo			x	x	x																							
Fabbricazione				x	x																							
Consegna													x															
Attivazione	x												x															
Generazione dati sicurezza																	x											
Trasmissione dati sicurezza																	x											
Disponibilità carta		x																										
Una carta conducente		x																										
Rintracciabilità carta		x																										
Officine autorizzate						x		x																				
Calibratura regolare di controllo						x		x				x	x			x												
Officine fidate						x		x																				
Conducenti fidati		x																										
Controlli applicazione legislatura		x				x		x	x		x		x		x			x	x									
Aggiornamento software																			x									
Funzioni di sicurezza																												
Identificazione e autenticazione																												
UIA_201 Identificazione sensore										x		x											x					x
UIA_202 Identità sensore										x		x											x					x
UIA_203 Autenticazione sensore										x		x											x					x
UIA_204 Reidentificazione e riautenticazione sensore										x		x											x					x
UIA_205 Autenticazione impossibile										x		x											x					
UIA_206 Autenticazione fallita										x		x										x					x	
UIA_207 Identificazione utente	x	x								x										x			x					x
UIA_208 Identità utente	x	x								x										x			x					x
UIA_209 Autenticazione utente	x	x								x										x			x					x
UIA_210 Riautenticazione utente	x	x								x										x			x					x
UIA_211 Misure di autenticazione	x	x								x										x			x					
UIA_212 Controlli PIN	x	x				x		x												x			x					
UIA_213 Autenticazione impossibile	x	x								x										x			x					

	Minacce																				Obiettivi IT									
	T.Access	T.Identification	T.Faults	T.Tests	T.Design	T.Calibration_Parameters	T.Card_Data_Exchange	T.Clock	T.Environment	T.Fake_Device	T.Hardware	T.Motion_Data	T.Non_Activated	T.Output _Data	T.Power_Supply		T.Security_Data	T.Software	T.Stored_Data		O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secured_Data_Exchange	
UIA_214 Autenticazione fallita	x	x								x													x							
UIA_215 Identificazione utente remoto	x	x																			x			x					x	
UIA_216 Identità utente remoto	x	x																			x			x						
UIA_217 Autenticazione utente remoto	x	x																			x			x					x	
UIA_218 Misure di autenticazione	x	x																			x			x						
UIA_219 Autenticazione impossibile	x	x																			x			x						
UIA_220 Autenticazione fallita	x	x																												
UIA_221 Identificazione dispositivo di gestione	x	x																			x			x						
UIA_222 Autenticazione dispositivo di gestione	x	x																			x			x						
UIA_223 Autenticazione impossibile	x	x																			x			x						
Controllo dell'accesso																														
ACC_201 Strategia di controllo dell'accesso	x					x		x									x		x		x									
ACC_202 Diritti di accesso alle funzioni	x					x		x													x									
ACC_203 Diritti di accesso alle funzioni	x					x		x													x									
ACC_204 ID VU																			x		x									
ACC_205 ID sensore collegato										x									x		x									
ACC_206 Dati calibratura	x					x													x		x									
ACC_207 Dati calibratura						x													x		x									
ACC_208 Dati regolazione ora								x											x		x									
ACC_209 Dati regolazione ora								x											x		x									
ACC_210 Dati sicurezza																	x		x		x									
ACC_211 Struttura file e condizioni d'accesso	x					x											x		x		x									
Responsabilità																														
ACT_201 Responsabilità conducenti																						x								
ACT_202 Dati ID VU																						x	x							
ACT_203 Responsabilità officine																						x								
ACT_204 Responsabilità agenti di controllo																						x								
ACT_205 Responsabilità movimento veicolo																						x								
ACT_206 Modifica dati responsabilità																			x						x			x		
ACT_207 Modifica dati responsabilità																			x						x			x		

	Minacce																		Obiettivi IT							
	T.Access	T.Identification	T.Faults	T.Tests	T.Design	T.Calibration_Parameters	T.Card_Data_Exchange	T.Clock	T.Environment	T.Fake_Device	T.Hardware	T.Motion_Data	T.Non_Activated	T.Output _Data	T.Power_Supply		T.Security_Data	T.Software	T.Stored_Data	O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secured_Data_Exchange
Verifica																												
AUD_201 Registrazioni di verifica																						x						
AUD_202 Elenco verifica anomalie	x						x				x	x		x	x				x			x						
AUD_203 Regole di memorizzazione registrazioni di verifica																						x						
AUD_204 Registrazioni di verifica sensore																						x						
AUD_205 Strumenti di verifica																						x						
Riutilizzo																												
REU_201 Riutilizzo																	x									x	x	
Accuratezza																												
ACR_201 Strategia di controllo del flusso di informazioni						x			x		x															x	x	
ACR_202 Trasferimenti interni														x											x	x	x	
ACR_203 Trasferimenti interni														x								x						
ACR_204 Integrità dati memorizzati																			x				x				x	
ACR_205 Integrità dati memorizzati																			x			x						
Affidabilità																												
RLB_201 Prove fabbricazione				x	x																						x	
RLB_202 Prove automatiche			x								x				x			x									x	
RLB_203 Prove automatiche											x				x			x				x						
RLB_204 Analisi software					x													x									x	
RLB_205 Input software																		x						x	x	x		
RLB_206 Apertura involucro					x				x		x			x			x	x	x					x		x		
RLB_207 Sabotaggio hardware											x																x	
RLB_208 Sabotaggio hardware											x											x						
RLB_209 Interruzioni alimentazione															x												x	
RLB_210 Interruzioni alimentazione															x							x						
RLB_211 Azzeramento			x																								x	
RLB_212 Disponibilità dati																										x	x	
RLB_213 Estrazione carta																											x	
RLB_214 Chiusura errata sessione carta																							x					
RLB_215 Applicazioni multiple																											x	
Scambio di dati																												
DEX_201 Importazione sicura dati di movimento												x																x
DEX_202 Importazione sicura dati di movimento												x							x									
DEX_203 Importazione sicura dati carta							x																					x

	Minacce																			Obiettivi IT								
	T.Access	T.Identification	T.Faults	T.Tests	T.Design	T.Calibration_Parameters	T.Card_Data_Exchange	T.Clock	T.Environment	T.Fake_Device	T.Hardware	T.Motion_Data	T.Non_Activated	T.Output _Data	T.Power_Supply		T.Security_Data	T.Software	T.Stored_Data	O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secured_Data_Exchange
DEX_204 Importazione sicura dati carta							x															x						
DEX_205 Esportazione sicura dati verso carta							x																					x
DEX_206 Prova d'origine																								x	x			
DEX_207 Prova d'origine																								x	x			
DEX_208 Esportazione sicura verso dispositivi esterni																								x	x			
Crittografia																												
CSP_201 Algoritmi																											x	x
CSP_202 Generazione chiavi																											x	x
CSP_203 Distribuzione chiavi																											x	x
CSP_204 Accesso a chiavi																											x	x
CSP_205 Distruzione chiavi																											x	x

OBIETTIVI GENERALI DI SICUREZZA PER LE CARTE TACHIGRAFICHE

1. **Introduzione**

Il presente documento contiene una descrizione della carta tachigrafica, delle minacce che deve essere in grado di neutralizzare e degli obiettivi di sicurezza che deve conseguire. Specifica le funzioni di sicurezza richieste e indica la robustezza minima dichiarata dei meccanismi di sicurezza e il grado di garanzia richiesto per lo sviluppo e la valutazione.

I requisiti cui fa riferimento il presente documento sono quelli indicati nel corpo dell'allegato I B. A fini di chiarezza, sono talvolta presenti ripetizioni tra i requisiti di cui all'allegato I B e quelli degli obiettivi di sicurezza. In caso di ambiguità tra un requisito di sicurezza e un requisito di cui all'allegato I B cui il requisito di sicurezza si riferisce, fa fede il requisito indicato nel corpo dell'allegato I B.

I requisiti di cui all'allegato I B cui non fanno riferimento gli obiettivi di sicurezza non sono oggetto di funzioni di sicurezza.

Una carta tachigrafica è una carta intelligente standard che prevede un'applicazione tachigrafica dedicata ed è conforme ai requisiti aggiornati di sicurezza funzionale e di garanzia applicabili alle carte intelligenti. Questo obiettivo di sicurezza comprende quindi solo i requisiti di sicurezza supplementari richiesti dall'applicazione tachigrafica.

A fini di rintracciabilità nella documentazione relativa allo sviluppo e alla valutazione, alle specifiche di ogni minaccia, obiettivo, procedura e funzione di sicurezza è stata assegnata un'apposita etichetta.

2. **Acronimi, definizioni e riferimenti normativi**

2.1. ***Acronimi***

IC	Integrated circuit — Circuito integrato (Componente elettronico destinato ad eseguire funzioni di elaborazione e/o memorizzazione)
OS	Operating system — Sistema operativo
PIN	Personal identification number — Numero di identificazione personale
ROM	Read only memory — Memoria a sola lettura
SFP	Security functions policy — Strategie in materia di funzioni di sicurezza
TBD	To be defined — Da definire
TOE	Target of evaluation — Obiettivo di valutazione
TSF	TOE security function — Funzione di sicurezza del TOE
VU	Vehicle unit — Unità elettronica di bordo

2.2. ***Definizioni***

Tachigrafo digitale	L'apparecchio di controllo
Dati sensibili	I dati memorizzati dalla carta tachigrafica che richiedono una protezione dell'integrità, della riservatezza e contro le modifiche non autorizzate (se applicabile per i dati di sicurezza). I dati sensibili comprendono i dati di sicurezza e i dati dell'utente
Dati di sicurezza	I dati specifici necessari per l'esecuzione delle funzioni di sicurezza (per es., chiavi crittografiche)
Sistema	Apparecchiature, persone o organizzazioni interessate in qualsiasi modo all'apparecchio di controllo
Utente	Qualsiasi entità (persona o entità IT esterna) estranea al TOE che interagisce con il TOE (eccetto quando usato nell'espressione “dati dell'utente”)

Dati dell'utente	Dati sensibili memorizzati nella carta tachigrafica, diversi dai dati di sicurezza. I dati dell'utente comprendono i dati di identificazione e i dati relativi alle attività
Dati di identificazione	I dati di identificazione comprendono i dati di identificazione della carta e i dati di identificazione del titolare della carta
Dati di identificazione della carta	Dati dell'utente relativi all'identificazione della carta definiti dai requisiti 190, 191, 192, 194, 215, 231 e 235
Dati di identificazione del titolare della carta	Dati dell'utente relativi all'identificazione del titolare della carta definiti dai requisiti 195, 196, 216, 232 e 236
Dati relativi alle attività	I dati relativi alle attività comprendono i dati relativi alle attività del titolare della carta, i dati relativi ad anomalie e guasti e i dati relativi alle attività di controllo
Dati relativi alle attività del titolare della carta	Dati dell'utente relativi alle attività eseguite dal titolare della carta definiti dai requisiti 197, 199, 202, 212, 212a, 217, 219, 221, 226, 227, 229, 230a, 233 e 237
Dati relativi ad anomalie e guasti	Dati dell'utente relativi alle anomalie o ai guasti definiti dai requisiti 204, 205, 207, 208 e 223
Dati relativi alle attività di controllo	Dati dell'utente relativi ai controlli dell'applicazione della legislazione definiti dai requisiti 210 e 225

2.3. ***Riferimenti normativi***

ITSEC	ITSEC — Criteri per la valutazione della sicurezza delle tecnologie dell'informazione, 1991
IC PP	Smart Card Integrated Circuit Protection Profile — version 2.0 — issue September 1998. Registered at French certification body under the number PP/9806. (Profilo di protezione del circuito integrato delle carte intelligenti — Versione 2.0 — settembre 1998. Registrato presso l'organismo francese di certificazione con il numero PP/9806)
ES PP	Smart Card Integrated Circuit With Embedded Software Protection Profile — version 2.0 — issue June 1991. Registered at French certification body under the number PP/9911. (Circuito integrato delle carte intelligenti con protezione software incorporata — Versione 2.0 — giugno 1999. Registrato presso l'organismo francese di certificazione con il numero PP/9911)

3. **Descrizione del prodotto**

3.1. ***Descrizione della carta tachigrafica e metodo d'impiego***

Una carta tachigrafica è una carta intelligente, descritta nelle norme IC PP e ES PP, che prevede un'applicazione destinata all'impiego con l'apparecchio di controllo.

La carta tachigrafica ha le seguenti funzioni di base:

— memorizzare i dati di identificazione della carta e del titolare della carta. Tali dati sono usati dall'unità elettronica di bordo per identificare il titolare della carta, fornire i corrispondenti diritti di accesso alle funzioni e ai dati e garantire la responsabilità delle attività al titolare della carta corrispondente,

— memorizzare i dati relativi alle attività del titolare della carta, i dati relativi ad anomalie e guasti e i dati relativi alle attività di controllo riguardanti il titolare della carta.

Una carta tachigrafica è quindi destinata all'impiego in un'interfaccia della carta di una unità elettronica di bordo. Può anche essere usata in qualsiasi lettore di carte (per es., un personal computer) che deve avere pieno diritto di accesso alla lettura di qualsiasi dato dell'utente.

Durante la fase finale d'impiego del ciclo di vita di una carta tachigrafica (fase 7 del ciclo di vita descritto in ES PP), soltanto le unità elettroniche di bordo possono scrivere i dati dell'utente nella carta.

I requisiti funzionali per una carta tachigrafica sono specificati nel corpo dell'allegato I B e nell'appendice 2.

3.2. ***Ciclo di vita della carta tachigrafica***

Il ciclo di vita della carta tachigrafica è conforme al ciclo di vita delle carte intelligenti previsto dalla norma ES PP.

3.3. ***Minacce***

Oltre alle minacce generali concernenti le carte intelligenti elencati nelle norme ES PP e IC PP, la carta tachigrafica può essere esposta alle minacce descritte di seguito.

3.3.1. *Finalità*

La finalità degli attacchi consiste nel modificare i dati dell'utente memorizzati nel TOE.

T.Ident_Data	Una modifica riuscita dei dati di identificazione conservati nel TOE (per es., il tipo di carta, la data di scadenza della carta o i dati di identificazione del titolare) consentirebbe un uso fraudolento del TOE e costituirebbe una grave minaccia per l'obiettivo di sicurezza generale del sistema.
T.Activity_Data	Una modifica riuscita dei dati relativi alle attività memorizzati nel TOE costituirebbe una minaccia per la sicurezza del TOE.
T.Data_Exchange	Una modifica riuscita dei dati relativi alle attività (aggiunta, cancellazione, modifica) durante l'importazione o l'esportazione costituirebbe una minaccia per la sicurezza del TOE.

3.3.2. *Percorsi di attacco*

Le proprietà del TOE possono essere compromesse:

— tentando di ottenere illecitamente informazioni sul modello dei prodotti hardware e software del TOE, in particolare sulle funzioni di sicurezza o sui dati di sicurezza. Le informazioni illecite si possono ottenere mediante attacchi al materiale di progettazione o di fabbricazione (furto, corruzione, ecc.) o mediante esame diretto del TOE (ispezione fisica, analisi inferenziale, ecc.);

— sfruttando le debolezze di progetto o di realizzazione del TOE (difetti degli elementi hardware, errori nel software, errori di trasmissione, errori indotti nel TOE da stress ambientale, debolezze delle funzioni di sicurezza quali le procedure di autenticazione, il controllo dell'accesso ai dati, le operazioni crittografiche, ecc.);

— modificando il TOE o le sue funzioni di sicurezza con attacchi di natura fisica, elettrica o logica o con una combinazione degli stessi.

3.4. ***Obiettivi di sicurezza***

L'obiettivo di sicurezza principale dell'intero sistema a tachigrafo digitale è il seguente:

O.Main	I dati soggetti al controllo delle autorità competenti devono essere disponibili e rispecchiare interamente ed accuratamente le attività dei conducenti e dei veicoli sottoposti al controllo per quanto riguarda i periodi di guida, lavoro, disponibilità e riposo e la velocità del veicolo.

Gli obiettivi di sicurezza principali del TOE, che contribuiscono a realizzare il suddetto obiettivo di sicurezza principale, sono quindi:

O.Card_Identification_Data	Il TOE deve preservare i dati di identificazione della carta e i dati di identificazione del titolare della carta memorizzati durante il processo di personalizzazione della carta.
O.Card_Activity_Storage	Il TOE deve preservare i dati dell'utente memorizzati nella carta dalle unità elettroniche di bordo.

3.5. ***Obiettivi di sicurezza relativi alle tecnologie dell'informazione (IT)***

Oltre agli obiettivi di sicurezza generali per le carte intelligenti elencati nelle norme ES PP e IC PP, gli obiettivi di sicurezza specifici IT del TOE, che contribuiscono a realizzare i suoi obiettivi di sicurezza generali durante la fase di impiego finale del suo ciclo di vita sono i seguenti:

O.Data_Access	Il TOE deve limitare i diritti di accesso alla scrittura dei dati dell'utente alle unità elettroniche di bordo autenticate.
O.Secure_Communications	Il TOE deve essere in grado di utilizzare protocolli e procedure di comunicazione sicuri tra la carta e l'interfaccia della carta quando richiesto dall'applicazione.

3.6. ***Mezzi fisici, procedure e personale***

I requisiti fisici e relativi alle procedure o al personale che contribuiscono a garantire la sicurezza del TOE sono elencati nelle norme ES PP e IC PP (nei capitoli relativi agli obiettivi di sicurezza per l'ambiente).

4. **Funzioni di sicurezza**

Il presente paragrafo definisce alcune operazioni permesse, come l'assegnazione o la selezione di cui alla norma ES PP, e prevede requisiti funzionali supplementari per le SEF.

4.1. ***Conformità ai profili di protezione***

CPP_301 Il TOE deve essere conforme alla norma IC PP.

CPP_302 Il TOE deve essere conforme alla norma ES PP, come ulteriormente precisato.

4.2. ***Identificazione e autenticazione dell'utente***

La carta deve identificare l'entità in cui è inserita e saper rilevare se si tratta di una unità elettronica di bordo autenticata o meno. La carta può esportare qualsiasi dato dell'utente, indipendentemente dall'entità cui è collegata, fatta eccezione per la carta di controllo che può esportare i dati di identificazione del titolare della carta soltanto verso unità elettroniche di bordo autenticate (in modo che l'agente incaricato del controllo possa accertare che l'unità elettronica di bordo non sia contraffatta vedendo il proprio nome sul dispositivo di visualizzazione o sui documenti stampati).

4.2.1. *Identificazione dell'utente*

Assegnazione (FIA_UID.1.1) *Elenco delle azioni mediate da TSF*: nessuna.

Assegnazione (FIA_ATD.1.1) *Elenco degli attributi di sicurezza*:

— USER_GROUP: VEHICLE_UNIT, NON_VEHICLE_UNIT,

— USER_ID: Numero di immatricolazione del veicolo (VRN) e codice dello Stato membro di immatricolazione (USER_ID è noto solo per USER_GROUP = VEHICLE_UNIT).

4.2.2. *Autenticazione dell'utente*

Assegnazione (FIA_UAU.1.1) *Elenco delle azioni mediate da TSF*:

— Carte del conducente e dell'officina: esportazione dei dati dell'utente con attributi di sicurezza (funzione di trasferimento dati carta),

— Carta di controllo: esportazione dei dati dell'utente senza attributi di sicurezza eccetto per i dati di identificazione del titolare della carta.

UIA_301 L'autenticazione di una unità elettronica di bordo deve essere eseguita dimostrando che essa possiede dati di sicurezza che solo il sistema può distribuire.

Selezione (FIA_UAU.3.1 e FIA_UAU.3.2): impedire.

Assegnazione (FIA_UAU.4.1) *Meccanismo/i di autenticazione identificato/i*: qualsiasi meccanismo di autenticazione.

UIA_302 La carta dell'officina fornisce un meccanismo di autenticazione supplementare verificando un codice PIN. (Questo meccanismo è usato dall'unità elettronica di bordo per accertare l'identità del titolare della carta e non è destinato a proteggere il contenuto della carta dell'officina).

4.2.3. *Autenticazioni fallite*

Le seguenti assegnazioni descrivono il comportamento della carta ad ogni autenticazione fallita dell'utente.

Assegnazione (FIA_AFL.1.1) *Numero*: 1, *elenco delle anomalie relative all'autenticazione*: autenticazione di un'interfaccia della carta.

Assegnazione (FIA_AFL.1.2) *Elenco di azioni*:

— avvisa l'entità collegata,

— considera l'utente come NON_VEHICLE_UNIT.

Le assegnazioni seguenti descrivono il comportamento della carta in caso di guasto del meccanismo di autenticazione supplementare richiesto in UIA_302.

Assegnazione (FIA_AFL.1.1) *Numero*: 5, *elenco delle anomalie relative all'autenticazione*: controlli PIN (carta dell'officina).

Assegnazione (FIA_AFL.1.2) *Elenco di azioni*:

— avvisa l'entità collegata,

— blocca la procedura di controllo del PIN in modo che ogni tentativo successivo di controllo del PIN fallisca,

— deve essere in grado di indicare agli utenti successivi il motivo del blocco.

4.3. ***Controllo dell'accesso***

4.3.1. *Strategia di controllo dell'accesso*

Durante la fase finale d'impiego del suo ciclo di vita, la carta tachigrafica è soggetta ad un'unica strategia delle funzioni di sicurezza (SFP) per il controllo dell'accesso, denominata AC_SFP.

Assegnazione (FDP_ACC.2.1) *Controllo dell'accesso SFP*: AC_SFP.

4.3.2. *Funzioni di controllo dell'accesso*

Assegnazione (FDP_ACF.1.1) *SFP per il controllo dell'accesso*: AC_SFP.

Assegnazione (FDP_ACF.1.1) *Gruppo denominato di attributi di sicurezza*: USER_GROUP.

Assegnazione (FDP_ACF.1.2) *Strategie che disciplinano l'accesso tra soggetti controllati e oggetti controllati usando operazioni controllate su oggetti controllati*:

— GENERAL_READ: I dati dell'utente possono essere letti nel TOE da qualsiasi utente, eccetto per i dati di identificazione del titolare della carta che possono essere letti nelle carte di controllo solo da VEHICLE_UNIT.

— IDENTIF_WRITE: I dati di identificazione possono essere scritti solo una volta, prima del termine della fase 6 del ciclo di vita della carta. Nessun utente può scrivere o modificare i dati di identificazione durante la fase di impiego finale del ciclo di vita della carta.

— ACTIVITY_WRITE: I dati relativi alle attività possono essere scritti nel TOE solo da VEHICLE_UNIT.

— SOFT_UPGRADE: Nessun utente può aggiornare il software del TOE.

— FILE_STRUCTURE: La struttura dei file e le condizioni di accesso vengono create prima del termine della fase 6 del ciclo di vita del TOE e quindi bloccate per impedire eventuali modifiche o cancellazioni future da parte degli utenti.

4.4. ***Responsabilità***

ACT_301 Il TOE conserva dati di identificazione permanenti.

ACT_302 Deve essere presente un'indicazione della data e dell'ora della personalizzazione del TOE. Tale indicazione rimane inalterabile.

4.5. ***Verifica***

Il TOE deve controllare le anomalie che indicano una potenziale violazione della sua sicurezza.

Assegnazione (FAU_SAA.1.2) *Sottoinsieme di anomalie verificabili definite*:

— autenticazione fallita del titolare della carta (5 controlli consecutivi dei PIN falliti),

— errore della prova automatica,

— errore di integrità dei dati memorizzati,

— errore di integrità nell'inserimento di dati relativi alle attività.

4.6. ***Accuratezza***

4.6.1. *Integrità dei dati memorizzati*

Assegnazione (FDP_SDI.2.2) *Azione*: avvisare l'entità collegata.

4.6.2. *Autenticazione dei dati di base*

Assegnazione (FDP_DAU.1.1) *Elenco dei tipi di oggetti o informazioni*: dati di attività.

Assegnazione (FDP_DAU.1.2) *Elenco dei soggetti*: tutti.

4.7. ***Affidabilità del servizio***

4.7.1. *Prove*

Selezione (FPT_TST.1.1): durante l'avviamento iniziale, periodicamente durante il funzionamento normale.

Nota: per durante l'avviamento iniziale s'intende prima dell'esecuzione del codice (non necessariamente durante la procedura Answer To Reset).

RLB_301 Le prove automatiche del TOE comprendono la verifica dell'integrità di ogni codice software non memorizzato in ROM.

RLB_302 Al rilevamento di un errore della prova automatica la TSF avvisa l'entità collegata.

RLB_303 Al completamento delle prove OS, tutti i comandi e le azioni specifiche per le prove vengono disabilitati o eliminati. Si deve escludere la possibilità di ripristinare l'impiego di tali comandi e azioni. I comandi associati esclusivamente ad una condizione del ciclo di vita non devono essere accessibili in un'altra condizione.

4.7.2. *Software*

RLB_304 Deve essere impedita l'analisi, la ricerca e correzione di errori e la modifica del software del TOE sul campo.

RLB_305 Non devono essere accettati input da fonti esterne come codici eseguibili.

4.7.3. *Alimentazione*

RLB_306 Il TOE rimane in condizione di sicurezza durante l'interruzione o le variazioni di alimentazione.

4.7.4. *Condizioni di azzeramento*

RLB_307 In caso di interruzione dell'alimentazione (o di variazioni dell'alimentazione) del TOE o qualora un'operazione venga interrotta prima del completamento, o in qualsiasi altra condizione di azzeramento, il TOE deve essere completamente azzerato.

4.8. ***Scambio di dati***

4.8.1. *Scambio di dati con una unità elettronica di bordo*

DEX_301 Il TOE verifica l'integrità e l'autenticità dei dati importati da una unità elettronica di bordo.

DEX_302 Al rilevamento di un errore di integrità dei dati importati, il TOE:

— avvisa l'entità che invia i dati,

— non usa i dati.

DEX_303 Il TOE esporta i dati dell'utente verso l'unità elettronica di bordo con attributi di sicurezza associati, in modo da consentire all'unità elettronica di bordo di verificare l'integrità e l'autenticità dei dati ricevuti.

4.8.2. *Esportazione di dati non verso una unità elettronica di bordo (funzione di trasferimento)*

DEX_304 Il TOE deve essere in grado di generare una prova d'origine per i dati trasferiti ad un dispositivo esterno.

DEX_305 Il TOE deve essere in grado di fornire al destinatario la possibilità di verificare la prova d'origine dei dati trasferiti.

DEX_306 Il TOE deve essere in grado di trasferire i dati a un dispositivo di memorizzazione esterno con attributi di sicurezza associati, in modo da consentire la verifica dell'integrità dei dati trasferiti.

4.9. ***Crittografia***

CSP_301 Se la TSF genera chiavi crittografiche, tale operazione si deve basare su algoritmi di generazione di chiavi crittografiche specificati e su dimensioni di chiavi crittografiche specificate. Le chiavi generate in sessioni crittografiche hanno un numero limitato (TBD dal fabbricante e non superiore a 240) di usi possibili.

CSP_302 Se la TSF distribuisce chiavi crittografiche, tale operazione si deve basare su metodi di distribuzione di chiavi crittografiche specificati.

5. **Definizione dei meccanismi di sicurezza**

I meccanismi di sicurezza richiesti sono specificati nell'appendice 11.

Tutti gli altri meccanismi di sicurezza sono definiti dal fabbricante del TOE.

6. **Robustezza minima dichiarata dei meccanismi**
La robustezza minima dei meccanismi per la carta tachigrafica è Elevata, secondo quanto stabilito nella norma ITSEC.

7. **Grado di garanzia**
Il grado di garanzia della carta tachigrafica è il livello ITSEC E3, secondo quanto stabilito nella norma ITSEC.

8. **Fondamento logico**
Le matrici riportate di seguito forniscono una spiegazione logica delle SEF supplementari, indicando:

— quale SEF neutralizza la minaccia indicata,

— quale SEF realizza l'obiettivo di sicurezza del sistema IT indicato.

	Minacce											Obiettivi IT								
	T.CLON*	T.DIS_ES2	T.T_ES	T.T_CMD	T.MOD_SOFT*	T.MOD_LOAD	T.MOD_EXE	T.MOD_SHARE	Ident_Data	Activity_Data	Data_Exchange	O.TAMPER_ES	O.CLON*	O.OPERATE*	O.FLAW*	O.DIS_MECHANISM2	O.DIS_MEMORY*	O.MOD_MEMORY*	Data_Access	Secured_Communications
UIA_301 Misure di autenticazione																			x	
UIA_302 Controlli PIN																			x	
ACT_301 Dati identificazione																				
ACT_302 Dati personalizzazione																				
RLB_301 Integrità software												x		x						
RLB_302 Prove automatiche												x		x						
RLB_303 Prove fabbricazione					x	x						x		x						
RLB_304 Analisi software					x		x	x				x		x						
RLB_305 Input software					x	x		x				x		x						
RLB_306 Alimentazione									x	x		x		x						
RLB_307 Azzeramento												x		x						
DEX_301 Importazione sicura di dati											x									x
DEX_302 Importazione sicura di dati											x									x
DEX_303 Esportazione sicura di dati verso la VU											x									x
DEX_304 Prova d'origine											x									x
DEX_305 Prova d'origine											x									x
DEX_306 Esportazione sicura verso dispositivi esterni											x									x
CSP_301 Generazione chiavi												x								x
CSP_302 Distribuzione chiavi												x								x

Appendice 11

MECCANISMI COMUNI DI SICUREZZA

INDICE

1. PRESCRIZIONI GENERALI

La presente appendice specifica i meccanismi di sicurezza atti a garantire:

— l'autenticazione reciproca tra le VU e le carte tachigrafiche, compresi gli accordi sulle chiavi di sessione,

— la riservatezza, l'integrità e l'autenticazione dei dati trasferiti tra le VU e le carte tachigrafiche,

— l'integrità e l'autenticazione dei dati trasferiti dalle VU a dispositivi di memorizzazione esterni,

— l'integrità e l'autenticazione dei dati trasferiti dalle carte tachigrafiche a dispositivi di memorizzazione esterni.

1.1. **Riferimenti normativi**

Nella presente appendice si rimanda alle seguenti norme:

SHA-1	National Institute of Standards and Technology (NIST). FIPS Publication 180-1: Secure Hash Standard. April 1995
PKCS1	RSA Laboratories. PKCS # 1: RSA Encryption Standard. Version 2.0. October 1998
TDES	National Institute of Standards and Technology (NIST). FIPS Publication 46-3: Data Encryption Standard. Progetto 1999
TDES-OP	ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation. 1998
ISO/IEC 7816-4	Information Technology — Identification cards — Integrated circuit(s) cards with contacts — Part 4: Interindustry commands for interexchange. First edition: 1995 + Amendment 1: 1997(Tecnologie dell'informazione — Carte di identificazione — Carte a circuito/i integrato/i con contatti — Parte 4: Comandi interindustriali per l'interscambio. Prima edizione: 1995 + Modifica 1: 1997)
ISO/IEC 7816-6	Information Technology — Identification cards — Integrated circuit(s) cards with contacts — Part 6: Interindustry data elements. First edition: 1996 + Cor 1: 1998. (Tecnologie dell'informazione — Carte di identificazione — Carte a circuito/i integrato/i con contatti — Parte 6: Elementi di dati interindustriali. Prima edizione: 1996 + Cor 1: 1998)
ISO/IEC 7816-8	Information Technology — Identification cards — Integrated circuit(s) cards with contacts — Part 8: Security related interindustry commands. First edition 1999. (Tecnologie dell'informazione — Carte di identificazione — Carte a circuito/i integrato/i con contatti — Parte 8: Comandi interindustriali concernenti la sicurezza. Prima edizione: 1999)
ISO/IEC 9796-2	Information Technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Mechanisms using a hash function. First edition: 1997. (Tecnologie dell'informazione — Tecniche di sicurezza — Schemi per firme digitali con recupero dei messaggi — Parte 2: Meccanismi che usano una funzione di hash. Prima edizione: 1997)
ISO/IEC 9798-3	Information Technology — Security techniques — Entity authentication mechanisms — Part 3: Entity authentication using a public key algorithm. Second edition 1998. (Tecnologie dell'informazione — Tecniche di sicurezza — Meccanismi di autenticazione di entità — Parte 3: Autenticazione di entità con un algoritmo a chiave pubblica. Seconda edizione: 1998)
ISO 16844-3	Road vehicles — Tachograph systems — Part 3: Motion sensor interface. (Veicoli stradali — Sistemi tachigrafici — Parte 3: Interfacce dei sensori di movimento)

1.2. **Simboli e acronimi**

Nella presente appendice sono stati usati i seguenti simboli e abbreviazioni:

(K_a, K_b, K_c)	Un insieme di chiavi utilizzate dall'algoritmo triplo di crittazione dei dati (triple data encryption)
CA	Organismo di certificazione
CAR	Riferimento dell'organismo di certificazione
CC	Totale di controllo crittografico
CG	Crittogramma
CH	Intestazione comando
CHA	Autorizzazione del titolare del certificato
CHR	Riferimento del titolare del certificato
D()	Decrittazione con DES
DE	Elemento di dati
DO	Oggetto di dati
d	Chiave privata RSA, esponente privato
e	Chiave pubblica RSA, esponente pubblico
E()	Crittazione con DES
EQT	Apparecchio
Hash()	Valore di hash, un prodotto di *hash*
Hash	Funzione di hash
KID	Identificazione chiave
Km	Chiave in TDES; master key definita nella norma ISO 16844-3
Km_{VU}	Chiave in TDES inserita nell'unità di bordo dei veicoli
Km_{WC}	Chiave in TDES inserita nella carta dell'officina
m	Messaggio, un numero intero compreso tra 0 e *n*-1
n	Chiavi RSA, modulo
PB	Byte di riempimento
PI	Byte indicatore di riempimento (da usare nel crittogramma per la riservatezza dei DO)
PV	Valore semplice
s	Firma, un numero intero compreso tra 0 e *n*-1
SSC	Contatore sequenza di invio
SM	Messaggistica sicura
TCBC	Modalità di funzionamento TDEA cifratore a blocchi incatenati
TDEA	Algoritmo triplo di crittazione dei dati
TLV	Valore lunghezza tag
VU	Unità elettronica di bordo
X.C	Certificato dell'utente X rilasciato da un organismo di certificazione
X.CA	Organismo di certificazione dell'utente X
$X.CA.PK_oX.C$	Operazione di apertura di un certificato per estrarre una chiave pubblica; si tratta di un operatore infisso, il cui operando di sinistra è la chiave pubblica di un organismo di certificazione e il cui operando di destra è il certificato rilasciato da tale organismo di certificazione; il risultato è la chiave pubblica dell'utente X il cui certificato è l'operando di destra

X.PK	Chiave pubblica RSA di un utente X
X.PK[I]	Cifratura RSA di un'informazione I, utilizzando la chiave pubblica dell'utente X
X.SK	Chiave privata RSA di un utente X
X.SK[I]	Cifratura RSA di un'informazione I, utilizzando la chiave privata dell'utente X
'xx'	Valore esadecimale
||	Operatore di concatenamento

2. SISTEMI E ALGORITMI CRITTOGRAFICI

2.1. **Sistemi crittografici**

CSM_001 Le unità elettroniche di bordo e le carte tachigrafiche usano un sistema RSA di crittografia tradizionale con chiave pubblica per fornire i seguenti meccanismi di sicurezza:

— autenticazione tra unità elettroniche di bordo e carte,

— trasporto di chiavi triple di sessione DES tra unità elettroniche di bordo e carte tachigrafiche,

— firma digitale dei dati trasferiti dalle unità elettroniche di bordo o dalle carte tachigrafiche verso dispositivi esterni.

CSM_002 Le unità elettroniche di bordo e le carte tachigrafiche usano un sistema di crittografia simmetrica T-DES per fornire un meccanismo atto a garantire l'integrità dei dati durante lo scambio di dati dell'utente tra unità elettroniche di bordo e carte tachigrafiche e per garantire, se applicabile, la riservatezza dello scambio di dati tra unità elettroniche di bordo e carte tachigrafiche.

2.2. **Algoritmi crittografici**

2.2.1. ***Algoritmo RSA***

CSM_003 L'algoritmo RSA è interamente definito dalle seguenti relazioni:

$$X.SK[m] = s = m^d \bmod n$$

$$X.PK[s] = m = s^e \bmod n$$

Una descrizione più esauriente della funzione RSA è riportata nella norma PKCS1.

L'esponente pubblico e nel calcolo RSA sarà differente da 2 in tutte le chiavi RSA generate.

2.2.2. ***Algoritmo di hash***

CSM_004 Il meccanismo di firma digitale utilizza l'algoritmo di hash SHA-1 definito nella norma SHA-1.

2.2.3. ***Algoritmo di crittazione dei dati***

CSM_005 Nella modalità di funzionamento con cifratore a blocchi incatenati si usano algoritmi basati sul DES.

3. CHIAVI E CERTIFICATI

3.1. **Generazione e distribuzione di chiavi**

3.1.1. ***Generazione e distribuzione di chiavi RSA***

CSM_006 Le chiavi RSA sono generate in base a tre livelli gerarchici funzionali:

— livello europeo,

— livello di Stato membro,

— livello di apparecchio.

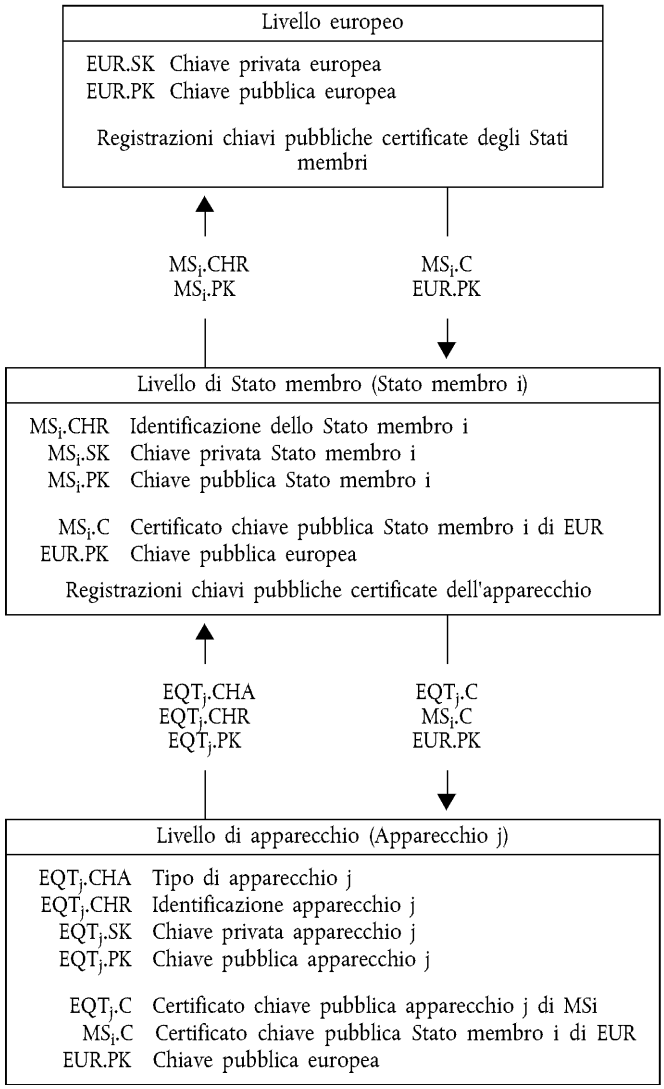
CSM_007 A livello europeo, viene generata un'unica coppia di chiavi europee (EUR.SK e EUR.PK). La chiave privata europea viene usata per certificare le chiavi pubbliche degli Stati membri. Vengono conservate le registrazioni di tutte le chiavi certificate. Queste funzioni sono espletate da un organismo europeo di certificazione, sotto l'autorità e la responsabilità della Commissione europea.

CSM_008 A livello di Stato membro, viene generata una coppia di chiavi dello Stato membro (MS.SK e MS.PK). Le chiavi pubbliche degli Stati membri sono certificate dall'organismo europeo di certificazione. La chiave privata degli Stati membri viene usata per certificare le chiavi pubbliche da inserire nell'apparecchio (unità elettronica di bordo o carta tachigrafica). Vengono conservate registrazioni di tutte le chiavi pubbliche certificate insieme all'identificazione dell'apparecchio cui sono destinate. Queste funzioni sono espletate da un organismo di certificazione nazionale. Gli Stati membri possono cambiare periodicamente la propria coppia di chiavi.

CSM_009 A livello di apparecchio, viene generata un'unica coppia di chiavi (EQT.SK e EQT.PK) che viene inserita in ciascun apparecchio. Le chiavi pubbliche degli apparecchi sono certificate da un organismo di certificazione nazionale. Queste funzioni possono essere espletate dai fabbricanti di apparecchi, dai centri che personalizzano gli apparecchi o dalle autorità degli Stati membri. Questa coppia di chiavi viene usata per l'autenticazione, la firma digitale e i servizi di cifratura.

CSM_010 Durante la generazione, il trasporto (se del caso) e l'immagazzinamento viene preservata la riservatezza delle chiavi private.

L'illustrazione seguente riepiloga il flusso di dati della suddetta procedura:



3.1.2. ***Chiavi di prova RSA***

CSM_011 Ai fini delle prove dell'apparecchio (comprese le prove di interoperabilità), l'organismo europeo di certificazione genera un'apposita diversa coppia di chiavi di prova europee e almeno due coppie di chiavi di prova per ogni Stato membro, le cui chiavi pubbliche sono certificate con la chiave di prova privata europea. I fabbricanti devono inserire nell'apparecchio sottoposto alle prove di omologazione chiavi di prova certificate da una di tali chiavi di prova degli Stati membri.

3.1.3. ***Chiavi per i sensori di movimento***

La riservatezza delle tre chiavi TDES indicate va opportunamente garantita sia in fase di generazione, che di trasferimento (se ha luogo) che di immagazzinamento.

Per garantire la compatibilità con apparecchi di registrazione conformi alla norma ISO 16844, l'organismo di certificazione europeo e gli organismi di certificazione degli Stati membri, garantiscono inoltre quanto segue.

CSM_036 L'organismo di certificazione europeo genera Km_{vu} e Km_{wc}, due triple chiavi DES uniche ed indipendenti, e quindi anche la chiave Km, ove:

$$Km = Km_{VU} \text{ XOR } Km_{WC}$$

L'organismo di certificazione europeo invia tali chiavi, applicando le opportune procedure di sicurezza, agli organismi di certificazione degli Stati membri che ne fanno richiesta.

CSM_037 Gli organismi di certificazione degli Stati membri devono:

— utilizzare Km per crittare i dati relativi ai sensori di movimento richiesti dai produttori di tali sensori (i dati da crittare con Km sono indicati nella norma ISO 16844-3),

— inviare Km_{vu} ai fabbricanti delle unità elettroniche di bordo, applicando le opportune procedure di sicurezza, in modo che essi possano inserirle in tali unità,

— assicurare che Km_{wc} sia inserita in tutte le carte di officina (`SensorInstallationSecData` nel fine elementare `Sensor_Installation_Data`) nel corso della personalizzazione della carta.

3.1.4. ***Generazione e distribuzione di chiavi triple di sessioni DES***

CSM_012 Nell'ambito della procedura di autenticazione reciproca, le unità elettroniche di bordo e le carte tachigrafiche generano e scambiano i dati necessari ad elaborare una chiave tripla comune di sessione DES. Tale scambio di dati è protetto ai fini della riservatezza mediante un meccanismo di crittazione RSA.

CSM_013 Questa chiave viene usata per tutte le successive operazioni crittografiche che utilizzano la messaggistica sicura. La sua validità scade al termine della sessione (estrazione della carta o azzeramento della carta) e/o dopo 240 impieghi (un impiego della chiave = un comando che utilizza la messaggistica sicura inviato alla carta e relativa risposta).

3.2. **Chiavi**

CSM_014 La lunghezza delle chiavi RSA (indipendentemente dal livello) è la seguente: modulo *n* 1024 bit, esponente pubblico *e* 64 bit al massimo, esponente privato *d* 1024 bit.

CSM_015 Le chiavi triple DES hanno il formato (K_a, K_b, K_a), dove K_a und K_b sono chiavi indipendenti lunghe 64 bit. Non deve essere impostato un bit di rilevamento errore di parità.

3.3. **Certificati**

CSM_016 I certificati delle chiavi pubbliche RSA sono certificati verificabili mediante carta (card verifiable) non autodescrittivi (non self-descriptive) (Rif.: ISO/IEC 7816-8).

3.3.1. ***Contenuto dei certificati***

CSM_017 I certificati delle chiavi pubbliche RSA sono costruiti con i dati sotto riportati nell'ordine seguente:

Dati	Formato	Byte	Osservazioni
CPI	INTEGER	1	Identificazione profilo certificato ('01' per questa versione)
CAR	OCTET STRING	8	Riferimento dell'organismo di certificazione
CHA	OCTET STRING	7	Autorizzazione del titolare del certificato
EOV	TimeReal	4	Termine di validità del certificato. Facoltativo, riempito con 'FF' se non utilizzato
CHR	OCTET STRING	8	Riferimento del titolare del certificato
n	OCTET STRING	128	Chiave pubblica (modulo)
e	OCTET STRING	8	Chiave pubblica (esponente pubblico)
		164	

Note:

1. L'"identificazione del profilo del certificato" (CPI) definisce la struttura precisa di un certificato di autenticazione. Si può usare come un'identificazione interna all'apparecchio di un elenco di intestazioni pertinente che descrive il concatenamento di elementi di dati nel certificato.

   L'elenco di intestazioni associato al contenuto di questo certificato è il seguente:

'4D'	'16'	'5F 29'	'01'	'42'	'08'	'5F 4B'	'07'	'5F 24'	'04'	'5F 20'	'08'	'7F 49'	'05'	'81'	'81 80'	'82'	'08'
Tag elenco intestazioni esteso	Lunghezza elenco intestazioni	Tag CPI	Lunghezza CPI	Tag CAR	Lunghezza CAR	Tag CHA	Lunghezza CHA	Tag EOV	Lunghezza EOV	Tag CHR	Lunghezza CHR	Tag chiave pubblica (costruito)	Lunghezza DO successivi	Tag modulo	Lunghezza modulo	Tag esponente pubblico	Lunghezza esponente pubblico

2. Il "riferimento dell'organismo di certificazione" (CAR) ha lo scopo di identificare l'organismo di certificazione che rilascia il certificato, in modo che l'elemento di dati si possa contemporaneamente usare come un'identificazione della chiave dell'organismo in riferimento alla chiave pubblica dell'organismo di certificazione (per la codifica, cfr. identificazione della chiave).

3. L'"autorizzazione del titolare del certificato" (CHA) è usata per identificare i diritti del titolare del certificato. È costituita dall'ID dell'applicazione tachigrafica e dal tipo di apparecchio cui è destinato il certificato (secondo l'elemento di dati *EquipmentType*, "00" per uno Stato membro).

4. Il "riferimento del titolare del certificato" (CHR) ha lo scopo di identificare inequivocabilmente il titolare del certificato, in modo che l'elemento di dati si possa contemporaneamente usare come un'identificazione della chiave di un soggetto in riferimento alla chiave pubblica del titolare del certificato.

5. Le identificazioni delle chiavi identificano inequivocabilmente il titolare del certificato o gli organismi di certificazione. Sono codificate come segue:

   5.1. Apparecchio (VU o carta):

Dati	N. di serie apparecchio	Data	Tipo	Fabbricante
Lunghezza	4 byte	2 byte	1 byte	1 byte
Valore	Intero	mm aa codifica BCD	Specifico per ciascun fabbricante	Codice fabbricante

Nel caso di una VU, il fabbricante, quando richiede i certificati, può conoscere o meno l'identificazione dell'apparecchio in cui saranno inserite le chiavi.

Nel primo caso, il fabbricante invia l'identificazione dell'apparecchio con la chiave pubblica all'organismo di certificazione del suo Stato membro. Il certificato conterrà l'identificazione dell'apparecchio e il fabbricante deve garantire che le chiavi e il certificato siano inseriti nell'apparecchio cui sono destinati. Il formato dell'identificazione della chiave è quello sopra riportato.

Nel secondo caso, il fabbricante deve identificare inequivocabilmente ciascuna richiesta di certificato e inviare tale identificazione con la chiave pubblica all'organismo di certificazione del suo Stato membro. Il certificato conterrà l'identificazione della richiesta. Il fabbricante deve comunicare all'organismo del suo Stato membro l'assegnazione della chiave all'apparecchio (cioè identificazione della richiesta di certificato, identificazione dell'apparecchio) dopo l'installazione della chiave nell'apparecchio. L'identificazione della chiave ha il formato seguente:

Dati	N. di serie richiesta certificato	Data	Tipo	Fabbricante
Lunghezza	4 byte	2 byte	1 byte	1 byte
Valore	Codifica BCD	mm aa codifica BCD	'FF'	Codice fabbricante

5.2. Organismo di certificazione:

Dati	Identificazione organismo	N. di serie chiave	Altre informazioni	Identificazione
Lunghezza	4 byte	1 byte	2 byte	1 byte
Valore	1 byte codice numerico paese 3 byte codice alfanumerico paese	Intero	Codifica aggiuntiva (specifica per CA) 'FF FF' se non utilizzato	'01'

Il numero di serie della chiave è usato per distinguere le diverse chiavi di uno Stato membro, nel caso in cui la chiave venga cambiata.

6. I verificatori dei certificati sanno implicitamente che la chiave pubblica certificata è una chiave RSA concernente l'autenticazione, la verifica delle firme digitali e la cifratura per i servizi di riservatezza [il certificato non contiene un'identificazione oggetto (object identifier) che lo specifichi].

3.3.2. ***Rilascio dei certificati***

CSM_018 Il certificato rilasciato è una firma digitale con recupero parziale del contenuto del certificato conformemente alla norma ISO/IEC 9796-2, con il "riferimento dell'organismo di certificazione" allegato.

$$X.C = X.CA.SK['6A' \,||\, C_r \,||\, \mathit{Hash}(Cc) \,||\, 'BC'] \,||\, C_n \,||\, X.CAR$$

Dove il contenuto del certificato $= Cc = \underset{106\ \text{byte}}{C_r} \,||\, \underset{58\ \text{byte}}{C_n}$

Note:

1. Questo certificato ha una lunghezza di 194 byte.

2. Anche il CAR, nascosto dalla firma, è allegato alla firma, in modo da consentire la selezione della chiave pubblica dell'organismo di certificazione per la verifica del certificato.

3. Il verificatore del certificato conosce implicitamente l'algoritmo usato dall'organismo di certificazione per firmare il certificato.

4. L'elenco di intestazioni associato al certificato rilasciato è il seguente:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
Tag certificato CV (costruito)	Lunghezza DO successivi	Tag firma	Lunghezza firma	Tag resto	Lunghezza resto	Tag CAR	Lunghezza CAR

3.3.3. ***Verifica e apertura dei certificati***

La verifica e l'apertura dei certificati consistono nel verificare la firma in base alla norma ISO/IEC 9796-2, recuperare il contenuto del certificato e la chiave pubblica contenuta: X.PK = X.CA.PK$_o$X.C, e nel verificare la validità del certificato.

CSM_019 La procedura prevede le fasi seguenti:

Verifica firma e recupero contenuto:

— da X.C recuperare Sign, C_n' e CAR′: X.C = Sign (128 byte) || C_n' (58 byte) || CAR' (8 byte)

— da CAR' selezionare la corretta chiave pubblica dell'organismo di certificazione (se non ancora effettuato con altri mezzi)

— aprire la firma con la chiave pubblica di CA: Sr′ = X.CA.PK [Sign],

— controllare che Sr′ inizi con ′6A′ e termini con ′BC′

— calcolare Cr′ e H′ da: Sr′ Sr' = '6A' || C_r' (106 byte) || H' (20 byte) || 'BC'

— recuperare il contenuto del certificato C′ = C_r' || C_n',

— controllare che sia *Hash*(C′) = H′

Se i controlli danno esito positivo il certificato è autentico, il suo contenuto è C′.

Verificare la validità. Da C′:

— se applicabile, controllare data termine validità.

Recuperare e memorizzare la chiave pubblica, l'identificazione della chiave, l'autorizzazione del titolare del certificato e il termine di validità del certificato da C′:

— X.PK = *n* || *e*

— X.KID = CHR

— X.CHA = CHA

— X.EOV = EOV

4. MECCANISMO DI AUTENTICAZIONE RECIPROCA

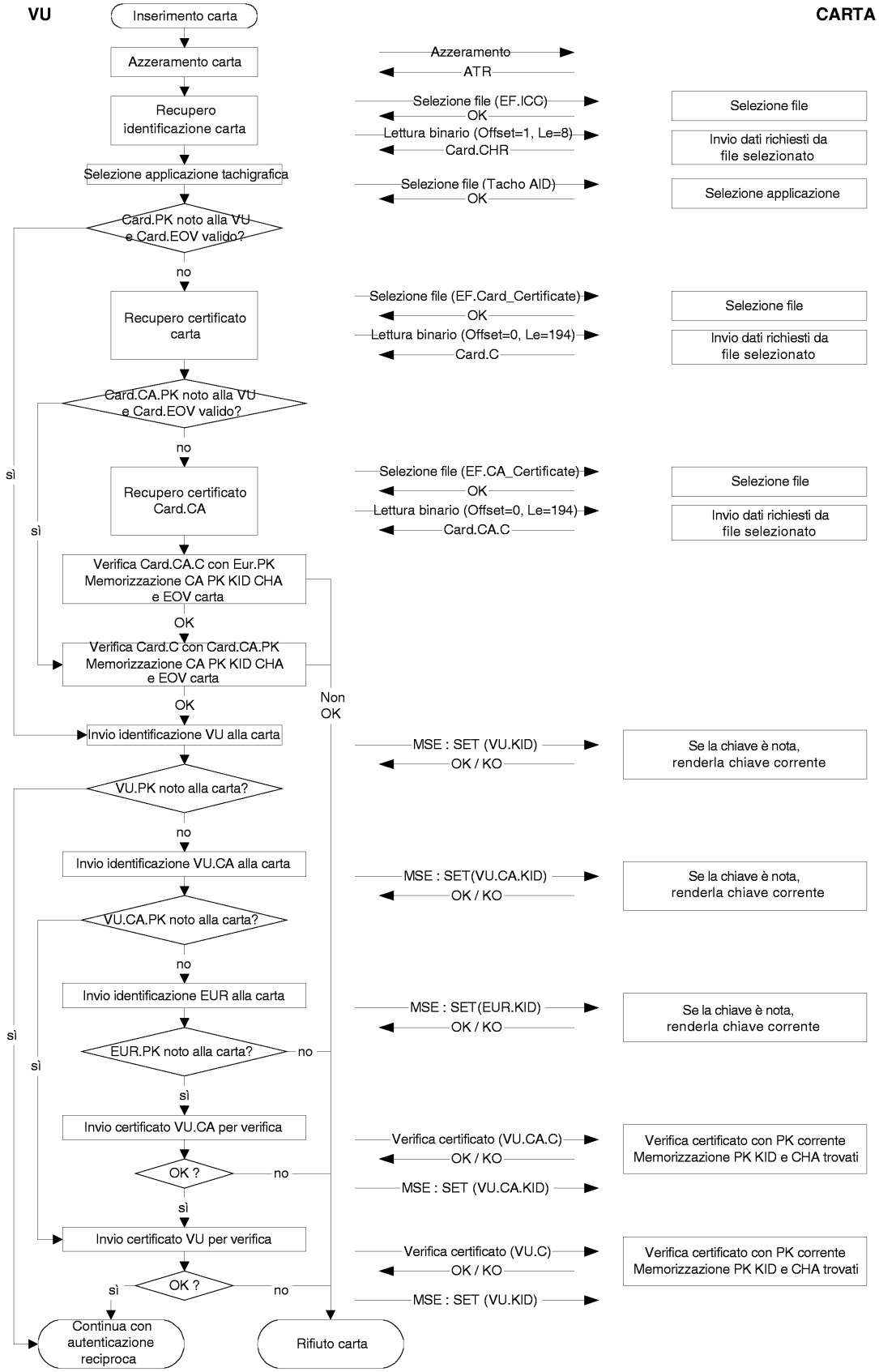
L'autenticazione reciproca tra le carte e le VU si basa sul principio seguente.

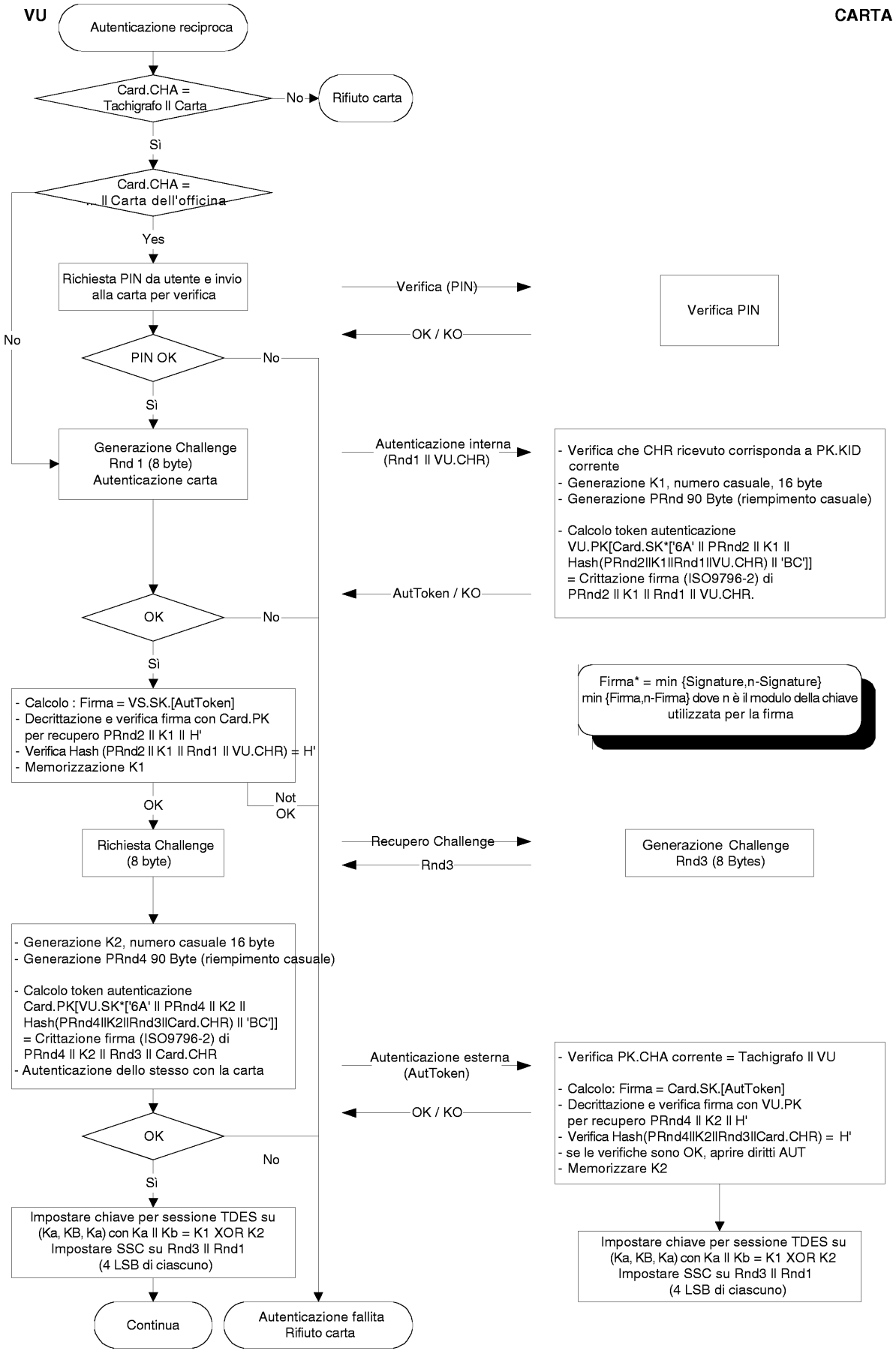
Ogni parte deve dimostrare all'altra di possedere una coppia di chiavi valida, di cui la chiave pubblica è stata certificata da un organismo di certificazione di uno Stato membro, il quale è stato certificato dall'organismo di certificazione europeo.

Tale dimostrazione è effettuata firmando con la chiave privata un numero casuale inviato dall'altra parte, che deve recuperare il numero casuale inviato quando verifica tale firma.

Il meccanismo è attivato dalla VU all'atto dell'inserimento della carta. Inizia con lo scambio di certificati e l'apertura delle chiavi pubbliche e termina con l'impostazione di una sessione della chiave.

CSM_020 Si utilizza il seguente protocollo [le frecce indicano i comandi e i dati scambiati (cfr. appendice 2)]:




VU
CARTA
Autenticazione reciproca
Card.CHA = Tachigrafo II Carta
No
Rifiuto carta
Sì
Card.CHA = ... II Carta dell'officina
Yes
Richiesta PIN da utente e invio alla carta per verifica
Verifica (PIN)
Verifica PIN
OK / KO
No
PIN OK
No
Sì
Generazione Challenge Rnd 1 (8 byte) Autenticazione carta
Autenticazione interna (Rnd1 II VU.CHR)
- Verifica che CHR ricevuto corrisponda a PK.KID corrente
- Generazione K1, numero casuale, 16 byte
- Generazione PRnd 90 Byte (riempimento casuale)
- Calcolo token autenticazione VU.PK[Card.SK*['6A' II PRnd2 II K1 II Hash(PRnd2IIK1IIRnd1IIVU.CHR) II 'BC']] = Crittazione firma (ISO9796-2) di PRnd2 II K1 II Rnd1 II VU.CHR.
AutToken / KO
OK
No
Sì
Firma* = min {Signature,n-Signature} min {Firma,n-Firma} dove n è il modulo della chiave utilizzata per la firma
- Calcolo : Firma = VS.SK.[AutToken]
- Decrittazione e verifica firma con Card.PK per recupero PRnd2 II K1 II H'
- Verifica Hash (PRnd2 II K1 II Rnd1 II VU.CHR) = H'
- Memorizzazione K1
OK
Not OK
Richiesta Challenge (8 byte)
Recupero Challenge
Rnd3
Generazione Challenge Rnd3 (8 Bytes)
- Generazione K2, numero casuale 16 byte
- Generazione PRnd4 90 Byte (riempimento casuale)
- Calcolo token autenticazione Card.PK[VU.SK*['6A' II PRnd4 II K2 II Hash(PRnd4IIK2IIRnd3IICard.CHR) II 'BC']] = Crittazione firma (ISO9796-2) di PRnd4 II K2 II Rnd3 II Card.CHR
- Autenticazione dello stesso con la carta
Autenticazione esterna (AutToken)
- Verifica PK.CHA corrente = Tachigrafo II VU
- Calcolo: Firma = Card.SK.[AutToken]
- Decrittazione e verifica firma con VU.PK per recupero PRnd4 II K2 II H'
- Verifica Hash(PRnd4IIK2IIRnd3IICard.CHR) = H'
- se le verifiche sono OK, aprire diritti AUT
- Memorizzare K2
OK / KO
OK
No
Sì
Impostare chiave per sessione TDES su (Ka, KB, Ka) con Ka II Kb = K1 XOR K2
Impostare SSC su Rnd3 II Rnd1
(4 LSB di ciascuno)
Impostare chiave per sessione TDES su (Ka, KB, Ka) con Ka II Kb = K1 XOR K2
Impostare SSC su Rnd3 II Rnd1
(4 LSB di ciascuno)
Continua
Autenticazione fallita
Rifiuto carta

5. MECCANISMI DI RISERVATEZZA, INTEGRITÀ E AUTENTICAZIONE DEI TRASFERIMENTI DI DATI TRA VU E CARTE

5.1 **Messaggistica sicura**

CSM_021 L'integrità dei trasferimenti di dati tra VU e carte deve essere protetta mediante messaggistica sicura, in conformità delle norme ISO/IEC 7816-4 e ISO/IEC 7816-8.

CSM_022 Quando è necessario proteggere i dati durante il trasferimento, un oggetto di dati del totale di controllo crittografico viene allegato agli oggetti di dati inviati all'interno del comando o della risposta. Il totale di controllo crittografico viene verificato dal destinatario.

CSM_023 Il totale di controllo crittografico dei dati inviati all'interno di un comando integra l'intestazione del comando e tutti gli oggetti di dati inviati (= > CLA = '0C', e tutti gli oggetti di dati sono incapsulati con tag in cui b1 = 1).

CSM_024 I byte di informazione-stato della risposta devono essere protetti da un totale di controllo crittografico quando la risposta non contiene campi di dati.

CSM_025 I totali di controllo crittografico hanno una lunghezza di 4 byte.

Quando si usa la messaggistica sicura, la struttura dei comandi e delle risposte è quindi:

i DO utilizzati sono una serie parziale dei DO della messaggistica sicura descritti nella norma ISO/IEC 7816-4:

Tag	Mnemonico	Significato
'81'	T_{PV}	Valore semplice, dati non codificati BER-TLV (da proteggere con CC)
'97'	T_{LE}	Valore di Le nel comando non sicuro (da proteggere con CC)
'99'	T_{SW}	Informazione-stato (da proteggere con CC)
'8E'	T_{CC}	Totale di controllo crittografico
'87'	$T_{PI\ CG}$	Byte indicatore di riempimento || Crittogramma (valore semplice, non codificato in BER-TLV)

Data una coppia comando-risposta non sicuri:

Intestazione comando	Contenuto comando
CLA INS P1 P2	[campo L_c] [Campo dati] [campo L_e]
quattro byte	L byte, indicati come B_1 - B_L

Contenuto risposta	Coda risposta
[Campo dati]	SW1 SW2
Byte dati L_r	due byte

La corrispondente coppia comando-risposta sicuri è:

Comando sicuro:

Intestazione comando (CH)	Contenuto comando										
CLA INS P1 P2	[nuovo campo L_c]	[nuovo campo dati]									[nuovo campo L_e]
'OC'	Lunghezza nuovo campo dati	T_{PV}	L_{PV}	PV	T_{LE}	L_{LE}	L_e	T_{CC}	L_{CC}	CC	'00'
		'81'	L_c	Campo dati	'97'	'01'	L_e	'8E'	'04'	CC	

Dati da integrare nel totale di controllo = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB

PB = byte di riempimento (80 .. 00), in base alle norme ISO-IEC 7816-4 e ISO 9797, metodo 2.

DO PV e LE sono presenti solo se sono presenti dati corrispondenti nel comando non sicuro.

Risposta sicura:

1. Caso in cui il campo dati della risposta non è vuoto e non deve essere protetto a fini di riservatezza:

Contenuto risposta						Coda risposta
[Nuovo campo dati]						Nuovi SW1 SW2
T_{PV}	L_{PV}	PV	T_{CC}	L_{CC}	CC	
'81'	L_r	Campo dati	'8E'	'04'	CC	

Dati da integrare nel totale di controllo = T_{PV} || L_{PV} || PV || PB

2. Caso in cui il campo dati della risposta non è vuoto e deve essere protetto a fini di riservatezza:

Contenuto risposta						Coda risposta
[Nuovo campo dati]						Nuovi SW1 SW2
$T_{PI\ CG}$	$L_{PI\ CG}$	PI CG	T_{CC}	L_{CC}	CC	
'87'		PI || CG	'8E'	'04'	CC	

Dati da trasportare da CG : dati non codificati BER-TLV e byte di riempimento.

Dati da integrare nel totale di controllo = $T_{PI\ CG}$ || $L_{PI\ CG}$ || PI CG || PB

3. Caso in cui il campo dati della risposta è vuoto:

Contenuto risposta						Coda risposta
[Nuovo campo dati]						Nuovi SW1 SW2
T_{SW}	L_{SW}	SW	T_{CC}	L_{CC}	CC	
'99'	'02'	Nuovi SW1 SW2	'8E'	'04'	CC	

Dati da integrare nel totale di controllo = T_{SW} || L_{SW} || SW || PB

5.2. **Trattamento degli errori della messaggistica sicura**

CSM_026 Quando la carta tachigrafica riconosce un errore di SM durante l'interpretazione di un comando, i byte di stato devono essere restituiti senza SM. Secondo la norma ISO/IEC 7816-4, i seguenti byte di stato sono definiti come indicazioni di errore di SM:

'66 88' Verifica di un totale di controllo crittografico fallita,

'69 87' Oggetti di dati SM previsti mancanti,

'69 88' Oggetti di dati SM non corretti.

CSM_027 Quando la carta tachigrafica restituisce i byte di stato senza DO SM o con un DO SM errato, la sessione deve essere annullata dalla VU.

5.3. **Algoritmo per il calcolo di totali di controllo crittografico**

CSM_028 I totali di controllo crittografico sono costruiti utilizzando un MAC particolareggiato, secondo ANSI X9.19, con DES:

— fase iniziale: il blocco di controllo iniziale y0 è E(Ka, SSC),

— fase sequenziale: i blocchi di controllo y1, …, yn sono calcolati utilizzando Ka,

— fase finale: il totale di controllo crittografico è calcolato in base all'ultimo blocco di controllo yn come segue: E[Ka, D(Kb, yn)],

dove E() significa crittazione con DES, e D() significa decrittazione con DES.

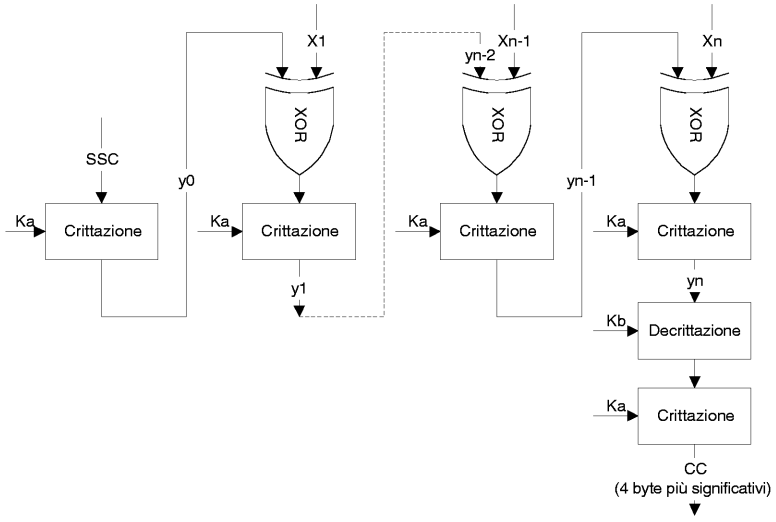
Vengono trasferiti i quattro byte più significativi del totale di controllo crittografico.

CSM_029 Il contatore sequenza di invio (SSC) viene inizializzato durante la procedura di accordo chiave al valore:

SSC iniziale: Rnd3 (4 byte meno significativi) || Rnd1 (4 byte meno significativi).

CSM_030 Il contatore sequenza di invio viene aumentato di un'unità prima di ogni calcolo del MAC (cioè, l'SSC per il primo comando è SSC iniziale + 1, l'SSC per la prima risposta è SSC iniziale + 2).

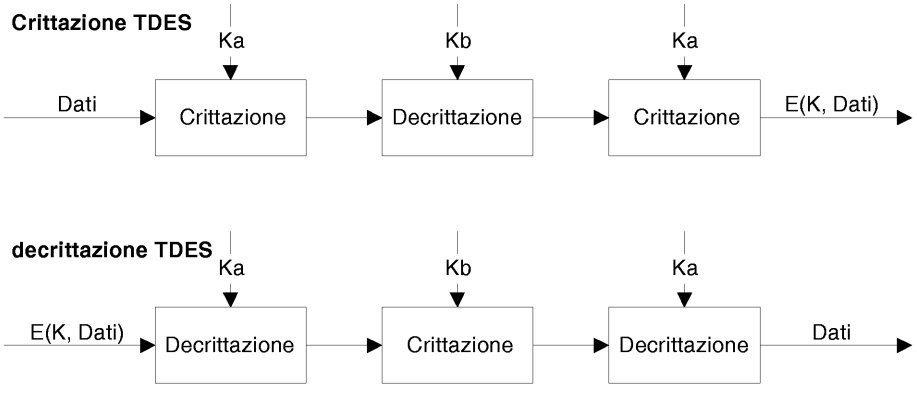
La figura seguente illustra il calcolo del MAC particolareggiato:



5.4. **Algoritmo per il calcolo di crittogrammi dei DO di riservatezza**

CSM_031 I crittogrammi sono calcolati utilizzando il TDEA nella modalità di funzionamento TCBC, secondo le norme TDES e TDES-OP e con il vettore nullo come blocco valore iniziale.

La figura seguente illustra l'applicazione di chiavi in TDES:



6. MECCANISMI DI FIRMA DIGITALE PER IL TRASFERIMENTO DI DATI

CSM_032 L'apparecchio intelligente dedicato (Intelligent dedicated equipment — IDE) memorizza i dati ricevuti da un apparecchio (VU o carta) durante una sessione di trasferimento all'interno di un file di dati fisico. Tale file deve contenere i certificati MS_i.C e EQT.C. Il file contiene firme digitali dei blocchi di dati secondo quanto specificato nell'appendice 7, Protocolli di trasferimento dei dati.

CSM_033 Le firme digitali dei dati trasferiti usano uno schema di firma digitale con appendice tale che i dati trasferiti possano, se del caso, essere letti senza necessità di decifrazione.

6.1. **Generazione della firma**

CSM_034 La generazione di firme dei dati da parte dell'apparecchio segue lo schema di firma con appendice definito nella norma PKCS1 con la funzione di hash SHA-1:

Firma = EQT.SK['00' || '01' || *PS* || '00' || DER(SHA-1(Dati))]

PS = Stringa di riempimento di ottetti con valore 'FF' tale che la lunghezza sia 128.

DER(SHA-1(M)) è la codifica dell'algoritmo ID per la funzione di hash e il valore di hash in un valore ASN.1 di tipo *DigestInfo* (regole di codifica distinte):

'30'||'21'||'30'||'09'||'06'||'05'||'2B'||'0E'||'03'||'02'||'1A'||'05'||'00'||'04'||'14'||Valore di hash.

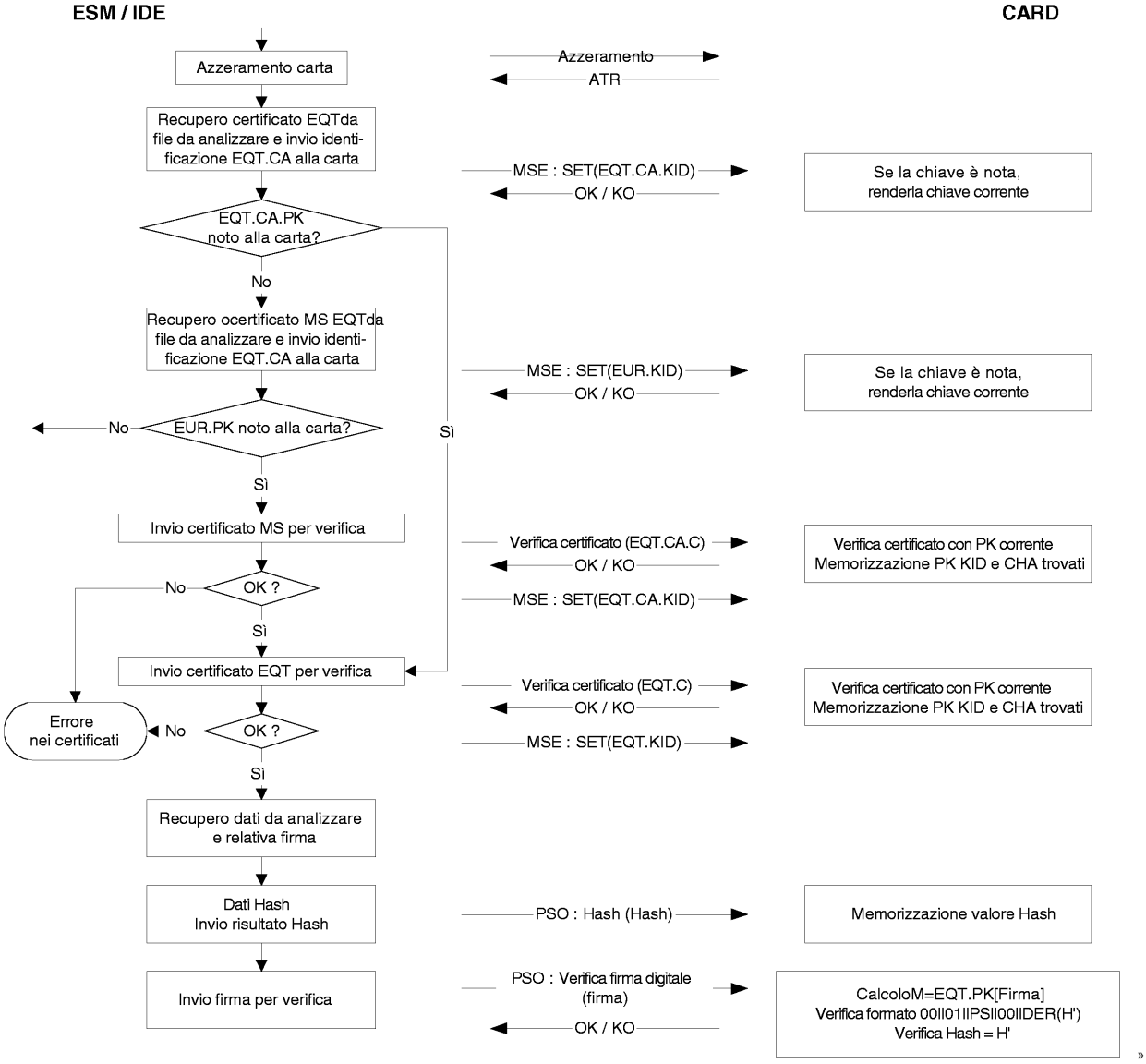
6.2. **Verifica della firma**

CSM_035 La verifica della firma di dati sui dati trasferiti segue lo schema di firma con appendice definito nella norma PKCS1 con la funzione di hash SHA-1.

La chiave pubblica europea EUR.PK deve essere nota al verificatore in modo indipendente (e fidato).

La tabella seguente illustra il protocollo che può seguire un IDE in cui sia stata inserita una carta di controllo per verificare l'integrità dei dati trasferiti e memorizzati nell'ESM (external storage media — dispositivo di memorizzazione esterno). La carta di controllo è usata per la decifrazione delle firme digitali. In questo caso, tale funzione può non essere implementata nell'IDE.

L'apparecchio che ha trasferito e firmato i dati da analizzare è indicato con EQT.


ESM / IDE
CARD
Azzeramento carta
Azzeramento
ATR
Recupero certificato EQTda file da analizzare e invio identificazione EQT.CA alla carta
MSE : SET(EQT.CA.KID)
OK / KO
Se la chiave è nota, renderla chiave corrente
EQT.CA.PK noto alla carta?
No
Recupero ocertificato MS EQTda file da analizzare e invio identificazione EQT.CA alla carta
MSE : SET(EUR.KID)
OK / KO
Se la chiave è nota, renderla chiave corrente
No
EUR.PK noto alla carta?
Sì
Sì
Invio certificato MS per verifica
Verifica certificato (EQT.CA.C)
OK / KO
Verifica certificato con PK corrente
Memorizzazione PK KID e CHA trovati
No
OK ?
MSE : SET(EQT.CA.KID)
Sì
Invio certificato EQT per verifica
Verifica certificato (EQT.C)
OK / KO
Verifica certificato con PK corrente
Memorizzazione PK KID e CHA trovati
Errore nei certificati
No
OK ?
MSE : SET(EQT.KID)
Sì
Recupero dati da analizzare e relativa firma
Dati Hash
Invio risultato Hash
PSO : Hash (Hash)
Memorizzazione valore Hash
Invio firma per verifica
PSO : Verifica firma digitale (firma)
OK / KO
CalcoloM=EQT.PK[Firma]
Verifica formato 00II01IIPSII00IIDER(H')
Verifica Hash = H'

»