

REGULAMENTUL (CE) NR. 1360/2002 AL COMISIEI**din 13 iunie 2002****de adaptare pentru a șaptea oară la progresul tehnic a Regulamentului (CEE) nr. 3821/85 al Consiliului privind aparatele de înregistrare în transportul rutier****(Text cu relevanță pentru SEE)**

COMISIA COMUNITĂȚILOR EUROPENE,

având în vedere Tratatul de instituire a Comunității Europene,

având în vedere Regulamentul (CEE) nr. 3821/85 al Consiliului din 20 decembrie 1985 privind aparatele de înregistrare în transportul rutier ⁽¹⁾, astfel cum a fost modificat ultima dată de Regulamentul (CE) nr. 2135/98 ⁽²⁾, în special articolele 17 și 18,

întrucât:

- (1) Specificațiile tehnice din anexa I (B) la Regulamentul (CEE) nr. 3821/85 trebuie adaptate la progresul tehnic, acordându-se o atenție specială securității generale a sistemului și capacității de interoperare a aparatelor de înregistrare și a cardurilor șoferilor.
- (2) Adaptarea aparatelor impune și adaptarea anexei II la Regulamentul (CEE) nr. 3821/85, în care sunt definite marcasele și certificatele de omologare.
- (3) Comitetul instituit prin articolul 18 din Regulamentul (CEE) nr. 3821/85 nu a emis un aviz privind măsurile cuprinse în propunere și, prin urmare, Comisia a prezentat Consiliului o propunere cu privire la aceste măsuri.
- (4) La expirarea perioadei prevăzute în articolul 18 alineatul (5) litera (b) din Regulamentul (CEE) nr. 3821/85, Consiliul nu adoptase o hotărâre și, în consecință, îi revine Comisiei adoptarea măsurilor respective,

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

Anexa la Regulamentul (CE) nr. 2135/98 se înlocuiește cu anexa la prezentul regulament.

Articolul 2

Anexa II la Regulamentul (CEE) nr. 3821/85 se modifică după cum urmează:

- (1) Capitolul I, punctul 1, primul paragraf se modifică după cum urmează:
 - semnul convențional pentru Grecia „GR” se înlocuiește cu „23”;
 - semnul convențional pentru Irlanda, „IRL” se înlocuiește cu „24”;
 - pentru Austria se adaugă semnul convențional „12”;
 - pentru Finlanda se adaugă semnul convențional „17”;
 - pentru Suedia se adaugă semnul convențional „5”.
- (2) Capitolul I, punctul 1, al doilea paragraf se modifică după cum urmează:
 - după cuvintele „foaie de înregistrare” se inserează textul „sau a unui card de tahograf”.
- (3) Capitolul I, punctul 2 se modifică după cum urmează:
 - după cuvintele „foaie de înregistrare” se inserează textul „și pe fiecare card de tahograf”.
- (4) În capitolul II, în titlu se adaugă următorul text: „PENTRU PRODUSELE CONFORME CU ANEXA I”.

⁽¹⁾ JO L 370, 31.12.1985, p. 8.⁽²⁾ JO L 274, 9.10.1998, p. 1.

(5) Se adaugă capitolul III după cum urmează:

„III. CERTIFICAT DE OMOLOGARE A PRODUSELOR CARE SUNT CONFORME CU DISPOZIȚIILE DIN ANEXA I B

Un stat care acordă o omologare emite solicitantului un certificat de omologare, al cărui model este prezentat în continuare. Când un stat membru informează alte state membre cu privire la omologările acordate sau, dacă este cazul, cu privire la omologările retrase, acesta folosește copii ale certificatului respectiv.

CERTIFICAT DE OMOLOGARE A PRODUSELOR CONFORME CU ANEXA I B

Denumirea administrației competente

Notificare privind ⁽³⁾:

- ☐ omologarea pentru
- ☐ retragerea omologării pentru
- ☐ un model de aparat de înregistrare
- ☐ o componentă a aparatului de înregistrare ⁽⁴⁾
- ☐ un card al șoferului
- ☐ un card al atelierului
- ☐ un card al societății
- ☐ un card al controlorului

Omologarea nr.

1. Marca fabricii sau marca comercială
2. Denumirea modelului
3. Numele producătorului
4. Adresa producătorului
5. Prezentat pentru omologare
6. Laboratorul/laboratoarele
7. Data și numărul testului/testelor
8. Data omologării
9. Data retragerii omologării
10. Modelul componentei/componentelor aparatului de înregistrare cu care trebuie utilizată componenta conform proiectării
11. Locul
12. Data
13. Documente descriptive anexate

14. Observații (inclusiv, dacă este cazul, poziția ștampilelor)

.....
(semnătura)

⁽³⁾ Bifați căsuțele corespunzătoare.

⁽⁴⁾ Menționați componenta la care se referă notificarea.”

Articolul 3

Prezentul regulament intră în vigoare în a douăzecea zi de la publicarea în *Jurnalul Oficial al Comunităților Europene*.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles, 13 iunie 2002

Pentru Comisie

Loyola DE PALACIO

Vicepreședinte

ANEXĂ

„ANEXA I B

CERINȚE PRIVIND CONSTRUCȚIA, TESTAREA, INSTALAREA ȘI INSPECȚIA

CUPRINS

I.	DEFINIȚII	10
II.	CARACTERISTICILE ȘI FUNCȚIILE GENERALE ALE APARATULUI DE ÎNREGISTRARE	14
1.	Caracteristici generale	14
2.	Funcții	14
3.	Moduri de funcționare	15
4.	Securitate	16
III.	CERINȚE DE CONSTRUCȚIE ȘI DE FUNCȚIONARE PENTRU APARATUL DE ÎNREGISTRARE...	16
1.	Monitorizarea introducerii și retragerii cardurilor	16
2.	Măsurarea vitezei și a distanței	16
2.1.	Măsurarea distanței parcurse	17
2.2.	Măsurarea vitezei	17
3.	Măsurarea timpului	17
4.	Monitorizarea activităților șoferului	18
5.	Monitorizarea stării șoferului	18
6.	Înregistrări manuale operate de șoferi	18
6.1.	Înregistrarea locurilor în care încep și/sau se încheie perioadele zilnice de muncă	18
6.2.	Înregistrarea manuală a activităților șoferului	18
6.3.	Înregistrarea situațiilor speciale	20
7.	Gestionarea blocărilor efectuate de societate	20
8.	Monitorizarea activităților de control	20
9.	Detectarea evenimentelor și/sau a anomaliilor	20
9.1.	Eveniment «introducerea unui card nevalabil»	20
9.2.	Eveniment «conflict card»	21
9.3.	Eveniment «suprapunerea unor intervale de timp»	21
9.4.	Eveniment «conducere fără card corespunzător»	21
9.5.	Eveniment «introducere card în timpul conducerii»	21
9.6.	Eveniment «încheiere incorectă a ultimei sesiuni»	21
9.7.	Eveniment «depășire de viteză»	21

9.8.	Eveniment «întrerupere a alimentării cu energie electrică»	22
9.9.	Eveniment «eroare la datele de mișcare»	22
9.10.	Eveniment «tentativă de violare a securității»	22
9.11.	Anomalie «card»	22
9.12.	Anomalie «aparat de înregistrare»	22
10.	Teste integrate și autoteste	22
11.	Citirea din memorie	22
12.	Înregistrarea și stocarea în memorie	23
12.1.	Date de identificare a aparatului	23
12.1.1.	Date de identificare a unității montate pe vehicul	23
12.1.2.	Date de identificare a senzorului de mișcare	23
12.2.	Elemente de securitate	24
12.3.	Date privind introducerea și retragerea cardului șoferului	24
12.4.	Date privind activitatea șoferului	25
12.5.	Locurile în care încep și/sau se încheie perioadele zilnice de muncă	25
12.6.	Date înregistrate de contorul de parcurs	25
12.7.	Date detaliate privind viteza	25
12.8.	Date privind evenimentele	25
12.9.	Date referitoare la proasta funcționare	27
12.10.	Date privind calibrarea	28
12.11.	Date privind reglarea orei	28
12.12.	Date privind activitățile de control	28
12.13.	Date privind blocările executate de societate	29
12.14.	Date privind activitățile de descărcare	29
12.15.	Date privind situații speciale	29
13.	Citirea de pe carduri de tahograf	29
14.	Înregistrarea și stocarea pe carduri de tahograf	29
15.	Afișare	30
15.1.	Afișajul implicit	30
15.2.	Afișarea avertismentelor	31
15.3.	Accesul la meniu	31
15.4.	Alte afișaje	31
16.	Tipărire	31
17.	Avertismente	32
18.	Descărcarea de date pe suporturi externe	33
19.	Date transmise unor dispozitive externe suplimentare	33
20.	Calibrare	34
21.	Reglarea orei	34

22.	Caracteristici	34
23.	Materiale	34
24.	Marcaje.....	35
IV.	CERINȚE FUNCȚIONALE ȘI DE CONSTRUCȚIE PENTRU CARDURILE DE TAHOGRAPH	35
1.	Date vizibile	35
2.	Securitate	38
3.	Standarde	38
4.	Specificații de mediu și electrice	38
5.	Stocarea datelor	38
5.1.	Date de identificare și securitate a cardului	39
5.1.1.	Identificarea aplicațiilor	39
5.1.2.	Identificarea microprocesorului	39
5.1.3.	Identificarea cardurilor cu circuite integrate	39
5.1.4.	Elemente de securitate.....	39
5.2.	Cardul șoferului	39
5.2.1.	Identificarea cardului	39
5.2.2.	Identificarea titularului cardului	40
5.2.3.	Informații privind permisul de conducere	40
5.2.4.	Date privind vehiculul folosit	40
5.2.5.	Date privind activitățile șoferului	40
5.2.6.	Locurile în care încep și/sau se încheie perioadele zilnice de muncă	41
5.2.7.	Date privind evenimentele	41
5.2.8.	Date privind anomaliile	42
5.2.9.	Date privind activitatea de control	42
5.2.10.	Date privind sesiunile de lucru cu cardul	42
5.2.11.	Date privind situații speciale	42
5.3.	Cardul atelierului	43
5.3.1.	Elemente de securitate.....	43
5.3.2.	Identificarea cardului	43
5.3.3.	Identificarea titularului cardului	43
5.3.4.	Date privind vehiculul folosit	43
5.3.5.	Date privind activitatea șoferului	43
5.3.6.	Date privind începutul și/sau sfârșitul perioadelor zilnice de muncă	43
5.3.7.	Date privind evenimentele și anomaliile	43
5.3.8.	Date privind activitățile de control.....	43
5.3.9.	Date privind calibrarea și reglarea orei	44
5.3.10.	Date privind situații speciale	44
5.4.	Cardul de control	44

5.4.1.	Identificarea cardului	44
5.4.2.	Identificarea titularului de card	44
5.4.3.	Date privind activitățile de control.....	44
5.5.	Cardul societății	45
5.5.1.	Identificarea cardului	45
5.5.2.	Identificarea titularului de card	45
5.5.3.	Date privind activitatea societății	45
V.	INSTALAREA APARATULUI DE ÎNREGISTRARE	45
1.	Instalare	45
2.	Placa de instalare	46
3.	Sigilare	46
VI.	CONTROALE, INSPECȚII ȘI REPARAȚII	47
1.	Omologarea secțiilor de montaj și a atelierelor.....	47
2.	Verificarea instrumentelor noi și a celor reparate	47
3.	Inspecția instalării	47
4.	Inspecții periodice	47
5.	Măsurarea erorilor	48
6.	Reparații	48
VII.	EMITEREA CARDURILOR.....	48
VIII.	OMOLOGAREA APARATELOR DE ÎNREGISTRARE ȘI A CARDURILOR DE TAHOGRAF	48
1.	Aspecte generale	48
2.	Certificatul de securitate	49
3.	Certificatul de funcționare	49
4.	Certificatul de interoperare	49
5.	Certificatul de omologare	50
6.	Procedură extraordinară: primele teste de interoperare	50

Apendicele 1. Dicționar de date

Apendicele 2. Specificații pentru cardurile de tahograf

Apendicele 3. Pictograme

Apendicele 4. Materiale tipărite

Apendicele 5. Afișaj

Apendicele 6. Interfețe externe

Apendicele 7. Protocol de descărcare a datelor

Apendicele 8. Protocol de calibrare

Apendicele 9. Omologare – lista testelor minime obligatorii

Apendicele 10. Obiective generale de securitate

Apendicele 11. Mecanisme de securitate comune

I. DEFINIȚII

În prezenta anexă:

(a) **«activare» înseamnă:**

etapa în care aparatul de înregistrare devine complet operațional și asigură toate funcțiile, inclusiv funcțiile de securitate;

Pentru activarea unui aparat de înregistrare trebuie folosit un card al atelierului și trebuie introdus un cod PIN;

(b) **«autentificare» înseamnă:**

o funcție destinată stabilirii și verificării unei identități;

(c) **«autenticitate» înseamnă:**

faptul că o informație provine de la o sursă a cărei identitate poate fi verificată;

(d) **«test integrat (BIT)» înseamnă:**

test care poate fi executat la comandă, declanșat de operator sau de un aparat extern;

(e) **«zi calendaristică» înseamnă:**

o zi cuprinsă între ora 00,00 și ora 24,00. Toate zilele calendaristice se raportează la ora UTC (ora universală coordonată);

(f) **«calibrare» înseamnă:**

actualizarea sau confirmarea parametrilor vehiculului care trebuie stocați în memorie. Parametrii vehiculului cuprind identificarea vehiculului (VIN – numărul de identificare al vehiculului, VRN – numărul de înmatriculare al vehiculului și statul membru de înmatriculare) și caracteristicile vehiculului (w, k, l, dimensiunea pneurilor, reglajele limitatorului de viteză, dacă este cazul, ora UTC din momentul respectiv, valoarea înregistrată de contorul de parcurs în momentul respectiv);

pentru calibrarea unui aparat de înregistrare trebuie folosit un card al atelierului;

(g) **«numărul cardului» înseamnă:**

un cod alfanumeric cu 16 poziții care reprezintă numărul unic de identificare al unui card de tahograf într-un stat membru. Numărul cardului conține un indice secvențial (dacă este cazul), un indice de înlocuire și un indice de reînnoire;

de aceea cardurile pot fi identificate numai pe baza codului statului membru emitent și a numărului cardului;

(h) **«indice secvențial al cardului» înseamnă:**

al 14-lea caracter alfanumeric din numărul cardului folosit pentru a deosebi diferitele carduri emise unei societăți sau unui organism care au dreptul de a li se emite mai multe carduri de tahograf. Societatea sau organismul respectiv sunt identificate în mod unic pe baza primelor 13 caractere ale numărului cardului;

(i) **«indice de reînnoire al cardului» înseamnă:**

al 16-lea caracter alfanumeric din numărul unui card, care este incrementat la fiecare reînnoire a cardului de tahograf;

(j) **«indice de înlocuire al cardului» înseamnă:**

al 15-lea caracter alfanumeric din numărul unui card, care este incrementat la fiecare înlocuire a cardului de tahograf;

(k) **«coeficient caracteristic al vehiculului» înseamnă:**

caracteristica numerică ce exprimă valoarea semnalului de ieșire emis de acea parte a vehiculului care face legătura dintre acesta și aparatul de înregistrare (arborele de ieșire al cutiei de viteze sau osie) când vehiculul parcurge o distanță de un kilometru în condiții de testare standard [vezi capitolul VI (5)]. Coeficientul caracteristic este exprimat în impulsuri pe kilometru ($w = \dots \text{imp/km}$);

(l) **«card al societății» înseamnă:**

un card de tahograf emis de autoritățile unui stat membru proprietarului sau titularului unor vehicule dotate cu aparate de înregistrare;

cardul societății identifică societatea și permite afișarea, descărcarea și tipărirea datelor stocate în aparatul de înregistrare blocat de societatea respectivă;

(m) **«constanta aparatului de înregistrare» înseamnă:**

caracteristica numerică reprezentând valoarea semnalului de intrare necesar pentru a indica și a înregistra o distanță de un kilometru parcursă; această constantă este exprimată în impulsuri pe kilometru ($k = \dots \text{imp/km}$);

(n) **«timp de conducere continuă» este calculat de aparatul de înregistrare astfel ⁽¹⁾:**

timpul de conducere continuă se calculează ca fiind timpii de conducere acumulați la un moment dat de un anumit șofer după încheierea ultimei perioade de minimum 45 de minute de DISPONIBILITATE sau de PAUZĂ/ODIHNĂ sau NECUNOSCUTĂ ⁽²⁾ (o astfel de perioadă poate fi împărțită în mai multe perioade de minimum 15 minute). La efectuarea calculelor în cauză se iau în considerare, după cum este necesar, activitățile anterioare stocate pe cardul șoferului. Dacă șoferul nu a introdus cardul său, calculele se bazează pe înregistrările din memorie corespunzătoare perioadei în curs în timpul căreia nu a fost introdus nici un card în lectorul relevant;

(o) **«card de control» înseamnă:**

un card de tahograf emis de autoritățile unui stat membru autorității naționale de control competente;

cardul de control identifică organismul de control și eventual persoana care răspunde de control și permite accesul la datele stocate în memorie sau pe cardul șoferului în vederea citirii, a tipăririi și/sau a descărcării acestora;

(p) **«durata cumulată a pauzelor» se calculează cu ajutorul aparatului de înregistrare după cum urmează ⁽¹⁾:**

durata cumulată a pauzelor de conducere se calculează ca fiind perioadele de DISPONIBILITATE sau de PAUZĂ/ODIHNĂ sau NECUNOSCUTE ⁽²⁾ de minimum 15 minute pentru un anumit șofer, acumulate după încheierea ultimei sale perioade de DISPONIBILITATE sau de PAUZĂ/ODIHNĂ sau NECUNOSCUTE ⁽²⁾ de minimum 45 de minute (o astfel de perioadă poate fi împărțită în mai multe perioade de minimum 15 minute).

Pentru calculele care trebuie efectuate se iau în considerare, după cum este necesar, activitățile anterioare stocate pe cardul șoferului. Perioadele necunoscute cu durată negativă (începutul perioadei necunoscute > sfârșitul perioadei necunoscute) cauzate de suprapunerile dintre două aparate de înregistrare diferite nu sunt luate în considerare la realizarea acestor calcule.

Dacă șoferul nu a introdus cardul său, calculele necesare se bazează pe înregistrările din memorie pentru perioada în curs în care nu a fost introdus nici un card în lectorul relevant;

(q) **«memorie» înseamnă:**

un dispozitiv de stocare a datelor electronice încorporat în aparatul de înregistrare;

(r) **«semnătură digitală» înseamnă:**

datele atașate unui bloc de informații sau transformarea criptografică a acestuia, permițându-i destinatarului să verifice autenticitatea și integritatea acestui bloc de informații;

(s) **«descărcare» înseamnă:**

copierea, o dată cu semnătura digitală, a unei părți sau a unui set complet de date stocate în memoria vehiculului sau în memoria unui card de tahograf;

descărcarea nu poate provoca în nici un caz modificarea sau ștergerea unor date;

⁽¹⁾ Această modalitate de calculare a timpului de conducere continuă și a duratei cumulate a pauzelor este utilizată de aparatul de înregistrare pentru calcularea avertismentului privind timpul de conducere continuă. Aceasta nu aduce atingere interpretării legale a acestor timpi.

⁽²⁾ Perioadele NECUNOSCUTE corespund perioadelor în care în aparatul de înregistrare nu a fost introdus un card al șoferului și în care nu au fost introduse manual date privind activitățile șoferului.

- (t) **«card al șoferului» înseamnă:**
un card de tahograf emis de autoritățile unui stat membru unui anumit șofer;
cardul șoferului identifică șoferul și permite stocarea datelor privind activitatea șoferului;
- (u) **«circumferință efectivă a pneurilor» înseamnă:**
media distanțelor parcurse de fiecare dintre roțile care pun în mișcare vehiculul (roți motoare) în cadrul unei rotații complete. Măsurarea acestor distanțe se realizează în condiții de testare standard [capitolul VI (5)] și se exprimă ca «l = ... mm». Producătorii de vehicule pot înlocui măsurarea acestor distanțe cu un calcul teoretic care se bazează pe distribuția greutateii pe osii când vehiculul este neîncărcat și în stare normală de funcționare ⁽¹⁾. Metodele pe care se bazează aceste calcule teoretice vor fi aprobate de o autoritate competentă a statului membru;
- (v) **«eveniment» înseamnă:**
operațiune anormală detectată de aparatul de înregistrare și care poate fi provocată de o tentativă de fraudă;
- (w) **«anomalie» înseamnă:**
operațiune anormală detectată de aparatul de înregistrare și care poate fi provocată de un deranjament sau de o defecțiune a aparatului;
- (x) **«instalare» înseamnă:**
montarea aparatului de înregistrare pe un vehicul;
- (y) **«senzor de mișcare» înseamnă:**
o parte a aparatului de înregistrare care furnizează un semnal reprezentativ pentru viteza vehiculului și/sau distanța parcursă;
- (z) **«card nevalabil» înseamnă:**
un card pentru care s-a detectat o anomalie, sau a cărui autentificare inițială a eșuat, sau a cărui dată de început al valabilității nu a fost încă atinsă, sau a cărui dată de expirare a fost depășită;
- (aa) **«în afara domeniului de aplicare» înseamnă:**
că nu este necesară utilizarea aparatului de înregistrare în conformitate cu dispozițiile Regulamentului (CEE) nr. 3820/85 al Consiliului;
- (bb) **«depășirea limitei de viteză» înseamnă:**
depășirea vitezei autorizate a vehiculului, definită ca orice perioadă de peste 60 de secunde pe parcursul căreia viteza măsurată a vehiculului depășește limita stabilită pentru limitatorul de viteză prevăzută în Directiva 92/6/CEE a Consiliului din 10 februarie 1992 privind instalarea și utilizarea limitatoarelor de viteză pentru anumite categorii de autovehicule din Comunitate ⁽²⁾;
- (cc) **«inspecție periodică» înseamnă:**
un set de operațiuni efectuate pentru a verifica dacă aparatul de înregistrare funcționează corespunzător și dacă reglajele acestuia corespund cu parametrii vehiculului;
- (dd) **«imprimantă» înseamnă:**
componenta aparatului de înregistrare cu ajutorul căreia se pot tipări datele stocate;
- (ee) **«aparat de înregistrare» înseamnă:**
întregul echipament destinat instalării pe vehiculele rutiere și care afișează, înregistrează și stochează în mod automat sau semiautomat detalii privind mișcările vehiculului respectiv și anumite perioade de muncă ale șoferilor acestuia;

⁽¹⁾ Directiva 97/27/CE din 22 iulie 1997 privind masele și dimensiunile anumitor categorii de autovehicule și ale remorcilor acestora, modificată prin Directiva 70/156/CEE (JO L 233, 25.8.1997, p. 1).

⁽²⁾ JO L 57, 2.3.1992, p. 27.

(ff) **«reînnoire» înseamnă:**

emiterea unui nou card de tahograf la data expirării cardului existent sau dacă acesta nu funcționează corect și a fost returnat autorității emitente. În cazurile de reînnoire trebuie să existe întotdeauna certitudinea că nu funcționează simultan două carduri valabile;

(gg) **«reparație» înseamnă:**

orice reparație efectuată la un senzor de mișcare sau la o unitate montată pe vehicul care impune deconectarea de la sursa de alimentare cu electricitate sau deconectarea de la alte componente ale aparatului de înregistrare sau deschiderea acestuia;

(hh) **«înlocuire» înseamnă:**

emiterea unui card de tahograf care să înlocuiască un card existent care a fost declarat pierdut, furat sau care nu funcționează corespunzător și care nu a fost returnat autorității emitente. În cazurile de înlocuire există întotdeauna riscul să funcționeze simultan două carduri valabile.

(ii) **«certificare a securității» înseamnă:**

proces prin care un organism de certificare ITSEC ⁽¹⁾ certifică faptul că aparatul de înregistrare (sau o componentă) sau cardul de tahograf investigat îndeplinesc cerințele de securitate definite în apendicele 10 – Obiective generale de securitate;

(jj) **«autotest» înseamnă:**

teste efectuate în mod ciclic și automat de către aparatul de înregistrare pentru a detecta anomalii;

(kk) **«card de tahograf» înseamnă:**

card cu memorie destinat utilizării împreună cu aparatul de înregistrare. Cardurile de tahograf îi permit aparatului de înregistrare să verifice identitatea (sau identitatea de grup) a posesorului cardului și permit transferul și stocarea de date. Cardurile de tahograf pot fi de următoarele tipuri:

- card al șoferului;
- card de control;
- card al atelierului;
- card al societății;

(ll) **«omologare» înseamnă:**

procesul de certificare, de către un stat membru, a faptului că aparatul de înregistrare (sau componenta) sau cardul de tahograf investigate îndeplinesc cerințele prezentului regulament;

(mm) **«dimensiunea pneurilor» înseamnă:**

desemnarea dimensiunilor pneurilor (de la roțile motoare externe) în conformitate cu Directiva 92/23/CEE din 31 martie 1992 ⁽²⁾;

(nn) **«identificarea vehiculului» înseamnă:**

numerele de identificare ale vehiculului: numărul de înmatriculare al vehiculului (VRN), care indică și statul membru de înmatriculare și numărul de identificare al vehiculului (VIN) ⁽³⁾;

(oo) **«unitate montată pe vehicul (UV)» înseamnă:**

aparatul de înregistrare, cu excepția senzorului de mișcare și a cablurilor, cu care este conectat senzorul de mișcare. Unitatea montată pe vehicul poate fi o unitate unică sau poate consta din mai multe unități distribuite în vehicul atât timp cât se respectă cerințele de securitate prevăzute în prezentul regulament;

⁽¹⁾ Recomandarea 95/144/CE a Consiliului din 7 aprilie 1995 privind criteriile comune de evaluare a securității în tehnologia informațiilor (JO L 93, 26.4.1995, p. 27).

⁽²⁾ JO L 129, 14.5.1992, p. 95.

⁽³⁾ Directiva 76/114/CEE din 18 decembrie 1975 privind apropierea legislațiilor statelor membre referitoare la plăcuțele și inscripțiile obligatorii pentru autovehicule și remorcile acestora, precum și amplasarea și metoda de atașare a acestora (JO L 24, 30.1.1976, p. 1).

(pp) **în cadrul calculelor efectuate de aparatul de înregistrare, «săptămână» înseamnă:**

perioada cuprinsă între orele 00.00 UTC luni și 24.00 UTC duminică;

(qq) **«cardul atelierului» înseamnă:**

un card de tahograf emis de autoritățile unui stat membru unui producător de aparate de înregistrare, unei secții de montaj, unui producător de vehicule sau unui atelier de service aprobat de statul membru respectiv;

Cardul atelierului identifică titularul cardului și permite testarea, calibrarea și descărcarea din aparatul de înregistrare.

II. CARACTERISTICI ȘI FUNCȚII GENERALE ALE APARATULUI DE ÎNREGISTRARE

000 Orice vehicul dotat cu aparat de înregistrare și care respectă dispozițiile din prezenta anexă trebuie să conțină un vitezometru și un contor de parcurs. Aceste funcții pot fi incluse în aparatul de înregistrare.

1. Caracteristici generale

Scopul aparatului de înregistrare este acela de a înregistra, stoca, afișa, tipări și genera date privind activitatea șoferului.

001 Aparatul de înregistrare include cabluri, un senzor de mișcare și o unitate montată pe vehicul.

002 Unitatea montată pe vehicul include o unitate de prelucrare, o memorie de date, un ceas care indică timpul real, două periferice de interfață pentru card cu memorie (șofer și copilot), o imprimantă, un afișaj, un avertizor vizual, un conector pentru calibrare/descărcare și dispozitive pentru înregistrarea de date de către utilizator.

Aparatul de înregistrare poate fi conectat la alte dispozitive cu ajutorul unor conectori suplimentari.

003 Inserarea sau conectarea la aparatul de înregistrare a oricărei funcții, aparat sau aparate omologate sau de alt tip nu trebuie să interfereze sau să fie susceptibilă de a interfera cu funcționarea corectă a aparatului de înregistrare ori să încalce sau să fie susceptibilă de a încălca dispozițiile din prezentul regulament.

Utilizatorii aparatului de înregistrare se identifică în fața acestuia prin intermediul cardurilor de tahograf.

004 Aparatul de înregistrare oferă drepturi selective de acces la date și la funcții pe baza tipului și/sau a identității utilizatorilor.

Aparatul de înregistrare înregistrează și stochează date în memoria sa și pe cardurile de tahograf.

Acest lucru se realizează în conformitate cu Directiva 95/46/CE din 24 octombrie 1995 privind protecția persoanelor în ceea ce privește prelucrarea datelor personale și libera circulație a acestui tip de date ⁽¹⁾.

2. Funcții

005 Aparatul de înregistrare asigură următoarele funcții:

- monitorizarea introducerilor și a extragerilor de carduri;
- măsurarea vitezei și a distanței;
- măsurarea timpului;
- monitorizarea activităților șoferului;
- monitorizarea stării șoferului;
- înregistrarea manuală de date de către șofer:
 - înregistrarea locurilor în care încep și/sau se încheie perioadele zilnice de muncă;
 - înregistrarea manuală a activităților șoferului;
 - înregistrarea situațiilor specifice;

⁽¹⁾ JO L 281, 23.11.1995, p. 31.

- gestionarea blocărilor executate de societate;
- monitorizarea activităților de control;
- detectarea unor evenimente și/sau anomalii;
- teste integrate și autoteste;
- citirea din memoria de date;
- înregistrarea și stocarea în memorie;
- citirea de pe carduri de tahograf;
- înregistrarea și stocarea pe carduri de tahograf;
- afișarea;
- tipărirea;
- avertizarea;
- descărcarea de date pe suporturi externe;
- date de ieșire transmise unor dispozitive externe suplimentare;
- calibrarea;
- reglarea orei.

3. Moduri de funcționare

006 Aparatul de înregistrare trebuie să aibă patru moduri de funcționare:

- modul operare;
- modul control;
- modul calibrare;
- modul societate.

007 Aparatul de înregistrare este comutat la următoarele moduri de funcționare pe baza cardurilor valabile de tahograf introduse în perifericele de interfață pentru carduri:

Mod de funcționare		Lector pentru cardul șoferului				
		Nu există card	Card al șoferului	Card de control	Card al atelierului	Card al societății
Lector pentru cardul copilotului	Nu există card	Operare	Operare	Control	Calibrare	Societate
	Card al șoferului	Operare	Operare	Control	Calibrare	Societate
	Card de control	Control	Control	Control (*)	Operare	Operare
	Card al atelierului	Calibrare	Calibrare	Operare	Calibrare (*)	Operare
	Card al societății	Societate	Societate	Operare	Operare	Societate (*)

008 (*) În aceste situații aparatul de înregistrare trebuie să folosească numai cardul de tahograf introdus în lectorul pentru cardul șoferului.

- 009 Aparatul de înregistrare refuză cardurile nevalabile introduse, permițând în astfel de cazuri numai afișarea, tipărirea sau descărcarea datelor stocate pe cardurile expirate.
- 010 Toate funcțiile enumerate la II.2 sunt disponibile în toate modurile de funcționare, cu următoarele excepții:
- funcția calibrare este accesibilă numai în modul calibrare;
 - funcția reglare oră este limitată în alte moduri decât modul calibrare;
 - funcțiile pentru înregistrarea manuală a datelor de către șofer sunt accesibile numai în modurile operare și calibrare;
 - gestionarea blocărilor executate de societate este accesibilă numai în modul societate;
 - funcția de urmărire a activităților de control este accesibilă numai în modul control;
 - funcția descărcare nu este accesibilă în mod operare (cu excepția cazurilor prevăzute în cerința 150).
- 011 Aparatul de înregistrare poate extrage orice date în vederea afișării, tipării sau descărcării pe suporturi externe, cu următoarele excepții:
- în modul operare, orice identificare personală (nume și prenume) care nu corespunde cardului de tahograf introdus este mascată și orice număr de card care nu corespunde cardului de tahograf introdus este mascat parțial (fiecare caracter de pe pozițiile cu număr impar – de la stânga la dreapta – este mascat).
 - în modul societate, datele privind șoferul (cerințele 081, 084 și 087) pot fi extrase numai pentru perioadele care nu au fost blocate de o altă societate (identificată pe baza primelor 13 caractere din numărul cardului societății).
 - dacă în aparatul de înregistrare nu a fost introdus nici un card, nu pot fi extrase date privind șoferul decât pentru ziua respectivă și pentru cele opt zile calendaristice anterioare zilei respective.

4. Securitate

Scopul sistemului de securitate este acela de a proteja memoria astfel încât să împiedice accesul neautorizat și manipularea datelor și de a detecta astfel de tentative, protejând integritatea și autenticitatea datelor transmise între senzorul de mișcare și unitatea montată pe vehicul, precum și a datelor transmise între aparatul de înregistrare și cardurile de tahograf și verificând integritatea și autenticitatea datelor descărcate.

- 012 Pentru a asigura securitatea sistemului, aparatul de înregistrare trebuie să respecte cerințele de securitate prevăzute în obiectivele pentru senzorul de mișcare și obiectivele generale de securitate prevăzute pentru unitatea montată pe vehicul (apendicele 10).

III. CERINȚE DE CONSTRUCȚIE ȘI DE FUNCȚIONARE PENTRU APARATUL DE ÎNREGISTRARE

1. Monitorizarea introducerii și retragerii cardurilor

- 013 Aparatul de înregistrare monitorizează perifericele de interfață pentru card pentru a depista introducerile și retragerile de carduri.
- 014 La introducerea unui card, aparatul de înregistrare detectează valabilitatea cardului de tahograf introdus, iar dacă este valabil identifică tipul cardului.
- 015 Aparatul de înregistrare trebuie proiectat astfel încât cardurile de tahograf să fie blocate în poziția corectă în perifericul de interfață pentru carduri.
- 016 Retragera cardurilor de tahograf este posibilă numai după oprirea vehiculului și după stocarea datelor relevante pe carduri. Retragera cardului se poate realiza numai prin acțiune pozitivă a utilizatorului.

2. Măsurarea vitezei și a distanței

- 017 Această funcție asigură măsurarea continuă și poate furniza valorile înregistrate de contorul de parcurs care corespund distanței totale parcurse de vehicul.
- 018 Această funcție asigură măsurarea continuă și poate furniza viteza vehiculului.

- 019 Funcția de măsurare a vitezei indică și dacă vehiculul se deplasează sau este oprit. Se consideră că vehiculul se deplasează în momentul în care funcția detectează o valoare mai mare de 1 imp/sec de la senzorul de mișcare timp de cel puțin cinci secunde, în caz contrar vehiculul fiind considerat oprit.

Dispozitivele pentru afișarea vitezei (vitezometru) și a distanței totale parcurse (contor de parcurs) instalate pe orice vehicul prevăzut cu un aparat de înregistrare care respectă dispozițiile din prezentul regulament trebuie să respecte cerințele privind limitele maxime de toleranță prevăzute în prezenta anexă (capitolul III punctul 2.1. și 2.2.).

2.1. Măsurarea distanței parcurse

- 020 Măsurarea distanței parcurse se poate realiza fie:
- cumulând atât mișcările de mers înainte, cât și pe cele de mers înapoi;
 - cumulând numai mișcările de mers înainte.
- 021 Aparatul de înregistrare măsoară distanțele parcurse între 0 și 9 999 999,9 km.
- 022 Distanța măsurată respectă următoarele limite de toleranță (distanța fiind de cel puțin 1 000 m):
- $\pm 1\%$ înainte de instalare;
 - $\pm 2\%$ la instalare și la inspecțiile periodice;
 - $\pm 4\%$ în timpul funcționării.
- 023 Distanța măsurată trebuie să aibă o rezoluție de 0,1 km sau mai bună.

2.2. Măsurarea vitezei

- 024 Aparatul de înregistrare măsoară viteze între 0 și 220 km/h.
- 025 Pentru a asigura o toleranță maximă de ± 6 km/h pentru viteza afișată în timpul funcționării și luând în considerare:
- o toleranță de ± 2 km/h pentru variațiile semnalului de intrare (variații provocate de pneuri etc.);
 - o toleranță de ± 1 km/h la măsurătorile efectuate în timpul instalării sau al inspecțiilor periodice,
- aparatul de înregistrare trebuie să măsoare viteza cu o toleranță de ± 1 km/h (la viteză constantă) dacă vitezele se încadrează între 20 și 180 km/h, iar coeficienții vehiculului între 4 000 și 25 000 imp/km.
- Notă: Datorită rezoluției stocării de date, se adaugă o toleranță suplimentară de $\pm 0,5$ km/h pentru vitezele stocate de aparatul de înregistrare.
- 025a Viteza trebuie măsurată corect, în limitele normale de toleranță, în cele 2 secunde de după finalizarea unei modificări a vitezei dacă viteza se modifică într-un ritm de până la 2 m/s^2 .
- 026 Măsurarea vitezei trebuie să aibă o rezoluție de 1 km/h sau mai bună.

3. Măsurarea timpului

- 027 Funcția de măsurare a timpului trebuie să asigure măsurarea continuă și digitală a datei și a orei UTC.
- 028 Aparatul de măsurat folosește întotdeauna pentru datare ora și data UTC (pentru înregistrări, imprimări, schimburi de date, afișare etc.).
- 029 Pentru afișarea orei locale este posibilă corectarea treptată a decalajului orar al orei afișate, la intervale de o jumătate de oră.
- 030 Abaterea de timp nu trebuie să depășească ± 2 secunde pe zi în condiții de omologare.
- 031 Rezoluția cu care este măsurat timpul trebuie să fie egală cu o secundă sau mai bună.
- 032 Măsurarea timpului nu trebuie să fie afectată de o întrerupere a alimentării cu energie electrică din exterior a cărei durată este mai mică de 12 luni în condiții de omologare.

4. Monitorizarea activităților șoferului

- 033 Această funcție monitorizează permanent și separat activitățile unui șofer și ale unui copilot.
- 034 Activitățile șoferului sunt CONDUCERE, MUNCĂ, DISPONIBILITATE sau PAUZĂ/ODIHNĂ.
- 035 Pilotul și/sau copilotul pot selecta manual MUNCĂ, DISPONIBILITATE sau PAUZĂ/ODIHNĂ.
- 036 Când vehiculul este în mișcare, se selectează automat activitatea CONDUCERE pentru șofer și DISPONIBILITATE pentru copilot.
- 037 Când vehiculul se oprește, pentru șofer se selectează automat MUNCĂ.
- 038 Se presupune că prima modificare a activității în termen de 120 de secunde de la selectarea automată a activității MUNCĂ din cauza opririi vehiculului s-a produs în momentul în care vehiculul s-a oprit (fiind astfel posibilă anularea modificării în MUNCĂ).
- 039 Această funcție transmite modificările activităților către funcțiile de înregistrare cu o rezoluție de un minut.
- 040 Dacă pe parcursul unui minut s-a petrecut o activitate de CONDUCERE, minutul calendaristic respectiv va fi considerat în întregime activitate de CONDUCERE.
- 041 Dacă o activitate de CONDUCERE survine atât în minutul anterior, cât și în minutul care precede orice minut calendaristic, minutul respectiv va fi considerat în întregime activitate de CONDUCERE.
- 042 Dacă un minut calendaristic oarecare nu este considerat minut de CONDUCERE conform cerințelor anterioare, întregul minut este considerat ca aparținând aceluși tip de activitate care reprezintă cea mai lungă activitate continuă derulată în minutul respectiv (sau cea mai recentă activitate în cazul unor activități cu durată egală).
- 043 Această funcție permite, de asemenea, monitorizarea constantă a timpului de conducere continuă și durata cumulată a pauzelor șoferului.

5. Monitorizarea stării șoferului

- 044 Această funcție monitorizează permanent și automat starea șoferului.
- 045 Când în aparat sunt introduse două carduri de șofer valabile, este selectat modul de conducere ECHIPAJ, iar în toate celelalte cazuri trebuie selectat modul SINGUR.

6. Înregistrări manuale realizate de șoferi

6.1. Înregistrarea locurilor în care încep și/sau se încheie perioadele zilnice de muncă

- 046 Această funcție permite înregistrarea locurilor în care încep și/sau se încheie perioadele zilnice de muncă ale șoferului și/sau ale copilotului.
- 047 Locurile sunt definite ca țări sau, dacă este cazul, ca țară și regiune.
- 048 În momentul retragerii unui card al șoferului (sau al atelierului), aparatul de înregistrare îi solicită șoferului/copilotului să introducă «locul în care se încheie perioada zilnică de muncă».
- 049 Aparatul de înregistrare trebuie să permită ignorarea acestei solicitări.
- 050 Înregistrarea locurilor în care perioadele de muncă încep și/sau se încheie trebuie să fie posibilă și în absența cardului sau în alte momente decât introducerea sau retragerea cardului.

6.2. Înregistrarea manuală a activităților șoferului

- 050a Exclusiv în momentul introducerii cardului șoferului (sau al atelierului), aparatul de înregistrare:
- îi reamintește titularului cardului data și ora ultimei retrageri a cardului
 - și
 - îi solicită titularului cardului să precizeze dacă introducerea respectivă a cardului reprezintă o continuare a perioadei zilnice de muncă în curs.

Aparatul de înregistrare îi permite titularului cardului să ignore întrebarea, fără a răspunde, sau să răspundă pozitiv, sau să răspundă negativ:

- dacă titularul cardului ignoră întrebarea, aparatul de înregistrare solicită «locul în care începe perioada zilnică de muncă». Aparatul de înregistrare permite ignorarea acestei solicitări. Dacă se introduce un loc, acesta este înregistrat în memorie și pe cardul de tahograf, fiind asociat momentului introducerii cardului.
- în cazul unui răspuns negativ sau pozitiv, aparatul de înregistrare îl invită pe titularul cardului să introducă activitățile manual, împreună cu datele și orele de început și de sfârșit ale acestora, fiind posibile numai activitățile MUNCĂ, DISPONIBILITATE sau PAUZĂ/ODIHNĂ, și numai în perioada cuprinsă între ultima retragere a cardului și introducerea cardului din momentul respectiv, fără a fi permise suprapuneri ale acestor activități. Procedurile aplicabile în acest caz sunt următoarele:
- dacă titularul cardului răspunde pozitiv la întrebare, aparatul de înregistrare îl invită să introducă manual, în ordine cronologică, activitățile din perioada dintre ultima retragere a cardului și introducerea cardului din momentul respectiv. Procesul se încheie în momentul în care ora unei activități introduse manual este aceeași cu ora introducerii cardului.
- în cazul în care titularul cardului răspunde negativ la întrebare, aparatul de înregistrare:
- îl invită pe titularul cardului să introducă manual, în ordine cronologică, activitățile desfășurate din momentul retragerii cardului până la sfârșitul perioadei zilnice de muncă corespondente (sau al activităților legate de vehiculul respectiv în cazul în care perioada zilnică de muncă continuă pe o foaie de înregistrare). De aceea, înainte ca aparatul de înregistrare să îi permită titularului cardului să introducă manual fiecare activitate, acesta trebuie să îi solicite titularului cardului să specifice dacă ora de încheiere a ultimei activități înregistrate reprezintă sfârșitul unei perioade anterioare de muncă (vezi nota de mai jos).

Notă: dacă titularul cardului nu precizează când s-a încheiat perioada anterioară de muncă și introduce manual o activitate a cărei oră de încheiere este egală cu cea a introducerii cardului, aparatul de înregistrare:

- presupune că perioada zilnică de muncă s-a încheiat la începutul primei perioade de ODIHNĂ (sau care rămâne ca NECUNOSCUȚĂ) de după retragerea cardului sau în momentul retragerii cardului dacă nu a fost introdusă nici o perioadă de odihnă (și dacă nici o perioadă nu rămâne NECUNOSCUȚĂ);
- presupune că ora inițială (vezi în continuare) este ora introducerii cardului;
- parcurge etapele descrise în continuare;
- în continuare, dacă ora de încheiere a perioadei de muncă respective este diferită de ora retragerii cardului sau dacă în momentul respectiv nu a fost introdus un loc de încheiere a perioadei de muncă respective, îi solicită titularului cardului să «confirme sau să introducă locul în care s-a încheiat perioada zilnică de muncă» (aparatul de înregistrare permite ignorarea acestei solicitări). Dacă se introduce un loc, acesta este înregistrat pe cardul de tahograf numai și numai dacă este diferit de cel introdus la retragerea cardului (în cazul în care a fost introdus un card), și este asociat cu ora de încheiere a perioadei de muncă;
- în continuare titularul cardului este invitat să «introducă o oră de începere» a perioadei zilnice de muncă curente (sau a activităților legate de vehiculul respectiv în cazul în care titularul cardului a folosit anterior o foaie de înregistrare pe parcursul acestei perioade) și i se solicită «locul de muncă în care începe perioada zilnică de muncă» (aparatul de înregistrare permite ignorarea acestei solicitări). Dacă este introdus un loc, acesta este înregistrat pe cardul de tahograf și asociat cu această oră de începere. Dacă ora începerii este ora introducerii cardului, locul va fi de asemenea înregistrat în memorie;
- în continuare, dacă această oră a începerii diferă de ora de introducere a cardului, aparatul îl invită pe titularul cardului să introducă manual, în ordine cronologică, activitățile desfășurate de la ora începerii până la ora introducerii cardului. Procesul se încheie în momentul în care ora de sfârșit a unei activități introduse manual este egală cu ora introducerii cardului;
- în continuare aparatul de înregistrare îi permite titularului cardului să modifice orice activitate introdusă manual, până în momentul validării prin selectarea unei comenzi specifice, iar apoi nu mai permite nici o modificare;
- dacă acest tip de răspunsuri la întrebarea inițială nu sunt urmate de introducerea de activități, aparatul de înregistrare consideră că titularul cardului a ignorat întrebarea.

Pe parcursul întregului proces descris anterior, aparatul de înregistrare permite numai următoarele perioade de așteptare până la introducerea datelor:

- timp de un minut, dacă nu se produce nici o interacțiune cu interfața om/mașină a aparatului (cu emiterea unui avertisment vizual și eventual auditiv după 30 de secunde);

sau

- dacă este retras cardul sau dacă este introdus un alt card al șoferului (sau al atelierului);

sau

- imediat ce vehiculul începe să se miște,

și în aceste cazuri aparatul de înregistrare validează orice date deja introduse.

6.3. Înregistrarea situațiilor speciale

050b Aparatul de înregistrare îi permite șoferului să introducă, în timp real, următoarele două condiții speciale:

- «ÎN AFARA DOMENIULUI DE APLICARE» (început, sfârșit)
- «TRASEU PARCURS PE FERIBOT/ÎN TREN»

Nu poate exista un «TRASEU PARCURS PE FERIBOT/ÎN TREN» dacă a fost deschisă o condiție de tip «ÎN AFARA DOMENIULUI DE APLICARE».

O condiție de tip «ÎN AFARA DOMENIULUI DE APLICARE» deschisă trebuie închisă în mod automat de către aparatul de înregistrare dacă se introduce sau se retrage un card al șoferului.

7. Gestionarea blocărilor efectuate de societate

- 051 Această funcție permite gestionarea blocărilor efectuate de o societate pentru a-și asigura accesul exclusiv la date în modul societate.
- 052 Blocările efectuate de societate constau dintr-o dată și o oră de începere (blocare) și dintr-o dată și o oră de sfârșit (deblocare) asociate identificării societății pe baza numărului cardului societății (la blocare).
- 053 O blocare poate fi «activată» sau «dezactivată» numai în timp real.
- 054 Deblocarea poate fi efectuată numai de societatea a cărei blocare este «activă» (conform identificării pe baza primelor 13 caractere din numărul cardului societății)
- sau
- 055 Deblocarea este automată dacă o altă societate efectuează o blocare.
- 055a Dacă o societate efectuează o blocare, iar blocarea anterioară a fost efectuată de aceeași societate, se consideră că blocarea anterioară nu a fost «dezactivată» și este încă «activă».

8. Monitorizarea activităților de control

- 056 Această funcție urmărește AFIȘAREA, TIPĂRIREA și DESCĂRCAREA activităților din UV și de pe card realizate în modul control.
- 057 Această funcție urmărește și activitățile de CONTROL AL DEPĂȘIRILOR DE VITEZĂ în modul control. Se consideră că a avut loc un control al depășirii de viteză dacă în modul control a fost transmis un mesaj «depășire de viteză» spre imprimantă sau pe ecran sau dacă au fost descărcate din memoria UV «evenimente sau anomalii».

9. Detectarea evenimentelor și/sau a anomaliilor

- 058 Această funcție detectează următoarele evenimente și/sau anomalii:

9.1. Eveniment «introducerea unui card nevalabil»

- 059 Acest eveniment este declanșat de introducerea oricărui card nevalabil și/sau la expirarea unui card valabil introdus.

9.2. **Eveniment «conflict card»**

060 Acest eveniment este declanșat la producerea oricăreia dintre combinațiile de carduri valabile notate cu X:

Conflict card		Lector pentru cardul șoferului				
		Nu există card	Card al șoferului	Card de control	Card al atelierului	Card al societății
Lector pentru cardul copilotului	Nu există card					
	Card al șoferului				X	
	Card de control			X	X	X
	Card al atelierului		X	X	X	X
	Card al societății			X	X	X

9.3. **Eveniment «suprapunerea unor intervale de timp»**

061 Acest eveniment este declanșat dacă ora/data ultimei retrageri a cardului șoferului, așa cum este citită de pe card, a survenit după data/ora din momentul respectiv înregistrată de aparatul de înregistrare în care este introdus cardul.

9.4. **Eveniment «conducere fără card corespunzător»**

062 Acest eveniment este declanșat de oricare dintre combinațiile de carduri de tahograf notate cu X din tabelul următor, atunci când activitatea șoferului este schimbată în CONDUCERE sau când intervine o schimbare a modului de funcționare în timp ce activitatea șoferului este CONDUCERE:

Conducere fără un card adecvat		Lector pentru cardul șoferului				
		Nu există card (sau cardul nu este valabil)	Card al șoferului	Card de control	Card al atelierului	Card al societății
Lector pentru cardul copilotului	Nu există card (sau cardul nu este valabil)	X		X		X
	Card al șoferului	X		X	X	X
	Card de control	X	X	X	X	X
	Card al atelierului	X	X	X		X
	Card al societății	X	X	X	X	X

9.5. **Eveniment «introducere card în timpul conducerii»**

063 Acest eveniment este declanșat la introducerea unui card de tahograf în orice lector dacă activitatea șoferului este CONDUCERE.

9.6. **Eveniment «încheiere incorectă a ultimei sesiuni»**

064 Acest eveniment este declanșat dacă la introducerea cardului aparatul de înregistrare detectează faptul că, în ciuda dispozițiilor din capitolul III alineatul (1), sesiunea anterioară nu a fost corect încheiată (cardul a fost retras înainte ca toate datele relevante să poată fi stocate pe acesta). Acest eveniment este declanșat numai de cardul șoferului și al atelierului.

9.7. **Eveniment «depășire de viteză»**

065 Acest eveniment este declanșat pentru fiecare depășire de viteză.

9.8. Eveniment «întrerupere a alimentării cu energie electrică»

- 066 Acest eveniment este declanșat, în celelalte moduri decât modul calibrare, în cazul oricărei întreruperi a alimentării cu energie electrică a senzorului de mișcare și/sau a unității montate pe vehicul care durează mai mult de 200 milisecunde. Pragul de întrerupere este stabilit de producător. Scăderea nivelului de energie produsă de pornirea motorului nu declanșează acest eveniment.

9.9. Eveniment «eroare la datele de mișcare»

- 067 Acest eveniment este declanșat în cazul întreruperii fluxului normal de date dintre senzorul de mișcare și unitatea montată pe vehicul și/sau în cazul unor erori de integritate sau de autentificare a datelor survenite în timpul schimbului de date dintre senzorul de mișcare și unitatea montată pe vehicul.

9.10. Eveniment «tentativă de violare a securității»

- 068 Acest eveniment este declanșat, în celelalte moduri decât modul calibrare, în cazul survenirii oricărui alt eveniment care afectează securitatea senzorului de mișcare și/sau a unității montate pe vehicul după cum indică obiectivele generale de securitate pentru aceste componente.

9.11. Anomalie «card»

- 069 Această anomalie este declanșată în cazul survenirii unei anomalii la un card de tahograf pe parcursul funcționării.

9.12. Anomalie «aparat de înregistrare»

- 070 Această anomalie este declanșată în cazul survenirii oricăreia dintre următoarele anomalii în celelalte moduri decât modul calibrare:

- anomalie internă UV;
- anomalie imprimantă;
- anomalie afișaj;
- anomalie descărcare;
- anomalie senzor.

10. Teste integrate și autoteste

- 071 Aparatul de înregistrare detectează el însuși anomaliile prin autoteste și teste integrate, după cum se arată în tabelul următor:

Elementul care trebuie testat	Autotest	Test integrat
Software		Integritate
Memorie	Acces	Acces, integritate a datelor
Periferece de interfață pentru carduri	Acces	Acces
Tastatură		Verificare manuală
Imprimantă	(la latitudinea producătorului)	Tipărire
Afișaj		Inspecție vizuală
Descărcare (se efectuează numai în timpul descărcărilor)	Funcționare corespunzătoare	
Senzor	Funcționare corespunzătoare	Funcționare corespunzătoare

11. Citirea din memorie

- 072 Aparatul de înregistrare trebuie să poată citi orice date stocate în memoria sa.

12. Înregistrarea și stocarea în memorie

În sensul prezentului paragraf,

- «365 de zile» înseamnă 365 de zile calendaristice de activitate medie a șoferilor pe un vehicul. Activitatea medie pe zi pe un vehicul implică cel puțin șase șoferi sau copiloți, șase cicluri de introducere și retragere de carduri și 256 de schimbări de activitate. Astfel, «365 de zile» implică cel puțin 2 190 de șoferi/copiloți, 2 190 de cicluri de introducere și retragere de carduri și 93 440 de schimbări de activitate;
- orele sunt înregistrate cu o rezoluție de un minut, cu excepția cazurilor în care se precizează altceva;
- valorile contorului de parcurs sunt înregistrate cu o rezoluție de un kilometru;
- vitezele sunt înregistrate cu o rezoluție de 1 km/h.

073 Datele stocate în memorie nu sunt afectate de întreruperile alimentării cu energie electrică din exterior care durează mai puțin de douăsprezece luni în condiții de omologare.

074 Aparatul de înregistrare poate înregistra și stoca implicit sau explicit în memoria sa următoarele:

12.1. Date de identificare a aparatului

12.1.1. Date de identificare a unității montate pe vehicul

075 Aparatul de înregistrare trebuie să poată stoca în memoria sa următoarele date de identificare a unității montate pe vehicul:

- numele producătorului;
- adresa producătorului;
- numărul de componentă;
- numărul de serie;
- numărul versiunii de software;
- data de instalare a versiunii de software;
- anul în care a fost produs aparatul;
- numărul de omologare.

076 Datele de identificare a unității montate pe vehicul sunt înregistrate și stocate definitiv de producătorul unității montate pe vehicul, cu excepția datelor privind software-ul și a numărului de omologare care pot fi modificate în cazul modernizării software-ului.

12.1.2. Date de identificare a senzorului de mișcare

077 Senzorul de mișcare trebuie să poată stoca în memoria sa următoarele date de identificare:

- numele producătorului;
- numărul de componentă;
- numărul de serie;
- numărul de omologare;
- identificatorul componentei integrate de securitate (de exemplu numărul de componentă al microprocesorului/procesorului intern);
- identificatorul sistemului de operare (de exemplu numărul versiunii de software).

078 Datele de identificare ale senzorului de mișcare sunt înregistrate și stocate definitiv în senzorul de mișcare de producătorul acestuia.

079 Unitatea montată pe vehicul trebuie să poată înregistra și stoca în memoria sa următoarele date de identificare ale senzorului de mișcare la care este conectată:

- numărul de serie;
- numărul de omologare;
- data primei cuplări.

12.2. *Elemente de securitate*

080 Aparatul de înregistrare trebuie să poată stoca următoarele elemente de securitate:

- cheia publică europeană;
- certificatul statului membru;
- certificatul aparatului;
- cheia privată a aparatului.

Elementele de securitate ale aparatului de înregistrare sunt incluse în aparat de către producătorul unității montate pe vehicul.

12.3. *Date privind introducerea și retragerea cardului șoferului*

081 Pentru fiecare ciclu de introducere și retragere a unui card al șoferului sau al atelierului, aparatul înregistrează și stochează în memoria sa următoarele:

- numele și prenumele titularului cardului așa cum sunt stocate pe card;
- numărul cardului, statul membru emitent și data de expirare, așa cum sunt stocate pe card;
- ora și data introducerii cardului;
- valoarea contorului de parcurs în momentul introducerii cardului;
- lectorul în care este introdus cardul;
- ora și data retragerii cardului;
- valoarea contorului de parcurs al vehiculului la retragerea cardului;
- următoarele informații privind vehiculul folosit anterior de șofer, așa cum sunt stocate pe card:
 - numărul și statul membru de înmatriculare;
 - data și ora retragerii cardului;
- un cod care indică dacă, la introducerea cardului, titularul acestuia a introdus manual activități sau nu.

082 Memoria trebuie să poată stoca aceste date timp de cel puțin 365 de zile.

083 La epuizarea capacității de stocare, datele noi înlocuiesc datele cele mai vechi.

12.4. Date privind activitatea șoferului

084 Aparatul de înregistrare înregistrează și stochează în memoria sa următoarele informații de fiecare dată când survine o modificare a activității șoferului și/sau a copilotului și/sau de fiecare dată când se modifică modul de conducere și/sau de fiecare dată când se introduce sau se retrage un card al șoferului sau al atelierului:

- modul de conducere (ECHIPA, SINGUR);
- lectorul (PILOT, COPILOT);
- starea cardului în lectorul relevant (INTRODUS, NEINTRODUS) (vezi nota);
- activitatea (CONDUCERE, DISPONIBILITATE, MUNCĂ, PAUZĂ/ODIHNĂ);
- data și ora modificării.

Notă: INTRODUS înseamnă că în lector este introdus un card valabil al șoferului sau al atelierului. NEINTRODUS înseamnă opusul, adică în lector nu este introdus un card valabil al șoferului sau al atelierului (de exemplu este introdus un card al societății sau nu este introdus nici un card).

Notă: Datele privind activitatea introduse manual de un șofer nu sunt înregistrate în memorie.

085 Memoria trebuie să poată stoca datele privind activitatea șoferului timp de cel puțin 365 de zile.

086 La epuizarea capacității de stocare, datele noi înlocuiesc datele cele mai vechi.

12.5. Locurile în care încep și/sau se încheie perioadele zilnice de muncă

087 Aparatul de înregistrare înregistrează și stochează în memoria sa următoarele informații atunci când un pilot/copilot ajunge în locul în care începe și/sau se încheie o perioadă zilnică de muncă:

- dacă este cazul, numărul cardului șoferului/copilotului și statul membru emitent;
- data și ora înregistrării datelor (sau ora/data legate de înregistrarea datelor dacă aceasta este efectuată în cadrul procedurii de introducere manuală a datelor);
- tipul datelor înregistrate (de început sau de sfârșit, situația înregistrării);
- țara și regiunea introdusă;
- valoarea contorului de parcurs al vehiculului.

088 Memoria trebuie să poată stoca datele privind începutul și/sau sfârșitul perioadelor zilnice de muncă timp de cel puțin 365 de zile (presupunând că un șofer face două înregistrări pe zi).

089 La epuizarea capacității de stocare, datele noi înlocuiesc datele cele mai vechi.

12.6. Date înregistrate de contorul de parcurs

090 Aparatul de înregistrare înregistrează în memoria sa valoarea contorului de parcurs al vehiculului și data respectivă la ora 00.00 a fiecărei zile calendaristice.

091 Memoria trebuie să poată stoca valorile contorului de parcurs de la ora 00.00 timp de cel puțin 365 de zile calendaristice.

092 La epuizarea capacității de stocare, datele noi înlocuiesc datele cele mai vechi.

12.7. Date detaliate privind viteza

093 Aparatul de înregistrare înregistrează și stochează în memorie viteza instantanee a vehiculului și data și ora corespunzătoare în fiecare secundă cel puțin pe parcursul ultimelor 24 de ore în care vehiculul a fost în mișcare.

12.8. Date privind evenimentele

În sensul prezentului paragraf, timpul este înregistrat cu o rezoluție de o secundă.

094

Aparatul de înregistrare înregistrează și stochează în memoria sa următoarele date pentru fiecare eveniment detectat, conform următoarelor reguli de stocare:

Eveniment	Reguli de stocare	Date care trebuie înregistrate pentru fiecare eveniment
Conflict card	— cele mai recente 10 evenimente.	— data și ora începerii evenimentului; — data și ora sfârșitului evenimentului; — tipul, numărul și statul membru emitent al celor două carduri care au generat conflictul.
Conducere fără un card adecvat	— evenimentul care a durat cel mai mult în fiecare din ultimele 10 zile în care acesta s-a produs; — cele mai lungi cinci evenimente care au survenit pe parcursul ultimelor 365 de zile	— data și ora începerii evenimentului; — data și ora sfârșitului evenimentului; — tipul, numărul și statul membru emitent al oricărui card introdus la începutul și/sau la sfârșitul evenimentului; — numărul de evenimente similare produse în ziua respectivă.
Introducerea cardului în timpul condusului	— ultimul eveniment survenit în fiecare dintre ultimele 10 zile în care acestea s-au produs.	— data și ora evenimentului; — tipul, numărul și statul membru emitent al cardului; — numărul de evenimente similare produse în ziua respectivă.
Încheiere incorectă a ultimei sesiuni	— cele mai recente 10 evenimente.	— data și ora introducerii cardului; — tipul, numărul și statul membru emitent al cardului; — datele din ultima sesiune așa cum au fost citite de pe card: — data și ora introducerii cardului; — numărul și statul membru de înmatriculare.
Depășire de viteză ⁽¹⁾	— cel mai grav eveniment survenit în fiecare din ultimele 10 zile în care acesta s-a produs (adică cel în care s-a înregistrat cea mai mare viteză medie); — cele mai grave cinci evenimente survenite în ultimele 365 de zile; — primul eveniment survenit după ultima calibrare.	— data și ora începerii evenimentului; — data și ora sfârșitului evenimentului; — viteza maximă măsurată pe parcursul evenimentului; — media aritmetică a vitezei măsurate în timpul evenimentului; — tipul, numărul și statul membru emitent al cardului șoferului (dacă este posibil); — numărul de evenimente similare produse în ziua respectivă.

⁽¹⁾ Aparatul de înregistrare trebuie de asemenea să înregistreze și să stocheze în memoria sa:

- data și ora ultimului CONTROL AL DEPĂȘIRILOR DE VITEZĂ;
- data și ora primei depășiri de viteză survenite după acest CONTROL AL DEPĂȘIRILOR DE VITEZĂ;
- numărul evenimentelor de depășire de viteză survenite după ultimul CONTROL AL DEPĂȘIRILOR DE VITEZĂ.

Eveniment	Reguli de stocare	Date care trebuie înregistrate pentru fiecare eveniment
Înteruperea alimentării cu energie electrică ⁽¹⁾	— evenimentul care a durat cel mai mult în fiecare din ultimele 10 zile în care s-a produs; — cele mai lungi cinci evenimente care au survenit pe parcursul ultimelor 365 de zile.	— data și ora începerii evenimentului; — data și ora sfârșitului evenimentului; — tipul, numărul și statul membru emitent al oricărui card introdus la începutul și/sau la sfârșitul evenimentului; — numărul de evenimente similare produse în ziua respectivă.
Eroare a datelor de mișcare	— evenimentul care a durat cel mai mult în fiecare din ultimele 10 zile în care s-a produs; — cele mai lungi cinci evenimente care au survenit pe parcursul ultimelor 365 de zile.	— data și ora începerii evenimentului; — data și ora sfârșitului evenimentului; — tipul, numărul și statul membru emitent al oricărui card introdus la începutul și/sau la sfârșitul evenimentului; — numărul de evenimente similare produse în ziua respectivă.
Tentativă de violare a securității	— cele mai recente 10 evenimente, pe tipuri de evenimente.	— data și ora începerii evenimentului; — data și ora sfârșitului evenimentului (dacă sunt relevante); — tipul, numărul și statul membru emitent al oricăruia dintre cele două carduri introduse la începutul și/sau la sfârșitul evenimentului; — tipul evenimentului.

095 ⁽¹⁾ Aceste date pot fi înregistrate numai după reconectarea la sursa de alimentare cu energie, iar orele pot fi cunoscute cu o precizie de un minut.

12.9. *Date privind anomaliile*

În sensul prezentului paragraf, timpul este înregistrat cu o rezoluție de o secundă.

096 Aparatul de înregistrare încearcă să înregistreze și să stocheze în memoria sa de date următoarele date pentru fiecare anomalie detectată pe baza următoarelor reguli de stocare:

Anomalie	Reguli de stocare	Date care trebuie înregistrate pentru fiecare anomalie
Anomalie a cardului	— cele mai recente 10 anomalii ale cardului șoferului.	— data și ora începerii anomaliei; — data și ora sfârșitului anomaliei; — tipul, numărul și statul membru emitent al cardului.
Anomalii ale aparatului de înregistrare	— cele mai recente 10 anomalii pentru fiecare tip de anomalie; — prima anomalie survenită după ultima calibrare.	— data și ora începerii anomaliei; — data și ora sfârșitului anomaliei; — tipul de anomalie; — tipul, numărul și statul membru emitent al oricărui card introdus la începutul și/sau la sfârșitul anomaliei.

12.10. Date privind calibrarea

- 097 Aparatul de înregistrare trebuie să înregistreze în memoria sa următoarele date relevante privind:
- parametrii de calibrare cunoscuți în momentul activării;
 - prima calibrare de după activare;
 - prima calibrare de după instalarea pe vehiculul respectiv (identificat pe baza numărului său de identificare);
 - cele mai recente cinci calibrări (dacă pe parcursul unei zile calendaristice au fost efectuate mai multe calibrări, nu este stocată decât ultima calibrare efectuată în ziua respectivă).
- 098 Pentru fiecare dintre aceste calibrări, se înregistrează următoarele date:
- scopul calibrării (activare, prima instalare, instalare, inspecție periodică);
 - numele și adresa atelierului;
 - numărul cardului atelierului, statul membru emitent al cardului și data de expirare a cardului;
 - identificarea vehiculului;
 - parametrii actualizați sau confirmați: w, k, l, dimensiunea pneurilor, reglajul limitatorului de viteză, contorul de parcurs (valorile vechi și cele noi), data și ora (valorile vechi și cele noi).
- 099 Senzorul de mișcare înregistrează și stochează în memoria sa următoarele date privind instalarea senzorului de mișcare:
- prima cuplare cu o UV (data, ora, numărul de omologare, numărul de serie al UV);
 - ultima cuplare cu o UV (data, ora, numărul de omologare, numărul de serie al UV).

12.11. Date privind reglarea orei

- 100 Aparatul de înregistrare înregistrează și stochează în memoria sa următoarele date relevante privind:
- cea mai recentă reglare a orei;
 - cele mai importante cinci reglări ale orei de la ultima calibrare,
- realizate în modul calibrare, dar nu în cadrul unei calibrări obișnuite [definiția (f)].
- 101 Pentru fiecare dintre aceste reglări ale orei sunt înregistrate următoarele date:
- data și ora, valoarea veche;
 - data și ora, valoarea nouă;
 - numele și adresa atelierului;
 - numărul cardului atelierului, statul membru emitent al cardului și data expirării cardului.

12.12. Date privind activitățile de control

- 102 Aparatul de înregistrare înregistrează și stochează în memorie următoarele date pentru cele mai recente 20 de activități de control:
- data și ora controlului;
 - numărul cardului de control și statul membru emitent al cardului;
 - tipul controlului (afișaj și/sau tipărire și/sau descărcare din UV și/sau descărcare de pe card).

- 103 Pentru descărcări se înregistrează și datele pentru cea mai îndepărtată și cea mai recentă zi care au fost descărcate.

12.13. Date privind blocările executate de societate

- 104 Aparatul de înregistrare înregistrează și stochează în memoria sa următoarele date pentru cele mai recente 20 de blocări efectuate de societate:

- data și ora blocării;
- data și ora deblocării;
- numărul cardului societății și statul membru emitent al cardului;
- numele și adresa societății.

12.14. Date privind activitățile de descărcare

- 105 Aparatul de înregistrare înregistrează și stochează în memoria sa următoarele date privind ultima descărcare de date din memorie pe un suport extern efectuată în mod societate sau calibrare:

- data și ora descărcării;
- numărul cardului societății sau al atelierului și statul membru emitent al cardului;
- numele societății sau al atelierului.

12.15. Date privind situații speciale

- 105a Aparatul de înregistrare înregistrează și stochează în memoria sa următoarele date privind situațiile speciale:

- data și ora înregistrării;
- tipul situației speciale.

- 105b Memoria trebuie să poată stoca date privind situațiile speciale timp de cel puțin 365 de zile (presupunând că pe zi se deschide și se închide în medie o situație specială). La epuizarea capacității de stocare, datele noi înlocuiesc datele cele mai vechi.

13. Citirea de pe carduri de tahograf

- 106 Aparatul de înregistrare trebuie să poată citi de pe cardurile de tahograf, în cazurile relevante, datele necesare:

- pentru a identifica tipul cardului, titularul cardului, vehiculul folosit anterior, data și ora ultimei retrageri a cardului și activitatea selectată în momentul respectiv;
- pentru a verifica dacă ultima sesiune pe card a fost încheiată corect;
- pentru a calcula timpul de conducere continuă, durata cumulată a pauzelor și durata cumulată de conducere pentru șofer pentru săptămâna respectivă și pentru cea anterioară;
- pentru a tipări documentele necesare privind datele înregistrate pe un card al șoferului;
- pentru a descărca datele de pe un card al șoferului pe un suport extern.

- 107 În cazul unei erori de citire, aparatul de înregistrare trebuie să încerce, de maximum trei ori, să efectueze aceeași comandă de citire, iar dacă nu reușește trebuie să declare cardul nevalabil și afectat de anomalii.

14. Înregistrarea și stocarea pe carduri de tahograf

- 108 Aparatul de înregistrare introduce «datele sesiunii de card» pe cardul șoferului sau al atelierului imediat după introducerea cardului.

- 109 Aparatul de înregistrare actualizează datele stocate pe cardurile valabile ale șoferului, atelierului și/sau de control pe baza tuturor datelor necesare relevante pentru perioada în care este introdus cardul și pentru titularul cardului. Datele stocate pe aceste carduri sunt precizate în capitolul IV.
- 109a Aparatul de înregistrare actualizează datele privind activitățile șoferului și locul (după cum se arată în capitolul IV la punctele 5.2.5 și 5.2.6) stocate pe cardurile valabile ale șoferului și/sau atelierului pe baza datelor privind activitatea și locul care au fost introduse manual de către titularul cardului.
- 110 Actualizarea datelor de pe cardurile de tahograf se face astfel încât, dacă acest lucru este necesar din punctul de vedere al capacității de stocare a cardului din momentul respectiv, datele cele mai recente să înlocuiască datele cele mai vechi.
- 111 În cazul unei erori de scriere, aparatul de înregistrare trebuie să încerce, de maximum trei ori, să efectueze aceeași comandă de scriere, iar dacă nu reușește trebuie să declare cardul nevalabil și afectat de anomalii.
- 112 Înainte de a elibera cardul șoferului și după ce toate datele relevante au fost stocate pe card, aparatul de înregistrare trebuie să reseteze datele privind sesiunea de card.

15. Afișare

- 113 Afișajul are cel puțin 20 de caractere.
- 114 Dimensiunile minime ale caracterelor sunt de 5 mm înălțime și 3,5 mm lățime.
- 114a Afișajul este compatibil cu seturile de caractere Latin 1 și Greek definite de ISO 8859 părțile 1 și 7, conform specificațiilor din apendicele 1 capitolul 4, «Seturi de caractere». Afișajul poate utiliza simboluri simplificate (de exemplu caracterele cu accent pot fi afișate fără accent sau minuscule pot fi afișate ca majusculele).
- 115 Afișajul este prevăzut cu iluminare corespunzătoare, fără efect de orbire.
- 116 Indicațiile trebuie să fie vizibile din exteriorul aparatului de înregistrare.
- 117 Aparatul de înregistrare trebuie să poată afișa:
- date implicite;
 - date privind avertismentele;
 - date privind accesul la meniu;
 - alte date solicitate de utilizator.
- Aparatul de înregistrare poate afișa și informații suplimentare, cu condiția ca acestea să poată fi distinse în mod clar de informațiile menționate anterior.
- 118 Afișajul aparatului de înregistrare poate folosi pictogramele sau combinațiile de pictograme din apendicele 3. Aparatul de înregistrare poate afișa și pictograme sau combinații de pictograme suplimentare, cu condiția ca acestea să poată fi distinse în mod clar de pictogramele sau combinațiile de pictograme menționate anterior.
- 119 Afișajul trebuie să fie întotdeauna PORNIT când vehiculul este în mișcare.
- 120 Aparatul de înregistrare poate oferi o aplicație manuală sau automată care să treacă afișajul în poziția OPRIT când vehiculul nu este în mișcare.

Formatul de afișare este descris în apendicele 5.

15.1. Afișajul implicit

- 121 Dacă nu trebuie afișate nici un fel de alte informații, aparatul de înregistrare afișează, implicit, următoarele:
- ora locală (rezultată pe baza orei UTC + decalajul setat de șofer);
 - modul de funcționare;
 - activitatea șoferului în momentul respectiv și activitatea copilotului în momentul respectiv;

- informații privind șoferul:
 - dacă activitatea curentă a acestuia este CONDUCERE, timpul de conducere continuă și durata cumulată a pauzelor la momentul respectiv;
 - dacă activitatea curentă a acestuia nu este CONDUCERE, durata activității curente în cauză (de la selectarea acesteia) și durata cumulată a pauzelor;
 - informații privind copilotul:
 - durata activității sale în momentul respectiv (de la selectarea acesteia).
- 122 Afișarea datelor pentru fiecare șofer trebuie să fie clară, simplă și lipsită de ambiguități. Dacă informațiile privind șoferul și copilotul nu pot fi afișate în același timp, aparatul de înregistrare afișează implicit informațiile privind șoferul și îi permite utilizatorului să afișeze informațiile privind copilotul.
- 123 Dacă lățimea afișajului nu permite afișarea implicită a modului de funcționare, aparatul de înregistrare afișează rapid, pentru un timp scurt, noul mod de funcționare, atunci când se produce schimbarea acestuia.
- 124 Aparatul de înregistrare afișează rapid numele titularului cardului la introducerea cardului.
- 124a La deschiderea unei condiții «ÎN AFARA DOMENIULUI DE APLICARE» afișajul implicit trebuie să indice prin intermediul unei pictograme relevante că este deschisă condiția respectivă. (Este permisă neafișarea simultană a activității curente a șoferului.)

15.2. *Afișarea avertismentelor*

- 125 Aparatul de înregistrare afișează informațiile privind avertismentele folosind în primul rând pictogramele din apendicele 3, completate dacă este necesar cu informații suplimentare codate numeric. Se poate adăuga de asemenea o descriere în cuvinte a avertizării, în limba selectată de șofer.

15.3. *Accesul la meniu*

- 126 Comenzile aparatului de înregistrare sunt accesibile prin intermediul unui meniu cu structură adecvată.

15.4. *Alte afișaje*

- 127 Următoarele informații trebuie să poată fi afișate selectiv, la cerere:
- ora și data UTC;
 - modul de funcționare (dacă nu este afișat implicit);
 - timpul de conducere continuă și durata cumulată a pauzelor pentru șofer;
 - timpul de conducere continuă și durata cumulată a pauzelor pentru copilot;
 - timpul de conducere continuă al șoferului pentru săptămâna în curs și pentru săptămâna anterioară;
 - timpul de conducere continuă al copilotului pentru săptămâna în curs și pentru săptămâna anterioară;
 - conținutul oricăruia dintre cele șase materiale tipărite, în format identic cu cel al materialelor tipărite.
- 128 Afișarea conținutului materialelor tipărite este secvențială, structurată pe linii. Dacă lățimea afișajului este mai mică de 24 de caractere, utilizatorul trebuie să aibă acces la informațiile complete printr-un mijloc adecvat (mai multe linii, derulare etc.). Afișarea liniilor din materialele tipărite care sunt alocate pentru informații scrise de mână nu este obligatorie.

16. *Tipărire*

- 129 Aparatul de înregistrare trebuie să poată tipări informații din memoria sa și/sau de pe cardurile de tahograf, sub forma următoarelor șase tipuri de materiale tipărite:
- material imprimat privind activitățile zilnice ale șoferului stocate pe card;
 - material imprimat privind activitățile zilnice ale șoferului stocate în unitatea montată pe vehicul;

- material imprimat privind evenimentele și anomaliile stocate pe card;
- material imprimat privind evenimentele și anomaliile stocate în unitatea montată pe vehicul;
- material imprimat privind datele tehnice;
- material imprimat privind depășirea de viteză.

Formatul detaliat și conținutul acestor materiale tipărite sunt descrise în apendicele 4.

La sfârșitul materialelor tipărite pot fi furnizate și date suplimentare.

Aparatul de înregistrare trebuie să poată oferi și alte materiale imprimate, cu condiția ca acestea să poată fi deosebite în mod clar de cele șase tipuri menționate anterior.

- 130 «Materialul tipărit privind activitățile șoferului stocate pe card» și «materialul tipărit privind evenimentele și anomaliile stocate pe card» trebuie să fie disponibile numai când în aparatul de înregistrare este introdus un card al șoferului sau al atelierului. Aparatul de înregistrare actualizează datele stocate pe cardurile respective înainte de a iniția tipărirea.
- 131 Pentru a genera «materialul tipărit privind activitățile șoferului stocate pe card» și «materialul tipărit privind evenimentele și anomaliile stocate pe card», aparatul de înregistrare trebuie:
- fie să selecteze automat cardul șoferului sau cardul atelierului dacă unul dintre acestea a fost introdus;
 - fie să dea o comandă de selectare a cardului-sursă sau să selecteze cardul din lectorul pentru cardul șoferului dacă în aparatul de înregistrare au fost introduse două carduri.
- 132 Imprimanta trebuie să poată tipări 24 de caractere pe fiecare linie.
- 133 Dimensiunile minime ale caracterelor sunt de 2,1 mm înălțime și 1,5 mm lățime.
- 133a Imprimanta trebuie să fie compatibilă cu seturile de caractere Latin 1 și Greek definite de ISO 8859 părțile 1 și 7, conform dispozițiilor din apendicele 1 capitolul 4 «Seturi de caractere».
- 134 Imprimantele trebuie proiectate astfel încât să realizeze aceste materiale tipărite cu o rezoluție care să elimine orice eventuală ambiguitate la citire.
- 135 Materialele tipărite trebuie să-și mențină dimensiunile și înregistrările în condiții normale de umiditate (între 10 și 90 %) și de temperatură.
- 136 Hârtia folosită de aparatul de înregistrare trebuie să fie prevăzută cu marcajul adecvat de omologare și să conțină indicații privind tipurile de aparate de înregistrare la care poate fi folosită. Materialele tipărite trebuie să își păstreze lizibilitatea și să poată fi identificate în condiții normale de depozitare (respectiv intensitate a luminii, umiditate și temperatură) timp de cel puțin un an.
- 137 Pe aceste documente trebuie să se poată adăuga și note de mână, cum ar fi semnătura șoferului.
- 138 Aparatul de înregistrare trebuie să poată gestiona rupturile din alimentarea cu hârtie în timpul activității de tipărire fie reluând imprimarea de la început după realimentarea cu hârtie, fie continuând imprimarea și oferind o trimitere clară la partea imprimată anterior.

17. Avertismente

- 139 Aparatul de înregistrare trebuie să avertizeze șoferul când detectează orice eveniment și/sau anomalie.
- 140 Este posibil ca avertismentul privind evenimentul de întrerupere a alimentării cu energie electrică să fie amânat până la reconectarea la sursă.
- 141 Aparatul de înregistrare trebuie să avertizeze șoferul cu 15 minute înainte de momentul în care timpul de conducere continuă al acestuia depășește 4 h și 30 min.
- 142 Avertismentele trebuie să fie vizuale. Pe lângă avertismentele vizuale pot fi date și avertismente sonore.

- 143 Avertismentele vizuale trebuie să poată fi recunoscute în mod clar de către utilizator, trebuie să se afle în câmpul vizual al șoferului și trebuie să fie perfect lizibile atât ziua cât și noaptea.
- 144 Avertismentele vizuale pot fi integrate în aparatul de înregistrare și/sau pot fi externe.
- 145 În cel de-al doilea caz avertismentele trebuie să fie marcate cu simbolul «T» și să fie de culoare galben-chihlimbar sau portocalie.
- 146 Avertismentele trebuie să dureze cel puțin 30 de secunde, cu excepția cazurilor când șoferul confirmă luarea lor la cunoștință prin apăsarea oricărei taste a aparatului de înregistrare. Această primă confirmare nu anulează afișarea cauzei avertismentului descrisă la punctul următor.
- 147 Cauza avertismentului trebuie afișată de aparatul de înregistrare și trebuie să rămână vizibilă până când șoferul confirmă luarea acesteia la cunoștință cu ajutorul unei anumite taste sau comenzi a aparatului de înregistrare.
- 148 Pot fi oferite și avertismente suplimentare, cu condiția ca acestea să nu poată fi confundate de șoferi cu cele descrise anterior.

18. Descărcarea de date pe suporturi externe

- 149 Aparatul de înregistrare trebuie să poată descărca la cerere date din memoria sa ori de pe un card al șoferului pe suporturi externe de stocare prin intermediul conectorului de calibrare/descărcare. Aparatul de înregistrare trebuie să actualizeze datele stocate pe cardul relevant înainte de a începe descărcarea.
- 150 În plus, aparatul de înregistrare poate oferi o caracteristică opțională, în orice mod de funcționare, constând din descărcarea de date printr-un alt conector către o societate autenticată prin intermediul acestui canal. În acest caz, pentru astfel de descărcări se aplică drepturile de acces la date din mod societate.
- 151 Descărcarea nu modifică și nici nu șterge datele stocate.

Interfața electrică a conectorului pentru calibrare/descărcare este descrisă în apendicele 6.

Protocoloalele de descărcare sunt descrise în apendicele 7.

19. Date transmise unor dispozitive externe suplimentare

- 152 Dacă aparatul de înregistrare nu include funcții de afișare a vitezei și/sau a valorii contorului de parcurs, aparatul de înregistrare furnizează un semnal/semnale de ieșire care să permită afișarea vitezei vehiculului (vitezometru) și/sau a distanței totale parcurse de vehicul (contor de parcurs).
- 153 Unitatea montată pe vehicul trebuie de asemenea să poată transmite următoarele date printr-o legătură serială dedicată independentă din magistrala de conectare CAN (ISO 11898 Vehicule rutiere – Schimb de informații digitale – Dispozitiv de gestionare a rețelei de comunicații de mare viteză CAN) și să permită prelucrarea acestora de către alte unități electronice instalate pe vehicul:
- data și ora UTC în momentul respectiv;
 - viteza vehiculului;
 - distanța totală parcursă de vehicul (contor de parcurs);
 - activitatea selectată pentru șofer și copilot în momentul respectiv;
 - informații privind existența unui card de tahograf introdus în lectorul pentru cardul șoferului și în lectorul pentru cardul copilotului și (dacă este cazul) informații privind elementele de identificare ale cardurilor respective (numărul cardurilor și statul membru emitent).

Mai pot fi transmise și alte date pe lângă cele care figurează pe această listă minimă.

Când motorul vehiculului este PORNIT, aceste date sunt transmise permanent. Când motorul vehiculului este OPRIT, transmisia este continuată cel puțin pentru toate modificările activității șoferului și/sau a copilotului și pentru orice introducere sau retragere a unui card de tahograf. Dacă aceste date nu au putut fi transmise în perioada în care motorul vehiculului a fost OPRIT, ele devin disponibile în momentul în care motorul vehiculului este din nou PORNIT.

20. Calibrare

- 154 Funcția de calibrare permite:
- cuplarea automată a senzorului de mișcare și a UV;
 - adaptarea digitală a constantei aparatului de înregistrare (k) la coeficientul caracteristic al vehiculului (w) (vehiculele care au mai mult de o osie trebuie dotate cu un dispozitiv de comutare cu ajutorul căruia aceste rapoarte să fie corelate automat cu raportul pe baza căruia aparatul a fost adaptat vehiculului);
 - ajustarea (fără restricții) a orei din momentul respectiv;
 - ajustarea valorii contorului de parcurs din momentul respectiv;
 - actualizarea datelor de identificare a senzorului de mișcare stocate în memorie;
 - actualizarea sau confirmarea altor parametri cunoscuți de aparatul de înregistrare: identificarea vehiculului, w, l, dimensiunea pneurilor și reglajele limitatorului de viteză, dacă este cazul.
- 155 Cuplarea senzorului de mișcare la UV implică cel puțin:
- actualizarea datelor privind instalarea senzorului de mișcare de la senzorul de mișcare (după cum este necesar),
 - copierea de la senzor în memoria de date a UV a datelor necesare pentru identificarea senzorului de mișcare.
- 156 Funcția calibrare trebuie să permită înregistrarea datelor necesare prin intermediul conectorului pentru calibrare/descărcare, în conformitate cu protocolul de calibrare descris în apendicele 8. Funcția de calibrare permite de asemenea înregistrarea datelor necesare prin alți conectori.

21. Reglarea orei

- 157 Funcția de reglare a orei trebuie să permită reglarea orei prin modificări în limita a maximum un minut efectuate la intervale de cel puțin șapte zile.
- 158 Funcția de reglare a orei trebuie să permită reglarea orei fără restricții în modul calibrare.

22. Caracteristici

- 159 Unitatea montată pe vehicul trebuie să funcționeze corect în intervalul de temperatură de la - 20 °C la 70 °C, iar senzorul de mișcare în intervalul de temperatură de la - 40 °C la 135 °C. Conținutul memoriei trebuie să se păstreze la temperaturi de până la - 40 °C.
- 160 Aparatul de înregistrare trebuie să funcționeze corect într-un interval de umiditate de 10 % până la 90 %.
- 161 Aparatul de înregistrare trebuie protejat de supratensiune, de inversarea polarității sursei de alimentare și de scurtcircuite.
- 162 Aparatul de înregistrare trebuie să respecte dispozițiile din Directiva Comisiei 95/54/CE din 31 octombrie 1995 ⁽¹⁾ de adaptare la progresul tehnic a Directivei Consiliului 72/245/CEE ⁽²⁾ privind compatibilitatea electromagnetică și trebuie protejat de descărcările electrostatice și de șocurile de instalare.

23. Materiale

- 163 Toate părțile componente ale aparatului de înregistrare trebuie să fie confecționate din materiale suficient de stabile și cu o rezistență mecanică suficientă și să aibă caracteristici electrice și magnetice stabile.
- 164 În condiții normale de utilizare toate piesele interne ale aparatului trebuie să fie protejate de umezeală și de praf.
- 165 Unitatea montată pe vehicul trebuie să respecte nivelul de protecție IP 40, iar senzorul de mișcare nivelul de protecție IP 64, conform normei IEC 529.

⁽¹⁾ JO L 266, 8.11.1995, p. 1.

⁽²⁾ JO L 152, 6.7.1972, p. 15.

- 166 Aparatul de înregistrare trebuie să respecte specificațiile tehnice aplicabile în domeniul proiectării ergonomice.
- 167 Aparatul de înregistrare trebuie să fie protejat de deteriorările accidentale.

24. Marcaje

- 168 Dacă aparatul de înregistrare afișează valoarea contorului de parcurs și viteza vehiculului, pe afișaj apar următoarele detalii:
- lângă cifra care indică distanța, unitatea de măsură a distanței, indicată prin prescurtarea «km»;
 - lângă cifra care indică viteza, indicația «km/h».
- Aparatul de înregistrare poate fi comutat, astfel încât să afișeze viteza în mile pe oră, în acest caz unitatea de măsură a vitezei fiind indicată prin prescurtarea «mph».
- 169 Pe fiecare componentă separată a aparatului de înregistrare trebuie atașată o plăcuță descriptivă care să conțină următoarele detalii:
- numele și adresa producătorului aparatului;
 - numărul de componentă și anul de fabricație al aparatului;
 - numărul de serie al aparatului;
 - marcajul de omologare pentru tipul de aparat în cauză.
- 170 Dacă spațiul fizic nu este suficient pentru afișarea tuturor detaliilor menționate anterior, plăcuța descriptivă trebuie să conțină cel puțin: numele și sigla producătorului și numărul de componentă al aparatului.

IV. CERINȚE FUNCȚIONALE ȘI DE CONSTRUCȚIE PENTRU CARDURILE DE TAHOGRAPH

1. Date vizibile

Pe față:

- 171 cuvintele «Card al șoferului» sau «Card de control» sau «Card al atelierului» sau «Card al societății» tipărite cu majuscule în limba/limbile oficiale a/ale statului membru emitent, în funcție de tipul cardului;
- 172 aceleași cuvinte în celelalte limbi oficiale ale Comunității, tipărite ca fundal al cardului:

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	KAPTA ΟΔΗΓΟΥ	KAPTA ΕΛΕΓΧΟΥ	KAPTA ΚΕΝΤΡΟΥ ΔΟΚΙΜΩΝ	KAPTA ΕΠΙΧΕΙΡΗΣΗΣ
EN	DRIVER CARD	CONTROL CARD	WORKSHOP CARD	COMPANY CARD
FR	CARTE DE CONDUCTEUR	CARTE DE CONTRÔLEUR	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	CONTOLEKAART	WERKPLAATSKAART	BEDRIJFSKAART
PT	CARTÃO DE CONDUTOR	CARTÃO DE CONTROLO	CARTÃO DO ENSAIO	CARTÃO DE EMPRESA
FI	KULJETTAJA KORTILLA	VALVONTAKORTTI	KORJAAMOKORTTI	YRITYSKORTILLA
SV	FÖRARKORT	KONTROLLKORT	VERKSTADSKORT	FÖRETAGSKORT

- 173 denumirea statului membru emitent al cardului (optional):

174 semnul distinctiv al statului membru emitent al cardului, tipărit cu alb într-un dreptunghi albastru și înconjurat de 12 stele galbene. Semnele distinctive sunt:

B Belgia
 DK Danemarca
 D Germania
 GR Grecia
 E Spania
 F Franța
 IRL Irlanda
 I Italia
 L Luxemburg
 NL Țările de Jos
 A Austria
 P Portugalia
 FIN Finlanda
 S Suedia
 UK Regatul Unit

175 informații specifice pentru cardul emis, numerotate după cum urmează:

	Card al șoferului	Card de control	Card al societății sau al atelierului
1.	Numele șoferului	Numele organismului de control	Numele societății sau al atelierului
2.	Prenumele șoferului	Numele controlorului (dacă este cazul)	Numele titularului cardului (dacă este cazul)
3.	Data nașterii șoferului	Prenumele controlorului (dacă este cazul)	Prenumele titularului cardului (dacă este cazul)
4.(a)	Data de la care este valabil cardul		
(b)	Data de expirare a cadrului (dacă există)		
(c)	Denumirea autorității emitente (poate fi tipărită pe pagina 2)		
(d)	Un număr diferit de cel de la rubrica 5, cu scop administrativ (opțional)		
5. (a)	Numărul permisului de conducere (la data emiterii cardului șoferului)		
5.(b)	Numărul cardului		
6.	Fotografia șoferului	Fotografia controlorului (opțional)	—
7.	Semnătura șoferului	Semnătura titularului (opțional)	
8.	Adresa oficială sau adresa poștală a titularului (opțional)	Adresa poștală a organismului de control	Adresa poștală a societății sau a atelierului

176 datele se scriu în format «zz/ll/aaaa» sau «zz.ll.aaaa» (zi, lună, an);

pe verso figurează:

177 explicații pentru elementele numerotate de pe fața cardului;

178 cu acordul special al titularului, exprimat în scris, pot fi adăugate informații care nu sunt legate de administrarea cardului, dar acestea nu trebuie să modifice în nici un fel folosirea modelului în calitate de card de tahograf.

MODEL COMUNITAR PENTRU CARDURILE DE TAHOGRAF	
FAȚĂ	VERSO
DRIVER CARD 1.  2.  3.  4a.  4b.  4c.  4d.  5a.  5b.  7.  (8.) MEMBER STATE 1.  2.  3.  4b.  4c.  4d.  5a.  5b.  7.  (8.)	1. Surname 2. First name(s) 3. Birth date 4a. Date of start of validity of card 4b. Administrative expiry date of card 4c. Issuing authority (4d.) No for national administrative purposes 5a. Driving license number 5b. Card number 6. Photograph 7. Signature (8.) Address Please return to: NAME OF AUTHORITY AND ADDRESS
CONTROL CARD 1.  2.  3.  4a.  4b.  4c.  4d.  5b.  7.  8. MEMBER STATE 1.  2.  3.  4b.  4c.  4d.  5b.  7.  8.	1. Control Body (2.) Surname (3.) First name(s) 4a. Date of start of validity of card (4b.) Administrative expiry date of card 4c. Issuing authority (4d.) No for national administrative purposes 5b. Card number (6.) Photograph (7.) Signature 8. Address Please return to: NAME OF AUTHORITY AND ADDRESS
WORKSHOP CARD 1.  2.  3.  4a.  4b.  4c.  4d.  5b.  7.  8. MEMBER STATE 1.  2.  3.  4b.  4c.  4d.  5b.  7.  8.	1. Workshop Name (2.) Surname (3.) First name(s) 4a. Date of start of validity of card 4b. Administrative expiry date of card 4c. Issuing authority (4d.) No for national administrative purposes 5b. Card number (7.) Signature 8. Address Please return to: NAME OF AUTHORITY AND ADDRESS
COMPANY CARD 1.  2.  3.  4a.  4b.  4c.  4d.  5b.  7.  8. MEMBER STATE 1.  2.  3.  4b.  4c.  4d.  5b.  7.  8.	1. Company Name (2.) Surname (3.) First name(s) 4a. Date of start of validity of card 4b. Administrative expiry date of card 4c. Issuing authority (4d.) No for national administrative purposes 5b. Card number (7.) Signature 8. Address Please return to: NAME OF AUTHORITY AND ADDRESS

179 Cardurile de tahograf pot fi tipărite pe fonduri având următoarele culori predominante:

- card al șoferului: alb;
- card de control: albastru;
- card al atelierului: roșu;
- card al societății: galben.

180 Cardurile de tahograf trebuie să aibă cel puțin următoarele caracteristici de protecție a corpului cardului împotriva falsificării și a manipulării neadecvate:

- un fond de securitate cu ghioșe și irizat;
- în zona fotografiei, fondul de securitate și fotografia trebuie să se suprapună;
- cel puțin o linie bicoloră microimprimată.

- 181 După consultarea Comisiei, statele membre pot adăuga culori sau marcaje cum ar fi simboluri naționale sau caracteristici de securitate, fără a aduce atingere celorlalte dispoziții din prezenta anexă.

2. Securitate

Securitatea sistemului este destinată protejării integrității și autenticității datelor schimbate între carduri și aparatul de înregistrare, protejării integrității și autenticității datelor descărcate de pe carduri, și permite numai realizarea anumitor operațiuni de scriere pe carduri efectuate de aparatul de înregistrare pentru a elimina orice posibilitate de falsificare a datelor stocate pe carduri, previne manipulările neadecvate și detectează orice tentativă de acest gen.

- 182 Pentru a asigura securitatea sistemului, cardurile de tahograf trebuie să îndeplinească cerințele de securitate definite în obiectivele generale de securitate pentru cardurile de tahograf (apendicele 10).

- 183 Cardurile de tahograf trebuie să poată fi citite și de alte aparate, cum ar fi calculatoarele personale.

3. Standarde

- 184 Cardurile de tahograf respectă următoarele standarde:

- ISO/IEC 7810 Carduri de identitate – Caracteristici fizice;
- ISO/IEC 7816 Carduri de identitate – Circuite integrate cu contacte:
 - Partea 1: Caracteristici fizice
 - Partea 2: Dimensiunile și poziția contactelor
 - Partea 3: Semnale electronice și protocoale de transmisie
 - Partea 4: Comenzi intersectoriale pentru schimburi
 - Partea 8: Comenzi intersectoriale de securitate;
- ISO/IEC 10373 Carduri de identitate – Metode de testare.

4. Specificații de mediu și electrice

- 185 Cardurile de tahograf trebuie să poată funcționa corect în toate condițiile climatice întâlnite în mod normal pe teritoriul Comunității și cel puțin în intervalul de temperatură de la – 25 °C la + 70 °C, cu creșteri ocazionale ale temperaturii până la + 85 °C; «ocazional» înseamnă cel mult 4 ore o dată și de cel mult 100 de ori pe întreaga durată de viață a cardului.
- 186 Cardurile de tahograf trebuie să poată funcționa corect în intervalul de umiditate de la 10 % la 90 %.
- 187 Cardurile de tahograf trebuie să poată funcționa corect timp de cinci ani dacă sunt folosite conform specificațiilor de mediu și electrice.
- 188 Funcționarea cardurilor de tahograf trebuie să respecte Directiva Comisiei 95/54/CE din 31 octombrie 1995 ⁽¹⁾ privind compatibilitatea electromagnetică și trebuie protejate de descărcări electrostatice.

5. Stocarea datelor

În înțelesul prezentului alineat,

- orele sunt înregistrate cu o rezoluție de un minut, ce excepția cazurilor în care se specifică altfel;
- valorile contorului de parcurs sunt înregistrate cu o rezoluție de un kilometru;
- vitezele sunt înregistrate cu o rezoluție de 1 km/h.

Funcțiile, comenzile și structura logică a cardurilor de tahograf care îndeplinesc cerințele de stocare a datelor sunt menționate în appendicele 2.

⁽¹⁾ JO L 266, 8.11.1995, p. 1.

- 189 Prezentul paragraf stabilește capacitatea minimă de stocare pentru diversele fișiere de date pentru aplicații. Cardurile de tahograf trebuie să poată transmite aparatului de înregistrare capacitatea de stocare din momentul respectiv a respectivelor fișiere de date.

Orice date suplimentare care ar putea fi stocate pe cardurile de tahograf, legate de celelalte aplicații susținute de card, trebuie stocate în conformitate cu Directiva 95/46/CE din 24 octombrie 1995 privind protecția persoanelor în privința prelucrării datelor personale și libera circulație a acestor date ⁽¹⁾.

5.1. *Date de identificare și securitate a cardului*

5.1.1. *Identificarea aplicațiilor*

- 190 Cardurile de tahograf trebuie să poată stoca următoarele date de identificare a aplicațiilor:

- identificarea aplicației de tahograf;
- identificarea tipului de card de tahograf.

5.1.2. *Identificarea microprocesorului*

- 191 Cardurile de tahograf trebuie să poată stoca următoarele date de identificare a circuitelor integrate:

- numărul de serie al circuitelor integrate;
- referințele de fabricație ale circuitelor integrate.

5.1.3. *Identificarea cardurilor cu circuite integrate*

- 192 Cardurile de tahograf trebuie să poată stoca următoarele date de identificare a cardurilor cu memorie:

- numărul de serie al cardului (inclusiv referințele de fabricație);
- numărul de omologare al cardului;
- identificatorul privat al cardului;
- identificatorul integratorului;
- identificatorul circuitului integrat.

5.1.4. *Elemente de securitate*

- 193 Cardurile de tahograf trebuie să poată stoca următoarele date privind elementele de securitate:

- cheia publică europeană;
- certificatul statului membru;
- certificatul cardului;
- cheia privată a cardului.

5.2. *Cardul șoferului*

5.2.1. *Identificarea cardului*

- 194 Cardul șoferului trebuie să poată stoca următoarele date de identificare a cardului:

- numărul cardului;
- statul membru emitent, denumirea autorității emitente, data emiterii;
- data de la care este valabil cardul, data expirării cardului.

⁽¹⁾ JO L 281, 23.11.1995, p. 31.

5.2.2. Identificarea titularului cardului

195 Cardul șoferului trebuie să poată stoca următoarele date de identificare a titularului cardului:

- numele titularului cardului;
- prenumele titularului;
- data nașterii;
- limba preferată de titular.

5.2.3. Informații privind permisul de conducere

196 Cardul șoferului trebuie să poată stoca următoarele date privind permisul de conducere:

- statul membru emitent, denumirea autorității emitente;
- numărul permisului de conducere (de la data emiterii cardului).

5.2.4. Date privind vehiculul folosit

197 Cardul șoferului trebuie să poată stoca, pentru fiecare zi calendaristică în care a fost folosit și pentru fiecare perioadă de folosire a unui anumit vehicul în ziua respectivă (o perioadă de utilizare include toate ciclurile consecutive de introducere/retragere a cardului în vehiculul respectiv din punctul de vedere al cardului), următoarele date:

- data și ora primei utilizări a vehiculului (adică prima introducere a cardului în perioada respectivă de utilizare, sau ora 00.00 dacă perioada de utilizare este în curs la ora respectivă);
- valoarea contorului de parcurs al vehiculului în momentul respectiv;
- data și ora ultimei utilizări a vehiculului (adică ultima retragere a cardului în perioada respectivă de utilizare sau ora 23.59 dacă perioada de utilizare este în curs la ora respectivă);
- valoarea contorului de parcurs al vehiculului în momentul respectiv;
- numărul de înmatriculare al vehiculului și statul membru de înmatriculare.

198 Cardul șoferului trebuie să poată stoca cel puțin 84 de astfel de înregistrări.

5.2.5. Date privind activitățile șoferului

199 Cardul șoferului trebuie să poată stoca, pentru fiecare zi calendaristică în care a fost folosit sau pentru care șoferul a introdus activități manual, următoarele informații:

- data;
- un contor de prezență zilnică (a cărui valoare crește cu o unitate pentru fiecare dintre zilele calendaristice respective);
- distanța totală parcursă de șofer pe parcursul zilei respective;
- starea șoferului la ora 00.00;
- în cazul oricăror modificări ale activității șoferului și/sau ale situației conducerii și/sau ale oricărei introduceri sau retrageri a cardului șoferului:
 - modul de conducere (ECHIPAJ, SINGUR);
 - lectorul (pentru ȘOFER, pentru COPILOT);
 - starea cardului (INTRODUS, NEINTRODUS);
 - activitatea (CONDUCERE, DISPONIBILITATE, MUNCĂ, PAUZĂ/ODIHNĂ);
 - ora modificării.

200 Memoria cardului șoferului trebuie să poată stoca date privind activitățile șoferului timp de cel puțin 28 de zile (activitatea medie a unui șofer este definită ca incluzând 93 de schimbări de activitate pe zi).

- 201 Datele menționate la cerințele 197 și 199 trebuie stocate astfel încât activitățile să poată fi identificate în ordinea producerii lor, chiar și în cazul unor suprapuneri ale unor intervale de timp.

5.2.6. *Locurile în care încep și/sau se încheie perioadele zilnice de muncă*

- 202 Cardul șoferului trebuie să poată stoca următoarele date privind locurile în care încep și/sau se încheie perioadele zilnice de muncă introduse de șofer:

- data și ora înregistrării (sau data/ora de care este legată înregistrarea dacă aceasta se efectuează pe parcursul unei proceduri de înregistrare manuală);
- tipul înregistrării (început sau sfârșit, situația înregistrării);
- țara și regiunea introdusă;
- valoarea contorului de parcurs al vehiculului.

- 203 Memoria cardului șoferului trebuie să poată stoca cel puțin 42 de perechi de astfel de înregistrări.

5.2.7. *Date privind evenimentele*

În sensul prezentului paragraf, ora este stocată cu o rezoluție de o secundă.

- 204 În timp ce este introdus, cardul șoferului trebuie să poată stoca date privind următoarele evenimente detectate de aparatul de înregistrare:

- suprapunerile unor intervale de timp (dacă evenimentul respectiv este provocat de card);
- introducerea cardului în timpul conducerii (dacă acest eveniment afectează cardul);
- încheierea incorectă a ultimei sesiuni (dacă acest eveniment afectează cardul);
- întreruperea alimentării cu energie electrică;
- eroare la nivelul datelor de mișcare;
- tentative de violare a securității.

- 205 Cardul șoferului trebuie să poată stoca următoarele date privind evenimentele prezentate în continuare:

- codul evenimentului;
- data și ora începutului evenimentului (sau a introducerii cardului dacă evenimentul era în curs în momentul respectiv);
- data și ora sfârșitului evenimentului (sau a retragerii cardului dacă evenimentul era în curs în momentul respectiv);
- numărul de înmatriculare și statul membru în care este înmatriculat vehiculul care a fost afectat de eveniment.

Notă: Pentru evenimentul «suprapunere a unor intervale de timp»:

- data și ora începutului evenimentului trebuie să corespundă datei și orei retragerii cardului din vehiculul precedent;
- data și ora sfârșitului evenimentului trebuie să corespundă datei și orei introducerii cardului în vehiculul folosit în momentul respectiv;
- datele privind vehiculul trebuie să fie cele ale vehiculului din momentul respectiv, care a declanșat evenimentul.

Notă: Pentru evenimentul: «încheiere incorectă a ultimei sesiuni»:

- data și ora începutului evenimentului trebuie să corespundă datei și orei de introducere a cardului pentru sesiunea care nu a fost corect încheiată;
- data și ora sfârșitului evenimentului trebuie să corespundă datei și orei introducerii cardului pentru sesiunea pe parcursul căreia a fost detectat evenimentul (sesiunea din momentul respectiv);
- datele privind vehiculul trebuie să fie datele vehiculului în care s-a desfășurat sesiunea care nu a fost corect încheiată.

- 206 Cardul șoferului trebuie să poată stoca date privind cele mai recente șase evenimente de fiecare tip (adică 36 de evenimente).

5.2.8. *Date privind anomaliile*

În sensul prezentului paragraf, orele sunt înregistrate cu o rezoluție de o secundă.

- 207 Cardul șoferului trebuie să poată stoca date privind următoarele anomalii detectate de aparatul de înregistrare în timp ce este introdus cardul:

- anomalie a cardului (dacă anomalia a fost provocată de card);
- anomalie a aparatului de înregistrare.

- 208 Cardul șoferului trebuie să poată stoca următoarele date privind aceste anomalii:

- codul anomaliei;
- data și ora începutului anomaliei (sau a introducerii cardului dacă anomalia era în curs în momentul respectiv);
- data și ora sfârșitului anomaliei (sau a retragerii cardului dacă anomalia era în curs în momentul respectiv);
- numărul de înmatriculare al vehiculului și statul membru de înmatriculare a vehiculului la care s-a produs anomalia.

- 209 Cardul șoferului trebuie să poată stoca date privind cele mai recente douăsprezece anomalii de fiecare tip (adică 24 de anomalii).

5.2.9. *Date privind activitatea de control*

- 210 Cardul șoferului trebuie să poată stoca următoarele date privind activitățile de control:

- data și ora controlului;
- numărul cardului de control și statul membru emitent;
- tipul controlului [afișaj și/sau tipărire și/sau descărcare din UV și/sau de pe card (vezi nota)];
- perioada descărcată, dacă a avut loc o descărcare;
- numărul de înmatriculare al vehiculului și statul membru de înmatriculare a vehiculului controlat.

Notă: cerințele de securitate impun ca descărcarea de pe card să poată fi înregistrată numai dacă se realizează prin intermediul unui aparat de înregistrare.

- 211 Cardul șoferului trebuie să poată stoca o astfel de înregistrare.

5.2.10. *Date privind sesiunile de lucru cu cardul*

- 212 Cardul șoferului trebuie să poată stoca date privind vehiculul în care a fost începută sesiunea în curs:

- data și ora începerii sesiunii (adică a introducerii cardului) cu o rezoluție de o secundă;
- numărul de înmatriculare al vehiculului și statul membru de înmatriculare.

5.2.11. *Date privind situații speciale*

- 212a Cardul șoferului trebuie să poată stoca următoarele date privind situațiile speciale introduse în timp ce cardul este introdus (indiferent în care dintre lectoare):

- data și ora introducerii;
- tipul situației speciale.

212b Cardul șoferului trebuie să poată stoca 56 de astfel de înregistrări.

5.3. Cardul atelierului

5.3.1. Elemente de securitate

213 Cardul atelierului trebuie să poată stoca un număr personal de identificare (cod PIN).

214 Cardul atelierului trebuie să poată stoca cheile criptografice necesare pentru cuplarea senzorilor de mișcare la unitățile montate pe vehicul.

5.3.2. Identificarea cardului

215 Cardul atelierului trebuie să poată stoca următoarele date de identificare a cardului:

- numărul cardului;
- statul membru emitent, denumirea autorității emitente, data emiterii;
- data de la care este valabil cardul, data expirării cardului.

5.3.3. Identificarea titularului cardului

216 Cardul atelierului trebuie să poată stoca următoarele date de identificare a titularului cardului:

- denumirea atelierului;
- adresa atelierului;
- numele titularului;
- prenumele titularului;
- limba preferată de titular.

5.3.4. Date privind vehiculul folosit

217 Cardul atelierului trebuie să poată stoca înregistrări de date privind vehiculul folosit, în același mod ca și cardul șoferului.

218 Cardul atelierului trebuie să poată stoca cel puțin 4 astfel de înregistrări.

5.3.5. Date privind activitatea șoferului

219 Cardul atelierului trebuie să poată stoca date privind activitatea șoferului, în același mod ca și cardul șoferului.

220 Cardul atelierului trebuie să poată stoca date privind activitatea șoferului pentru cel puțin o zi de activitate medie a șoferului.

5.3.6. Date privind începutul și/sau sfârșitul perioadelor zilnice de muncă

221 Cardul atelierului trebuie să poată stoca înregistrări de date privind începutul și/sau sfârșitul perioadelor zilnice de muncă, în același mod ca și cardul șoferului.

222 Cardul atelierului trebuie să poată stoca cel puțin trei perechi de astfel de înregistrări.

5.3.7. Date privind evenimentele și anomaliile

223 Cardul atelierului trebuie să poată stoca înregistrări de date privind evenimentele și anomaliile, în același mod ca și cardul șoferului.

224 Cardul atelierului trebuie să poată stoca date privind cele mai recente trei evenimente de fiecare tip (adică 18 evenimente) și cele mai recente șase erori de fiecare tip (adică 12 erori).

5.3.8. Date privind activitățile de control

225 Cardul atelierului trebuie să poată stoca înregistrări ale datelor activităților de control, în același mod ca și cardul șoferului.

5.3.9. Date privind calibrarea și reglarea orei

- 226 Cardul atelierului trebuie să poată stoca înregistrări privind calibrările și/sau reglările orei realizate în timp ce cardul este introdus în aparatul de înregistrare.
- 227 Fiecare fișă de calibrare trebuie să conțină următoarele date:
- scopul calibrării (prima instalare, instalare, inspecție periodică);
 - identificarea vehiculului;
 - parametrii actualizați sau confirmați [w, k, l, dimensiunea pneurilor, reglajul limitatorului de viteză, contorul de parcurs (valorile vechi și cele noi), data și ora (valorile vechi și cele noi)];
 - identificarea aparatului de înregistrare (numărul de componentă al UV, numărul de serie al UV, numărul de serie al senzorului de mișcare).
- 228 Cardul atelierului trebuie să poată stoca cel puțin 88 de astfel de înregistrări.
- 229 Cardul atelierului trebuie să fie prevăzut cu un contor care să indice numărul total de calibrări efectuate cu cardul respectiv.
- 230 Cardul atelierului trebuie să fie prevăzut cu un contor care să indice numărul total de calibrări efectuate după ultima descărcare de date.

5.3.10. Date privind situații speciale

- 230a Cardul atelierului trebuie să poată stoca date relevante privind diferite situații speciale, în același mod ca și cardul șoferului. Cardul atelierului trebuie să poată stoca cel puțin două astfel de înregistrări.

5.4. Cardul de control

5.4.1. Identificarea cardului

- 231 Cardul de control trebuie să poată stoca următoarele date de identificare a cardului:
- numărul cardului;
 - statul membru emitent, denumirea autorității emitente, data emiterii;
 - data de la care este valabil cardul, data expirării cardului (dacă există).

5.4.2. Identificarea titularului cardului

- 232 Cardul de control trebuie să poată stoca următoarele date de identificare a titularului cardului:
- denumirea organismului de control;
 - adresa organismului de control;
 - numele titularului cardului;
 - prenumele titularului;
 - limba preferată de titular.

5.4.3. Date privind activitățile de control

- 233 Cardul de control trebuie să poată stoca următoarele date privind activitățile de control:
- data și ora controlului;
 - tipul controlului (afișaj și/sau tipărire și/sau descărcare din UV și/sau de pe card);

- perioada descărcată (dacă este cazul);
- numărul de înmatriculare al vehiculului și autoritatea care a înmatriculat vehiculul controlat;
- numărul cardului și statul membru emitent al cardului de șofer controlat.

234 Cardul de control trebuie să poată stoca cel puțin 230 de astfel de înregistrări.

5.5. Cardul societății

5.5.1. Identificarea cardului

235 Cardul societății trebuie să poată stoca următoarele date de identificare a cardului:

- numărul cardului;
- statul membru emitent, denumirea autorității emitente, data emiterii;
- data de la care este valabil cardul, data expirării cardului (dacă există).

5.5.2. Identificarea titularului cardului

236 Cardul societății trebuie să poată stoca următoarele date de identificare a titularului cardului:

- denumirea societății;
- adresa societății.

5.5.3. Date privind activitatea societății

237 Cardul societății trebuie să poată stoca următoarele date privind activitatea societății:

- data și ora activității;
- tipul activității (blocare și/sau deblocare UV și/sau descărcare din UV și/sau de pe card);
- perioada descărcată (dacă este cazul);
- numărul de înmatriculare al vehiculului și autoritatea statului membru care a înmatriculat vehiculul;
- numărul cardului și statul membru emitent (în cazul unei descărcări de pe card).

238 Cardul societății trebuie să poată stoca cel puțin 230 de astfel de înregistrări.

V. INSTALAREA APARATULUI DE ÎNREGISTRARE

1. Instalare

- 239 Aparatele de înregistrare noi sunt livrate neactivate secțiilor de montaj sau producătorilor de vehicule, cu toți parametrii de calibrare prevăzuți în capitolul III alineatul (20) setați la valori implicite actualizate. În cazurile în care nu se aplică nici o valoare, parametrii alfabetici sunt setați ca șiruri de «?», iar parametrii numerici sunt setați pe «0».
- 240 Înainte de activare, aparatul de înregistrare trebuie să permită accesul la funcția de calibrare, chiar dacă nu este în mod calibrare.
- 241 Înainte de activare, aparatul de înregistrare nu trebuie nici să înregistreze, nici să stocheze datele menționate în capitolul III punctele 12.3.-12.9. și nici datele menționate la punctele 12.12.-12.14. inclusiv.
- 242 În timpul instalării, producătorii de vehicule trebuie să preseteze toți parametrii cunoscuți.

- 243 Producătorii de vehicule sau secțiile de montaj trebuie să activeze aparatul de înregistrare montat înainte ca vehiculul să părăsească locul în care s-a efectuat instalarea.
- 244 Activarea aparatului de înregistrare trebuie să se declanșeze automat la prima introducere a cardului atelierului în oricare dintre dispozitivele de interfață pentru carduri.
- 245 Dacă este cazul, operațiunile speciale de cuplare a senzorului de mișcare și a unității montate pe vehicul trebuie să se realizeze automat, înainte sau în timpul activării.
- 246 După activare, aparatul de înregistrare controlează integral drepturile de acces la funcții și date.
- 247 Funcțiile de înregistrare și stocare ale aparatului de înregistrare trebuie să funcționeze integral după activarea acestuia.
- 248 După instalare trebuie să se efectueze calibrarea. Prima calibrare include înregistrarea numărului de înmatriculare al vehiculului și se efectuează în termen de două săptămâni de la instalare sau de la alocarea numărului de înmatriculare (se ia în considerare data care survine cel mai târziu dintre cele două).
- 248a Aparatul de înregistrare trebuie poziționat în vehicul astfel încât șoferul să aibă acces la toate funcțiile de pe scaunul său.

2. Placa de instalare

- 249 După instalarea și verificarea aparatului de înregistrare, pe sau sub acesta se aplică o placă de instalare vizibilă și ușor accesibilă. După fiecare inspecție efectuată de o secție de montaj sau de un atelier autorizat, în locul plăcii existente se aplică una nouă.
- 250 Placa trebuie să conțină cel puțin următoarele informații:
- denumirea, adresa sau marca comercială a secției de montaj sau a atelierului autorizat;
 - coeficientul caracteristic al vehiculului, sub forma «w = ... imp/km»;
 - constanta aparatului de înregistrare, sub forma «k = ... imp/km»;
 - circumferința efectivă a pneurilor sub forma «l = ... mm»;
 - dimensiunea pneurilor;
 - data la care a fost determinat coeficientul caracteristic al vehiculului și data măsurării circumferinței efective a pneurilor;
 - numărul de identificare al vehiculului.

3. Sigilare

- 251 Se sigilează următoarele părți:
- orice conexiune care, dacă ar fi întreruptă, ar provoca alterări sau pierderi de date care nu pot fi detectate;
 - placa de instalare, cu excepția cazurilor în care este fixată într-un mod care nu permite îndepărtarea sa fără distrugerea marcajelor pe care le conține.
- 252 Sigiliile menționate anterior pot fi îndepărtate:
- în caz de urgență;
 - pentru instalarea, ajustarea sau repararea unui limitator de viteză sau a altui dispozitiv care contribuie la siguranța rutieră, cu condiția ca aparatul de înregistrare să funcționeze în continuare corect și în mod precis și să fie resigilat de o secție de montaj sau de un atelier aprobat (în conformitate cu dispozițiile din capitolul VI) imediat după montarea limitatorului de viteză sau a oricărui alt dispozitiv care contribuie la siguranța rutieră sau în termen de șapte zile în celelalte cazuri.

- 253 De fiecare dată când aceste sigilii sunt rupte, se depune o declarație scrisă privind motivele acțiunii respective la autoritatea competentă.

VI. CONTROALE, INSPECȚII ȘI REPARAȚII

Cerințele privind situațiile în care pot fi rupte sigiliile, așa cum sunt prevăzute în articolul 12 alineatul (5) din Regulamentul (CEE) nr. 3821/85, astfel cum a fost modificat ultima dată prin Regulamentul (CE) nr. 2135/98, sunt definite în capitolul V partea 3 din prezenta anexă.

1. Omologarea secțiilor de montaj și a atelierelor

Statele membre aprobă, controlează în mod regulat și certifică organisme de control însărcinate cu efectuarea de:

- instalări;
- controale;
- inspecții;
- reparații.

În cadrul articolului 12 alineatul (1) din prezentul regulament, cardurile atelierului sunt emise numai secțiilor de montaj și/sau atelierelor aprobate pentru activarea și/sau calibrarea aparatelor de înregistrare în conformitate cu prezenta anexă și, cu excepția cazurilor justificate în mod corespunzător:

- care nu sunt eligibile pentru acordarea unui card al societății;
- și ale căror activități profesionale nu sunt de natură să compromită securitatea globală a sistemului definită în appendicele 10.

2. Verificarea instrumentelor noi și a celor reparate

- 254 Pentru fiecare dispozitiv în parte, indiferent dacă este nou sau reparat, trebuie verificat dacă funcționează corespunzător și dacă citirile și înregistrările pe care le efectuează sunt precise și respectă limitele prevăzute în capitolul III punctul 2.1. și punctul 2.2 și dacă este sigilat și calibrat în conformitate cu dispozițiile din capitolul V partea 3.

3. Inspecția instalării

- 255 La instalarea pe un vehicul, întreaga instalație (inclusiv aparatul de înregistrare) trebuie să respecte dispozițiile privind limitele maxime de toleranță prevăzute în capitolul III punctul 2.1. și punctul 2.2.

4. Inspecții periodice

- 256 Inspecțiile periodice ale aparatelor montate pe vehicule trebuie să se efectueze după orice reparație a aparatului sau după orice modificare a coeficientului caracteristic al vehiculului sau a circumferințelor efective ale pneurilor sau după o eroare a aparatului de indicare a orei UTC mai mare de 20 minute sau dacă numărul de înmatriculare a fost modificat și cel puțin o dată în termen de doi ani (24 de luni) de la ultima inspecție.

- 257 În cadrul inspecțiilor trebuie să se verifice:

- dacă aparatul de înregistrare funcționează corespunzător, inclusiv în ceea ce privește funcția de stocare a datelor pe carduri de tahograf;
- dacă este asigurată respectarea dispozițiilor din capitolul III punctele 2.1 și 2.2 privind limitele maxime de toleranță la instalare;
- dacă aparatul de înregistrare poartă marca de omologare;
- dacă placa de instalare este fixată;
- dacă sigiliile de pe aparat și de pe celelalte părți ale instalației sunt intacte;
- dimensiunea pneurilor și circumferința efectivă a pneurilor.

258 Aceste inspecții trebuie să cuprindă o calibrare.

5. Măsurarea erorilor

259 Măsurarea erorilor la instalare și în timpul utilizării se realizează în următoarele condiții, care trebuie considerate condiții de testare standard:

- vehiculul este descărcat, în stare normală de funcționare;
- presiunea pneurilor este conformă cu instrucțiunile producătorului;
- uzura pneurilor este în limita acceptată în conformitate cu legislația națională;
- mișcarea vehiculului:
 - vehiculul avansează, pe baza acțiunii motorului său, în linie dreaptă, pe teren plat, cu o viteză de 50 ± 5 km/h. Distanța de măsurare trebuie să fie de cel puțin 1 000 m.
- pentru testare pot fi folosite și metode alternative, de exemplu bancuri de probă adecvate, cu condiția ca acestea să aibă o precizie asemănătoare.

6. Reparații

260 Atelierele trebuie să poată descărca date din aparatele de înregistrare pentru a le restitui societății de transport în cauză.

261 Atelierele autorizate emit societăților de transport un certificat care atestă că datele nu pot fi descărcate în cazurile în care un deranjament al aparatului de control face imposibilă descărcarea datelor înregistrate anterior, chiar și după reparațiile efectuate de atelierul respectiv. Atelierul păstrează timp de cel puțin un an un exemplar din fiecare certificat de acest tip pe care îl emite.

VII. EMITEREA CARDURILOR

Procesele de emiteră a cardurilor introduse de statele membre respectă următoarele dispoziții:

- 262 Numărul de card al primului card de tahograf emis unui solicitant conține un indice secvențial (dacă este necesar), un indice de înlocuire și un indice de reînnoire setat la «0».
- 263 Primele 13 cifre ale numărului de card al tuturor cardurilor nenominale de tahograf emise aceluiași organism de control sau aceluiași atelier sau aceleași societăți sunt identice, indicele secvențial fiind diferit.
- 264 În cazul emiterii unui card de tahograf pentru înlocuirea unui card existent, numărul de card al acestuia este identic cu cel al cardului înlocuit, cu excepția indicelui de înlocuire, a cărui valoare este mărită cu «1» (în ordinea 0, ..., 9, A, ..., Z).
- 265 Cardurile de tahograf emise pentru a înlocui un card de tahograf existent trebuie să aibă aceeași dată de expirare ca și cardul înlocuit.
- 266 În cazul emiterii unui card de tahograf pentru reînnoirea unui card existent, numărul de card al acestuia este identic cu cel al cardului înlocuit, cu excepția indicelui de înlocuire, a cărui valoare este resetată la «0», și cu excepția indicelui de reînnoire a cărui valoare este mărită cu «1» (în ordinea 0, ..., 9, A, ..., Z).
- 267 Schimbarea unui card de tahograf existent în vederea modificării datelor administrative respectă regulile de reînnoire dacă se produce în același stat membru sau regulile aplicabile primei eliberări în cazul în care se produce în alt stat membru.
- 268 Pentru cardurile nenominale ale atelierelor sau cardurile de control, la «numele titularului cardului» se menționează denumirea atelierului sau a organismului de control.

VIII. OMOLOGAREA APARATELOR DE ÎNREGISTRARE ȘI A CARDURILOR DE TAHOGRAF

1. Aspecte generale

În sensul prezentului capitol, cuvintele «aparat de înregistrare» înseamnă «aparat de înregistrare sau componentele acestuia». Pentru cablul/cablurile care conectează senzorul de mișcare la UV nu este necesară nici un fel de omologare. Hârtia utilizată de aparatul de înregistrare pentru înregistrări este considerată o componentă a aparatului de înregistrare.

- 269 Aparatul de înregistrare trebuie prezentat în vederea omologării împreună cu orice eventuale dispozitive suplimentare integrate.
- 270 Omologarea aparatelor de înregistrare și a cardurilor de tahograf trebuie să cuprindă teste de securitate, teste de funcționare și teste de interoperare. Rezultatele pozitive obținute la fiecare dintre aceste teste sunt confirmate prin intermediul unui certificat adecvat.
- 271 Autoritățile de omologare din statele membre nu acordă certificate de omologare în conformitate cu articolul 5 din prezentul regulament atât timp cât nu dețin:
- un certificat de securitate;
 - un certificat de funcționare;
 - un certificat de interoperare,
- pentru aparatul de înregistrare sau pentru cardul de tahograf care face obiectul cererii de omologare.
- 272 Orice modificare a software-ului sau a hardware-ului aparatului sau a naturii materialelor utilizate pentru producerea acestuia sunt notificate, înainte de a fi introduse, autorității care a omologat aparatul. Autoritatea respectivă îi confirmă producătorului extinderea omologării sau poate solicita o actualizare sau o confirmare a certificatelor de funcționare, de securitate și/sau de interoperare relevante.
- 273 Procedurile de actualizare *in situ* a software-ului aparatelor de înregistrare trebuie aprobate de autoritatea care a omologat aparatul de înregistrare. Actualizarea software-ului nu trebuie să modifice și nici să șteargă nici un fel de date privind activitatea șoferului stocate în aparatul de înregistrare. Software-ul poate fi actualizat numai pe răspunderea producătorului aparatului.

2. Certificatul de securitate

- 274 Certificatul de securitate este eliberat în conformitate cu dispozițiile din apendicele 10 la prezenta anexă.

3. Certificatul de funcționare

- 275 Fiecare candidat la omologare trebuie să furnizeze autorității de omologare a statului membru toate materialele și întreaga documentație pe care aceasta le consideră necesare.
- 276 Producătorului i se eliberează un certificat de funcționare numai după obținerea de rezultate pozitive cel puțin la toate testele de funcționare prevăzute în apendicele 9.
- 277 Autoritatea de omologare eliberează certificatul de funcționare. Acest certificat indică, pe lângă numele beneficiarului și identificarea modelului, o listă detaliată a testelor efectuate și a rezultatelor obținute.

4. Certificatul de interoperare

- 278 Testele de interoperare sunt realizate de un singur laborator, sub autoritatea și pe răspunderea Comisiei Europene.
- 279 Laboratorul înregistrează cererile de efectuare de teste de interoperare depuse de producători în ordinea cronologică a sosirii acestora.
- 280 Cererile sunt înregistrate oficial numai în momentul în care laboratorul deține:
- întregul set de materiale și documentele necesare pentru realizarea unor astfel de teste de interoperare;
 - certificatul de securitate relevant;
 - certificatul de funcționare relevant.
- Data înregistrării cererii trebuie comunicată producătorului.
- 281 Laboratorul nu efectuează nici un test de interoperare pentru aparatele de înregistrare sau cardurile de tahograf pentru care nu există un certificat de securitate și un certificat de funcționare.
- 282 Orice producător care solicită efectuarea unui test de interoperare trebuie să se angajeze să cedeze laboratorului întregul set de materiale și toate documentele pe care le-a furnizat pentru realizarea testelor.

- 283 Testele de interoperare se realizează în conformitate cu dispozițiile alineatului (5) din apendicele 9 la prezenta anexă, pentru toate tipurile de aparate de înregistrare sau de carduri de tahograf:
- a căror omologare este încă valabilă;
 - sau
 - care urmează să fie omologate și dețin un certificat de interoperare valabil.
- 284 Certificatul de interoperare este eliberat de către laborator producătorului numai după obținerea unui rezultat pozitiv la toate testele de interoperare obligatorii.
- 285 Dacă rezultatele testelor de interoperare nu sunt pozitive pentru aparatele de înregistrare sau cardul/cardurile de tahograf, în conformitate cu cerința 283, nu se eliberează certificatul de interoperare decât după ce producătorul a efectuat modificările necesare și a obținut rezultate pozitive la testele de interoperare. Laboratorul identifică sursa problemei împreună cu producătorul afectat de anomalia de interoperare respectivă și încearcă să îl ajute pe acesta să găsească o soluție tehnică. În cazul în care producătorul și-a modificat produsul, acesta trebuie să se informeze pe lângă autoritățile competente dacă certificatul de securitate și certificatul de funcționare sunt încă valabile.
- 286 Certificatul de interoperare este valabil șase luni. Acesta expiră la sfârșitul perioadei respective dacă producătorul nu primește un certificat de omologare relevant. Acesta este transmis de producător autorității de omologare a statului membru care a emis certificatul de funcționare.
- 287 Nici un element care ar putea sta la originea unei anomalii de interoperare nu trebuie folosit în scopul obținerii de profit sau pentru obținerea unei poziții dominante.

5. Certificatul de omologare

- 288 Autoritatea de omologare a statului membru poate elibera certificatul de omologare imediat ce a intrat în posesia celor trei certificate solicitate.
- 289 Autoritatea de omologare trebuie să transmită o copie a certificatului de omologare laboratorului însărcinat cu realizarea testelor de interoperare în momentul în care aceasta este eliberată producătorului.
- 290 Laboratorul însărcinat cu efectuarea testelor de interoperare trebuie să furnizeze pe un sit web o listă actualizată a modelelor de aparate de înregistrare și de carduri de tahograf:
- pentru care a fost înregistrată o cerere de efectuare de teste de interoperare;
 - pentru care a fost acordat un certificat de interoperare (chiar dacă este provizoriu);
 - pentru care a fost acordat un certificat de omologare.

6. Procedură extraordinară: primele teste de interoperare

- 291 Pe parcursul unei perioade de patru luni de la certificarea capacității de interoperare a unei prime perechi aparat de înregistrare/carduri de tahograf (carduri ale șoferului, ale atelierului, de control și ale societății), orice certificat de interoperare eliberat (inclusiv primul) în urma cererilor înregistrate pe parcursul acestei perioade este considerat provizoriu.
- 292 Dacă, la sfârșitul perioadei menționate anterior, toate produsele în cauză pot interopera, toate certificatele de interoperare care le vizează devin definitive.
- 293 Dacă, pe parcursul acestei perioade apar anomalii de interoperare, laboratorul însărcinat cu efectuarea testelor de interoperare trebuie să identifice cauzele problemelor cu ajutorul producătorilor implicați și să îi invite să facă modificările necesare.
- 294 Dacă, la sfârșitul acestei perioade, problemele de interoperare persistă, laboratorul însărcinat cu realizarea testelor de interoperare, în colaborare cu producătorii în cauză și cu autoritățile de omologare care au eliberat certificatul de funcționare aferent, trebuie să identifice cauzele anomaliilor de interoperare și să identifice modificările care trebuie efectuate de către fiecare dintre producătorii în cauză. Căutarea soluțiilor tehnice trebuie să dureze maximum două luni, după care, dacă nu este identificată o soluție comună, Comisia, după consultarea laboratorului însărcinat cu efectuarea testelor de interoperare, decide care dintre aparate și carduri primesc un certificat definitiv de interoperare și precizează motivul pe baza căruia a fost adoptată decizia respectivă.
- 295 Orice solicitare de efectuare a unor teste de interoperare înregistrată de laborator între sfârșitul perioadei de patru luni de după eliberarea primului certificat provizoriu de interoperare și data deciziei adoptate de Comisie menționată în cerința 294 trebuie amânată până la rezolvarea problemelor inițiale de interoperare. Apoi cererile respective sunt tratate în ordinea cronologică în care au fost înregistrate.

Apendicele 1

DICȚIONAR DE DATE

CUPRINS

1.	Introducere	56
1.1.	Metoda de stabilire a definițiilor tipurilor de date	56
1.2.	Referințe	56
2.	Definirea tipurilor de date	57
2.1.	ActivityChangeInfo	57
2.2.	Address	58
2.3.	BCDString	58
2.4.	CalibrationPurpose	58
2.5.	CardActivityDailyRecord	59
2.6.	CardActivityLengthRange	59
2.7.	CardApprovalNumber	59
2.8.	CardCertificate	59
2.9.	CardChipIdentification	59
2.10.	CardConsecutiveIndex	60
2.11.	CardControlActivityDataRecord	60
2.12.	CardCurrentUse	60
2.13.	CardDriverActivity	60
2.14.	CardDrivingLicenceInformation	61
2.15.	CardEventData	61
2.16.	CardEventRecord	61
2.17.	CardFaultData	62
2.18.	CardFaultRecord	62
2.19.	CardIccIdentification	62
2.20.	CardIdentification	63
2.21.	CardNumber	63
2.22.	CardPlaceDailyWorkPeriod	63
2.23.	CardPrivateKey	64
2.24.	CardPublicKey	64
2.25.	CardRenewalIndex	64
2.26.	CardReplacementIndex	64
2.27.	CardSlotNumber	64
2.28.	CardSlotsStatus	64
2.29.	CardStructureVersion	65

2.30.	CardVehicleRecord	65
2.31.	CardVehiclesUsed	65
2.32.	Certificate	66
2.33.	CertificateContent	66
2.34.	CertificateHolderAuthorisation	66
2.35.	CertificateRequestID	67
2.36.	CertificationAuthorityKID	67
2.37.	CompanyActivityData	67
2.38.	CompanyActivityType	68
2.39.	CompanyCardApplicationIdentification	68
2.40.	CompanyCardHolderIdentification	68
2.41.	ControlCardApplicationIdentification	69
2.42.	ControlCardControlActivityData	69
2.43.	ControlCardHolderIdentification	69
2.44.	ControlType	70
2.45.	CurrentDateTime	70
2.46.	DailyPresenceCounter	70
2.47.	Datef	71
2.48.	Distance	71
2.49.	DriverCardApplicationIdentification	71
2.50.	DriverCardHolderIdentification	71
2.51.	EntryTypeDailyWorkPeriod	72
2.52.	EquipmentType	72
2.53.	EuropeanPublicKey	72
2.54.	EventFaultType	72
2.55.	EventFaultRecordPurpose	73
2.56.	ExtendedSerialNumbe	74
2.57.	FullCardNumber	74
2.58.	HighResOdometer	74
2.59.	HighResTripDistance	74
2.60.	HolderName	74
2.61.	K-ConstantOfRecordingEquipment	75
2.62.	KeyIdentifier	75
2.63.	L-TyreCircumference	75
2.64.	Language	75
2.65.	LastCardDownload	75
2.66.	ManualInputFlag	75
2.67.	ManufacturerCode	76

2.68.	MemberStateCertificate	76
2.69.	MemberStatePublicKey	77
2.70.	Name	77
2.71.	NationAlpha	77
2.72.	NationNumeric	78
2.73.	NoOfCalibrationRecords	79
2.74.	NoOfCalibrationSinceDownload	79
2.75.	NoOfCardPlaceRecords	79
2.76.	NoOfCardVehicleRecords	79
2.77.	NoOfCompanyActivityRecords	79
2.78.	NoOfControlActivityRecords	80
2.79.	NoOfEventsPerType	80
2.80.	NoOfFaultsPerType	80
2.81.	OdometerValueMidnight	80
2.82.	OdometerShort	80
2.83.	OverspeedNumber	80
2.84.	PlaceRecord	80
2.85.	PreviousVehicleInfo	81
2.86.	PublicKey	81
2.87.	RegionAlpha	81
2.88.	RegionNumeric	81
2.89.	RSAPublicModulus	82
2.90.	RSAPrivateExponent	82
2.91.	RSAPublicExponent	82
2.92.	SensorApprovalNumber	82
2.93.	SensorIdentification	82
2.94.	SensorInstallation	83
2.95.	SensorInstallationSecData	83
2.96.	SensorOSIdentifier	83
2.97.	SensorPaired	83
2.98.	SensorPairingDate	84
2.99.	SensorSerialNumber	84
2.100.	SensorSCIdentifier	84
2.101.	Signature	84
2.102.	SimilarEventsNumber	84
2.103.	SpecificConditionType	84
2.104.	SpecificConditionRecord	84
2.105.	Speed	85

2.106.	SpeedAuthorised	85
2.107.	SpeedAverage	85
2.108.	SpeedMax	85
2.109.	TDSessionKey	85
2.110.	TimeReal	85
2.111.	TyreSize	85
2.112.	VehicleIdentificationNumber	86
2.113.	VehicleRegistrationIdentification	86
2.114.	VehicleRegistrationNumber	86
2.115.	VuActivityDailyData	86
2.116.	VuApprovalNumber	86
2.117.	VuCalibrationData	86
2.118.	VuCalibrationRecord	87
2.119.	VuCardIWDData	87
2.120.	VuCardIWRecord	88
2.121.	VuCertificate	88
2.122.	VuCompanyLocksData	88
2.123.	VuCompanyLocksRecord	89
2.124.	VuControlActivityData	89
2.125.	VuControlActivityRecord	89
2.126.	VuDataBlockCounter	89
2.127.	VuDetailedSpeedBlock	89
2.128.	VuDetailedSpeedData	90
2.129.	VuDownloadablePeriod	90
2.130.	VuDownloadActivityData	90
2.131.	VuEventData	90
2.132.	VuEventRecord	91
2.133.	VuFaultData	91
2.134.	VuFaultRecord	91
2.135.	VuIdentification	92
2.136.	VuManufacturerAddress	92
2.137.	VuManufacturerName	92
2.138.	VuManufacturingDate	92
2.139.	VuOverSpeedingControlData	93
2.140.	VuOverSpeedingEventData	93
2.141.	VuOverSpeedingEventRecord	93
2.142.	VuPartNumber	93
2.143.	VuPlaceDailyWorkPeriodData	94

2.144.	VuPlaceDailyWorkPeriodRecord	94
2.145.	VuPrivateKey	94
2.146.	VuPublicKey	94
2.147.	VuSerialNumber	94
2.148.	VuSoftInstallationDate	94
2.149.	VuSoftwareIdentification	94
2.150.	VuSoftwareVersion	95
2.151.	VuSpecificConditionData	95
2.152.	VuTimeAdjustmentData	95
2.153.	VuTimeAdjustmentRecord	95
2.154.	W-VehicleCharacteristicConstant	95
2.155.	WorkshopCardApplicationIdentification	96
2.156.	WorkshopCardCalibrationData	96
2.157.	WorkshopCardCalibrationRecord	96
2.158.	WorkshopCardHolderIdentification	97
2.159.	WorkshopCardPIN	97
3.	Definirea domeniilor de valori și de dimensiuni	98
3.1.	Definiții pentru cardul șoferului	98
3.2.	Definiții pentru cardul atelierului	98
3.3.	Definiții pentru cardul de control	98
3.4.	Definiții pentru cardul societății	98
4.	Seturi de caractere	98
5.	Codarea	98

1. INTRODUCERE

Prezentul apendice cuprinde precizări privind formatele de date, elementele de date și structurile de date care trebuie utilizate de aparatul de înregistrare și de cardurile de tahograf.

1.1. Metoda de stabilire a definițiilor tipurilor de date

În acest apendice se recurge la Notația specificațiilor structurilor de date în conversiile sintactice numărul unu (ASN.1) pentru a defini tipurile de date. Acest lucru permite definirea unor date simple și structurate, fără a fi necesar un transfer specific de sintaxă (reguli de codare) care să depindă de aplicație și de mediu.

Convențiile de denumire a tipurilor ASN.1 sunt realizate conform standardului ISO/IEC 8824-1. Acest lucru implică următoarele aspecte:

- în cazurile în care este posibil, semnificația tipului de date este indicată prin intermediul denumirilor alese;
- dacă un tip de date reprezintă o combinație de alte tipuri de date, denumirea tipului de date în cauză constituie totuși o singură secvență de caractere alfabetică care încep cu o majusculă, dar se mai utilizează și alte majuscule în cadrul denumirii pentru a atribui semnificația corespondentă fiecărei părți;
- în general, denumirile tipurilor de date sunt legate de denumirile tipurilor de date din care sunt alcătuite, ale aparatelor în care sunt stocate datele și ale funcției atribuite datelor în cauză.

Dacă un tip ASN.1 este deja definit în cadrul unui alt standard și dacă trebuie utilizat de aparatul de înregistrare, definiția tipului ASN.1 în cauză este cuprinsă în prezentul apendice.

Pentru a permite aplicarea mai multor tipuri de reguli de codare, anumite tipuri ASN.1 cuprinse în prezentul apendice sunt condiționate de identificatorii de domenii de valori. Identificatorii de domenii de valori sunt definiți în alineatul (3).

1.2. Referințe

În prezentul apendice se utilizează următoarele referințe:

ISO 639	Cod pentru reprezentarea numelor limbilor. Prima ediție: 1988
EN 726-3	Sisteme de carduri de identificare – Carduri și terminale de telecomunicații cu circuit(e) integrat(e) – Partea 3: Cerințe privind cardurile indiferent de aplicația acestora. Decembrie 1994
ISO 3779	Vehicule rutiere – Numărul de identificare al vehiculelor (NIV) – Conținut și structură. Ediția a treia: 1983
ISO/IEC 7816-5	Tehnologia informației – Carduri de identificare – Carduri cu circuit(e) integrat(e) cu contacte – Partea 5: Sistemul de numerotare și procedura de înregistrare pentru identificatorii de aplicație. Prima ediție: 1994 + Modificarea 1: 1996
ISO/IEC 8824-1	Tehnologia informației – Notația specificațiilor structurilor de date în conversiile sintactice numărul unu (ASN.1): Specificații privind notarea de bază. Ediția a doua: 1998
ISO/IEC 8825-2	Tehnologia informației – Reguli de codare ASN.1: Specificații privind Regulile de codare condensată (PER). Ediția a doua: 1998
ISO/IEC 8859-1	Tehnologia informației – Set de caractere grafice codate în octet unic – Partea 1: Alfabetul latin nr. 1. Prima ediție: 1998
ISO/IEC 8859-7	Tehnologia informației – Set de caractere grafice codate în octet unic – Partea 7: Alfabetul latin/grec. Prima ediție: 1987
ISO 16844-3	Vehicule rutiere – Sisteme de tahograf – Interfața senzorului de mișcare. WD 3-20/05/99.

2. DEFINIREA TIPURILOR DE DATE

Pentru fiecare din următoarele tipuri de date, valoarea implicită corespundătoare conținutului «necunoscut» sau «nu este cazul» va consta din completarea elementului de date cu octeți «FF».

2.1. ActivityChangeInfo

Acest tip de date permite codarea, într-un cuvânt de doi octeți, a stării lectorului la 00.00 și/sau a stării șoferului la 00.00 și/sau a modificărilor de activitate și/sau a modificărilor modului de conducere și/sau a modificărilor stării cardului șoferului sau copilotului. Acest tip de date se raportează la cerințele 084, 109a, 199 și 219.

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

Atribuirea valorii – Octet aliniat: 's'p'aattttttttttt'B (16 biți)

Pentru înregistrările în memorie (sau starea lectorului):

's'B	Lector:
'0'B:	ȘOFER
'1'B:	COPILOT
'c'B	Modul de conducere:
'0'B:	SINGUR
'1'B:	ECHIPAJ
'p'B	Starea cardului șoferului (sau al atelierului) în lectorul adecvat:
'0'B:	INTRODUS, cardul este introdus
'1'B:	NEINTRODUS, nu s-a introdus nici un card (sau se retrage cardul)
'aa'B	Activitate:
'00'B:	PAUZĂ/ODIHNĂ
'01'B:	DISPONIBILITATE
'10'B:	MUNCĂ
'11'B:	CONDUCERE
'ttttttttttt'B	Momentul modificării: Numărul de minute de la 00h00 în ziua respectivă.

Pentru înregistrările de pe cardul șoferului (sau al atelierului) (și ale stării șoferului):

's'B	Lector (nu este relevant dacă 'p' = 1, cu excepția notei de mai jos):
'0'B:	ȘOFER
'1'B:	COPILOT
'c'B	Modul de conducere (cazul 'p' = 0) sau Starea următoarei activități (cazul 'p' = 1):
'0'B:	SINGUR
'0'B:	NECUNOSCUȚĂ
'1'B:	ECHIPAJ
'1'B:	CUNOSCUȚĂ (= introdus manual)
'p'B	Starea cardului:
'0'B:	INTRODUS, cardul este introdus în aparatul de înregistrare
'1'B:	NEINTRODUS, nu s-a introdus nici un card (sau se retrage cardul)

'aa'B	Activitate (nu este relevantă dacă 'p' = 1 și 'c' = 0, cu excepția notei de mai jos):
'00'B:	PAUZĂ/ODIHNĂ
'01'B:	DISPONIBILITATE
'10'B:	MUNCĂ
'11'B:	CONDUCERE
'ttttttttttt'B	Momentul modificării: Numărul de minute de la 00h00 în ziua dată.

Notă pentru cazul de «retragere a cardului»:

La retragerea cardului:

- 's' este relevant și indică lectorul din care a fost retras cardul
- 'c' trebuie să fie setat la 0
- 'p' trebuie să fie setat la 1
- 'aa' trebuie să codeze activitatea curentă selectată în acel moment

Ca urmare a unei introduceri manuale de date, biții 'c' și 'aa' din cuvânt (stocați pe un card) pot fi înlocuiți mai târziu pentru a reflecta introducerea de date.

2.2. Address

O adresă.

Address ::= SEQUENCE {

```

    codePage                      INTEGER (0..255),
    address                       OCTET STRING (SIZE(35))
}
```

codePage precizează partea din standardul ISO/IEC 8859 folosită la codarea adresei,

address este o adresă codată conform paginii adecvate de coduri din standardul ISO/IEC 8859.

2.3. BCDString

BCDString se aplică pentru o reprezentare a zecimalei în cod binar (BCD). Acest tip de date se utilizează pentru a reprezenta o unitate zecimală într-un semioctet (4 biți). BCDString se bazează pe ISO/IEC 8824-1 'CharacterStringType'.

```

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

BCDString folosește o notare «hstring». Caracterul din extremitatea stângă a șirului hexadecimal este cel mai important semioctet din primul octet. Pentru a obține un multiplu de octeți, se inserează semiocteți nuli, în cantitatea necesară, din poziția semioctetului din extremitatea stângă a primului octet.

Cifrele permise sunt: 0, 1, ..., 9.

2.4. CalibrationPurpose

Cod care explică de ce s-a înregistrat un set de parametri de calibrare. Acest tip de date se raportează la cerințele 097 și 098.

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

Atribuirea valorii:

'00'H valoare rezervată

'01'H activare: înregistrarea parametrilor de calibrare cunoscuți în momentul activării UV

'02'H prima instalare: prima calibrare a UV după prima activare a acesteia

'03'H instalare: prima calibrare a UV în vehiculul în cauză

'04'H inspecție periodică

2.5. CardActivityDailyRecord

Informații, stocate pe un card, privind activitățile șoferului într-o anumită zi calendaristică. Acest tip de date se raportează la cerințele 199 și 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 este lungimea totală în octeți a înregistrării zilnice anterioare. Valoarea maximă este dată de lungimea ȘIRULUI DE OCTEȚI care conține aceste înregistrări [vezi CardActivityLengthRange în alineatul (3)]. Atunci când această înregistrare devine cea mai veche înregistrare zilnică, valoarea lui activityPreviousRecordLength trebuie setată la 0.

activityRecordLength este lungimea totală în octeți a acestei înregistrări. Valoarea maximă este dată de lungimea ȘIRULUI DE OCTEȚI care conține aceste înregistrări.

activityRecordDate este data înregistrării.

activityDailyPresenceCounter este contorul prezenței zilnice pentru card în ziua respectivă.

activityDayDistance este distanța totală parcursă în ziua respectivă.

activityChangeInfo este setul de date ActivityChangeInfo pentru șofer în ziua respectivă. Acesta poate conține maximum 1 440 valori (o activitate pe minut). Acest set de date cuprinde întotdeauna activityChangeInfo care codează starea șoferului la 00.00.

2.6. CardActivityLengthRange

Numărul de octeți de pe un card al șoferului sau un card al atelierului, disponibil pentru stocarea înregistrărilor privind activitatea șoferului.

```
CardActivityLengthRange ::= INTEGER(0..216-1)
```

Atribuirea valorii: vezi alineatul (3).

2.7. CardApprovalNumber

Numărul de omologare al cardului.

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

Atribuirea valorii: Neprecizată.

2.8. CardCertificate

Certificat al cheii publice a cardului.

```
CardCertificate ::= Certificate
```

2.9. CardChipIdentification

Informații, stocate pe un card, privind identificarea Circuitului integrat (CI) al cardului (cerința 191).

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

icSerialNumber este numărul de serie al circuitului integrat (CI) definit în EN 726-3.

icManufacturingReferences reprezintă identificatorul producătorului circuitului integrat și elementele de fabricație definite în EN 726-3.

2.10. CardConsecutiveIndex

Un indice secvential al cardului [definitia h)].

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

Atribuirea valorii: (vezi capitolul VII din prezenta anexă)

Ordine de incrementare: '0, ..., 9, A, ..., Z, a, ..., z'.

2.11. CardControlActivityDataRecord

Informații, stocate pe un card al șoferului sau al atelierului, privind ultimul control la care a fost supus șoferul (cerințele 210 și 225).

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

controlType este tipul controlului.

controlTime reprezintă data și ora controlului.

controlCardNumber este numărul complet al cardului inspectorului de control care a efectuat controlul.

controlVehicleRegistration este numărul de înmatriculare al vehiculului (VRN) și statul membru de înmatriculare a vehiculului supus controlului.

controlDownloadPeriodBegin și **controlDownloadPeriodEnd** reprezintă perioada descărcată, în cazul în care se efectuează o descărcare de date.

2.12. CardCurrentUse

Informații privind utilizarea efectivă a cardului (cerința 212).

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

sessionOpenTime este ora la care cardul a fost introdus pentru utilizarea curentă. Acest element se setează la 0 în momentul retragerii cardului.

sessionOpenVehicle este identificarea vehiculului utilizat în prezent, la introducerea cardului. Acest element se setează la 0 în momentul retragerii cardului.

2.13. CardDriverActivity

Informații, stocate pe un card al șoferului sau al atelierului, privind activitățile șoferului (cerințele 199 și 219).

[illegible]

activityPointerOldestDayRecord este specificarea începutului locației de stocare în memorie (numărul de octeți de la începutul șirului) în cea mai veche înregistrare completă aferentă unei zile din șirul activityDailyRecords. Valoarea maximă este dată de lungimea șirului.

activityPointerNewestDayRecord este specificarea începutului locației de stocare în memorie (numărul de octeți de la începutul șirului) în cea mai recentă înregistrare completă aferentă unei zile din șirul activityDailyRecords. Valoarea maximă este dată de lungimea șirului.

activityDailyRecords este spațiul disponibil pentru stocarea datelor privind activitatea șoferului (structura datelor: CardActivityDailyRecord) pentru fiecare zi calendaristică în care s-a utilizat cardul.

Atribuirea valorii: acest șir de octeți este completat în mod ciclic cu înregistrări din CardActivityDailyRecord. La prima utilizare, stocarea începe la primul octet din șir. Toate înregistrările noi se adaugă la sfârșitul înregistrării anterioare respective. Atunci când șirul devine complet, stocarea se reia de la primul octet din șir, indiferent dacă există o întrerupere în interiorul unui element de date. Înainte de a plasa noi date privind activitatea în șir (prin extinderea activityDailyRecord curent sau prin introducerea unui nou activityDailyRecord) care să înlocuiască datele mai vechi privind activitatea, activityPointerOldestDayRecord trebuie actualizat pentru a indica noua locație a celei mai vechi înregistrări complete aferente unei zile, iar activityPreviousRecordLength pentru această (nouă) cea mai veche înregistrare zilnică completă trebuie resetat la 0.

2.14. CardDrivingLicenceInformation

Informații, stocate pe un card al șoferului, privind permisul de conducere al titularului cardului (cerința 196).

```
CardDrivingLicenceInformation ::= SEQUENCE {
    drivingLicenceIssuingAuthority      Name,
    drivingLicenceIssuingNation         NationNumeric,
    drivingLicenceNumber                 IA5String(SIZE(16))
}
```

drivingLicenceIssuingAuthority este autoritatea care răspunde de eliberarea permisului de conducere.

drivingLicenceIssuingNation este naționalitatea autorității care a eliberat permisul de conducere.

drivingLicenceNumber este numărul permisului de conducere.

2.15. CardEventData

Informații, stocate pe un card al șoferului sau al atelierului, privind evenimentele care se raportează la titularul cardului (cerințele 204 și 223).

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

CardEventData este o secvență, în ordine crescătoare a valorilor EventFaultType, a cardEventRecords (cu excepția înregistrărilor privind tentativele de violare a sistemului de securitate, care sunt cuprinse în ultimul set al secvenței).

cardEventRecords este o serie de înregistrări de evenimente pentru un anumit tip de evenimente (sau categorie pentru evenimentele privind tentativele de violare a sistemului de securitate).

2.16. CardEventRecord

Informații, stocate pe un card al șoferului sau al atelierului, privind un eveniment care se referă la titularul cardului (cerințele 205 și 223).

```
CardEventRecord ::= SEQUENCE {
    eventType                EventFaultType,
    eventBeginTime            TimeReal,
    eventEndTime              TimeReal,
    eventVehicleRegistration  VehicleRegistrationIdentification
}
```

eventType este tipul de eveniment.

eventBeginTime este data și ora la care a început evenimentul.

eventEndTime este data și ora la care s-a încheiat evenimentul.

eventVehicleRegistration este numărul de înmatriculare al vehiculului și statul membru de înmatriculare în care a avut loc evenimentul.

2.17. CardFaultData

Informații, stocate pe un card al șoferului sau al atelierului, privind anomaliile care se raportează la titularul cardului (cerințele 207 și 223).

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

CardFaultData este o secvență care cuprinde un set de înregistrări ale anomaliilor aparatului de înregistrare, urmat de un set de înregistrări privind anomaliile cardului.

cardFaultRecords este un set de înregistrări de anomalii dintr-o anumită categorie de anomalii (aparat de înregistrare sau card).

2.18. CardFaultRecord

Informații, stocate pe un card al șoferului sau al atelierului, privind o anomalie care se raportează la titularul cardului (cerințele 208 și 223).

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

faultType este tipul de anomalie.

faultBeginTime este data și ora la care a început anomalia.

faultEndTime este data și ora la care s-a încheiat anomalia.

faultVehicleRegistration este numărul de înmatriculare și statul membru de înmatriculare al vehiculului în care s-a produs anomalia.

2.19. CardIccIdentification

Informații, stocate pe un card, privind identificarea cardului cu circuit integrat (CI) (cerința 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 este modul Clockstop definit în EN 726-3.

cardExtendedSerialNumber este numărul de serie al cardului cu circuit integrat și referința producătorului cardului cu circuit integrat, definite în EN 726-3 și detaliate în tipul de date ExtendedSerialNumber.

cardApprovalNumber este numărul de omologare al cardului.

cardPersonaliserID este identificarea distinctă a cardului, definită în EN 726-3.

embedderIcAssemblerId este identificatorul integratorului/al asamblorului de circuit integrat definit în EN 726-3.

icIdentifier este identificatorul circuitului integrat de pe card și al producătorului circuitului integrat definit în EN 726-3.

2.20. CardIdentification

Informații, stocate pe un card, privind identificarea cardului (cerințele 194, 215, 231, 235).

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

cardIssuingMemberState este codul statului membru care emite cardul.

cardNumber este numărul de card al cardului.

cardIssuingAuthorityName este denumirea autorității care a emis cardul.

cardIssueDate este data emiterii cardului pentru titularul acestuia din prezent.

cardValidityBegin este data de la care cardul este valabil.

cardExpiryDate este data la care expiră valabilitatea cardului.

2.21. CardNumber

Un număr de card conform definiției de la litera (g).

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

driverIdentification este identificarea individuală a unui șofer într-un stat membru.

ownerIdentification este identificarea individuală a unei societăți, a unui atelier sau a unui organism de control în cadrul unui stat membru.

cardConsecutiveIndex este indicele secvențial al cardului.

cardReplacementIndex este indicele de înlocuire a cardului.

cardRenewalIndex este indicele de reînnoire a cardului.

Prima secvență din selecție este adecvată pentru a coda un număr de card al șoferului, a doua secvență din selecție este adecvată pentru a coda numerele de carduri al atelierului, de control și, respectiv, al societății.

2.22. CardPlaceDailyWorkPeriod

Informații, stocate pe un card al șoferului sau al atelierului, privind locurile în care începe și/sau se încheie activitatea de muncă cotidiană (cerințele 202 și 221).

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

placePointerNewestRecord este indicele ultimei înregistrări actualizate a locului.

Atribuirea valorii: Număr care corespunde contorului înregistrării locului, începând de la «0» pentru prima ocurență a înregistrărilor locului din structură.

placeRecords este seria de înregistrări care conțin informații privind locurile introduse.

2.23. CardPrivateKey

Cheia privată a unui card.

```
CardPrivateKey ::= RSAKeyPrivateExponent
```

2.24. CardPublicKey

Cheia publică a unui card.

```
CardPublicKey ::= PublicKey
```

2.25. CardRenewalIndex

Un indice de reînnoire a cardului [definiția (i)].

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

Atribuirea valorii: (vezi capitolul VII din prezenta anexă).

'0' Cardul original.

Ordin de creștere: '0, ..., 9, A, ..., Z'.

2.26. CardReplacementIndex

Un indice de înlocuire a cardului [definiția (j)].

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

Atribuirea valorii: (vezi capitolul VII din prezenta anexă).

'0' Cardul original.

Ordin de creștere: '0, ..., 9, A, ..., Z'.

2.27. CardSlotNumber

Cod care face distincția între cele două lectoare ale unității montate pe vehicul.

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

Atribuirea valorii: nu există specificații suplimentare în acest sens.

2.28. CardSlotStatus

Cod care indică tipurile de carduri introduse în cele două lectoare ale unității montate pe vehicul.

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

}

vehiclePointerNewestRecord este indicele ultimei înregistrări actualizate a vehiculului.

Atribuirea valorii: Număr care corespunde contorului înregistrărilor vehiculului, începând de la «0» pentru prima ocurență a înregistrărilor vehiculului în structură.

cardVehicleRecords este seria de înregistrări care conțin informații privind vehiculele utilizate.

2.32. Certificate

Certificatul unei chei publice emise de o autoritate de certificare.

Certificate ::= OCTET STRING (SIZE(194))

Atribuirea valorii: semnătură digitală cu recuperarea parțială a conținutului certificatului conform apendicelui 11: «Mecanisme de securitate comune»: Semnătura (128 octeți) || restul cheii publice (58 octeți) || referința autorității de certificare (8 octeți).

2.33. CertificateContent

Conținutul (accesibil) al certificatului unei chei publice conform apendicelui 11: «Mecanisme de securitate comune».

```
CertificateContent ::= SEQUENCE {
    certificateProfileIdentifier      INTEGER(0..255),
    certificationAuthorityReference  KeyIdentifier,
    certificateHolderAuthorisation    CertificateHolderAuthorisation,
    certificateEndOfValidity          TimeReal,
    certificateHolderReference        KeyIdentifier,
    publicKey                        PublicKey
}
```

certificateProfileIdentifier este versiunea certificatului corespunzător.

Atribuirea valorii:
'01h' pentru această versiune.

CertificationAuthorityReference precizează autoritatea de certificare care a emis certificatul. De asemenea, aceste date desemnează cheia publică a autorității de certificare în cauză.

certificateHolderAuthorisation precizează drepturile deținătorului certificatului.

certificateEndOfValidity este data la care certificatul expiră din punct de vedere administrativ.

certificateHolderReference identifică deținătorul certificatului. De asemenea, aceste date desemnează cheia publică a deținătorului de certificat în cauză.

publicKey este cheia publică certificată prin intermediul certificatului în cauză.

2.34. CertificateHolderAuthorisation

Identificarea drepturilor unui deținător de certificat.

```
CertificateHolderAuthorisation ::= SEQUENCE {
    tachographApplicationID          OCTET STRING (SIZE(6))
    equipmentType                    EquipmentType
}
```

tachographApplicationID este identificatorul de aplicație pentru aplicația de tahograf.

Atribuirea valorii: 'FFh' '54h' '41h' '43h' '48h' '4Fh'. Acest ID al aplicației este un identificator de aplicație exclusiv neomologat conform standardului ISO/IEC 7816-5.

equipmentType este identificarea tipului de aparat pentru care se emite certificatul.

Atribuirea valorii: în conformitate cu tipul de date EquipmentType. 0, dacă certificatul este emis de unul din statele membre.

2.35. CertificateRequestID

Identificarea individuală a unei cereri de certificat. Se poate utiliza și ca Identificator al cheii publice a vehiculului dacă numărul de serie al unității montate pe vehicul căreia îi este destinată cheia nu este cunoscut în momentul emiterii certificatului.

```
CertificateRequestID ::= SEQUENCE {
    requestSerialNumber          INTEGER(0..232-1)
    requestMonthYear             BCDString(SIZE(2))
    crIdentifier                 OCTET STRING(SIZE(1))
    manufacturerCode            ManufacturerCode
}
```

requestSerialNumber este un număr de serie aferent cererii de certificat, fiind un număr unic pentru producător și pentru luna definită mai jos.

requestMonthYear este identificarea lunii și a anului în care s-a depus cererea de certificat.

Atribuirea valorii: Codarea BCD a lunii (două cifre) și a anului (ultimele două cifre).

crIdentifier: este un identificador care are rolul de a face distincția între o cerere de certificat și un număr de serie complet.

Atribuirea valorii: «FFh».

manufacturerCode este codul numeric al producătorului care solicită acordarea certificatului.

2.36. CertificationAuthorityKID

Identificatorul cheii publice a unei autorități de certificare (un stat membru sau Autoritatea europeană de certificare).

```
CertificationAuthorityKID ::= SEQUENCE {
    nationNumeric                NationNumeric
    nationAlpha                  NationAlpha
    keySerialNumber              INTEGER(0..255)
    additionalInfo               OCTET STRING(SIZE(2))
    caIdentifier                 OCTET STRING(SIZE(1))
}
```

nationNumeric este codul numeric național al autorității de certificare.

nationAlpha este codul alfanumeric național al autorității de certificare.

keySerialNumber este numărul de serie care face distincția între diferitele chei ale autorității de certificare dacă aceste chei se modifică.

additionalInfo este un câmp de doi octeți pentru introducerea unor codări suplimentare (specifice autorității de certificare).

caIdentifier este un identificador care face distincția dintre un Identificator al cheii autorității de certificare și identificadorii altor chei.

Atribuirea valorii: '01h'.

2.37. CompanyActivityData

Informații, stocate pe un card al societății, privind activitățile efectuate prin intermediul cardului (cerința 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 este indicele ultimei înregistrări a activității societății actualizate de sistem.

Atribuirea valorii: Număr care corespunde contorului înregistrărilor activităților societății, începând de la «0» pentru prima ocurență a unei înregistrări a activității societății în structură.

companyActivityRecords este o serie a tuturor înregistrărilor activităților societății.

companyActivityRecord este o secvență de informații privind o activitate a societății.

companyActivityType este tipul de activitate a societății.

companyActivityTime este data și ora la care se desfășoară activitatea societății.

cardNumberInformation reprezintă numărul cardului și statul membru care a emis cardul pentru cardul descărcat, dacă este cazul.

vehicleRegistrationInformation reprezintă VRN-ul și statul membru de înmatriculare a vehiculului care au fost descărcate, blocate sau deblocate.

downloadPeriodBegin și **downloadPeriodEnd** reprezintă perioada descărcată din unitatea montată pe vehicul, dacă este cazul.

2.38. CompanyActivityType

Cod care indică o activitate desfășurată de o societate prin utilizarea propriului card al societății.

```

CompanyActivityType ::= INTEGER {
    card downloading                (1),
    VU downloading                  (2),
    VU lock-in                       (3),
    VU lock-out                      (4)
}

```

2.39. CompanyCardApplicationIdentification

Informații, stocate pe un card al societății, privind identificarea aplicației de pe card (cerința 190).

```

CompanyCardApplicationIdentification ::= SEQUENCE {
    typeOfTachographCardId          EquipmentType,
    cardStructureVersion             CardStructureVersion,
    noOfCompanyActivityRecords       NoOfCompanyActivityRecords
}

```

typeOfTachographCardId precizează tipul de card implementat.

cardStructureVersion precizează versiunea structurii implementate în card.

noOfCompanyActivityRecords este numărul înregistrărilor activităților societății care pot fi stocate pe card.

2.40. CompanyCardHolderIdentification

Informații, stocate pe un card al societății, privind identificarea titularului cardului (cerința 236).

```

CompanyCardHolderIdentification ::= SEQUENCE {
    companyName                      Name,
    companyAddress                   Address,
    cardHolderPreferredLanguage      Language
}

```

companyName este numele societății deținătoare.

companyAddress este adresa societății deținătoare.

cardHolderPreferredLanguage este limba preferată de titularul cardului.

2.41. ControlCardApplicationIdentification

Informații, stocate pe un card de control, privind identificarea aplicației de pe card (cerința 190).

```
ControlCardApplicationIdentification ::= SEQUENCE {
    typeOfTachographCardId      EquipmentType,
    cardStructureVersion         CardStructureVersion,
    noOfControlActivityRecords   NoOfControlActivityRecords
}
```

typeOfTachographCardId precizează tipul de card implementat.

cardStructureVersion precizează versiunea structurii implementate în card.

noOfControlActivityRecords este numărul înregistrărilor activităților de control care pot fi stocate pe card.

2.42. ControlCardControlActivityData

Informații, stocate pe un card de control, privind activitățile de control efectuate prin intermediul cardului (cerința 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 este indicele ultimei înregistrări a activității de control actualizate de sistem.

Atribuirea valorii: Număr care corespunde contorului înregistrărilor activităților de control, începând de la «0» pentru prima ocurență a unei înregistrări a activității de control în structură.

controlActivityRecords este o serie a tuturor înregistrărilor activităților de control.

controlActivityRecord este o secvență de informații privind o activitate de control.

controlType este tipul de control.

controlTime este data și ora la care se desfășoară controlul.

controlledCardNumber reprezintă numărul cardului și statul membru emitent de card al cardului controlat.

controlledVehicleRegistration reprezintă VRN-ul și statul membru de înmatriculare a vehiculului în care s-a efectuat controlul.

controlDownloadPeriodBegin și **controlDownloadPeriodEnd** reprezintă perioada descărcată de pe card, dacă este cazul.

2.43. ControlCardHolderIdentification

Informații, stocate pe un card de control, privind identificarea titularului cardului (cerința 232).

```
ControlCardHolderIdentification ::= SEQUENCE {
    controlBodyName                Name,
    controlBodyAddress             Address,
    cardHolderName                 HolderName,
    cardHolderPreferredLanguage    Language
}
```

controlBodyName este numele organismului de control al titularului cardului.

controlBodyAddress este adresa organismului de control al titularului cardului.

cardHolderName este numele și prenumele titularului cardului de control.

cardHolderPreferredLanguage este limba preferată de către titularul cardului.

2.44. ControlType

Cod care indică activitățile desfășurate în timpul unui control. Acest tip de date se raportează la cerințele 102, 210 și 225.

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

Atribuirea valorii – Octet aliniat: 'c'p'dxxxx'B (8 biți)

'c'B	descărcarea informațiilor de pe card:
'0'B:	informațiile de pe card nu sunt descărcate în timpul acestei activități de control
'1'B:	informațiile de pe card sunt descărcate în timpul acestei activități de control
'v'B	descărcarea informațiilor din UV:
'0'B:	informațiile din UV nu sunt descărcate în timpul acestei activități de control
'1'B:	informațiile din UV sunt descărcate în timpul acestei activități de control
'p'B	imprimarea:
'0'B:	nu se efectuează imprimarea datelor în timpul acestei activități de control
'1'B:	se efectuează imprimarea datelor în timpul acestei activități de control
'd'B	afișajul:
'0'B:	nu se utilizează afișajul în timpul acestei activități de control
'1'B:	se utilizează afișajul în timpul acestei activități de control
'xxxx'B	Nu se utilizează.

2.45. CurrentDateTime

Data și ora din momentul respectiv, afișate de aparatul de înregistrare.

```
CurrentDateTime ::= TimeReal
```

Atribuirea valorii: nu se furnizează indicații suplimentare.

2.46. DailyPresenceCounter

Contor, stocat într-un driver de pe cardul șoferului sau al atelierului, incrementat cu o unitate pentru fiecare zi calendaristică din momentul în care cardul a fost introdus într-o UV. Acest tip de date se raportează la cerințele 199 și 219.

```
DailyPresenceCounter ::= BCDString(SIZE(2))
```

Valoarea atribuită: Numerotare consecutivă, cu valoare maximă = 9 999, începând apoi din nou de la 0. În momentul primei emiteri a cardului, numerotarea este setată la 0.

2.47. Datef

Data exprimată în format numeric care poate fi imprimat pe loc.

```
Datef ::= SEQUENCE {
    year      BCDString(SIZE(2)),
    month     BCDString(SIZE(1)),
    day       BCDString(SIZE(1))
}
```

Atribuirea valorii:

YYYY	anul
mm	luna
dd	ziua

'00000000'H denotă în mod explicit absența unei date.

2.48. Distance

Distanța parcursă (rezultatul calculării diferenței dintre două valori afișate de contorul de parcurs al unui vehicul, în kilometri).

```
Distance ::= INTEGER(0..216-1)
```

Atribuirea valorii: Binar fără semn. Valoarea în kilometri în domeniul de valori 0-9 999 km.

2.49. DriverCardApplicationIdentification

Informații, stocate pe un card al șoferului, privind identificarea aplicației de pe card (cerința 190).

```
DriverCardApplicationIdentification ::= SEQUENCE {
    typeOfTachographCardId      EquipmentType,
    cardStructureVersion         CardStructureVersion,
    noOfEventsPerType            NoOfEventsPerType,
    noOfFaultsPerType           NoOfFaultsPerType,
    activityStructureLength      CardActivityLengthRange,
    noOfCardVehicleRecords      NoOfCardVehicleRecords,
    noOfCardPlaceRecords        NoOfCardPlaceRecords
}
```

typeOfTachographCardId precizează tipul de card implementat.

cardStructureVersion precizează versiunea structurii implementate în card.

noOfEventsPerType reprezintă numărul de evenimente în funcție de tipul de eveniment, pe care cardul le poate înregistra.

noOfFaultsPerType este numărul de anomalii, în funcție de tipul de anomalie, care pot fi înregistrate pe card.

activityStructureLength indică numărul de octeți disponibili pentru stocarea înregistrărilor activităților.

noOfCardVehicleRecords este numărul de înregistrări ale vehiculului care pot fi conținute de un card.

noOfCardPlaceRecords este numărul de locuri care pot fi înregistrate pe card.

2.50. DriverCardHolderIdentification

Informații, stocate pe un card al șoferului, privind identificarea titularului cardului (cerința 195).

```
DriverCardHolderIdentification ::= SEQUENCE {
    cardHolderName      HolderName,
    cardHolderBirthDate Datef,
    cardHolderPreferredLanguage Language
}
```

cardHolderName este numele și prenumele titularului cardului șoferului.

cardHolderBirthDate este data de naștere a titularului cardului șoferului.

cardHolderPreferredLanguage este limba preferată de titularul cardului.

2.51. EntryTypeDailyWorkPeriod

Cod care face distincția între începutul și sfârșitul unei înregistrări a locului unde s-a desfășurat o perioadă a activității zilnice și condițiile în care s-a realizat înregistrarea respectivă.

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)

}

Atribuirea valorii: conform standardului ISO/IEC8824-1.

2.52. EquipmentType

Cod care face distincția între diferitele tipuri de aparat pentru aplicația de tahograf.

EquipmentType ::= INTEGER(0..255)

-- Reserved	(0),
-- Driver Card	(1),
-- Workshop Card	(2),
-- Control Card	(3),
-- Company Card	(4),
-- Manufacturing Card	(5),
-- Vehicle Unit	(6),
-- Motion Sensor	(7),
-- RFU	(8..255)

Atribuirea valorii: Conform standardului ISO/IEC 8824-1.

Valoarea 0 este rezervată pentru a desemna un stat membru sau Europa în câmpul CHA din certificate.

2.53. EuropeanPublicKey

Cheia publică europeană.

EuropeanPublicKey ::= PublicKey

2.54. EventFaultType

Cod prin care se caracterizează un eveniment sau o anomalie.

EventFaultType ::= OCTET STRING (SIZE(1))

Atribuirea valorii:

'0x'H	Evenimente generale
'00'H	Fără detalii suplimentare
'01'H	Introducerea unui card nevalabil
'02'H	Conflict card
'03'H	Suprapunere a unor intervale de timp
'04'H	Conducere fără utilizarea cardului corespunzător
'05'H	Introducere a cardului în timpul condusului
'06'H	Ultima sesiune de utilizare a cardului incorect încheiată
'07'H	Depășire de viteză

'08'H	Întrerupere a alimentării cu curent
'09'H	Eroare a datelor de mișcare
'0A'H .. '0F'H	RUU
'1x'H	Evenimente legate de unitatea montată pe vehicul privind tentativele de violare a securității
'10'H	Fără detalii suplimentare
'11'H	Eroare de autentificare a senzorului de mișcare
'12'H	Eroare de autentificare a cardului de tahograf
'13'H	Modificare neautorizată a senzorului de mișcare
'14'H	Eroare de integritate afectând introducerea datelor pe card
'15'H	Eroare de integritate afectând datele stocate privind utilizatorul
'16'H	Eroare de transfer intern al datelor
'17'H	Deschidere neautorizată a carcasei
'18'H	Sabotare a echipamentului
'19'H .. '1F'H	RUU
'2x'H	Evenimente privind tentative de violare a securității legate de senzor
'20'H	Fără detalii suplimentare
'21'H	Eroare de autentificare
'22'H	Eroare de integritate afectând datele stocate
'23'H	Eroare de transfer intern al datelor
'24'H	Deschidere neautorizată a carcasei
'25'H	Sabotare a echipamentului
'26'H .. '2F'H	RUU
'3x'H	Anomalii la aparatul de înregistrare
'30'H	Fără detalii suplimentare
'31'H	Anomalie internă la UV
'32'H	Anomalie a imprimantei
'33'H	Anomalie de afișaj
'34'H	Anomalie la descărcarea informațiilor
'35'H	Anomalie a senzorului
'36'H .. '3F'H	RUU
'4x'H	Anomalii ale cardului
'40'H	Fără detalii suplimentare
'41'H .. '4F'H	RUU
'50'H .. '7F'H	RUU
'80'H .. 'FF'H	Specific producătorului

2.55. EventFaultRecordPurpose

Cod care explică de ce s-a înregistrat un anumit eveniment sau o anumită anomalie.

EventFaultRecordPurpose ::= OCTET STRING (SIZE(1))

Atribuirea valorii:

'00'H	unul dintre cele mai recente (sau ultimele) 10 evenimente sau anomalii
'01'H	evenimentul cu cea mai mare durată într-una din ultimele 10 zile în care a survenit
'02'H	unul dintre cele 5 evenimente cu cea mai lungă durată care au survenit în ultimele 365 de zile
'03'H	ultimul eveniment într-una din ultimele 10 zile în care a survenit
'04'H	cel mai grav eveniment într-una din ultimele 10 zile în care a survenit
'05'H	unul dintre cele mai grave 5 evenimente care au survenit în ultimele 365 de zile
'06'H	primul eveniment sau prima anomalie care a survenit după ultima calibrare
'07'H	un eveniment sau o anomalie în desfășurare
'08'H .. '7F'H	RUU
'80'H .. 'FF'H	specific producătorului

2.56. ExtendedSerialNumber

Identificare individuală a unui echipament. Poate fi utilizat și ca Identificator al cheii publice a unui echipament.

```
ExtendedSerialNumber ::= SEQUENCE {
    serialNumber                INTEGER(0..232-1)
    monthYear                   BCDString(SIZE(2))
    type OCTET                  STRING(SIZE(1))
    manufacturerCode            ManufacturerCode
}
```

serialNumber este numărul de serie al echipamentului, unic pentru producător, tipul echipamentului și luna descrisă în continuare.

monthYear este identificarea lunii și a anului de producție (sau a numărului de serie atribuit).

Atribuirea valorii: Codarea BCD a lunii (două cifre) și a anului (ultimele două cifre).

type este un identificator al tipului de echipament.

Atribuirea valorii: specifică producătorului, cu valoarea rezervată «FFh».

manufacturerCode este codul numeric al producătorului echipamentului.

2.57. FullCardNumber

Cod prin care se identifică complet un card de tahograf.

```
FullCardNumber ::= SEQUENCE {
    cardType                    EquipmentType,
    cardIssuingMemberState      NationNumeric,
    cardNumber                   CardNumber
}
```

cardType este tipul cardului de tahograf.

cardIssuingMemberState este codul statului membru care a emis cardul.

cardNumber este numărul cardului.

2.58. HighResOdometer

Valoarea indicată de contorul de parcurs al vehiculului; distanța cumulată parcursă de vehicul în timpul exploatării acestuia.

```
HighResOdometer ::= INTEGER(0..232-1)
```

Atribuirea valorii: Binar fără semn. Valoare exprimată în 1/200 km și cuprinsă în domeniul de valori 0-21 055 406 km.

2.59. HighResTripDistance

O distanță parcursă pe întreaga durată sau într-o parte a cursei.

```
HighResTripDistance ::= INTEGER(0..232-1)
```

Atribuirea valorii: Binar fără semn. Valoare exprimată în 1/200 km și cuprinsă în domeniul de valori 0-21 055 406 km.

2.60. HolderName

Numele și prenumele unui titular al cardului.

```
HolderName ::= SEQUENCE {
    holderSurname                Name,
    holderFirstNames             Name
}
```

holderSurname este numele (numele de familie) al titularului. Acest nume de familie nu cuprinde titluri.

Atribuirea valorii: dacă un astfel de card nu este personal, holderSurname conține aceleași informații ca și companyName, workshopName sau controlBodyName.

holderFirstNames reprezintă prenumele și inițialele titularului.

2.61. **K-ConstantOfRecordingEquipment**

Constanta aparatului de înregistrare [definiția (m)].

K-ConstantOfRecordingEquipment ::= INTEGER(0..2¹⁶-1)

Atribuirea valorii: Impulsuri pe kilometru într-un domeniu de valori de la 0 la 64 255 impulsuri/km.

2.62. **KeyIdentifier**

Un identificator unic al unei chei publice utilizat pentru a desemna și a selecta cheia respectivă. Acest identificator desemnează și deținătorul cheii.

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

Prima alternativă este adecvată pentru a desemna cheia publică a unei unități montate pe vehicul sau a unui card de tahograf.

A doua alternativă este adecvată pentru a desemna cheia publică a unei unități montate pe vehicul (în cazul în care numărul de serie al unității montate pe vehicul nu poate fi cunoscut în momentul eliberării certificatului).

A treia alternativă este adecvată pentru a desemna cheia publică a unui stat membru.

2.63. **L-Tyre Circumference**

Circumferința efectivă a pneurilor [definiția (u)].

L-TyreCircumference ::= INTEGER(0..2¹⁶-1)

Atribuirea valorii: Binar fără semn, valoarea exprimată în 1/8 mm și cuprinsă în domeniul de valori 0-8 031 mm.

2.64. **Language**

Codul de identificare a unei limbi.

Language ::= IA5String(SIZE(2))

Atribuirea valorii: O codare de două litere, minuscule, conform standardului ISO 639.

2.65. **LastCardDownload**

Data și ora, stocate pe un card al șoferului, la care s-a efectuat ultima descărcare a informațiilor de pe card (în alte scopuri decât în vederea unui control). Această dată poate fi actualizată de o UV sau de orice lector de card.

LastCardDownload ::= TimeReal

Atribuirea valorii: nu se furnizează indicații suplimentare.

2.66. **ManualInputFlag**

Cod care specifică dacă un titular de card a introdus manual activitățile șoferului la introducerea cardului sau nu (cerința 081).

```
ManualInputFlag ::= INTEGER {
    noEntry                (0)
    manualEntries          (1)
}
```

Atribuirea valorii: nu se furnizează indicații suplimentare.

2.67. ManufacturerCode

Cod de identificare al unui producător.

```
ManufacturerCode ::= INTEGER(0..255)
```

Atribuirea valorii:

'00'H	Nu există informații disponibile
'01'H	Valoare rezervată
'02'H .. '0F'H	Rezervat pentru o utilizare ulterioară
'10'H	ACTIA
'11'H .. '17'H	Rezervat pentru producătorii al căror nume începe cu 'A'
'18'H .. '1F'H	Rezervat pentru producătorii al căror nume începe cu 'B'
'20'H .. '27'H	Rezervat pentru producătorii al căror nume începe cu 'C'
'28'H .. '2F'H	Rezervat pentru producătorii al căror nume începe cu 'D'
'30'H .. '37'H	Rezervat pentru producătorii al căror nume începe cu 'E'
'38'H .. '3F'H	Rezervat pentru producătorii al căror nume începe cu 'F'
'40'H	Giesecke & Devrient GmbH
'41'H	GEM plus
'42'H .. '47'H	Rezervat pentru producătorii al căror nume începe cu 'G'
'48'H .. '4F'H	Rezervat pentru producătorii al căror nume începe cu 'H'
'50'H .. '57'H	Rezervat pentru producătorii al căror nume începe cu 'I'
'58'H .. '5F'H	Rezervat pentru producătorii al căror nume începe cu 'J'
'60'H .. '67'H	Rezervat pentru producătorii al căror nume începe cu 'K'
'68'H .. '6F'H	Rezervat pentru producătorii al căror nume începe cu 'L'
'70'H .. '77'H	Rezervat pentru producătorii al căror nume începe cu 'M'
'78'H .. '7F'H	Rezervat pentru producătorii al căror nume începe cu 'N'
'80'H	OSCARD
'81'H .. '87'H	Rezervat pentru producătorii al căror nume începe cu 'O'
'88'H .. '8F'H	Rezervat pentru producătorii al căror nume începe cu 'P'
'90'H .. '97'H	Rezervat pentru producătorii al căror nume începe cu 'Q'
'98'H .. '9F'H	Rezervat pentru producătorii al căror nume începe cu 'R'
'A0'H	SETEC
'A1'H	SIEMENS VDO
'A2'H	STONERIDGE
'A3'H .. 'A7'H	Rezervat pentru producătorii al căror nume începe cu 'S'
'AA'H	TACHOCONTROL
'AB'H .. 'AF'H	Rezervat pentru producătorii al căror nume începe cu 'T'
'B0'H .. 'B7'H	Rezervat pentru producătorii al căror nume începe cu 'U'
'B8'H .. 'BF'H	Rezervat pentru producătorii al căror nume începe cu 'V'
'C0'H .. 'C7'H	Rezervat pentru producătorii al căror nume începe cu 'W'
'C8'H .. 'CF'H	Rezervat pentru producătorii al căror nume începe cu 'X'
'D0'H .. 'D7'H	Rezervat pentru producătorii al căror nume începe cu 'Y'
'D8'H .. 'DF'H	Rezervat pentru producătorii al căror nume începe cu 'Z'

2.68. MemberStateCertificate

Certificatul unei chei publice a unui stat membru, eliberat de Autoritatea europeană de certificare.

```
MemberStateCertificate ::= Certificate
```

2.69. MemberStatePublicKey

Cheia publică a unui stat membru.

MemberStatePublicKey ::= PublicKey

2.70. Name

Un nume.

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

codePage precizează partea din standardul ISO/IEC 8859 care se utilizează pentru codarea numelui.

name este numele codat conform paginii corespunzătoare de coduri din standardul ISO/IEC 8859.

2.71. NationAlpha

Trimiterea alfabetică la o anumită țară, în conformitate cu modalitatea convențională de codare a numelor țărilor pe autocolantele de pe barele de protecție ale vehiculelor și/sau din documentele de asigurare ale vehiculelor armonizate la nivel internațional (cartea verde).

NationAlpha ::= IA5String(SIZE(3))

Atribuirea valorii:

' '	Nu există informații disponibile
'A'	Austria
'AL'	Albania
'AND'	Andorra
'ARM'	Armenia
'AZ'	Azerbaidjan
'B'	Belgia
'BG'	Bulgaria
'BIH'	Bosnia și Herțegovina
'BY'	Belarus
'CH'	Elveția
'CY'	Cipru
'CZ'	Republica Cehă
'D'	Germania
'DK'	Danemarca
'E'	Spania
'EST'	Estonia
'F'	Franța
'FIN'	Finlanda
'FL'	Liechtenstein
'FR'	Insulele Feroe
'UK'	Regatul Unit, Alderney, Guernesey, Jersey, Isle of Man, Gibraltar
'GE'	Georgia
'GR'	Grecia
'H'	Ungaria
'HR'	Croația
'I'	Italia
'IRL'	Irlanda
'IS'	Islanda
'KZ'	Kazahstan
'L'	Luxemburg
'LT'	Lituania
'LV'	Letonia
'M'	Malta
'MC'	Monaco

'MD'	Republica Moldova
'MK'	Macedonia
'N'	Norvegia
'NL'	Țările de Jos
'P'	Portugalia
'PL'	Polonia
'RO'	România
'RSM'	San Marino
'RUS'	Federația Rusă
'S'	Suedia
'SK'	Slovacia
'SLO'	Slovenia
'TM'	Turkmenistan
'TR'	Turcia
'UA'	Ucraina
'V'	Statul Vatican
'YU'	Iugoslavia
'UNK'	Necunoscut
'EC'	Comunitatea Europeană
'EUR'	Restul Europei
'WLD'	Restul lumii

2.7.2. NationNumeric

Cod numeric care desemnează o țară.

NationNumeric ::= INTEGER(0..255)

Atribuirea valorii:

-- Nu există informații disponibile	(00)H,
-- Austria	(01)H,
-- Albania	(02)H,
-- Andorra	(03)H,
-- Armenia	(04)H,
-- Azerbaidjan	(05)H,
-- Belgia	(06)H,
-- Bulgaria	(07)H,
-- Bosnia și Herțegovina	(08)H,
-- Belarus	(09)H,
-- Elveția	(0A)H,
-- Cipru	(0B)H,
-- Republica Cehă	(0C)H,
-- Germania	(0D)H,
-- Danemarca	(0E)H,
-- Spania	(0F)H,
-- Estonia	(10)H,
-- Franța	(11)H,
-- Finlanda	(12)H,
-- Liechtenstein	(13)H,
-- Insulele Feroe	(14)H,
-- Regatul Unit	(15)H,
-- Georgia	(16)H,
-- Grecia	(17)H,
-- Ungaria	(18)H,
-- Croația	(19)H,
-- Italia	(1A)H,
-- Irlanda	(1B)H,
-- Islanda	(1C)H,

-- Kazahstan	(1D) H,
-- Luxemburg	(1E) H,
-- Lituania	(1F) H,
-- Letonia	(20) H,
-- Malta	(21) H,
-- Monaco	(22) H,
-- Republica Moldova	(23) H,
-- Macedonia	(24) H,
-- Norvegia	(25) H,
-- Țările de Jos	(26) H,
-- Portugalia	(27) H,
-- Polonia	(28) H,
-- România	(29) H,
-- San Marino	(2A) H,
-- Federația Rusă	(2B) H,
-- Suedia	(2C) H,
-- Slovacia	(2D) H,
-- Slovenia	(2E) H,
-- Turkmenistan	(2F) H,
-- Turcia	(30) H,
-- Ucraina	(31) H,
-- Statul Vatican	(32) H,
-- Iugoslavia	(33) H,
-- RUU	(34 . . FC) H,
-- Comunitatea Europeană	(FD) H,
-- Restul Europei	(FE) H,
-- Restul lumii	(FF) H

2.73. NoOfCalibrationRecords

Numărul de înregistrări ale operațiunilor de calibrare care pot fi stocate pe un card al atelierului.

NoOfCalibrationRecords ::= INTEGER(0..255)

Atribuirea valorii: vezi alineatul (3).

2.74. NoOfCalibrationsSinceDownload

Contor care indică numărul de operațiuni de calibrare efectuate cu un card al atelierului de la ultima descărcare a informațiilor de pe cardul în cauză (cerința 230).

NoOfCalibrationsSinceDownload ::= INTEGER(0..2¹⁶-1),

Atribuirea valorii: Nu se furnizează indicații suplimentare.

2.75. NoOfCardPlaceRecords

Numărul de înregistrări de locuri care pot fi stocate pe un card al șoferului sau al atelierului.

NoOfCardPlaceRecords ::= INTEGER(0..255)

Atribuirea valorii: vezi alineatul (3).

2.76. NoOfCardVehicleRecords

Numărul de înregistrări privind vehiculele utilizate care pot fi stocate pe un card al șoferului sau al atelierului.

NoOfCardVehicleRecords ::= INTEGER(0..2¹⁶-1)

Atribuirea valorii: vezi alineatul (3).

2.77. NoOfCompanyActivityRecords

Numărul de înregistrări ale activităților societății care pot fi stocate pe un card al societății.

NoOfCompanyActivityRecords ::= INTEGER(0..2¹⁶-1)

Atribuirea valorii: vezi alineatul (3).

2.78. NoOfControlActivityRecords

Numărul de înregistrări ale activităților de control care pot fi stocate pe un card.

`NoOfControlActivityRecords ::= INTEGER(0..216-1)`

Atribuirea valorii: vezi alineatul (3).

2.79. NoOfEventsPerType

Numărul de evenimente, în funcție de tipul de eveniment, care pot fi stocate pe un card.

`NoOfEventsPerType ::= INTEGER(0..255)`

Atribuirea valorii: vezi alineatul (3).

2.80. NoOfFaultsPerType

Numărul de anomalii, în funcție de tipul de anomalie, care pot fi stocate pe un card.

`NoOfFaultsPerType ::= INTEGER(0..255)`

Atribuirea valorii: = vezi alineatul (3).

2.81. OdometerValueMidnight

Valoarea indicată de contorul de parcurs al vehiculului la miezul nopții într-o zi dată (cerința 090).

`OdometerValueMidnight ::= OdometerShort`

Atribuirea valorii: nu se furnizează indicații suplimentare.

2.82. OdometerShort

Valoarea indicată de contorul de parcurs al vehiculului, în formă prescurtată.

`OdometerShort ::= INTEGER(0..224-1)`

Atribuirea valorii: Binar fără semn. Valoare exprimată în kilometri și cuprinsă în domeniul de valori 0-9 999 999 km.

2.83. OverspeedNumber

Numărul evenimentelor de depășire de viteză de la ultimul control privind depășirea de viteză.

`OverspeedNumber ::= INTEGER(0..255)`

Atribuirea valorii: 0 înseamnă că nu s-a produs nici un eveniment de depășire de viteză de la ultimul control privind depășirea de viteză, 1 înseamnă că s-a produs un eveniment de depășire de viteză de la ultimul control privind depășirea de viteză, iar ...255 înseamnă că s-au produs 255 sau mai multe evenimente de depășire de viteză de la ultimul control privind depășirile de viteză.

2.84. PlaceRecord

Informații privind un loc unde începe sau se încheie o perioadă de muncă zilnică (cerințele 087, 202, 221).

```
PlaceRecord ::= SEQUENCE {
    entryTime                               TimeReal,
    entryTypeDailyWorkPeriod               EntryTypeDailyWorkPeriod,
    dailyWorkPeriodCountry                  NationNumeric,
    dailyWorkPeriodRegion                   RegionNumeric,
    vehicleOdometerValue                    OdometerShort
}
```

entryTime reprezintă data și ora aferente înregistrării.

entryTypeDailyWorkPeriod este tipul de înregistrare.

dailyWorkPeriodCountry este țara înregistrată.

dailyWorkPeriodRegion este regiunea înregistrată.

vehicleOdometerValue este valoarea contorului de parcurs în momentul efectuării înregistrării locului.

2.85. PreviousVehicleInfo

Informații privind vehiculul utilizat anterior de un șofer atunci când acesta și-a introdus cardul în unitatea montată pe vehicul (cerința 081).

```
PreviousVehicleInfo ::= SEQUENCE {
    vehicleRegistrationIdentification      VehicleRegistrationIdentification,
    cardWithdrawalTime                    TimeReal
}
```

vehicleRegistrationIdentification reprezintă VRN-ul vehiculului și statul membru de înmatriculare a acestuia.

cardWithdrawalTime reprezintă data și ora la care a fost retras cardul.

2.86. PublicKey

O cheie publică RSA.

```
PublicKey ::= SEQUENCE {
    rsaKeyModulus          RSAKeyModulus,
    rsaKeyPublicExponent   RSAKeyPublicExponent
}
```

rsaKeyModulus este modulul perechii de chei.

rsaKeyPublicExponent este exponentul public al perechii de chei.

2.87. RegionAlpha

Referință alfabetică la o regiune dintr-o anumită țară.

```
RegionAlpha ::= IA5STRING(SIZE(3))
```

Atribuirea valorii:

' ' Nu există informații disponibile.

Spania:

'AN'	Andalucía
'AR'	Aragón
'AST'	Asturias
'C'	Cantabria
'CAT'	Cataluña
'CL'	Castilla-León
'CM'	Castilla-La-Mancha
'CV'	Valencia
'EXT'	Extremadura
'G'	Galicia
'IB'	Baleares
'IC'	Canarias
'LR'	La Rioja
'M'	Madrid
'MU'	Murcia
'NA'	Navarra
'PV'	País Vasco

2.88. RegionNumeric

Referință numerică a unei regiuni dintr-o anumită țară.

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

Atribuirea valorii:

'00'H Nu există informații disponibile.

Spania:

'01'H Andalucía
 '02'H Aragón
 '03'H Asturias
 '04'H Cantabria
 '05'H Cataluña
 '06'H Castilla-León
 '07'H Castilla-La-Mancha
 '08'H Valencia
 '09'H Extremadura
 '0A'H Galicia
 '0B'H Baleares
 '0C'H Canarias
 '0D'H La Rioja
 '0E'H Madrid
 '0F'H Murcia
 '10'H Navarra
 '11'H País Vasco

2.89. RSAKeyModulus

Modulul unei perechi de chei RSA.

Atribuirea valorii: Neprecizată.

`RSAKeyModulus ::= OCTET STRING (SIZE(128))`

2.90. RSAKeyPrivateExponent

Exponentul privat al unei perechi de chei RSA.

Atribuirea valorii: Neprecizată.

`RSAKeyPrivateExponent ::= OCTET STRING (SIZE(128))`

2.91. RSAKeyPublicExponent

Exponentul public al unei perechi de chei RSA.

Atribuirea valorii: Neprecizată.

`RSAKeyPublicExponent ::= OCTET STRING (SIZE(8))`

2.92. SensorApprovalNumber

Numărul de omologare al senzorului.

Atribuirea valorii: Neprecizată.

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

2.93. SensorIdentification

Informații, stocate într-un senzor de mișcare, privind identificarea senzorului de mișcare (cerința 077).

```
SensorIdentification ::= SEQUENCE {
    sensorSerialNumber          SensorSerialNumber,
    sensorApprovalNumber       SensorApprovalNumber,
    sensorSCIdentifier          SensorSCIdentifier,
    sensorOSIdentifier          SensorOSIdentifier
}
```

sensorSerialNumber este numărul de serie complet al senzorului de mișcare (include numărul de componentă și codul producătorului).

sensorApprovalNumber este numărul de omologare al senzorului de mișcare.

sensorSCIdentifier este identificatorul componente de securitate a senzorului de mișcare.

sensorOSIdentifier este identificatorul sistemului de operare al senzorului de mișcare.

2.94. SensorInstallation

Informații, stocate într-un senzor de mișcare, privind instalarea senzorului de mișcare (cerința 099).

```
SensorInstallation ::= SEQUENCE {
    sensorPairingDateFirst          SensorPairingDate,
    firstVuApprovalNumber          VuApprovalNumber,
    firstVuSerialNumber            VuSerialNumber,
    sensorPairingDateCurrent       SensorPairingDate,
    currentVuApprovalNumber        VuApprovalNumber,
    currentVUSerialNumber          VuSerialNumber
}
```

sensorPairingDateFirst este data la care s-a efectuat prima cuplare a senzorului de mișcare cu unitatea montată pe vehicul.

firstVuApprovalNumber este numărul de omologare al primei unități montate pe vehicul cuplate la senzorul de mișcare.

firstVuSerialNumber este numărul de serie al primei unități montate pe vehicul cuplate la senzorul de mișcare.

sensorPairingDateCurrent este data cuplării din prezent a senzorului de mișcare la unitatea montată pe vehicul.

currentVuApprovalNumber este numărul de omologare al unității montate pe vehicul cuplată în prezent la senzorul de mișcare.

currentVUSerialNumber este numărul de serie al unității montate pe vehicul cuplată în prezent la senzorul de mișcare.

2.95. SensorInstallationSecData

Informații, stocate pe un card al atelierului, privind datele de securitate necesare pentru cuplarea senzorilor de mișcare la unitățile montate pe vehicul (cerința 214).

```
SensorInstallationSecData ::= TDesSessionKey
```

Atribuirea valorii: în conformitate cu standardul ISO 16844-3.

2.96. SensorOSIdentifier

Identificator al sistemului de operare al senzorului de mișcare.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Atribuirea valorii: specifică producătorului.

2.97. SensorPaired

Informații, stocate într-o unitate montată pe vehicul, privind identificarea senzorului de mișcare cuplat la unitatea montată pe vehicul (cerința 079).

```
SensorPaired ::= SEQUENCE {
    sensorSerialNumber          SensorSerialNumber,
    sensorApprovalNumber        SensorApprovalNumber,
    sensorPairingDateFirst      SensorPairingDate
}
```

sensorSerialNumber este numărul de serie al senzorului de mișcare cuplat în prezent la unitatea montată pe vehicul.

sensorApprovalNumber este numărul de omologare al senzorului de mișcare cuplat în prezent la unitatea montată pe vehicul.

sensorPairingDateFirst este data primei cuplări la unitatea montată pe vehicul a senzorului de mișcare cuplat în prezent la unitatea montată pe vehicul.

2.98. **SensorPairingDate**

Data cuplării unui senzor de mișcare la o unitate montată pe vehicul.

`SensorPairingDate ::= TimeReal`

Atribuirea valorii: Neprecizată.

2.99. **SensorSerialNumber**

Numărul de serie al senzorului de mișcare.

`SensorSerialNumber ::= ExtendedSerialNumber`

2.100. **SensorSCIdentifier**

Identificatorul componentei de securitate a senzorului de mișcare.

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

Atribuirea valorii: specifică producătorului componentei.

2.101. **Signature**

O semnătură digitală.

`Signature ::= OCTET STRING (SIZE(128))`

Atribuirea valorii: în conformitate cu apendicele 11, «Mecanisme de securitate comune».

2.102. **SimilarEventsNumber**

Numărul de evenimente similare dintr-o singură zi dată (cerința 094).

`SimilarEventsNumber ::= INTEGER(0..255)`

Atribuirea valorii: 0 nu se utilizează, 1 înseamnă că s-a produs și s-a înregistrat în acea zi un singur eveniment de tipul respectiv, 2 înseamnă că s-au produs două evenimente de tipul respectiv în ziua dată (a fost stocat numai unul), ...255 înseamnă că s-au produs 255 sau mai multe evenimente de tipul respectiv în ziua dată.

2.103. **SpecificConditionType**

Cod care desemnează o condiție specifică (cerințele 050b, 105a, 212a și 230a).

`SpecificConditionType ::= INTEGER(0..255)`

Atribuirea valorii:

'00'H	RUU
'01'H	În afara sferei de aplicare – Început
'02'H	În afara sferei de aplicare – Sfârșit
'03'H	Traseu parcurs pe feribot/în tren
'04'H .. 'FF'H	RUU

2.104. **SpecificConditionRecord**

Informații, stocate pe un card al șoferului, un card al atelierului sau într-o unitate montată pe vehicul, privind o condiție specifică (cerințele 105a, 212a și 230a).

```
SpecificConditionRecord ::= SEQUENCE {
    entryTime                               TimeReal,
    specificConditionType                   SpecificConditionType
}
```

entryTime reprezintă data și ora înregistrării.

specificConditionType este codul prin care se identifică condiția specifică.

2.105. **Speed**

Viteza vehiculului (km/h).

```
Speed ::= INTEGER(0..255)
```

Atribuirea valorii: kilometru pe oră în domeniul de valori 0-220 km/h.

2.106. **SpeedAuthorised**

Viteza maximă autorizată a vehiculului (definiția bb).

```
SpeedAuthorised ::= Speed
```

2.107. **SpeedAverage**

Viteza medie dintr-un interval stabilit în prealabil (km/h).

```
SpeedAverage ::= Speed
```

2.108. **SpeedMax**

Viteza maximă măsurată într-un interval stabilit în prealabil.

```
SpeedMax ::= Speed
```

2.109. **TDesSessionKey**

O cheie de sesiune triplă DES.

```
TDesSessionKey ::= SEQUENCE {
    tDesKeyA                               OCTET STRING (SIZE(8))
    tDesKeyB                               OCTET STRING (SIZE(8))
}
```

Atribuirea valorii: nu se furnizează indicații suplimentare.

2.110. **TimeReal**

Cod pentru un câmp combinat de dată și oră, unde data și ora se exprimă ca secunde peste 00h.00m.00s. la 1 ianuarie 1970 GMT.

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

Atribuirea valorii – Octet aliniat: Numărul de secunde începând de la miezul nopții în 1 ianuarie 1970 GMT.

Data/ora maximă posibilă este în anul 2106.

2.111. **TyreSize**

Indicarea dimensiunilor pneurilor.

```
TyreSize ::= IA5String(SIZE(15))
```

Atribuirea valorii: în conformitate cu Directiva 92/23/CEE din 31.03.1992, JO L 129, p. 95.

2.112. VehicleIdentificationNumber

Numărul de identificare al vehiculului (VIN) care desemnează vehiculul în ansamblu, fiind reprezentat în mod normal de numărul de serie al șasiului sau de numărul cadrului.

VehicleIdentificationNumber ::= IA5String(SIZE(17))

Atribuirea valorii: Conform definiției din standardul ISO 3779.

2.113. VehicleRegistrationIdentification

Identificarea unui vehicul, unică în Europa (VRN și statul membru).

```
VehicleRegistrationIdentification ::= SEQUENCE {
    vehicleRegistrationNation      NationNumeric,
    vehicleRegistrationNumber      VehicleRegistrationNumber
}
```

vehicleRegistrationNation este statul în care este înmatriculat vehiculul.

vehicleRegistrationNumber este numărul de înmatriculare al vehiculului (VRN).

2.114. VehicleRegistrationNumber

Numărul de înmatriculare al vehiculului (VRN). Numărul de înmatriculare este atribuit de autoritatea competentă în materie de înmatriculare a vehiculelor.

```
VehicleRegistrationNumber ::= SEQUENCE {
    codePage                      INTEGER (0..255),
    vehicleRegNumber              OCTET STRING (SIZE(13))
}
```

codePage precizează partea din standardul ISO/IEC 8859 utilizată pentru a coda numărul de înmatriculare al vehiculului.

vehicleRegNumber este un VRN codat conform paginii de coduri adecvate din standardul ISO/IEC 8859.

Atribuirea valorii: proprie fiecărei țări.

2.115. VuActivityDailyData

Informații, stocate într-o unitate montată pe vehicul, privind modificările activității și/sau ale modului de conducere și/sau modificările stării cardului într-o anumită zi calendaristică (cerința 084) și privind starea lectoarelor la 00.00h din acea zi.

```
VuActivityDailyData ::= SEQUENCE {
    noOfActivityChanges           INTEGER SIZE(0..1440),
    activityChangeInfos           SET SIZE(noOfActivityChanges) OF
                                ActivityChangeInfo
}
```

noOfActivityChanges este numărul cuvintelor de tip ActivityChangeInfo cuprinse în setul activityChangeInfos.

activityChangeInfos este setul de cuvinte de tip ActivityChangeInfo stocate în UV pe durata zilei. Acest set cuprinde întotdeauna două cuvinte de tip ActivityChangeInfo care indică starea celor două lectoare la ora 00.00 în ziua respectivă.

2.116. VuApprovalNumber

Numărul de omologare al unității montate pe vehicul.

VuApprovalNumber ::= IA5String(SIZE(8))

Atribuirea valorii: Neprecizată.

2.117. VuCalibrationData

Informații, stocate într-o unitate montată pe vehicul, privind operațiunile de calibrare a aparatului de înregistrare (cerința 098).

```
VuCalibrationData ::= SEQUENCE {
    noOfVuCalibrationRecords      INTEGER(0..255),
    vuCalibrationRecords SET      SIZE(noOfVuCalibrationRecords) OF
                                VuCalibrationRecord
}
```

noOfVuCalibrationRecords este numărul de înregistrări cuprinse în setul **vuCalibrationRecords**.

vuCalibrationRecords este setul de înregistrări de calibrare.

2.118. VuCalibrationRecord

Informații, stocate într-o unitate montată pe vehicul, privind o calibrare a aparatului de înregistrare (cerința 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 este scopul calibrării.

workshopName, **workshopAddress** reprezintă numele și adresa atelierului.

workshopCardNumber reprezintă cardul atelierului utilizat în timpul operațiunii de calibrare.

workshopCardExpiryDate este data de expirare a cardului.

vehicleIdentificationNumber este numărul de identificare al vehiculului.

vehicleRegistrationIdentification conține numărul de înmatriculare al vehiculului și statul membru de înmatriculare.

wVehicleCharacteristicConstant este constanta caracteristică a vehiculului.

kConstantOfRecordingEquipment este constanta aparatului de înregistrare.

lTyreCircumference este circumferința efectivă a pneurilor.

tyreSize este dimensiunea pneurilor montate pe vehicul.

authorisedSpeed este viteza autorizată a vehiculului.

oldOdometerValue, **newOdometerValue** reprezintă vechea și, respectiv, noua valoare indicată de contorul de parcurs.

oldTimeValue, **newTimeValue** reprezintă vechile și, respectiv, noile valori reprezentând data și ora.

nextCalibrationDate este data următoarei calibrări care corespunde tipului specificat în câmpul **CalibrationPurpose** și care va fi efectuată de autoritatea de inspecție competentă.

2.119. VuCardIWData

Informații, stocate într-o unitate montată pe vehicul, privind ciclurile de introducere și de retragere a cardurilor șoferului sau a cardurilor atelierului în unitatea montată pe vehicul (cerința 081).

```
VuCardIWData ::= SEQUENCE {
    noOfIWRecords                INTEGER(0..216-1),
    vuCardIWRecords              SET SIZE(noOfIWRecords) OF
                                VuCardIWRecord
}
```

noOfIWRecords este numărul de înregistrări cuprinse în setul **vuCardIWRecords**.

vuCardIWRecords este un set de înregistrări privind ciclurile de introducere și de retragere a cardurilor.

2.120. **VuCardIWRecord**

Informații, stocate într-o unitate montată pe vehicul, privind un ciclu de introducere și de retragere a unui card al șoferului sau al unui card al atelierului din unitatea montată pe vehicul (cerința 081).

```
VuCardIWRecord ::= SEQUENCE {
    cardHolderName                HolderName,
    fullCardNumber                FullCardNumber,
    cardExpiryDate                TimeReal,
    cardInsertionTime             TimeReal,
    vehicleOdometerValueAtInsertion OdometerShort,
    cardSlotNumber                CardSlotNumber,
    cardWithdrawalTime            TimeReal,
    vehicleOdometerValueAtWithdrawal OdometerShort,
    previousVehicleInfo            PreviousVehicleInfo
    manualInputFlag                ManualInputFlag
}
```

cardHolderName reprezintă numele și prenumele titularului unui card al șoferului sau al atelierului, așa cum sunt acestea stocate pe card.

fullCardNumber reprezintă tipul cardului, statul membru care l-a eliberat și numărul cardului, așa cum sunt stocate pe card.

cardExpiryDate este data de expirare a cardului, așa cum este stocată pe card.

cardInsertionTime reprezintă data și ora de introducere a cardului.

vehicleOdometerValueAtInsertion este valoarea indicată de contorul de parcurs al vehiculului în momentul introducerii cardului.

cardSlotNumber este lectorul în care se introduce cardul.

cardWithdrawalTime reprezintă data și ora de retragere a cardului.

vehicleOdometerValueAtWithdrawal este valoarea indicată de contorul de parcurs al vehiculului în momentul retragerii cardului.

previousVehicleInfo conține informații privind vehiculul precedent folosit de șofer, așa cum este acesta stocat pe card.

manualInputFlag este un cod prin care se indică dacă titularul cardului a introdus manual activitățile șoferului la introducerea cardului.

2.121. **VuCertificate**

Certificatul cheii publice a unității montate pe vehicul.

```
VuCertificate ::= Certificate
```

2.122. **VuCompanyLocksData**

Informații, stocate într-o unitate montată pe vehicul, privind blocările executate de societate (cerința 104).

```
VuCompanyLocksData ::= SEQUENCE {
    noOfLocks                INTEGER(0..20),
    vuCompanyLocksRecords    SET SIZE(noOfLocks) OF
                             VuCompanyLocksRecord
}
```

noOfLocks este numărul de blocări enumerate în **vuCompanyLocksRecords**.

vuCompanyLocksRecords este setul de înregistrări ale blocărilor executate de societate.

2.123. VuCompanyLocksRecord

Informații, stocate într-o unitate montată pe vehicul, privind o singură blocare executată de societate (cerința 104).

```
VuCompanyLocksRecord ::= SEQUENCE {
    lockInTime                TimeReal,
    lockOutTime               TimeReal,
    companyName               Name,
    companyAddress            Address,
    companyCardNumber         FullCardNumber
}
```

lockInTime, **lockOutTime** reprezintă data și ora blocării și, respectiv, a deblocării.

companyName, **companyAddress** reprezintă numele și adresa societății în raport cu blocarea.

companyCardNumber reprezintă cardul utilizat la blocare.

2.124. VuControlActivityData

Informații, stocate într-o unitate montată pe vehicul, privind controalele efectuate prin utilizarea unității montate pe vehicul respective (cerința 102).

```
VuControlActivityData ::= SEQUENCE {
    noOfControls               INTEGER(0..20),
    vuControlActivityRecords   SET SIZE(noOfControls) OF
                                VuControlActivityRecord
}
```

noOfControls este numărul de controale enumerate în **vuControlActivityRecords**.

vuControlActivityRecords este setul de înregistrări ale activităților de control.

2.125. VuControlActivityRecord

Informații, stocate într-o unitate montată pe vehicul, privind un control efectuat prin utilizarea unității montate pe vehicul respective (cerința 102).

```
VuControlActivityRecord ::= SEQUENCE {
    controlType                ControlType,
    controlTime                TimeReal,
    controlCardNumber          FullCardNumber,
    downloadPeriodBeginTime    TimeReal,
    downloadPeriodEndTime      TimeReal
}
```

controlType este tipul de control.

controlTime reprezintă data și ora la care s-a realizat controlul.

ControlCardNumber reprezintă cardul de control utilizat la efectuarea controlului.

downloadPeriodBeginTime este – în caz de descărcare – ora de începere a intervalului de descărcare a informațiilor.

downloadPeriodEndTime este – în caz de descărcare – ora de încheiere a intervalului de descărcare a informațiilor.

2.126. VuDataBlockCounter

Contor, stocat pe un card, care indică secvențial ciclurile de introducere și de retragere a cardului din unitățile montate pe vehicul.

```
VuDataBlockCounter ::= BCDString(SIZE(2))
```

Atribuirea valorii: numerotare consecutivă până la valoarea maximă de 9 999, iar apoi numerotarea reîncepe de la 0.

2.127. VuDetailedSpeedBlock

Informații, stocate într-o unitate montată pe vehicul, privind viteza detaliată a vehiculului timp de un minut în care vehiculul s-a aflat în mișcare (cerința 093).

```
VuDetailedSpeedBlock ::= SEQUENCE {
    speedBlockBeginDate          TimeReal,
    speedsPerSecond              SEQUENCE SIZE (60) OF Speed
}
```

speedBlockBeginDate este data și ora primei viteze cuprinse în blocul de date.

speedsPerSecond este secvența cronologică de viteze măsurate în fiecare secundă din minutul care a început cu **speedBlockBeginDate** (inclusiv).

2.128. VuDetailedSpeedData

Informații, stocate într-o unitate montată pe vehicul, privind viteza detaliată a vehiculului.

```
VuDetailedSpeedData ::= SEQUENCE
    noOfSpeedBlocks          INTEGER (0..216-1),
    vuDetailedSpeedBlocks    SET SIZE (noOfSpeedBlocks) OF
                             VuDetailedSpeedBlock
}
```

noOfSpeedBlocks este numărul de blocuri de date privind viteza din setul **vuDetailedSpeedBlocks**.

vuDetailedSpeedBlocks este setul de blocuri de date detaliate privind viteza.

2.129. VuDownloadablePeriod

Cele mai vechi și cele mai recente date în raport cu care unitatea montată pe vehicul conține informații privind activitățile șoferului (cerințele 081, 084 sau 087).

```
VuDownloadablePeriod ::= SEQUENCE {
    minDownloadableTime        TimeReal
    maxDownloadableTime        TimeReal
}
```

minDownloadableTime reprezintă cea mai veche dată și oră stocată în UV la care s-a realizat o introducere a cardului, o modificare a activității sau o înregistrare de loc.

maxDownloadableTime reprezintă cea mai recentă dată și oră stocată în UV la care s-a realizat o retragere a cardului, o modificare a activității sau o înregistrare de loc.

2.130. VuDownloadActivityData

Informații, stocate într-o unitate montată pe vehicul, privind ultima descărcare a acestuia (cerința 105).

```
VuDownloadActivityData ::= SEQUENCE {
    downloadingTime            TimeReal,
    fullCardNumber              FullCardNumber,
    companyOrWorkshopName      Name
}
```

downloadingTime este data și ora la care s-a realizat descărcarea informațiilor.

fullCardNumber reprezintă cardul utilizat pentru autorizarea descărcării.

companyOrWorkshopName este numele societății sau al atelierului.

2.131. VuEventData

Informații, stocate într-o unitate montată pe vehicul, privind anumite evenimente (cerința 094, cu excepția evenimentelor privind depășirile de viteză).

```
VuEventData ::= SEQUENCE {
    noOfVuEvents                INTEGER (0..255),
    vuEventRecords              SET SIZE (noOfVuEvents) OF VuEventRecord
}
```

noOfVuEvents este numărul de evenimente enumerate în setul **vuEventRecords**.

vuEventRecords este un set de înregistrări ale evenimentelor.

2.132. VuEventRecord

Informații, stocate într-o unitate montată pe vehicul, privind un eveniment (cerința 094, cu excepția evenimentelor legate de depășirile de viteză).

```
VuEventRecord ::= SEQUENCE {
    eventType                      EventFaultType,
    eventRecordPurpose             EventFaultRecordPurpose,
    eventBeginTime                 TimeReal,
    eventEndTime                   TimeReal,
    cardNumberDriverSlotBegin      FullCardNumber,
    cardNumberCodriverSlotBegin    FullCardNumber,
    cardNumberDriverSlotEnd        FullCardNumber,
    cardNumberCodriverSlotEnd      FullCardNumber,
    similarEventsNumber            SimilarEventsNumber
}
```

eventType este tipul de eveniment.

eventRecordPurpose este motivul pentru care s-a efectuat înregistrarea evenimentului respectiv.

eventBeginTime reprezintă data și ora de începere a evenimentului.

eventEndTime reprezintă data și ora la care s-a încheiat evenimentul.

cardNumberDriverSlotBegin reprezintă cardul introdus în lectorul șoferului la începutul evenimentului.

cardNumberCodriverSlotBegin reprezintă cardul introdus în lectorul copilotului la începutul evenimentului.

cardNumberDriverSlotEnd reprezintă cardul introdus în lectorul șoferului la sfârșitul evenimentului.

cardNumberCodriverSlotEnd reprezintă cardul introdus în lectorul copilotului la sfârșitul evenimentului.

similarEventsNumber este numărul evenimentelor similare care s-au produs în aceeași zi.

Această secvență poate fi utilizată pentru toate evenimentele, cu excepția evenimentelor de depășire de viteză.

2.133. VuFaultData

Informații, stocate într-o unitate montată pe vehicul, privind anomalii (cerința 096).

```
VuFaultData ::= SEQUENCE {
    noOfVuFaults                  INTEGER(0..255),
    vuFaultRecords SET             SIZE(noOfVuFaults) OF VuFaultRecord
}
```

noOfVuFaults este numărul anomaliilor enumerate în setul vuFaultRecords.

vuFaultRecords este setul de înregistrări ale anomaliilor.

2.134. VuFaultRecord

Informații, stocate într-o unitate montată pe vehicul, privind o anomalie (cerința 096).

```
VuFaultRecord ::= SEQUENCE {
    faultType                      EventFaultType,
    faultRecordPurpose             EventFaultRecordPurpose,
    faultBeginTime                 TimeReal,
    faultEndTime                   TimeReal,
    cardNumberDriverSlotBegin      FullCardNumber,
    cardNumberCodriverSlotBegin    FullCardNumber,
    cardNumberDriverSlotEnd        FullCardNumber,
    cardNumberCodriverSlotEnd      FullCardNumber
}
```

faultType este tipul de anomalie care afectează aparatul de înregistrare.

faultRecordPurpose este motivul pentru care s-a efectuat înregistrarea anomaliei respective.

faultBeginTime reprezintă data și ora de începere a anomaliei.

faultEndTime reprezintă data și ora de încetare a anomaliei.

cardNumberDriverSlotBegin reprezintă cardul introdus în lectorul șoferului la începutul anomaliei.

cardNumberCodriverSlotBegin reprezintă cardul introdus în lectorul copilotului la începutul anomaliei.

cardNumberDriverSlotEnd reprezintă cardul introdus în lectorul șoferului la încetarea anomaliei.

cardNumberCodriverSlotEnd reprezintă cardul introdus în lectorul copilotului la încetarea anomaliei.

2.135. **VuIdentification**

Informații, stocate într-o unitate montată pe vehicul, privind identificarea unității montate pe vehicul (cerința 075).

```
VuIdentification ::= SEQUENCE {
    vuManufacturerName          VuManufacturerName,
    vuManufacturerAddress       VuManufacturerAddress,
    vuPartNumber                VuPartNumber,
    vuSerialNumber              VuSerialNumber,
    vuSoftwareIdentification     VuSoftwareIdentification,
    vuManufacturingDate         VuManufacturingDate,
    vuApprovalNumber            VuApprovalNumber
}
```

vuManufacturerName este numele producătorului unității montate pe vehicul.

vuManufacturerAddress este adresa producătorului unității montate pe vehicul.

vuPartNumber este numărul de componentă al unității montate pe vehicul.

vuSerialNumber este numărul de serie al unității montate pe vehicul.

vuSoftwareIdentification identifică software-ul implementat în unitatea montată pe vehicul.

vuManufacturingDate este data de fabricație a unității montate pe vehicul.

vuApprovalNumber este numărul de omologare al unității montate pe vehicul.

2.136. **VuManufacturerAddress**

Adresa producătorului unității montate pe vehicul.

```
VuManufacturerAddress ::= Address
```

Atribuirea valorii: Neprecizată.

2.137. **VuManufacturerName**

Numele producătorului unității montate pe vehicul.

```
VuManufacturerName ::= Name
```

Atribuirea valorii: Neprecizată.

2.138. **VuManufacturingDate**

Data de fabricație a unității montate pe vehicul.

```
VuManufacturingDate ::= TimeReal
```

Atribuirea valorii: Neprecizată.

2.139. VuOverSpeedingControlData

Informații, stocate într-o unitate montată pe vehicul, privind evenimentele de depășire de viteză care s-au produs de la ultimul control al depășirilor de viteză (cerința 095).

```
VuOverSpeedingControlData ::= SEQUENCE {
    lastOverspeedControlTime      TimeReal,
    firstOverspeedSince           TimeReal,
    numberOfOverspeedSince        OverspeedNumber
}
```

lastOverspeedControlTime reprezintă data și ora la care s-a efectuat ultimul control al depășirilor de viteză.

firstOverspeedSince reprezintă data și ora primului eveniment de depășire de viteză după efectuarea controlului privind depășirea de viteză.

numberOfOverspeedSince este numărul de evenimente de depășire de viteză de la ultimul control al depășirilor de viteză.

2.140. VuOverSpeedingEventData

Informații, stocate într-o unitate montată pe vehicul, privind evenimentele de depășire de viteză (cerința 094).

```
VuOverSpeedingEventData ::= SEQUENCE {
    noOfVuOverSpeedingEvents      INTEGER(0..255),
    vuOverSpeedingEventRecords    SET SIZE(noOfVuOverSpeedingEvents) OF
                                   VuOverSpeedingEventRecord
}
```

noOfVuOverSpeedingEvents este numărul de evenimente enumerate în setul **vuOverSpeedingEventRecords**.

vuOverSpeedingEventRecords este un set de înregistrări ale evenimentelor de depășire de viteză.

2.141. VuOverSpeedingEventRecord

Informații, stocate într-o unitate montată pe vehicul, privind evenimentele de depășire de viteză (cerința 094).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
    eventType                     EventFaultType,
    eventRecordPurpose            EventFaultRecordPurpose,
    eventBeginTime                TimeReal,
    eventEndTime                  TimeReal,
    maxSpeedValue                 SpeedMax,
    averageSpeedValue             SpeedAverage,
    cardNumberDriverSlotBegin     FullCardNumber,
    similarEventsNumber           SimilarEventsNumber
}
```

eventType este tipul de eveniment.

eventRecordPurpose este scopul în care s-a realizat înregistrarea evenimentului în cauză.

eventBeginTime este data și ora de începere a evenimentului.

eventEndTime este data și ora la care evenimentul s-a încheiat.

maxSpeedValue este viteza maximă măsurată în timpul evenimentului.

averageSpeedValue este media aritmetică a vitezei măsurate în timpul evenimentului.

cardNumberDriverSlotBegin reprezintă cardul introdus în lectorul șoferului la începutul evenimentului.

similarEventsNumber este numărul de evenimente similare care s-au produs în ziua respectivă.

2.142. VuPartNumber

Numărul de componentă al unității montate pe vehicul.

```
VuPartNumber ::= IA5String(SIZE(16))
```

Atribuirea valorii: Proprie producătorului UV.

2.143. VuPlaceDailyWorkPeriodData

Informații, stocate într-o unitate montată pe vehicul, privind locurile în care șoferii încep sau încheie o perioadă de activitate zilnică (cerința 087).

```
VuPlaceDailyWorkPeriodData ::= SEQUENCE {
    noOfPlaceRecords                INTEGER(0..255),
    vuPlaceDailyWorkPeriodRecords   SET SIZE(noOfPlaceRecords) OF
                                   VuPlaceDailyWorkPeriodRecord
}
```

noOfPlaceRecords este numărul de înregistrări enumerate în setul **vuPlaceDailyWorkPeriodRecords**.

vuPlaceDailyWorkPeriodRecords este un set de înregistrări privind locul.

2.144. VuPlaceDailyWorkPeriodRecord

Informații, stocate într-o unitate montată pe vehicul, privind un loc în care un șofer începe sau încheie o perioadă de activitate zilnică (cerința 087).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
    fullCardNumber                  FullCardNumber,
    placeRecord                     PlaceRecord
}
```

fullCardNumber reprezintă tipul de card al șoferului, statul membru care a emis cardul și numărul cardului.

placeRecord conține informații privind locul înregistrat.

2.145. VuPrivateKey

Cheia privată a unei unități montate pe vehicul.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.146. VuPublicKey

Cheia publică a unei unități montate pe vehicul.

```
VuPublicKey ::= PublicKey
```

2.147. VuSerialNumber

Numărul de serie al unității montate pe vehicul (cerința 075).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.148. VuSoftInstallationDate

Data instalării versiunii de software în unitatea montată pe vehicul.

```
VuSoftInstallationDate ::= TimeReal
```

Atribuirea valorii: Neprecizată.

2.149. VuSoftwareIdentification

Informații, stocate într-o unitate montată pe vehicul, privind software-ul instalat.

```
VuSoftwareIdentification ::= SEQUENCE {
    vuSoftwareVersion                VuSoftwareVersion,
    vuSoftInstallationDate           VuSoftInstallationDate
}
```

vuSoftwareVersion este numărul versiunii software-ului instalat în unitatea montată pe vehicul.

vuSoftInstallationDate este data instalării versiunii de software.

2.150. VuSoftwareVersion

Numărul versiunii de software instalate în unitatea montată pe vehicul.

`VuSoftwareVersion ::= IA5String(SIZE(4))`

Atribuirea valorii: Neprecizată.

2.151. VuSpecificConditionData

Informații, stocate într-o unitate montată pe vehicul, privind condițiile specifice.

```
VuSpecificConditionData ::= SEQUENCE {
    noOfSpecificConditionRecords          INTEGER(0..216-1)
    specificConditionRecords              SET SIZE (noOfSpecificConditionRecords) OF
                                          SpecificConditionRecord
}
```

noOfSpecificConditionRecords este numărul de înregistrări enumerate în setul **specificConditionRecords**.

specificConditionRecords este un set de înregistrări privind condițiile specifice.

2.152. VuTimeAdjustmentData

Informații, stocate într-o unitate montată pe vehicul, privind operațiunile de reglare a orei efectuate în afara unei calibrări periodice (cerința 101).

```
VuTimeAdjustmentData ::= SEQUENCE {
    noOfVuTimeAdjRecords                 INTEGER(0..6),
    vuTimeAdjustmentRecords              SET SIZE (noOfVuTimeAdjRecords) OF
                                          VuTimeAdjustmentRecord
}
```

noOfVuTimeAdjRecords este numărul de înregistrări din **vuTimeAdjustmentRecords**.

vuTimeAdjustmentRecords este un set de înregistrări ale operațiunilor de reglare a orei.

2.153. VuTimeAdjustmentRecord

Informații, stocate într-o unitate montată pe vehicul, privind o operațiune de reglare a orei efectuată în afara unei calibrări periodice (cerința 101).

```
VuTimeAdjustmentRecord ::= SEQUENCE {
    oldTimeValue                         TimeReal,
    oldTimeValue                         TimeReal,
    newTimeValue                         TimeReal,
    workshopName                         Name,
    workshopAddress                      Address,
    workshopCardNumber                  FullCardNumber
}
```

oldTimeValue, **newTimeValue** sunt valorile vechi și, respectiv, noi ale datei și orei.

workshopName, **workshopAddress** reprezintă numele și adresa atelierului.

workshopCardNumber reprezintă cardul atelierului utilizat pentru a efectua operațiunile de reglare a orei.

2.154. W-VehicleCharacteristicConstant

Constanta caracteristică a vehiculului [definiția k)].

`W-VehicleCharacteristicConstant ::= INTEGER(0..216-1)`

Atribuirea valorii: Impulsuri pe kilometru în domeniul de valori 0-64 255 impulsuri/km.

2.155. WorkshopCardApplicationIdentification

Informații, stocate pe un card al atelierului, privind identificarea aplicației de pe card (cerința 190).

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
    typeOfTachographCardId          EquipmentType,
    cardStructureVersion             CardStructureVersion,
    noOfEventsPerType                NoOfEventsPerType,
    noOfFaultsPerType                NoOfFaultsPerType,
    activityStructureLength           CardActivityLengthRange,
    noOfCardVehicleRecords           NoOfCardVehicleRecords,
    noOfCardPlaceRecords             NoOfCardPlaceRecords,
    noOfCalibrationRecords           NoOfCalibrationRecords
}
```

typeOfTachographCardId precizează tipul de card implementat.

cardStructureVersion precizează versiunea structurii implementate în card.

noOfEventsPerType reprezintă numărul de evenimente în funcție de tipul de eveniment, pe care cardul le poate înregistra.

noOfFaultsPerType este numărul de anomalii în funcție de tipul de anomalie care pot fi înregistrate pe card.

activityStructureLength indică numărul de octeți disponibili pentru stocarea înregistrărilor activităților.

noOfCardVehicleRecords este numărul de înregistrări privind vehiculul care pot fi conținute de un card.

noOfCardPlaceRecords este numărul de locuri care pot fi înregistrate pe card.

noOfCalibrationRecords este numărul de înregistrări ale operațiunilor de calibrare care pot fi stocate pe card.

2.156. WorkshopCardCalibrationData

Informații, stocate pe un card al atelierului, privind activitatea din atelier efectuată prin intermediul cardului (cerințele 227 și 229).

```
WorkshopCardCalibrationData ::= SEQUENCE {
    calibrationTotalNumber           INTEGER(0..216-1),
    calibrationPointerNewestRecord    INTEGER(0..NoOfCalibrationRecords-1),
    calibrationRecords                SET SIZE(NoOfCalibrationRecords) OF
                                      WorkshopCardCalibrationRecord
}
```

calibrationTotalNumber este numărul total de operațiuni de calibrare efectuate prin intermediul cardului.

calibrationPointerNewestRecord este indicele ultimei înregistrări actualizate a unei calibrări.

Atribuirea valorii: Număr corespunzând contorului înregistrării de calibrare, începând cu «0» pentru prima ocurență a unei înregistrări de calibrare în structura respectivă.

calibrationRecords este un set de înregistrări care conțin informații privind calibrarea și/sau operațiunile de reglare a orei.

2.157. WorkshopCardCalibrationRecord

Informații, stocate pe un card al atelierului, privind o calibrare efectuată prin intermediul cardului (cerința 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 este scopul calibrării.

vehicleIdentificationNumber este numărul de identificare al vehiculului.

vehicleRegistration conține VRN și statul membru de înmatriculare.

wVehicleCharacteristicConstant este constanta caracteristică a vehiculului.

kConstantOfRecordingEquipment este constanta aparatului de înregistrare.

ITyreCircumference este circumferința efectivă a pneurilor.

tyreSize este dimensiunea pneurilor montate pe vehicul.

authorisedSpeed este viteza maximă autorizată a vehiculului.

oldOdometerValue, **newOdometerValue** reprezintă vechea și, respectiv, noua valoare indicată de contorul de parcurs.

oldTimeValue, **newTimeValue** reprezintă vechile și, respectiv, noile valori reprezentând data și ora.

nextCalibrationDate este data următoarei calibrări care corespunde tipului specificat în câmpul CalibrationPurpose și care va fi efectuată de autoritatea de inspecție competentă.

vuPartNumber, **vuSerialNumber** și **sensorSerialNumber** sunt elementele de date pentru identificarea aparatului de înregistrare.

2.158. WorkshopCardHolderIdentification

Informații, stocate pe un card al atelierului, privind identificarea titularului cardului (cerința 216).

```

WorkshopCardHolderIdentification ::= SEQUENCE {
    workshopName                Name,
    workshopAddress              Address,
    cardHolderName               HolderName,
    cardHolderPreferredLanguage  Language
}

```

workshopName este numele atelierului titularului cardului.

workshopAddress este adresa atelierului titularului cardului.

cardHolderName este numele și prenumele titularului cardului (de exemplu, numele mecanicului).

cardHolderPreferredLanguage este limba preferată de titularul cardului.

2.159. WorkshopCardPIN

Numărul individual de identificare al cardului atelierului (cerința 213).

```

WorkshopCardPIN ::= IA5String(SIZE(8))

```

Atribuirea valorii: PIN-ul cunoscut de titularul cardului, completat la dreapta cu o serie de octeți «FF» care poate conține până la 8 octeți.

3. DEFINIREA DOMENIILOR DE VALORI ȘI DE DIMENSIUNI

Definirea variabilelor utilizate în definițiile din alineatul (2).

TimeRealRange:: = $2^{32} - 1$

3.1. Definiții pentru cardul șoferului

Denumirea variabilei	Minim	Maxim
CardActivityLengthRange	5 544 octeți (28 zile 93 modificări de activitate pe zi)	13 776 octeți (28 zile 240 modificări de activitate pe zi)
NoOfCardPlaceRecords	84	112
NoOfCardVehicleRecords	84	200
NoOfEventsPerType	6	12
NoOfFaultsPerType	12	24

3.2. Definiții pentru cardul atelierului:

Denumirea variabilei	Minim	Maxim
CardActivityLengthRange	198 octeți (1 zi 93 modificări de activitate)	492 octeți (1 zi 240 modificări de activitate)
NoOfCardPlaceRecords	6	8
NoOfCardVehicleRecords	4	8
NoOfEventsPerType	3	3
NoOfEventsPerType	6	6
NoOfCalibrationRecords	88	255

3.3. Definiții pentru cardul de control:

Denumirea variabilei	Minim	Maxim
NoOfControlActivityRecords	230	520

3.4. Definiții pentru cardul societății:

Denumirea variabilei	Minim	Maxim
NoOfCompanyActivityRecords	230	520

4. SETURI DE CARACTERE

Șirurile IA5 utilizează caracterele ASCII definite în standardul ISO/IEC 8824-1. În scopul lizibilității și pentru a facilita desemnarea caracterelor, atribuirea valorilor acestora este indicată în continuare. În caz de divergență, aplicarea ISO/IEC 8824-1 are prioritate față de prezenta notă informativă.

! " # \$ % & ' () * + , - . / 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 { | } ~

În alte șiruri de caractere (adresă, nume, numărul de înmatriculare al vehiculului) se utilizează, în plus, caracterele definite de codurile 192-255 din standardul ISO/IEC 8859-1 (setul de caractere Latin 1) sau ISO/IEC 8859-7 (setul de caractere Greek).

5. CODAREA

La efectuarea codării conform normelor de codare ASN.1, toate tipurile de date definite se codează conform standardului ISO/IEC 8825-2, varianta aliniată.

Apendicele 2

SPECIFICAȚII PENTRU CARDURILE DE TAHOGRAF

Cuprins

1.	Introducere	101
1.1.	Abrevieri	101
1.2.	Trimiteri	102
2.	Caracteristici electrice și fizice	102
2.1.	Tensiunea de alimentare și consumul de electricitate	102
2.2.	Tensiunea de programare Tpp	103
2.3.	Generare și frecvență ceas	103
2.4.	Contact I/I	103
2.5.	Stări ale cardului	103
3.	Hardware și comunicații	103
3.1.	Introducere	103
3.2.	Protocol de transmisie	103
3.2.1.	Protocoale	103
3.2.2.	RLR	104
3.2.3.	SPT	105
3.3.	Condiții de acces (CA)	105
3.4.	Criptarea datelor	106
3.5.	Trecerea în revistă a comenzilor și codurilor de eroare	106
3.6.	Descrierea comenzilor	107
3.6.1.	Select file (selectare fișier)	107
3.6.1.1	Selectarea după denumire (IDA)	107
3.6.1.2.	Selectarea unui fișier elementar utilizând identificatorul fișierului	108
3.6.2.	Read Binary (citire date)	108
3.6.2.1	Comandă fără mesagerie securizată	109
3.6.2.2.	Comandă cu mesagerie securizată	109
3.6.3.	Update binary (actualizare date)	111
3.6.3.1.	Comandă fără mesagerie securizată	111
3.6.3.2.	Comanda cu mesagerie securizată	112
3.6.4.	Get challenge (obținere intervenție)	113
3.6.5.	Verify (verificare)	113
3.6.6.	Get response (obținere răspuns)	114
3.6.7.	PSO: verify certificate (verificare certificat)	114
3.6.8.	Internal authenticate (autentificare internă)	115

3.6.9.	External authenticate (autentificare externă)	116
3.6.10.	Manage security environment (gestionarea mediului de securitate)	117
3.6.11.	PSO: hash (distribuire)	118
3.6.12.	Perform hash of file (executare funcție de distribuire pe fișier)	118
3.6.13.	PSO: compute digital signature (calcul semnătură digitală)	119
3.6.14.	PSO: verify digital signature (verificare semnătură digitală)	120
4.	Structura cardului de tahograf	120
4.1.	Structura cardului șoferului	121
4.2.	Structura cardului atelierului	123
4.3.	Structura cardului de control	125
4.4.	Structura cardului societății	127

I. INTRODUCERE

1.1. Abrevieri

În înțelesul prezentului apendice, se aplică următoarele abrevieri:

CA	condiții de acces
IDA	identificator aplicație
INT	întotdeauna
UDPA	unitate de date a protocolului de aplicație (structura unei comenzi)
RLR	răspuns la resetare
AUT	autentificat
C6, C7	contactele nr. 6 și 7 de pe card conform descrierii din ISO/IEC 7816-2
cc	cicluri ceas
VTC	informații de verificare a titularului de card
CLA	octet de clasă al unei comenzi UDPA
FD	fișier dedicat. Un FD poate conține alte fișiere (FE sau FD)
FE	fișier elementar
CRP	criptat: accesul este posibil doar prin codarea datelor
uet	unitate elementară de timp
CI	circuit integrat
CCI	card cu circuite integrate
ID	identificator
PIF	periferic de interfață
DCI	dimensiunea câmpului de informații
DCIC	dimensiunea câmpului de informații pentru card
DCIP	dimensiunea câmpului de informații în periferic (pentru terminal)
INS	octet de instrucțiuni pentru o comandă UDPA
Lc	lungimea datelor de intrare pentru o comandă UDPA
Le	lungimea datelor prevăzute (date de ieșire pentru o comandă)
FP	fișier principal
P1-P2	octeți de parametrare
ADN	adresă nod utilizată în protocolul T = 1
NIC	niciodată
PIN	număr personal de identificare
PRO MS	protejat cu mesagerie securizată
SPT	selectare protocol transmisie
RUU	rezervat pentru utilizări ulterioare

RST	resetare (a cardului)
MS	mesagerie securizată
SW1-SW2	octeți de stare
TS	caracter inițial RLR
TPP	tensiune programare
XXh	valoarea XX în notație hexadecimală
	operator de concatenare 03 04 = 0304.

1.2. Trimiteri

În prezentul apendice se face trimitere la următoarele standarde:

EN 726-3	Sisteme de carduri de identificare – Carduri și terminale de telecomunicații cu circuit(e) integrat(e) – Partea 3: Cerințe pentru card independente de aplicație. Decembrie 1994.
ISO/IEC 7816-2	Tehnologia informației – Carduri de identificare – Carduri cu circuit(e) integrat(e) cu contacte – Partea 2: Dimensiunea și localizarea contactelor. Prima ediție: 1999.
ISO/IEC 7816-3	Tehnologia informației – Carduri de identificare – Carduri cu circuit(e) integrat(e) cu contacte – Partea 3: Semnale electronice și protocol de transmisie. Ediția 2: 1997.
ISO/IEC 7816-4	Tehnologia informației – Carduri de identificare – Carduri cu circuit(e) integrat(e) cu contacte – Partea 4: Comenzi interindustriale de intercomunicații. Prima ediție: 1995 + Modificarea 1: 1997.
ISO/IEC 7816-6	Tehnologia informației – Carduri de identificare – Carduri cu circuit(e) integrat(e) cu contacte – Partea 6: Elemente de date interindustriale. Prima ediție: 1996 + Cor 1: 1998.
ISO/IEC 7816-8	Tehnologia informației – Carduri de identificare – Carduri cu circuit(e) integrat(e) cu contacte – Partea 8: Comenzi interindustriale legate de securitate. Prima ediție: 1999.
ISO/IEC 9797	Tehnologia informației – Tehnici de securitate – mecanism de asigurare a integrității datelor cu funcție de verificare criptografică utilizând un algoritm de cifrare în bloc. Ediția 2: 1994.

2. CARACTERISTICI ELECTRICE ȘI FIZICE

TCS_200 Toate semnalele electronice sunt conforme cu ISO/IEC 7816-3, dacă nu există dispoziții diferite.

TCS_201 Localizarea și dimensiunile contactelor cadrului sunt conforme cu ISO/IEC 7816-2.

2.1. Tensiunea de alimentare și consumul de electricitate

TCS_202 Cardul funcționează conform specificațiilor în limitele de consum prevăzute în ISO/IEC 7816-3.

TCS_203 Cardul funcționează la $V_{cc} = 3 \text{ V} (\pm 0,3 \text{ V})$ sau $V_{cc} = 5 \text{ V} (\pm 0,5 \text{ V})$.

Selectarea tensiunii se face conform ISO/IEC 7816-3.

2.2. Tensiunea de programare Tpp

- TCS_204 Cardul nu necesită o tensiune de programare la contactul C6. Se prevede că acest contact C6 nu este conectat într-un PIF. Contactul C6 poate fi conectat la tensiunea V_{cc} în card, dar nu va fi conectat la masă. Această tensiune nu ar trebui interpretată în nici un caz.

2.3. Generare și frecvență ceas

- TCS_205 Cardul funcționează într-un interval de frecvență de la 1 la 5 MHz. Într-o sesiune de lucru cu cardul, frecvența ceasului poate varia cu $\pm 2\%$. Frecvența ceasului este generată de unitatea de pe vehicul și nu de card în sine. Coeficientul de utilizare poate varia între 40 și 60 %.
- TCS_206 Ceasul extern poate fi oprit în condițiile cuprinse în fișierul cardului FE_{CCI}. Primul octet din corpul fișierului FE_{CCI} codifică condițiile pentru modul Ceas oprit (vezi EN 726-3 pentru mai multe detalii):

Inferior	Superior		
Bit 3	Bit 2	Bit 1	
0	0	1	Oprire ceas permisă, fără nivel preferat
0	1	1	Oprire ceas permisă, se preferă nivelul superior
1	0	1	Oprire ceas permisă, se preferă nivelul inferior
0	0	0	Oprire ceas nepermisă
0	1	0	Oprire ceas permisă doar la nivelul superior
1	0	0	Oprire ceas permisă doar la nivelul inferior

Biții 4-8 nu se utilizează.

2.4. Contact I/I

- TCS_207 Contactul I/I C7 este utilizat pentru recepționarea datelor de la și pentru transmiterea datelor către PIF. În cursul funcționării, cardul și PIF nu pot fi simultan în mod emisie. Dacă ambele unități sunt în mod emisie, cardul nu se deteriorează. Dacă nu emite, cardul intră automat în mod recepție.

2.5. Stări ale cardului

- TCS_208 Cardul funcționează în două stări când se află sub tensiune:

- starea de funcționare atunci când execută comenzi sau se află în interfațare cu Unitatea digitală,
- starea de repaus în toate celelalte momente; în această stare toate datele sunt reținute de card.

3. HARDWARE ȘI COMUNICAȚII

3.1. Introducere

Acest punct descrie funcționalitatea minimă impusă pentru cardurile de tahograf și UV pentru a se asigura funcționarea corectă și capacitatea de interoperare a acestora.

Cardurile de tahograf sunt conforme, în cea mai mare măsură posibilă, cu normele disponibile ISO/IEC aplicabile (în special ISO/IEC 7816). Cu toate acestea, comenzile și protocoalele sunt descrise integral pentru a specifica anumite utilizări limitate sau anumite diferențe, dacă acestea există. Comenzile specificate sunt conforme în totalitate cu normele la care se face trimitere, cu excepția cazurilor indicate.

3.2. Protocol de transmisie

- TCS_300 Protocolul de transmisie este conform cu ISO/IEC 7816-3. În special, UV recunoaște prelungirile timpului de așteptare transmise de card.

3.2.1. Protocoale

- TCS_301 Cardul furnizează atât protocolul T = 0, cât și protocolul T = 1.

TCS_302 T = 0 este protocolul implicit, prin urmare este necesară o comandă SPT pentru schimbarea protocolului la T = 1.

TCS_303 Periferele sunt compatibile cu convenția în ambele protocoale: convenția directă este deci obligatorie pentru card.

TCS_304 RLR conține în caracterul TA3 octetul privind dimensiunea câmpului de informații în periferic. Această valoare este de cel puțin «F0h» (= 240 octeți).

Protocoalele se supun următoarelor restricții:

TCS_305 T = 0

- Perifericul de interfață primește un răspuns pe I/I după partea crescătoare a semnalului la RST de la 400 cc.
- Perifericul de interfață poate citi caractere separate de 12 uet.
- Perifericul de interfață citește un caracter eronat și repetiția acestuia dacă sunt separate de 13 uet. Dacă este detectat un caracter eronat, se poate declanșa semnalul de eroare pe I/I între 1 uet și 2 uet. Perifericul suportă o întârziere de 1 uet.
- Perifericul de interfață acceptă un RLR de 33 de octeți (TS + 32).
- Dacă RLR conține TC1, se prevede timpul suplimentar de gardă pentru caracterele transmise de către perifericul de interfață, deși caracterele transmise de card pot fi totuși separate de 12 uet. Același lucru se aplică și caracterului CFP transmis de card după un caracter P3 emis de perifericul de interfață.
- Perifericul de interfață ține cont de un caracter NUL emis de card.
- Perifericul de interfață acceptă modul complementar pentru o CFP.
- Comanda «get response» (obține un răspuns) nu poate fi utilizată în modul de înlănțuire pentru a obține date a căror lungime ar putea depăși 255 de octeți.

TCS_306 T = 1

- Octet ADN: neutilizat (ADN se setează la '00').
- ABANDONARE bloc S: neutilizată.
- Eroare de stare TPP bloc S: neutilizată.
- Lungimea totală de înlănțuire pentru un câmp de date nu va depăși 255 de octeți (cerință asigurată de PIF).
- Dimensiunea câmpului de informații al perifericului (DCIP) este indicată de PIF imediat după RLR: PIF transmite cererea DCI pentru blocul S după RLR, iar cardul transmite DCI pentru blocul S. Valoarea recomandată pentru DCIP este de 254 de octeți.
- Cardul nu va solicita o reajustare a DCI.

3.2.2. RLR

TCS_307 Perifericul verifică octeții RLR, în conformitate cu ISO/IEC 7816-3. Nu se verifică și caracterele istorice ale RLR.

Exemplu de Biprotocol de bază RLR conform ISO/IEC 7816-3

Caracter	Valoare	Observații
TS	'3Bh'	Indică convenția directă
T0	'85h'	TD1 prezent; sunt prezenți 5 octeți istorici
TD1	'80h'	TD2 prezent; de utilizat T = 0
TD2	'11h'	TA3 prezent; de utilizat T = 1
TA3	'XXh (cel puțin 'F0h)'	Dimensiunea câmpului de informații al cardului (DCIC)
TH1-TH5	'XXh'	Caractere istorice
TCK	'XXh'	Caracter de verificare (SAU exclusiv)

TCS_308 După Răspunsul la Resetare (RLR), Fișierul Principal (FP) este selectat implicit și devine Director Curent.

3.2.3. SPT

TCS_309 Protocolul implicit este T = 0. Pentru a seta protocolul T = 1, perifericul trebuie să transmită cardului o comandă SPT (abreviată, de asemenea, PPS).

TCS_310 Întrucât protocoalele T = 0 și T = 1 sunt ambele obligatorii pentru card, SPT de bază pentru schimbarea protocolului este obligatorie pentru card.

SPT poate fi utilizată, conform indicațiilor din ISO/IEC 7816-3, pentru a trece la rate binare mai mari decât cea implicită propusă de card în RLR, dacă există o astfel de rată implicită [octetul TA(1)].

Ratele binare mai mari sunt opționale pentru card.

TCS_311 În cazul în care cardul nu suportă alte rate binare decât rata implicită (sau dacă rata binară selectată nu este suportată), cardul răspunde la SPT în mod corect, în conformitate cu ISO/IEC 7816-3, omițând octetul PPS1.

Următoarele sunt exemple de SPT de bază pentru selectarea protocolului:

Caracter	Valoare	Observații
PPSS	'FFh'	Caracterul de inițializare
PPS0	'00h' sau '01h'	PPS1-PPS3 nu sunt prezente; '00h' pentru a selecta T0, '01h' pentru a selecta T1
PK	'XXh'	Caracter de verificare: 'XXh' = 'FFh' dacă PPS0 = '00h' 'XXh' = 'FEh' dacă PPS0 = '01h'

3.3. Condiții de acces (CA)

Condițiile de acces (CA) pentru comenzile UPDATE_BINARY și READ_BINARY sunt definite pentru fiecare Fișier Elementar.

TCS_312 Înainte de a accesa fișierul prin intermediul acestor comenzi trebuie să fie îndeplinite CA pentru fișierul curent.

Definițiile condițiilor disponibile de acces sunt următoarele:

- INT: Acțiunea este posibilă întotdeauna și poate fi executată fără nici o restricție.
- NIC: Acțiunea nu este niciodată posibilă.
- AUT: Dreptul corespunzător unei autentificări reușite trebuie deschis (se realizează prin comanda EXTERNAL_AUTHENTICATE).
- PRO MS: Comanda trebuie transmisă printr-o sumă de control criptografic utilizând mesageria securizată (vezi apendicele 11).
- AUT și PRO MS (combinate).

Pentru comenzile de procesare (UPDATE_BINARY și READ_BINARY) pot fi setate pe card următoarele condiții:

	UPDATE_BINARY	READ_BINARY
INT	Da	Da
NIC	Da	Da
AUT	Da	Da
PRO MS	Da	Nu
AUT și PRO MS	Da	Nu

Condiția de acces PRO MS nu este disponibilă pentru comanda READ_BINARY. Acest lucru înseamnă că prezența unei sume de control criptografic pentru comanda READ nu este niciodată obligatorie. Cu toate acestea, atribuind valoarea 'OC' pentru clasă, este posibilă utilizarea comenzii READ_BINARY cu mesageria securizată, conform punctului 3.6.2.

3.4. Criptarea datelor

În cazul în care trebuie protejată confidențialitatea datelor care urmează a fi citite dintr-un fișier, fișierul este marcat «Criptat». Criptarea se face prin utilizarea mesageriei securizate (vezi apendicele 11).

3.5. Trecerea în revistă a comenzilor și a codurilor de eroare

Comenzile și organizarea fișierelor se bazează pe și este conformă cu ISO/IEC 7816-4.

TCS_313 Prezenta secțiune descrie următoarele perechi comandă-răspuns UDPA:

Comanda	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 Orice mesaj de răspuns conține cuvintele de stare SW1 și SW2, care indică situația procesării unei comenzi.

SW1	SW2	Semnificație
90	00	Procesare normală
61	XX	Procesare normală. XX = numărul de octeți de răspuns disponibili
62	81	Procesare de avertisment. O parte din datele din răspuns pot fi corupte
63	CX	VPC eronate (PIN). Numărul încercărilor rămase este dat de 'X'
64	00	Eroare de execuție – Starea memoriei nevolatile nemodificată. Eroare de integritate
65	00	Eroare de execuție – Starea memoriei nevolatile modificată
65	81	Eroare de execuție – Starea memoriei nevolatile modificată – Pană de memorie
66	88	Eroare de securitate: sumă de control criptografic eronată (în cursul mesageriei securizate) sau certificat eronat (la verificarea certificatului) sau criptogramă eronată (în cursul autentificării externe) sau semnătură eronată (în cursul verificării semnăturii)
67	00	Lungime eronată (Lc sau Le)
69	00	Comandă interzisă (nici un răspuns disponibil în T = 0)
69	82	Starea de securitate nesatisfăcută
69	83	Metoda de autentificare blocată
69	85	Condițiile de utilizare nesatisfăcute
69	86	Comandă nepermisă (FE curent absent)
69	87	Pachete de date așteptate prin mesageria securizată absente
69	88	Pachete de date din mesageria securizată incorecte
6A	82	Fișierul nu poate fi găsit
6A	86	Parametrii P1-P2 greșiți
6A	88	Datele menționate nu pot fi găsite
6B	00	Parametri eronați (deplasare în afara FE)

SW1	SW2	Semnificație
6C	XX	Lungime eronată, SW2 indică lungimea exactă. Nu este transmis nici un câmp de date
6D	00	Cod de instrucțiuni incompatibil sau incorect
6E	00	Clasă incompatibilă
6F	00	Alte erori de verificare

3.6. Descrierea comenzilor

Prezentul capitol descrie comenzile obligatorii pentru cardurile de tahograf.

Apendicele 11, Mecanisme comune de securitate, cuprinde detalii suplimentare relevante privind operațiunile criptografice implicate.

Toate comenzile sunt descrise independent de protocolul utilizat ($T = 0$ sau $T = 1$). Octeții UDPA CLA, INS, P1, P2, Lc și Le sunt indicați întotdeauna. Dacă Lc sau Le nu sunt necesare pentru comanda descrisă, lungimea, valoarea și descrierea respective sunt vide.

TCS_315 Dacă sunt necesari ambii octeți de lungime (Lc și Le), comanda descrisă trebuie să fie separată în două părți dacă PIF utilizează protocolul $T = 0$: PIF transmite comanda conform descrierii cu $P3 = Lc + \text{date}$, iar apoi transmite a comandă GET_RESPONSE (vezi punctul 3.6.6) cu $P3 = Le$.

TCS_316 Dacă sunt necesari ambii octeți de lungime, iar $Le = 0$ (mesagerie securizată):

- Când se utilizează protocolul $T = 1$, cardul răspunde la $Le = 0$ trimițând toate datele de ieșire disponibile.
- Când se utilizează protocolul $T = 0$, PIF transmite prima comandă cu $P3 = Lc + \text{date}$, cardul răspunde (la această valoare implicită $Le = 0$) cu octeții de stare '61La', unde La este numărul de octeți de răspuns disponibili. PIF generează apoi o comandă GET_RESPONSE cu $P3 = La$ pentru a citi datele.

3.6.1. Select file (selectare fișier)

Această comandă respectă ISO/IEC 7816-4, dar are o utilizare restricționată comparativ cu comanda definită în normă.

Comanda SELECT FILE se utilizează:

- pentru a selecta o aplicație FD (selectarea după denumire obligatorie);
- pentru a selecta un fișier elementar corespunzător ID de fișier prezentat.

3.6.1.1. Selectarea după denumire (IDA)

Această comandă permite selectarea unei aplicații FD în card.

TCS_317 Această comandă poate fi executată de oriunde din structura fișierelor (după RLR sau în orice moment).

TCS_318 Selectarea unei aplicații resetează mediul curent de securitate. După selectarea aplicației, nu este selectată nici o cheie publică activă, iar cheia din sesiunea anterioară nu mai este disponibilă pentru mesageria securizată. Se pierde, de asemenea, condiția de acces AUT.

TCS_319 Mesaj de comandă

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'04h'	Selecție după denumire (IDA)
P2	1	'0Ch'	Nu se așteaptă răspuns
Lc	1	'NNh'	Numărul de octeți trimis de card (lungime IDA): '06h' pentru aplicația de tahograf
#6-#(5 + NN)	NN	'XX..XXh'	IDA: 'FF 54 41 43 48 4F' pentru aplicația de tahograf

Nu este necesar un răspuns la comanda SELECT FILE (Le absent în T = 1, sau nu se solicită un răspuns în T = 0).

TCS_320 Mesaj de răspuns (nu se solicită răspuns)

Octet	Lungime	Valoare	Descriere
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

- dacă comanda reușește, cardul transmite '9000';
- dacă nu se regăsește aplicația corespunzătoare IDA, se transmite starea de procesare '6A82';
- în T = 1, dacă este prezent octetul Le, se transmite starea '6700';
- în T = 0, dacă se solicită un răspuns după comanda SELECT FILE, se transmite starea '6900';
- dacă aplicația selectată este considerată coruptă (este detectată o eroare de integritate în atributele fișierului), se transmite starea de procesare '6400' sau '6581'.

3.6.1.2. *Selectarea unui fișier elementar utilizând identificatorul fișierului*

TCS_321 Mesaj de comandă

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'02h'	Selectarea unui FE din FD curent
P2	1	'0Ch'	Nu se așteaptă răspuns
Lc	1	'02h'	Numărul de octeți trimis către card
#6-#7	2	'XXXXh'	Identificatorul fișierului

Nu este necesar un răspuns la comanda SELECT FILE (Le absent în T = 1 sau nu se solicită un răspuns în T = 0).

TCS_322 Mesaj de răspuns (nu se solicită răspuns)

Octet	Lungime	Valoare	Descriere
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

- dacă comanda reușește, cardul transmite '9000';
- dacă nu se regăsește fișierul corespunzător identificatorului de fișier, se transmite starea de procesare '6A82';
- în T = 1, dacă este prezent octetul Le, se transmite starea '6700';
- în T = 0, dacă se solicită un răspuns după comanda SELECT FILE, se transmite starea '6900';
- dacă fișierul selectat este considerat corupt (este detectată o eroare de integritate în atributele fișierului), se transmite starea de procesare '6400' sau '6581'.

3.6.2. **Read binary (citire date)**

Această comandă respectă ISO/IEC 7816-4, dar are o utilizare restricționată comparativ cu comanda definită în norma respectivă.

Comanda READ BINARY se utilizează pentru citirea datelor dintr-un fișier transparent.

Răspunsul cardului constă în transmiterea datelor citite, opțional încadrate într-o structură de mesagerie securizată.

TCS_323 Comanda poate fi executată doar dacă starea de securitate îndeplinește atributele de securitate definite pentru FE pentru funcția READ (citire).

3.6.2.1. Comandă fără mesagerie securizată

Această comandă permite PIF să citească datele din FE selectat, fără mesagerie securizată.

TCS_324 Nu este posibilă citirea datelor dintr-un fișier marcat «criptat» cu această comandă.

TCS_325 Mesaj de comandă

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	Nu se solicită mesagerie securizată
INS	1	'B0h'	
P1	1	'XXh'	Decalaj în octeți de la începutul fișierului: cel mai semnificativ octet
P2	1	'XXh'	Decalaj în octeți de la începutul fișierului: cel mai puțin semnificativ octet
Le	1	'XXh'	Lungimea datelor așteptate, numărul de octeți de citit

Notă: octetul 8 din P1 trebuie setat la 0.

TCS_326 Mesaj de răspuns

Octet	Lungime	Valoare	Descriere
#1-#X	X	'XX..XXh'	Date citite
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

- dacă comanda reușește, cardul transmite '9000';
- dacă nu este selectat un FE, se transmite starea de procesare '6986';
- dacă nu sunt satisfăcute condițiile de acces pentru fișierul selectat, comanda este întreruptă cu '6982';
- dacă decalajul nu este compatibil cu dimensiunea FE (Decalaj > dimensiune FE), se transmite starea de procesare '6B00';
- dacă dimensiunea datelor de citit nu este compatibilă cu dimensiunea FE (Decalaj + Le > dimensiune FE), se transmite starea de procesare '6700' sau '6Cxx', unde 'xx' indică lungimea exactă;
- dacă este detectată o eroare de integritate în atributele fișierului, cardul consideră că fișierul este corupt și irecuperabil, iar starea de procesare transmisă este '6400' sau '6581';
- dacă este detectată o eroare de integritate în datele stocate, cardul transmite datele solicitate, iar starea de procesare transmisă este '6281'.

3.6.2.2. Comandă cu mesagerie securizată

Această comandă permite PIF să citească date din FE selectat prin mesagerie securizată, pentru a verifica integritatea datelor primite și pentru a proteja confidențialitatea datelor în cazul în care FE este marcat prin «criptat».

TCS_327 Mesaj de comandă

Octet	Lungime	Valoare	Descriere
CLA	1	'0Ch'	Mesagerie securizată solicitată
INS	1	'B0h'	INS
P1	1	'XXh'	P1 (decalaj în octeți de la începutul fișierului): Cel mai semnificativ octet
P2	1	'XXh'	P2 (decalaj în octeți de la începutul fișierului): Cel mai puțin semnificativ octet
Lc	1	'09h'	Lungimea datelor de intrare pentru mesageria securizată
#6	1	'97h'	T _{LE} : Marcator pentru specificația lungimii așteptate
#7	1	'01h'	L _{LE} : Lungimea lungimii așteptate
#8	1	'NNh'	Specificația lungimii așteptate (Le originală): Numărul de octeți de citit

Octet	Lungime	Valoare	Descriere
#9	1	'8Eh'	T _{CC} : Marcator pentru suma de control criptografic
#10	1	'04h'	L _{CC} : Lungimea următoarei sume de control criptografic
#11-#14	4	'XX..XXh'	Sumă de control criptografic (cei mai importanți 4 octeți)
Le	1	'00h'	Conform specificațiilor din ISO/IEC 7816-4

TCS_328 Mesaj de răspuns dacă FE nu este marcat «criptat» și dacă formatul de intrare pentru mesageria securizată este corect:

Octet	Lungime	Valoare	Descriere
#1	1	'81h'	T _{PV} : Marcator pentru valoarea datelor comune
#2	L	'NNh' sau '81 NNh'	L _{PV} : lungimea datelor transmise (= Le originală) L este de 2 octeți dacă L _{PV} > 127 octeți
#(2 + L)-#(1 + L + NN)	NN	'XX..XXh'	Valoarea datelor comune
#(2 + L + NN)	1	'8Eh'	T _{CC} : Marcator pentru suma de control criptografic
#(3 + L + NN)	1	'04h'	L _{CC} : Lungimea următoarei sume de control criptografic
#(4 + L + NN)-#(7 + L + NN)	4	'XX..XXh'	Sumă de control criptografic (cei mai importanți 4 octeți)
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

TCS_329 Mesaj de răspuns dacă FE este marcat «criptat» și dacă formatul de intrare pentru mesageria securizată este corect:

Octet	Lungime	Valoare	Descriere
#1	1	'87h'	T _{PI CG} : Marcator pentru date criptate (criptogramă)
#2	L	'MMh' sau '81 MMh'	L _{PI CG} : lungimea datelor criptate transmise (diferită de Le originală a comenzii din cauza completării) L este de doi octeți dacă L _{PI CG} > 127 octeți
#(2 + L)-#(1 + L + MM)	MM	'01XX..XXh'	Date criptate: indicator de completare și criptogramă
#(2 + L + MM)	1	'8Eh'	T _{CC} : Marcator pentru suma de control criptografic
#(3 + L + MM)	1	'04h'	L _{CC} : Lungimea următoarei sume de control criptografic
#(4 + L + MM)-#(7 + L + MM)	4	'XX..XXh'	Sumă de control criptografic (cei mai importanți 4 octeți)
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

Datele criptate transmise conțin un prim octet care indică modul de completare utilizat. Pentru aplicația de tahograf, indicatorul de completare are întotdeauna valoarea '01h', ceea ce arată că modul de completare utilizat este cel specificat în ISO/IEC 7816-4 (un octet cu valoarea '80h' urmat de câțiva octeți nuli: ISO/IEC 9797 metoda 2).

Stările «obișnuite» de procesare, descrise pentru comanda READ BINARY fără mesagerie securizată (vezi punctul 3.6.2.1) pot fi transmise utilizând structurile de mesaj de răspuns descrise mai sus, cu un marcator '99h' (conform TCS 335).

În plus, pot apărea unele erori specifice mesageriei securizate. În acest caz, starea de procesare este transmisă simplu, fără a mai implica o structură de mesagerie securizată.

TCS_330 Mesaj de răspuns pentru un format incorect de intrare pentru mesageria securizată

Octet	Lungime	Valoare	Descriere
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

— Dacă nu este disponibilă o cheie activă de sesiune, starea de procesare transmisă este '6A88'. Acest lucru se întâmplă dacă cheia de sesiune nu a fost încă generată sau dacă valabilitatea acesteia a expirat (în acest caz PIF trebuie să ruleze din nou un proces de autentificare reciprocă pentru a seta o nouă cheie de sesiune).

— Dacă unele dintre pachetele de date așteptate (conform specificațiilor de mai sus) lipsesc din formatul de mesagerie securizată, starea de procesare transmisă este '6987': această eroare se produce dacă lipsește un marcator așteptat sau dacă corpul comenzii nu este construit corect.

- Dacă unele pachete de date sunt incorecte, starea de procesare transmisă este '6988': această eroare se produce dacă toți marcatorii necesari sunt prezenți, dar unele lungimi sunt diferite de cele așteptate.
- Dacă verificarea sumei de control criptografic eșuează, starea de procesare transmisă este '6688'.

3.6.3. *Update binary (actualizare date)*

Această comandă respectă ISO/IEC 7816-4, dar are o utilizare restricționată comparativ cu comanda definită în normă.

Mesajul de comandă UPDATE BINARY inițializează actualizarea (ștergere + scriere) octeților deja prezenți într-un FE cu octeți dați în comanda UDPA.

TCS_331 Comanda poate fi executată doar dacă starea de securitate satisface atributele de securitate definite pentru FE pentru funcția UPDATE (dacă controlul accesului funcției UPDATE include o PRO MS, comenzii trebuie să i se adauge o mesagerie securizată).

3.6.3.1. *Comandă fără mesagerie securizată*

Această comandă permite PIF să scrie date în FE selectat, fără ca integritatea datelor primite să fie verificată de card. Acest mod simplu este permis doar dacă fișierul corespunzător nu este marcat «criptat».

TCS_332 Mesaj de comandă

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	Nu se solicită mesagerie securizată
INS	1	'D6h'	Decalaj în octeți de la începutul fișierului: cel mai semnificativ octet
P1	1	'XXh'	
P2	1	'XXh'	Decalaj în octeți de la începutul fișierului: cel mai puțin semnificativ octet
Lc	1	'NNh'	Lungimea Lc a datelor de actualizat. Numărul de octeți de scris
#6-#(5 + NN)	NN	'XX..XXh'	Date de scris

Notă: octetul 8 din P1 trebuie setat la 0.

TCS_333 Mesaj de răspuns

Octet	Lungime	Valoare	Descriere
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

- dacă comanda reușește, cardul transmite '9000';
- dacă nu este selectat un FE, starea de procesare transmisă este '6986';
- dacă Condițiile de Acces ale fișierului selectat nu sunt îndeplinite, comanda este întreruptă cu '6982';
- dacă decalajul nu este compatibil cu dimensiunea FE (decalaj > dimensiunea FE), starea de procesare transmisă este '6B00';
- dacă dimensiunea datelor care urmează să fie scrise nu este compatibilă cu dimensiunea FE (decalaj + Le > dimensiunea FE), starea de procesare transmisă este '6700';
- dacă este detectată o eroare de integritate în atributele fișierului, cardul consideră că fișierul este corupt și irecuperabil, iar starea de procesare transmisă este '6400' sau '6500';
- dacă scrierea nu reușește, starea de procesare transmisă este '6581'.

3.6.3.2. Comanda cu mesagerie securizată

Această comandă permite PIF să scrie date în FE selectat, cardul verificând integritatea datelor primite. Întrucât nu este necesară păstrarea confidențialității, datele nu sunt criptate.

TCS_334 Mesaj de comandă

Octet	Lungime	Valoare	Descriere
CLA	1	'0Ch'	Mesagerie securizată solicitată
INS	1	'D6h'	INS
P1	1	'XXh'	Decalaj în octeți de la începutul fișierului: cel mai semnificativ octet
P2	1	'XXh'	Decalaj în octeți de la începutul fișierului: cel mai puțin semnificativ octet
Lc	1	'XXh'	Lungimea câmpului de date securizate
#6	1	'81h'	T _{PV} : marcator pentru valoarea normală a datelor
#7	L	'NNh' sau '81NNh'	L _{PV} : Lungimea datelor transmise L este de 2 octeți dacă L _{PV} > 127 octeți
#(7 + L) - #(6 + L + NN)	NN	'XX..XXh'	Valoare date comune (date de scris)
#(7 + L + NN)	1	'8Eh'	T _{CC} : marcator pentru suma de control criptografic
#(8 + L + NN)	1	'04h'	L _{CC} : Lungimea următoarei sume de control criptografic
#(9 + L + NN) - #(12 + L + NN)	4	'XX..XXh'	Sumă de control criptografic (cei mai importanți 4 octeți)
Le	1	'00h'	Conform specificațiilor din ISO/IEC 7816-4

TCS_335 Mesaj de răspuns dacă formatul de intrare pentru mesagerie securizată este corect

Octet	Lungime	Valoare	Descriere
#1	1	'99h'	T _{SW} : Marcator pentru cuvinte de stare (de protejat de către CC)
#2	1	'02h'	L _{SW} : lungimea cuvintelor de stare transmise
#3-#4	2	'XXXXh'	Cuvinte de stare (SW1, SW2)
#5	1	'8Eh'	T _{CC} : Marcator pentru suma de control criptografic
#6	1	'04h'	L _{CC} : Lungimea următoarei sume de control criptografic
#7-#10	4	'XX..XXh'	Sumă de control criptografic (cei mai importanți 4 octeți)
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

Stările «obișnuite» de procesare, descrise pentru comanda UPDATE BINARY fără mesagerie securizată (vezi punctul 3.6.3.1) pot fi transmise utilizând structura de mesaj de răspuns descrisă anterior.

În plus, pot apărea unele erori legate specific de mesagerie securizată. În acest caz, starea de procesare este transmisă simplu, fără a mai implica o structură de mesagerie securizată.

TCS_336 Mesaj de răspuns în caz de eroare în mesagerie securizată

Octet	Lungime	Valoare	Descriere
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

- dacă nu este disponibilă o cheie de sesiune, se transmite starea de procesare '6A88';
- dacă unele dintre obiectele informative așteptate (conform specificațiilor de mai sus) lipsesc din formatul de mesagerie securizată, starea de procesare transmisă este '6987': această eroare se produce dacă lipsește un marcator așteptat sau dacă corpul comenzii nu este construit corect;
- dacă unele obiecte de date sunt incorecte, starea de procesare transmisă este '6988': această eroare se produce dacă toți marcatorii necesari sunt prezenți, dar unele lungimi sunt diferite de cele așteptate;
- dacă verificarea sumei de control criptografic eșuează, starea de procesare transmisă este '6688'.

3.6.4. *Get challenge (obținere intervenție)*

Această comandă respectă ISO/IEC 7816-4, dar are o utilizare restricționată comparativ cu comanda definită în normă.

Comanda GET CHALLENGE solicită cardului să emită o provocare pentru a fi utilizată într-o procedură de securitate în cadrul căreia sunt transmise cardului o criptogramă sau date codificate.

TCS_337 Provocarea emisă de card este valabilă doar pentru următoarea comandă, care utilizează provocarea, transmisă cardului.

TCS_338 Mesaj de comandă

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	CLA
INS	1	'84h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Le	1	'08h'	Le (Lungimea intervenției așteptate)

TCS_339 Mesaj de răspuns

Octet	Lungime	Valoare	Descriere
#1-#8	8	'XX..XXh'	Intervenție
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

- Dacă comanda reușește, cardul transmite '9000';
- dacă Le este diferită de '08h', starea de procesare este '6700';
- dacă parametrii P1-P2 sunt incorecți, starea de procesare este '6A86'.

3.6.5. *Verify (verificare)*

Această comandă respectă ISO/IEC 7816-4, dar are o utilizare restricționată comparativ cu comanda definită în normă.

Comanda Verify inițializează în card comparația dintre datele VPC (PIN) transmise din comandă cu VPC de referință stocate în card.

Notă: PIN introdus de utilizator trebuie completat la dreapta de către PIF cu octeți FFh până la lungimea de 8 octeți.

TCS_340 Dacă comanda reușește, sunt deschise drepturile corespunzătoare prezentării VPC, iar numărul încercărilor de introducere a VPC rămase este reinițializat.

TCS_341 O comparație eșuată este înregistrată în card pentru a limita numărul încercărilor ulterioare de utilizare a VPC de referință.

TCS_342 Mesaj de comandă

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	CLA
INS	1	'20h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (VPC verificate sunt cunoscute implicit)
Lc	1	'08h'	Lungimea codului VPC transmis
#6-#13	8	'XX..XXh'	VPC

TCS_343 Mesaj de răspuns

Octet	Lungime	Valoare	Descriere
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

- dacă comanda reușește, cardul transmite '9000';
- dacă nu se regăsesc VPC de referință, starea de procesare transmisă este '6A88';
- dacă VPC este blocat (numărul de încercări rămase pentru VPC este nul), starea de procesare transmisă este '6983'. O dată în această stare, VPC nu mai pot fi niciodată prezentate cu succes;
- dacă comparația nu reușește, numărul încercărilor rămase scade și se transmite stare '63CX' ($X > 0$, X fiind egal cu numărul încercărilor rămase pentru introducerea VPC. $X = 'F'$, numărul încercărilor de introducere a VPC este mai mare decât 'F');
- dacă VPC de referință sunt considerate corupte, starea de procesare transmisă este '6400' sau '6581'.

3.6.6. *Get response (obținere răspuns)*

Această comandă respectă ISO/IEC 7816-4.

Această comandă (necesară și disponibilă doar pentru protocolul $T = 0$) este utilizată pentru a transmite datele pregătite din card la perifericul de interfață (în cazul în care o comandă include atât Lc, cât și Le).

Comanda GET_RESPONSE trebuie emisă imediat după comanda de pregătire a datelor, altfel datele sunt pierdute. După executarea comenzii GET_RESPONSE (cu excepția cazurilor în care se produce eroarea '61xx' sau '6Cxx', vezi mai jos), datele pregătite anterior nu mai sunt disponibile.

TCS_344 Mesaj de comandă

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	
INS	1	'C0h'	
P1	1	'00h'	
P2	1	'00h'	
Le	1	'XXh'	Numărul de octeți așteptați

TCS_345 Mesaj de răspuns

Octet	Lungime	Valoare	Descriere
#1-#X	X	'XX..XXh'	Date
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

- Dacă comanda reușește, cardul transmite '9000'.
- Dacă nu au fost pregătite date de către card, starea de procesare transmisă este '6900' sau '6F00'.
- Dacă Le depășește numărul de octeți disponibili sau dacă Le este nulă, starea de procesare transmisă este '6Cxx', unde 'xx' reprezintă numărul exact de octeți disponibili. În acest caz, datele pregătite sunt în continuare disponibile pentru o comandă GET_RESPONSE ulterioară.
- Dacă Le nu este nulă, dar este mai mică decât numărul de octeți disponibili, datele solicitate sunt transmise în mod normal de către card, starea de procesare transmisă fiind '61xx', unde 'xx' indică numărul de octeți suplimentari care sunt disponibili pentru o comandă GET_RESPONSE ulterioară.
- Dacă comanda nu este suportată de card (protocol $T = 1$), cardul transmite '6D00'.

3.6.7. *PSO: verify certificate (verificare certificat)*

Această comandă respectă ISO/IEC 7816-8, dar are o utilizare restricționată comparativ cu comanda definită în normă.

Cardul utilizează comanda VERIFY CERTIFICATE pentru a obține o cheie publică din afară și pentru a verifica valabilitatea acesteia.

TCS_346 În cazul în care o comandă VERIFY CERTIFICATE reușește, cheia publică este stocată pentru o utilizare ulterioară în mediul de securitate. Această cheie se setează explicit pentru a fi utilizată de către comanda SME (vezi punctul 3.6.10) în cadrul comenzilor legate de securitate (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE sau VERIFY CERTIFICATE), folosindu-se identificatorul de cheie.

TCS_347 În orice caz, comanda VERIFY CERTIFICATE utilizează cheia publică selectată anterior de către comanda SME pentru deschiderea certificatului. Această cheie trebuie să aparțină unui stat membru sau Europei.

TCS_348 Mesaj de comandă

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	CLA
INS	1	'2Ah'	Executarea unei operațiuni de securitate
P1	1	'00h'	P1
P2	1	'AEh'	P2: date codificate non BER-TLV (concatenarea elementelor de date)
Lc	1	'CEh'	Lc: Lungimea certificatului, 194 octeți
#6-#199	194	'XX..XXh'	Certificat: concatenarea elementelor de date (conform descrierii din apendicele 11)

TCS_349 Mesaj de răspuns

Octet	Lungime	Valoare	Descriere
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

- dacă comanda reușește, cardul transmite '9000';
- dacă verificarea certificatului eșuează, starea de procesare transmisă este '6688'. Procesul de verificare și de deschidere a certificatului, conform descrierii din apendicele 11,
- dacă în mediul de securitate nu există o cheie publică, se transmite '6A88';
- dacă cheia publică selectată (utilizată pentru deschiderea certificatului) este considerată coruptă, starea de procesare transmisă este '6400' sau '6581';
- dacă cheia publică selectată (utilizată pentru deschiderea certificatului) are un CHA.LSB (CertificateHolderAuthorisation.equipmentType) diferit de '00' (adică nu aparține unuia dintre statele membre sau Europei), starea de procesare transmisă este '6985'.

3.6.8. Internal authenticate (autentificare internă)

Această comandă respectă ISO/IEC 7816-4.

Utilizând comanda INTERNAL AUTHENTICATE, PIF poate să autentifice cardul.

Procesul de autentificare este descris în apendicele 11. Acesta include următoarele enunțuri:

TCS_350 Comanda INTERNAL AUTHENTICATE utilizează cheia privată a cardului (selectată implicit) pentru a semna datele de autentificare, inclusiv K1 (primul element pentru compatibilitatea cheilor de sesiune) și RND1, și utilizează cheia publică selectată (prin intermediul ultimei comenzi SME) pentru a cripta semnătura și pentru a forma jetonul de autentificare (mai multe detalii în apendicele 11).

TCS_351 Mesaj de comandă

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	CLA
INS	1	'88h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Lc	1	'10h'	Lungimea datelor transmise de card
#6-#13	8	'XX..XXh'	Intervenție utilizată pentru autentificarea cardului
#14-#21	8	'XX..XXh'	UV.RDC (vezi apendicele 11)
Le	1	'80h'	Lungimea datelor așteptate de la card

TCS_352 Mesaj de răspuns

Octet	Lungime	Valoare	Descriere
#1-#128	128	'XX..XXh'	Jeton de autentificare a cardului (vezi apendicele 11)
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

- Dacă comanda reușește, cardul transmite '9000';
- dacă în mediul de securitate nu există o cheie publică, starea de procesare transmisă este '6A88';
- dacă în mediul de securitate nu există o cheie privată, starea de procesare transmisă este '6A88';
- dacă UV.RDC nu corespunde identificatorului cheii publice curente, starea de procesare transmisă este '6A88';
- dacă cheia privată este considerată coruptă, starea de procesare transmisă este '6400' sau '6581'.

TCS_353 Dacă comanda INTERNAL AUTHENTICATE reușește, cheia de sesiune activă, dacă există, este ștearsă și nu mai este disponibilă. Pentru a face disponibilă o nouă cheie de sesiune trebuie executată cu succes comanda EXTERNAL_AUTHENTICATE.

3.6.9. External authenticate (autentificare externă)

Această comandă respectă ISO/IEC 7816-4.

Utilizând comanda EXTERNAL AUTHENTICATE, cardul poate autentifica PIF.

Procesul de autentificare este descris în apendicele 11. Acesta include următoarele enunțuri:

TCS_354 Comanda EXTERNAL AUTHENTICATE trebuie dată imediat după o comandă GET CHALLENGE. Cardul emite o intervenție spre exterior (RND3).

TCS_355 Verificarea criptogramei utilizează RND3 (intervenția emisă de card), cheia privată a cardului (selectată implicit) și cheia publică selectată anterior de către comanda SME.

TCS_356 Cardul verifică criptograma, iar dacă aceasta este corectă se deschide condiția de acces AUT.

TCS_357 Criptograma de intrare cuprinde al doilea element indicând compatibilitatea cheilor de sesiune K2.

TCS_358 Mesaj de comandă

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (cheia publică de utilizat este cunoscută implicit și a fost setată anterior de către comanda SME)
Lc	1	'80h'	Lc (Lungimea datelor transmise cardului)
#6-#133	128	'XX..XXh'	Criptogramă (vezi apendicele 11)

TCS_359 Mesaj de răspuns

Octet	Lungime	Valoare	Descriere
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

- Dacă comanda reușește, cardul transmite '9000';
- dacă în mediul de securitate nu există o cheie publică, se transmite '6A88';
- dacă CHA a cheii publice selectate nu este concatenarea IDA a aplicației de tahograf și a unui tip de aparat UV, starea de procesare transmisă este '6F00' (vezi apendicele 11);
- dacă în mediul de securitate nu există o cheie privată, starea de procesare transmisă este '6A88';
- dacă verificarea criptogramei este eronată, starea de procesare transmisă este '6688';
- dacă comanda nu urmează imediat unei comenzi GET CHALLENGE, starea de procesare transmisă este '6985';
- dacă cheia privată selectată este considerată coruptă, starea de procesare transmisă este '6400' sau '6581'.

TCS_360 Dacă comanda EXTERNAL AUTHENTICATE reușește și dacă prima parte a cheii de sesiune este disponibilă dintr-o comandă INTERNAL AUTHENTICATE executată de curând cu succes, cheia de sesiune este setată pentru comenzile ulterioare care utilizează mesageria securizată.

TCS_361 Dacă prima parte a cheii de sesiune nu este disponibilă dintr-o comandă anterioară INTERNAL AUTHENTICATE, cea de-a doua parte a cheii de sesiune, transmisă de PIF, nu este stocată în card. Acest mecanism asigură executarea procesului de autentificare reciprocă în ordinea specificată în apendicele 11.

3.6.10. *Manage security environment (gestionare mediu de securitate)*

Această comandă este utilizată pentru setarea unei chei publice pentru autentificare.

Această comandă respectă ISO/IEC 7816-8. Utilizarea acestei comenzi este restricționată față de standardul corespunzător.

TCS_362 Cheia menționată în câmpul de date al SME este valabilă pentru fiecare fișier din FD al tahografului.

TCS_363 Cheia menționată în câmpul de date al SME rămâne cheia publică activă până la următoarea comandă SME corectă.

TCS_364 Dacă cheia menționată nu este (deja) prezentă în card, mediul de securitate rămâne neschimbat.

TCS_365 Mesaj de comandă

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	CLA
INS	1	'22h'	INS
P1	1	'C1h'	P1: cheia menționată valabilă pentru toate operațiunile criptografice
P2	1	'B6h'	P2 (date menționate privind semnătura digitală)
Lc	1	'0Ah'	Lc: lungimea câmpului de date subsecvent
#6	1	'83h'	Marcator pentru menționarea unei chei publice în cazuri asimetrice
#7	1	'08h'	Lungimea trimiterii (identificator cheie)
#8-#15	08h	'XX..XXh'	Identificator cheie conform specificațiilor din apendicele 11

TCS_366 Mesaj de răspuns

Octet	Lungime	Valoare	Descriere
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

- Dacă comanda reușește, cardul transmite '9000';
- dacă cheia menționată nu este prezentă în card, starea de procesare transmisă este '6A88';
- dacă unele dintre pachetele de date așteptate lipsesc în formatul de mesagerie securizată, este transmisă starea de procesare '6987'. Același lucru se poate întâmpla dacă lipsește marcatorul '83h';
- dacă unele dintre pachetele de date sunt incorecte, starea de procesare transmisă este '6988'. Același lucru se poate întâmpla dacă lungimea identificatorului cheii nu este '08h';
- dacă cheia selectată este considerată coruptă, starea de procesare transmisă este '6400' sau '6581'.

3.6.11. **PSO: hash (distribuire)**

Această comandă se utilizează pentru a transfera pe card rezultatul unui calcul de distribuie aplicat anumitor date. Această comandă se utilizează pentru verificarea semnăturilor digitale. Valoarea de distribuie este stocată în EEPROM pentru comanda ulterioară de verificare a semnăturilor digitale.

Această comandă respectă ISO/IEC 7816-8. Utilizarea acestei comenzi este restricționată comparativ cu standardul corespunzător.

TCS_367 Mesaj de comandă

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	CLA
INS	1	'2Ah'	Executare a unei operațiuni de securitate
P1	1	'90h'	Transmitere cod de distribuie
P2	1	'A0h'	Marcator: câmpul de date conține DO relevante pentru funcția de distribuie
Lc	1	'16h'	Lungimea Lc a câmpului de date subsecvent
#6	1	'90h'	Marcator pentru codul de distribuie
#7	1	'14h'	Lungimea codului de distribuie
#8-#27	20	'XX.XXh'	Cod de distribuie

TCS_368 Mesaj de răspuns

Octet	Lungime	Valoare	Descriere
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

- Dacă comanda reușește, cardul transmite '9000';
- dacă unele dintre obiectele de date așteptate (conform specificațiilor de mai sus) lipsesc, este transmisă starea de procesare '6988'. Același lucru se poate întâmpla dacă lipsește unul dintre marcatorii '90h';
- dacă unele dintre obiectele de date sunt incorecte, starea de procesare transmisă este '6988'. Același lucru se poate întâmpla dacă marcatorul necesar este prezent, dar lungimea acestuia este diferită de '14h'.

3.6.12. **Perform hash of file (executare funcție de distribuie pe fișier)**

Această comandă nu respectă ISO/IEC 7816-8. Astfel, octetul CLA din această comandă indică o utilizare exclusivă a comenzii PERFORM SECURITY OPERATION/HASH.

TCS_369 Comanda PERFORM HASH OF FILE se utilizează pentru a executa funcția de distribuie pe zona de date a FE transparent selectat.

TCS_370 Rezultatul operațiunii de distribuire este stocat în card. Ulterior, acesta poate fi utilizat pentru a obține semnătura digitală a fișierului, utilizând comanda PSO_COMPUTE_DIGITAL_SIGNATURE. Acest rezultat rămâne disponibil pentru comanda COMPUTE DIGITAL SIGNATURE până la următoarea executare cu succes a comenzii PERFORM HASH OF FILE.

TCS_371 Mesaj de comandă

Octet	Lungime	Valoare	Descriere
CLA	1	'80h'	CLA
INS	1	'2Ah'	Executare operațiune de securitate
P1	1	'90h'	Marcator: distribuire
P2	1	'00h'	P2: distribuire a datelor din fișierul transparent selectat

TCS_372 Mesaj de răspuns

Octet	Lungime	Valoare	Descriere
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

- Dacă comanda reușește, cardul transmite '9000';
- dacă nu este selectată o aplicație, este transmisă starea de procesare '6985';
- dacă FE selectat este considerat corupt (eroare în atributele fișierului sau de integritate a datelor stocate), starea de procesare transmisă este '6400' sau '6581';
- dacă fișierul selectat nu este un fișier transparent, starea de procesare transmisă este '6986'.

3.6.13. PSO: compute digital signature (calcul semnătură digitală)

Această comandă se utilizează pentru calcularea semnăturii digitale pentru codul de distribuire calculat anterior (vezi PERFORM HASH OF FILE, punctul 3.6.12).

Această comandă respectă ISO/IEC 7816-8. Utilizarea acestei comenzi este restricționată comparativ cu standardul corespunzător.

TCS_373 Cheia privată a cardului este utilizată pentru a calcula semnătura digitală și este cunoscută implicit de către card.

TCS_374 Cardul execută o semnătură digitală utilizând o metodă de completare în conformitate cu PKCS1 (vezi apendicele 11 pentru detalii).

TCS_375 Mesaj de comandă

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	CLA
INS	1	'2Ah'	Executare operațiune de securitate
P1	1	'9Eh'	Semnătură digitală de transmis
P2	1	'9Ah'	Marcator: câmpul de date conține datele de semnat. Întrucât nu este inclus un câmp de date, se presupune că datele sunt deja prezente în card (distribuie pe fișier)
Le	1	'80h'	Le (Lungimea semnăturii așteptate)

TCS_376 Mesaj de răspuns

Octet	Lungime	Valoare	Descriere
#1-#128	128	'XX..XXh'	Semnătura codului de distribuie calculat anterior
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

- Dacă comanda reușește, cardul transmite '9000';
- dacă cheia privată selectată implicit este considerată coruptă, starea de procesare transmisă este '6400' sau '6581'.

3.6.14. PSO: verify digital signature (verificare semnătură digitală)

Această comandă se utilizează pentru a verifica semnătura digitală, furnizată ca intrare, în conformitate cu PCKS1 a unui mesaj, al cărui cod de distribuire este cunoscut de către card. Algoritmul semnăturii este cunoscut implicit de către card.

Această comandă respectă ISO/IEC 7816-8. Utilizarea comenzii este restricționată comparativ cu standardul corespunzător.

TCS_377 Comanda VERIFY DIGITAL SIGNATURE utilizează întotdeauna cheia publică selectată de comanda anterioară MANAGE SECURITY ENVIRONMENT și codul de distribuire anterior introdus prin intermediul unei comenzi PSO: hash.

TCS_378 Mesaj de comandă

Octet	Lungime	Valoare	Descriere
CLA	1	'00h'	CLA
INS	1	'2Ah'	Executare operațiune de securitate
P1	1	'00h'	Marcator: câmpul de date conține DO relevante pentru verificare
P2	1	'A8h'	
Lc	1	'83h'	
#28	1	'9Eh'	Marcator pentru semnătura digitală
#29-#30	2	'8180h'	Lungimea semnăturii digitale (128 de octeți, codificați în conformitate cu ISO/IEC 7816-6)
#31-#158	128	'XX.XXh'	Conținutul semnăturii digitale

TCS_379 Mesaj de răspuns

Octet	Lungime	Valoare	Descriere
SW	2	'XXXXh'	Cuvinte de stare (SW1, SW2)

- Dacă comanda reușește, cardul transmite '9000';
- dacă verificarea semnăturii eșuează, starea de procesare transmisă este '6688'. Procesul de verificare este descris în apendicele 11;
- dacă nu este selectată o cheie publică, starea de procesare transmisă este '6A88';
- dacă unele dintre obiectele de date (conform specificațiilor de mai sus) lipsesc, este transmisă starea de procesare '6987'. Acest lucru se poate întâmpla dacă marcatorul necesar este absent;
- dacă nu este disponibil un cod de distribuire pentru procesarea comenzii (ca urmare a unei comenzi PSO: hash anterioare), starea de procesare transmisă este '6985';
- dacă unele dintre obiectele de date sunt incorecte, starea de procesare transmisă este '6988'. Acest lucru se poate întâmpla dacă lungimea unuia dintre obiectele de date necesare este incorectă;
- dacă cheia publică selectată este considerată coruptă, starea de procesare transmisă este '6400' sau '6581'.

4. STRUCTURA CARDULUI DE TAHOGRAF

Această secțiune prezintă structurile fișierelor de stocare a datelor accesibile ale cardurilor de tahograf.

Nu prezintă structurile interne care depind de producătorul cardului, precum antetele fișierelor, nici stocarea și procesarea elementelor de date necesare pentru utilizare internă, precum EuropeanPublicKey, CardPrivateKey, TDesSessionKey sau WorkshopCardPin.

Capacitatea utilă de memorare a cardurilor de tahograf trebuie să fie minimum 11 Kocteți. Pot fi utilizate capacități superioare. În acest caz, structura cardului rămâne aceeași, dar crește numărul de înregistrări ale unor elemente din structură. Prezenta secțiune specifică valorile minime și maxime pentru numărul acestor înregistrări.

4.1. Structura cardului șoferului

TCS_400 După personalizarea cardului șoferului, acesta are următoarea structură permanentă a fișierelor și următoarele condiții de accesare a fișierelor:

Fișier	ID fișier	Condiții de acces		
		Citire	Actualizare	Criptat
MF	3F00			
EF ICC	0002	INT	NIC	Nu
EF IC	0005	INT	NIC	Nu
DF Tachograph	0500			
EF Application_Identification	0501	INT	NIC	Nu
EF Card_Certificate	C100	INT	NIC	Nu
EF CA_Certificate	C108	INT	NIC	Nu
EF Identification	0520	INT	NIC	Nu
EF Card_Download	050E	INT	INT	Nu
EF Driving_Licence_Info	0521	INT	NIC	Nu
EF Events_Data	0502	INT	PRO MS/AUT	Nu
EF Faults_Data	0503	INT	PRO MS/AUT	Nu
EF Driver_Activity_Data	0504	INT	PRO MS/AUT	Nu
EF Vehicles_Used	0505	INT	PRO MS/AUT	Nu
EF Places	0506	INT	PRO MS/AUT	Nu
EF Current_Usage	0507	INT	PRO MS/AUT	Nu
EF Control_Activity_Data	0508	INT	PRO MS/AUT	Nu
EF Specific_Conditions	0522	INT	PRO MS/AUT	Nu

TCS_401 Structura tuturor FE trebuie să fie transparentă.

TCS_402 Citirea cu mesagerie securizată trebuie să fie posibilă pentru toate fișierele din DF Tachograph.

TCS_403 Cardul șoferului are următoarea structură de date:

Fișier/Element de date	Nr. înregistrări	Dimensiune (octeți)		Valori implicite
		Min	Max	
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 Următoarele valori, utilizate pentru a specifica dimensiunile din tabelul de mai sus, reprezintă valorile pentru numărul minim și maxim de înregistrări pe care structura de date a cardului șoferului trebuie să le utilizeze:

		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	5 544 octeți (28 zile * 93 modificări de activitate)	13 776 octeți (28 zile * 240 modificări de activitate)

4.2. Structura cardului atelierului

TCS_405 După personalizarea cardului atelierului, acesta are următoarea structură permanentă a fișierelor și următoarele condiții de accesare a fișierelor:

Fișier	ID fișier	Condiții de acces		
		Citire	Actualizare	Criptat
MF	3F00	INT		
EF ICC	0002	INT	NIC	Nu
EF IC	0005	INT	NIC	Nu
DF Tachograph	0500			
EF Application_Identification	0501	INT	NIC	Nu
EF Card_Certificate	C100	INT	NIC	Nu
EF CA_Certificate	C108	INT	NIC	Nu
EF Identification	0520	INT	NIC	Nu
EF Card_Download	0509	INT	INT	Nu
EF Calibration	050A	INT	PRO MS/AUT	Nu
EF Sensor_Installation_Data	050B	INT	NIC	Nu
EF Events_Data	0502	INT	PRO MS/AUT	Nu
EF Faults_Data	0503	INT	PRO MS/AUT	Nu
EF Driver_Activity_Data	0504	INT	PRO MS/AUT	Nu
EF Vehicles_Used	0505	INT	PRO MS/AUT	Nu
EF Places	0506	INT	PRO MS/AUT	Nu
EF Current_Usage	0507	INT	PRO MS/AUT	Nu
EF Control_Activity_Data	0508	INT	PRO MS/AUT	Nu
EF Specific_Conditions	0522	INT	PRO MS/AUT	Nu

TCS_406 Structura tuturor FE trebuie să fie transparentă.

TCS_407 Citirea cu mesagerie securizată trebuie să fie posibilă pentru toate fișierele din DF Tachograph.

TCS_408 Cardul atelierului are următoarea structură de date:

Fișier/Element de date	Nr. înregistrări	Dimensiune (octeți)		Valori implicite
		Min	Max	
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	
entryTime	4	4	{00..00}
SpecificConditionType	1	1	{00}

TCS_409 Următoarele valori, utilizate pentru a specifica dimensiunile din tabelul de mai sus, reprezintă valorile pentru numărul minim și maxim de înregistrări pe care structura de date a cardului atelierului trebuie să le utilizeze:

		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 octeți (1 zi * 93 modificări de activitate)	492 octeți (1 zi * 240 modificări de activitate)

4.3. Structura cardului de control

TCS_410 După personalizarea cardului de control, acesta are următoarea structură permanentă a fișierelor și următoarele condiții de accesare a fișierelor:

Fișier	ID fișier	Condiții de acces		
		Citire	Actualizare	Criptat
MF	3F00			
EF ICC	0002	INT	NIC	Nu
EF IC	0005	INT	NIC	Nu
DF Tachograph	0500			
EF Application_Identification	0501	INT	NIC	Nu
EF Card_Certificate	C100	INT	NIC	Nu
EF CA_Certificate	C108	INT	NIC	Nu
EF Identification	0520	INT	NIC	Nu
EF Controller_Activity_Data	050C	INT	PRO MS/AUT	Nu

TCS_411 Structura tuturor FE trebuie să fie transparentă.

TCS_412 Citirea cu mesagerie securizată trebuie să fie posibilă pentru toate fișierele din DF Tachograph.

TCS_413 Cardul de control are următoarea structură de date:

Fișier/Element de date	Nr. înregistrări	Dimensiune (octeți)		Nr. înregistrări
		Min	Max	
MF		11219	24559	
EF ICC		25	25	
CardIccIdentification		25	25	
clockStop		1	1	{00}
cardExtendedSerialNumber		8	8	{00..00}
cardApprovalNumber		8	8	{20..20}
cardPersonaliserID		1	1	{00}
embedderIcAssemblerId		5	5	{00..00}
icIdentifier		2	2	{00..00}
EF IC		8	8	
CardChipIdentification		8	8	
icSerialNumber		4	4	{00..00}
icManufacturingReferences		4	4	{00 00}
DF Tachograph		11186	24526	
EF Application_Identification		5	5	
ControlCardApplicationIdentification		5	5	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfControlActivityRecords		2	2	{00 00}
EF Card_Certificate		194	194	
CardCertificate		194	194	{00..00}
EF CA_Certificate		194	194	
MemberStateCertificate		194	194	{00..00}
EF Identification		211	211	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		146	146	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Controller_Activity_Data		10582	23922	
ControlCardControlActivityData		10582	23922	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		10580	23920	
controlActivityRecord	n ₇	46	46	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_414 Următoarele valori, utilizate pentru a specifica dimensiunile din tabelul de mai sus, reprezintă valorile pentru numărul minim și maxim de înregistrări pe care structura de date a cardului de control trebuie să le utilizeze:

		Min	Max
n ₇	NoOfControlActivityRecords	230	520

4.4. Structura cardului societății

TCS_415 După personalizarea cardului societății, acesta are următoarea structură permanentă a fișierelor și următoarele condiții de accesare a fișierelor:

Fișier	ID fișier	Condiții de acces		
		Citire	Actualizare	Criptat
MF	3F00			
EF ICC	0002	INT	NIC	Nu
EF IC	0005	INT	NIC	Nu
DF Tachograph	0500			
EF Application_Identification	0501	INT	NIC	Nu
EF Card_Certificate	C100	INT	NIC	Nu
EF CA_Certificate	C108	INT	NIC	Nu
EF Identification	0520	AUT	NIC	Nu
EF Company_Activity_Data	050D	INT	PRO MS/AUT	Nu

TCS_416 Structura tuturor FE trebuie să fie transparentă.

TCS_417 Citirea cu mesagerie securizată trebuie să fie posibilă pentru toate fișierele din DF Tachograph.

TCS_418 Cardul societății are următoarea structură de date:

Fișier/Element de date	Nr. înregistrări	Dimensiune (octeți)		Valori implicite
		Min	Max	
MF		11147	24487	
EF ICC		25	25	
CardIccIdentification		25	25	
clockStop		1	1	{00}
cardExtendedSerialNumber		8	8	{00..00}
cardApprovalNumber		8	8	{20..20}
cardPersonaliserID		1	1	{00}
embedderIcAssemblerId		5	5	{00..00}
icIdentifier		2	2	{00..00}
EF IC		8	8	
CardChipIdentification		8	8	
icSerialNumber		4	4	{00..00}
icManufacturingReferences		4	4	{00..00}
DF Tachograph		11114	24454	
EF Application_Identification		5	5	
CompanyCardApplicationIdentification		5	5	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfCompanyActivityRecords		2	2	{00 00}
EF Card_Certificate		194	194	
CardCertificate		194	194	{00..00}
EF CA_Certificate		194	194	
MemberStateCertificate		194	194	{00..00}
EF Identification		139	139	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
CompanyCardHolderIdentification		74	74	
companyName		36	36	{00, 20..20}
companyAddress		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Company_Activity_Data		10582	23922	
CompanyActivityData		10582	23922	
companyPointerNewestRecord		2	2	{00 00}
companyActivityRecords		10580	23920	
companyActivityRecord	n ₈	46	46	
companyActivityType		1	1	{00}
companyActivityTime		4	4	{00..00}
cardNumberInformation				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
vehicleRegistrationInformation				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}

cardNumberInformation			
cardType	1	1	{00}
cardIssuingMemberState	1	1	{00}
cardNumber	16	16	{20..20}
downloadPeriodBegin	4	4	{00..00}
downloadPeriodEnd	4	4	{00..00}

TCS_419 Următoarele valori, utilizate pentru a specifica dimensiunile din tabelul de mai sus, reprezintă valorile pentru numărul minim și maxim de înregistrări pe care structura de date a cardului societății trebuie să le utilizeze:

		Min	Max
n8	NoOfCompanyActivityRecords	230	520

*Apendicele 3***PICTOGRAME**

PIC_001 Aparatul de înregistrare poate utiliza următoarele pictograme și combinații de pictograme:

1. Pictograme de bază

	Persoane	Acțiuni	Moduri de funcționare
	Societate		Mod societate
	Controlor	Control	Mod control
	Șofer	Conducere	Mod operațional
	Atelier/stație testare	Inspecție/calibrare	Mod calibrare
	Producător		
	Activități	Durată	
	Disponibilitate	Perioadă de disponibilitate în curs	
	Conducere	Perioadă de conducere continuă	
	Odihnă	Perioadă de odihnă în curs	
	Muncă	Perioadă de muncă în curs	
	Pauză	Perioade de pauză cumulate	
	Necunoscută		
	Aparat	Funcții	
	Lector șofer		
	Lector copilot		
	Card		
	Ceas		
	Afișaj	Afișare	
	Stocare externă	Descărcare	
	Alimentare		
	Imprimantă/imprimare	Imprimare	
	Senzor		
	Dimensiune pneuri		
	Vehicul/unitate montată pe vehicul		
	Condiții specifice		
	În afara domeniului de aplicare		
	Traversare pe feribot/tren		
	Diverse		
	Evenimente		Anomalii
	Începutul perioadei zilnice de muncă		Sfârșitul perioadei zilnice de muncă
	Loc		Introducere manuală a activităților șoferului
	Securitate		Viteză
	Ora		Total/rezumat
	Calificative		
	Zilnic		
	Săptămânal		
	Două săptămâni		
	De la sau până la		

2. COMBINAȚII DE PICTOGRAME

	Diverse		
	Loc de control		Loc de încheiere a perioadei zilnice de muncă
	Loc de începere a perioadei zilnice de muncă		Până la ora
	De la ora		Din vehicul
	Din vehicul		În afara domeniului de aplicare, sfârșit
	În afara domeniului de aplicare, început		

Carduri

	Cardul șoferului
	Cardul societății
	Card de control
	Cardul atelierului
	Nici un card

Conducere

	Conducere în echipaj
	Durată conducere pentru o săptămână
	Durată conducere pentru două săptămâni

Tipăriri

	Tipărire zilnică a activităților șoferului extrase din card
	Tipărire zilnică a activităților șoferului extrase din UV
	Tipărirea evenimentelor și anomaliilor extrase din card
	Tipărirea evenimentelor și anomaliilor extrase din VU
	Tipărirea datelor tehnice
	Tipărirea depășirilor de viteză

Evenimente

	Inserarea unui card nevalabil
	Conflict card
	Suprapunere de timp
	Conducere fără un card adecvat
	Inserarea cardului în timpul condusului
	Ultima sesiune a cardului nu a fost încheiată corect
	Depășire a vitezei autorizate
	Întrerupere a alimentării cu electricitate
	Eroare privind datele de mișcare
	Încălcarea securității
	Reglarea orei (în atelier)
	Control pentru depășirea vitezei autorizate

Anomalii

	Anomalie a cardului (lector pentru cardul șoferului)
	Anomalie a cardului (lector pentru cardul copilotului)
	Anomalie a afișajului
	Anomalie la descărcare
	Anomalie a imprimantei
	Anomalie a senzorului
	Anomalie internă a UV

Proceduri pentru introduceri manuale

	Aceași perioadă de muncă zilnică?
	Sfârșitul perioadei anterioare de muncă?
	Confirmați și introduceți locul de încheiere a perioadei de muncă
	Introduceți ora de pornire
	Introduceți locul de începere a perioadei de muncă.

Notă: În apendicele 4 sunt definite alte combinații de pictograme, pentru formarea de blocuri de tipărire sau identificatori de înregistrări.

Apendicele 4

MATERIALE TIPĂRITE

CUPRINS

1. Generalități	133
2. Specificații privind blocurile de date	133
3. Specificații referitoare la tipărire	139
3.1. Tipărirea zilnică a activităților șoferului de pe card	140
3.2. Tipărirea zilnică a activităților șoferului din UV	140
3.3. Tipărirea evenimentelor și anomaliilor de pe card	141
3.4. Tipărirea evenimentelor și anomaliilor din UV	141
3.5. Tipărirea datelor tehnice	142
3.6. Tipărirea depășirilor vitezei autorizate	142

1. GENERALITĂȚI

Fiecare document tipărit este construit prin înlănțuirea a diverse blocuri de date, identificate, dacă este cazul, prin intermediul unui identificator de bloc.

Un bloc de date conține una sau mai multe înregistrări, identificate, dacă este cazul, prin intermediul unui identificator de înregistrare.

- PRT_001 Când un identificator de înregistrare urmează imediat după un identificator de bloc, identificatorul de înregistrare nu este tipărit.
- PRT_002 În cazul în care un element de date este necunoscut sau nu trebuie tipărit din motive determinate de dreptul de acces la date, în locul acestuia sunt tipărite spații.
- PRT_003 Dacă întregul conținut al unei linii este necunoscut sau nu trebuie tipărit, este omisă întreaga linie.
- PRT_004 La tipărire, câmpurile de date numerice sunt aliniate la dreapta, cu un spațiu de separare pentru mii și milioane și fără zerouri la început.
- PRT_005 La tipărire, câmpurile de date constituite din șiruri de caractere sunt aliniate la stânga și completate cu spații până la lungimea elementului de date sau tăiate la lungimea elementului de date, dacă este necesar (nume și adrese).

2. SPECIFICAȚII PRIVIND BLOCURILE DE DATE

În acest capitol sunt utilizate următoarele notații convenționale pentru formatare:

- caracterele **aldine** indică faptul că trebuie imprimat un text normal (textul se tipărește cu caractere normale);
- caracterele normale reprezintă variabile (pictograme sau date) care la tipărire trebuie înlocuite cu valorile lor;
- denumirile variabilelor au fost completate cu liniuțe de subliniere () pentru a ilustra lungimea elementului de date disponibil pentru variabila în cauză;
- datele sunt specificate în formatul «zz/ll/aaaa» (zi, lună,an). Se poate utiliza, de asemenea, un format «zz.ll.aaaa»;
- termenul «identificarea cardului» reprezintă combinația dintre: tipul de card, reprezentat printr-o combinație de pictograme, codul statului membru care a emis cardul, o bară oblică orientată spre dreapta și numărul cardului cu indexul de înlocuire și indexul de reînnoire separate de un spațiu:

P		x	x	x	/	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Combinatie de pictograme de card	Codul statului membru emitent	Primele 14 caractere din numărul cardului (inclusiv, dacă este cazul, un index consecutiv)																				Indice de înlocuire		Indice de reînnoire

- PRT_006 Documentele tipărite utilizează următoarele blocuri de date și/sau înregistrări de date, în conformitate cu următoarele semnificații și formate:

Numărul blocului sau înregistrării
Semnificație

Format date

1. Data și ora la care a fost tipărit documentul

zz/ll/aaaa hh:mm (UTC)

2. **Tipul de tipărire**

Identificator de bloc

Combinație de pictograme de tipărire (vezi apendicele 3), setarea limitatorului de viteză (tipărire doar la depășirea vitezei autorizate).

----------
Picto xxx km/h

3. **Identificarea titularului cardului**

Identificator de bloc. P = pictogramă a unei persoane

Numele titularului cardului

Prenumele titularului cardului (dacă este cazul)

Identificarea cardului

Data expirării cardului (dacă este cazul)

În cazul în care cardul nu este un card individual și nu are înscris numele titularului cardului, se tipărește în locul acestuia numele societății, al atelierului sau al organismului de control.

-----P-----
P Numele _____
Prenumele _____
Identificare_card _____
zz/ll/aaaa

4. **Identificarea vehiculului**

Identificator de bloc

(VIN)

Stat membru de înregistrare și VRN.

----------
 VIN _____
Nat/VRN _____

5. **Identificarea UV**

Identificator de bloc

Denumirea fabricantului UV

Număr de componentă al UV.

----------
 Fabricant_UV _____
Nr_referință_UV _____

6. **Ultima calibrare a aparatului de înregistrare**

Identificator de bloc

Numele atelierului

Identificarea cardului atelierului

Data calibrării.

----------
 Numele _____
Identificarea_cardului _____
 zz/ll/aaaa

7. **Ultimul control (efectuat de un ofițer de control)**

Identificator de bloc

Identificarea cardului controlorului

Data, ora și tipul controlului

Tipul de control: Până la patru pictograme. Tipul de control poate fi (o combinație de):

 : Descărcare de pe card,  : descărcare de pe UV,  : tipărire,  : afișare.

----------
Identificarea_cardului _____
 ZZ/ll/aaa hh:mm pppp

8. **Activitățile șoferului stocate pe card în ordine cronologică**

Identificator de bloc

Data interogării (ziua calendaristică ce face obiectul tipăririi) + contor de prezență zilnică a cardului.

----------
dd/mm/yyyy xxx

8.1. *Intervalul în care cardul nu a fost inserat*8.1a. *Identificator de înregistrare (începutul intervalului)*8.1b. *Interval necunoscut. Ora de începere și de încheiere, durata*8.1c. *Activitate introdusă manual*

Pictogramă a unei activități, ora de începere și de încheiere (inclusiv), durata, perioadele de odihnă cu o durată de cel puțin o oră sunt marcate cu un asterisc.

----------
 hh:mm hh:mm hh:mm
A hh:mm hh:mm hh:mm *

- 8.2. *Inserarea cardului în lectorul S*
 Identificator de înregistrare. S = pictograma lectorului
 Statul membru de înmatriculare a vehiculului și VRN
 Kilometrajul vehiculului la inserarea cardului.
- 8.3. *Activitate (cu cardul inserat)*
 Pictogramă a unei activități, ora de începere și de încheiere (inclusiv), durata, starea echipajului (pictogramă de echipaj dacă există un ECHIPAJ, spații libere pentru mod SINGUR), perioadele de odihnă cu o durată de cel puțin o oră sunt marcate cu un asterisc.
- 8.3a. *Condiție specifică. Ora introducerii, pictogramă (sau combinație de pictograme) pentru condiții specifice.*
- 8.4. *Retragerea cardului*
 Kilometrajul vehiculului și distanța parcursă de la ultima inserare pentru care se cunoaște kilometrajul.
9. **Activitățile șoferului stocate într-o UV, per lector, în ordine cronologică**
 Identificator de bloc
 Data interogării (ziua calendaristică ce face obiectul tipăririi)
 Kilometrajul vehiculului la 00:00 și 24:00.
10. **Activități desfășurate în lectorul S**
 Identificator de bloc.
- 10.1. *Intervalul în care în lectorul S nu era inserat un card*
 Identificator de înregistrare
 Nici un card inserat
 Kilometrajul vehiculului la începutul intervalului.
- 10.2. *Inserarea cardului*
 Identificator de înregistrare a inserării cardului
 Numele șoferului
 Prenumele șoferului
 Identificarea cardului șoferului
 Data expirării cardului șoferului
 SM de înregistrare și VRN ale vehiculului utilizat anterior
 Data și ora retragerii cardului din vehiculul anterior
 Linie liberă
 Kilometrajul vehiculului la inserarea cardului, introducerea manuală a marcajului pentru activitățile șoferului (M dacă da, spațiu dacă nu).
- 10.3. *Activitate*
 Pictogramă a unei activități, ora de începere și de încheiere (inclusiv), durata, starea echipajului (pictogramă de echipaj dacă există un ECHIPAJ, spații libere pentru mod SINGUR), perioadele de odihnă cu o durată de cel puțin o oră sunt marcate cu un asterisc.

-----S-----
 A Nat / VRN _____
 x xxx xxx km

A hh:mm hh:mm hh:mm ☐☐ *

hh:mm ----- pppp -----

x xxx xxx km; x xxx km

-----☐-----
 zz/11/aaaa
 x xxx xxx - x xxx xxx km

----- S -----

 ☐☐ ---
 x xxx xxx km

 ☐ Numele _____
 Prenumele _____
 Identificarea_cardului _____
 zz/11/aaaa
 A → Nat / NIV _____
 zz/11/aaa hh:mm
 x xxx xxx km M

A hh:mm hh:mm hh:mm ☐☐ *

- 10.3a. *Condiție specifică. Ora introducerii, pictogramă (sau combinație de pictograme) pentru condiții specifice.*

hh:mm - - - - - pppp - - - - -

- 10.4. *Retragerea cardului sau Sfârșitul unui interval «Nici un card»*
Kilometrajul vehiculului la retragerea cardului sau la sfârșitul intervalului «Nici un card» și distanța parcursă de la inserare sau de la începutul intervalului «Nici un card»

x xxx xxx km; x xxx km

11. Rezumat zilnic

Identificator de bloc.

- - - - - Σ - - - - -

- 11.1. *Rezumat UV pentru perioadele în care nu există card în lectorul șoferului*

Identificator de bloc.

1 0 - - -

- 11.2. *Rezumat UV pentru perioadele în care nu există card în lectorul copilotului*

Identificator de bloc.

2 0 - - -

- 11.3. *Rezumat UV zilnic per șofer*

Identificator de înregistrare

Numele șoferului

Prenumele șoferului

Identificarea cardului șoferului.

 0 Numele _____
 Prenumele _____
 Identificarea_cardului _____

- 11.4. *Introducerea locului unde începe și/sau se încheie o perioadă zilnică de muncă*

pi = pictograma locului la început/sfârșit, ora, țara, regiunea, kilometraj.

pi hh:mm Țara Reg
 x xxx xxx km

- 11.5. *Totalurile activităților (dintr-un card)*

Durata totală de conducere, distanța parcursă

Durata totală de muncă și de disponibilitate

Durata totală de odihnă și necunoscută

Durata totală a activităților echipajului.

0 hh:mm x xxx km
 ✱ hh:mm 0 hh:mm
 H hh:mm ? hh:mm
 00 hh:mm

- 11.6. *Totalurile activităților (perioade în care nu a existat nici un card în lectorul șoferului)*

Durata totală de conducere, distanța parcursă

Durata totală de muncă și de disponibilitate

Durata totală de odihnă.

0 hh:mm x xxx km
 ✱ hh:mm 0 hh:mm
 H hh:mm

- 11.7. *Totalurile activităților (perioade în care nu a existat card în lectorul copilotului)*

Durata totală de muncă și de disponibilitate

Durata totală de odihnă.

✱ hh:mm 0 hh:mm
 H hh:mm

11.8 Totalurile activităților (per șofer, ambele lectoare incluse)

Durata totală de conducere, distanța parcursă

Durata totală de muncă și disponibilitate

Durata totală de odihnă

Durata totală a activităților echipajului.

Când este necesară tipărirea unui document zilnic pentru ziua curentă, rezumatul informațiilor zilnice este întocmit pe baza datelor disponibile în momentul tipăririi.

⊠ hh:mm x xxx km
 ✖ hh:mm ⊠ hh:mm
 ⊠ hh:mm
 ⊠⊠ hh:mm

12. Evenimente și/sau anomalii pe un card

12.1. Identificator de bloc pentru ultimele 5 «Evenimente și Anomalii» de pe un card

----- ! ✖ ⊠ -----

12.2. Identificator de bloc pentru toate «Evenimentele» înregistrate pe un card

----- ! ⊠ -----

12.3. Identificator de bloc pentru toate «Anomaliile» de pe un card

----- ✖ ⊠ -----

12.4. Înregistrarea unui Eveniment și/sau a unei Anomalii

Identificator de înregistrare

Pictogramă de eveniment/anomalie, scopul înregistrării, data și ora declanșării,

Cod suplimentar de eveniment/anomalie (dacă există), durata

Stat membru de înregistrare și VRN ale vehiculului în care a avut loc evenimentul/anomalia.

 Pic zz/11/aaaa hh:mm
 ! xxx hh:mm
 ⊠ Nat/NIV -----

13. Evenimente și/sau anomalii stocate sau active în UV

13.1. Identificator de bloc pentru ultimele 5 «Evenimente și Anomalii» dintr-o UV

----- ! ✖ ⊠ -----

13.2. Identificator de bloc pentru toate «Evenimentele» active într-o UV

----- ! ⊠ -----

13.3. Identificator de bloc pentru toate «Anomaliile» înregistrate sau active într-o UV

----- ✖ ⊠ -----

13.4. Înregistrarea unui eveniment și/sau a unei anomalii

Identificator de înregistrare

Pictogramă de eveniment/anomalie, scopul înregistrării, data și ora declanșării,

Cod suplimentar de eveniment/anomalie (dacă există), numărul evenimentelor similare din aceeași zi, durata

Identificarea cardurilor inserate la începutul sau la sfârșitul evenimentului sau al anomaliei (până la 4 linii fără a se repeta de două ori același număr de card)

Cazuri în care nu au fost inserate carduri

Scopul înregistrării (p) este un cod numeric care explică motivele pentru care evenimentul sau anomalia au fost înregistrate, codificat în conformitate cu elementul de date EventFaultRecordPurpose.

 Pic (p) zz/11/aaaa hh:mm
 ! xxx (xxx) hh:mm
 Identificarea_cardului -----
 Identificarea_cardului -----
 Identificarea_cardului -----
 Identificarea_cardului -----
 ⊠ ---

14. **Identificarea UV**

Identificator de bloc
 Denumirea fabricantului UV
 Adresa fabricantului UV
 Numărul de referință al UV
 Numărul de omologare al UV
 Seria UV
 Anul de fabricație a UV
 Versiunea software-ului UV și data instalării acestuia.

```

-----B-----
B Denumirea _____
  Adresa   _____
  Nr. Ref.  _____
  Omol     _____
  Serie    _____
  aaa
  V      xx.xx.xx      zz/11/aaaa
  
```

15. **Identificarea senzorului**

Identificator de bloc
 Seria senzorului
 Numărul de omologare a senzorului
 Data primei instalări a senzorului

```

-----L-----
L Serie _____
  Omol _____
  zz/11/aaaa
  
```

16. **Data calibrării**

Identificator de bloc.

```

-----T-----
  
```

16.1. **Înregistrarea calibrării**

Identificator de înregistrare
 Atelierul care a realizat calibrarea
 Adresa atelierului
 Identificarea cardului atelierului
 Data expirării cardului atelierului
 Linie liberă
 Data calibrării + scopul calibrării
 VIN
 Statul membru de înregistrare și VRN
 Coeficientul caracteristic al vehiculului
 Constanta aparatului de înregistrare
 Circumferința efectivă a pneurilor
 Dimensiunea pneurilor montate
 Setările limitatorului de viteză
 Valoarea nouă și veche a kilometrajului
 Scopul calibrării (p) este un cod numeric care explică
 motivul pentru care acești parametri de calibrare au fost
 înregistrați, codificat în conformitate cu elementul de
 date CalibrationPurpose.

```

-----
T Denumirea_atelierului _____
  Adresa_atelierului _____
  Identificarea_cardului _____
  zz/11/aaaa

T zz/11/aaaa      (p)
A NIdV _____
  Nat/NIV _____
w xx xxx Imp/km
k xx xxx Imp/km
l xx xxx mm
• Dim Cauciuc _____
> xxx km/h
x xxx xxx - x xxx xxx km
  
```

17. **Reglarea orei**

Identificator de bloc.

```

-----O-----
  
```

17.1. **Înregistrarea reglării orei**

Identificator de înregistrare
 Data și ora vechi
 Data și ora noi
 Atelierul care a efectuat reglarea orei
 Adresa atelierului
 Identificarea cardului atelierului
 Data expirării cardului atelierului.

```

-----
! O zz/11/aaaa hh:mm
  O zz/11/aaaa hh:mm
T Denumirea_atelierului _____
  Adresa_atelierului _____
  Identificarea_cardului _____
  zz/11/aaaa
  
```

18. **Evenimentele și anomaliile cele mai recente înregistrate în UV**
 Identificator de bloc
 Data și ora celui mai recent eveniment
 Data și ora celei mai recente anomalii
19. **Informații privind controlul depășirii vitezei autorizate**
 Identificator de bloc
 Data și ora ultimului CONTROL PRIVIND DEPĂȘIREA VITEZEI AUTORIZATE
 Data/ora primei depășiri a vitezei autorizate și numărul depășirilor ulterioare de viteză.
20. **Controlul privind depășirea vitezei autorizate**
- 20.1. Identificator de bloc pentru «Prima depășire a vitezei autorizate după ultima calibrare».
- 20.2. Identificator de bloc pentru «Cele mai grave 5 depășiri de viteză în ultimele 365 de zile».
- 20.3. Identificator de bloc pentru «Cea mai gravă depășire de viteză pentru fiecare dintre ultimele 10 zile de ocurență»
- 20.4. *Identificator de înregistrare*
 Data, ora și durata
 Viteza maximă și viteza medie. Numărul de evenimente similare din ziua respectivă
 Numele șoferului
 Prenumele șoferului
 Identificarea cardului șoferului
- 20.5. Dacă într-un bloc nu există nici o înregistrare a unei depășiri de viteză
21. **Informații scrise de mână**
 Identificator de bloc
- 21.1. *Locul efectuării controlului*
- 21.2. *Semnătura controlorului*
- 21.3. *De la ora*
- 21.4. *La ora*
- 21.5. *Semnătura șoferului*
 «Informații scrise de mână»: introduceți suficiente rânduri libere deasupra unui element scris de mână, pentru a putea scrie informațiile necesare sau pentru a aplica o semnătură.

3. SPECIFICAȚII REFERITOARE LA TIPĂRIRE

În prezentul capitol s-au folosit următoarele notații convenționale:

N
N
X/Y

Tipărirea blocului sau a înregistrării cu numărul N

Tipărirea blocului sau a înregistrării cu numărul N repetată ori de câte ori este necesar

Tipărirea blocurilor sau a înregistrărilor X și/sau Y, după caz, cu repetarea operațiunii ori de câte ori este necesar

3.1. Tipărirea zilnică a activităților șoferului de pe card

PRT_007 Tipărirea zilnică din card a activităților șoferului se face în conformitate cu următorul format:

1	Data și ora la care se tipărește documentul
2	Tipul de tipărire
3	Identificarea controlorului (dacă în UV este inserat un card de control)
3	Identificarea șoferului (din cardul supus tipăririi)
4	Identificarea vehiculului (vehiculul din care se tipărește documentul)
5	Identificarea UV (UV din care se tipărește documentul)
6	Ultima calibrare a acestei UV
7	Ultimul control căruia i-a fost supus șoferul controlat
8	Delimitator al activităților șoferului
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Activitățile șoferului în ordine cronologică
11	Delimitator al rezumatului zilnic
11.4	Locuri introduse în ordine cronologică
11.5	Totaluri ale activităților
12.1	Evenimente sau anomalii din delimitatorul cardului
12.4	Înregistrări de evenimente/anomalii (ultimele 5 evenimente sau anomalii înregistrate în card)
13.1	Evenimente sau anomalii din delimitatorul UV
13.4	Înregistrări de evenimente/anomalii (ultimele 5 evenimente sau anomalii înregistrate sau în curs în UV)
21.1	Locul controlului
21.2	Semnătura controlorului
21.5	Semnătura șoferului

3.2. Tipărirea zilnică a activităților șoferului din UV

PRT_008 Tipărirea zilnică a activităților șoferului din UV se face în conformitate cu următorul format:

1	Data și ora la care se tipărește documentul
2	Tipul de tipărire
3	Identificarea titularului cardului (pentru toate cardurile inserate în UV)
4	Identificarea vehiculului (vehiculul din care se tipărește documentul)
5	Identificarea UV (UV din care se tipărește documentul)
6	Ultima calibrare a acestei UV
7	Ultimul control căruia i-a fost supus aparatul de înregistrare
9	Delimitator al activităților șoferului
10	Delimitator al lectorului șoferului (fanta 1)
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Activitățile șoferului în ordine cronologică (lectorul șoferului)
10	Delimitator al lectorului copilotului (fanta 2)
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Activitățile șoferului în ordine cronologică (lectorul copilotului)
11	Delimitator al rezumatului zilnic
11.1	Rezumat al perioadelor în care nu exista card în lectorul șoferului
11.4	Locuri introduse în ordine cronologică
11.6	Totaluri ale activităților

11.2	Rezumatul perioadelor în care nu a existat un card în lectorul copilotului
11.4	Locuri introduse în ordine cronologică
11.7	Totaluri ale activităților
11.3	Rezumatul activităților pentru un șofer incluzând ambele lectoare
11.4	Locuri introduse de șoferul respectiv, în ordine cronologică
11.7	Totaluri ale activităților pentru șoferul respectiv
13.1	Delimitator de evenimente/anomalii
13.4	Înregistrări de evenimente/anomalii (Ultimele 5 anomalii sau evenimente înregistrate sau active în UV)
21.1	Locul controlului
21.2	Semnătura controlorului
21.3	De la ora (spațiu disponibil pentru un șofer care nu deține un card, pentru a putea indica aici perioadele relevante pentru el)
21.4	La ora
21.5	Semnătura șoferului

3.3. Tipărirea evenimentelor și a anomaliilor de pe card

PRT_009 Tipărirea evenimentelor sau anomaliilor din card se face în conformitate cu următorul format:

1	Data și ora la care se tipărește documentul
2	Tipul de tipărire
3	Identificarea controlorului (dacă în UV este inserat un card de control)
3	Identificarea șoferului (din cardul supus tipăririi)
4	Identificarea vehiculului (vehiculul din care se tipărește documentul)
12.2	Delimitator de evenimente
12.4	Înregistrări de evenimente (toate evenimentele înregistrate în card)
12.3	Delimitator de anomalii
12.4	Înregistrări de anomalii (toate anomaliile înregistrate în card)
21.1	Locul controlului
21.2	Semnătura controlorului
21.5	Semnătura șoferului

3.4. Tipărirea evenimentelor și a anomaliilor din UV

PRT_010 Tipărirea evenimentelor sau a anomaliilor din UV se face în conformitate cu următorul format:

1	Data și ora la care se tipărește documentul
2	Tipul de tipărire
3	Identificarea titularului cardului (pentru toate cardurile inserate în UV)
4	Identificarea vehiculului (vehiculul din care se tipărește documentul)
13.2	Delimitator de evenimente
13.4	Înregistrări de evenimente (toate evenimentele înregistrate sau active în UV)
13.3	Delimitator de anomalii
13.4	Înregistrări de anomalii (toate anomaliile înregistrate sau active în UV)
21.1	Locul controlului
21.2	Semnătura controlorului
21.5	Semnătura șoferului

3.5. Tipărirea datelor tehnice

PRT_011 Tipărirea datelor tehnice se face în conformitate cu următorul format:

1	Data și ora la care se tipărește documentul
2	Tipul de tipărire
3	Identificarea titularului cardului (pentru toate cardurile inserate în UV)
4	Identificarea vehiculului (vehiculul din care se tipărește documentul)
14	Identificarea UV
15	Identificarea senzorului
16	Delimitatorul datelor de calibrare
16.1	Înregistrări ale calibrărilor (toate înregistrările disponibile în ordine cronologică)
17	Delimitator al reglării orei
17.1	Înregistrări privind reglarea orei (toate înregistrările disponibile din înregistrări privind reglarea orei și datele de calibrare)
18	Cel mai recent eveniment și cea mai recentă anomalie înregistrate în UV

3.6. Tipărirea depășirilor vitezei autorizate

PRT_012 Tipărirea depășirilor vitezei autorizate se face în conformitate cu următorul format:

1	Data și ora la care se tipărește documentul
2	Tipul de tipărire
3	Identificarea titularului cardului (pentru toate cardurile inserate în UV)
4	Identificarea vehiculului (vehiculul din care se tipărește documentul)
19	Informații privind controlul depășirilor de viteză
20.1	Identificatorul datelor privind depășirile de viteză
20.4 / 20.5	Prima depășire a vitezei autorizate după ultima calibrare
20.2	Identificatorul datelor privind depășirile de viteză
20.4 / 20.5	Cele mai grave 5 depășiri ale vitezei autorizate din ultimele 365 de zile
20.3	Identificatorul datelor privind depășirile de viteză
20.4 / 20.5	Cele mai grave depășiri ale vitezei autorizate din fiecare din ultimele 10 zile de ocurență
21.1	Locul controlului
21.2	Semnătura controlorului
21.5	Semnătura șoferului.

*Apendicele 5***AFIŞAJ**

În prezentul apendice s-au folosit următoarele convenții de prezentare a formatului:

- caracterele **aldine** indică textul care urmează să fie afișat (afișajul rămâne în caractere normale);
- caracterele normale indică variabilele (pictograme sau date) care trebuie să fie înlocuite cu valorile lor pentru afișare:
 - zz ll aaaa: ziua, luna, anul
 - hh: orele
 - mm: minutele
 - D: pictograma duratei
 - EF: combinația pictogramelor de eveniment sau anomalie
 - O: pictograma modului de funcționare

DIS_001 Aparatul de înregistrare afișează datele folosind următoarele formate:

Date	Format
Afișaj implicit	
Ora locală	Hh:mm
Modul de funcționare	O
Informații privind șoferul	1 Dhhmm hhmm
Informații privind copilotul	2 Dhhmm
Condiții în afara domeniului de aplicare	OUT
Afișaj de avertizare	
Depășirea timpului de conducere continuă	1 0hhmm hhmm
Eveniment sau anomalie	EF
Alte afișaje	
data UTC	UTC 0gg/mm/aaaa o UTC 0gg.mm.aaaa
ora	Hh:mm
Timpul de conducere continuă și durata cumulată a pauzelor șoferului	1 0hhmm hhmm
Timpul de conducere continuă și durata cumulată a pauzelor copilotului	2 0hhmm hhmm
Timpul de conducere cumulată al șoferului pentru săptămâna precedentă și cea curentă	1 0 hhhhmm
Timpul de conducere cumulată al copilotului pentru săptămâna precedentă și cea curentă	2 0 hhhhmm

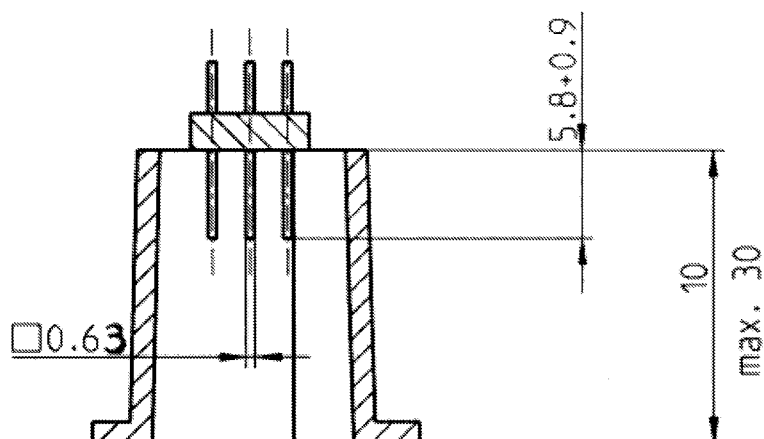
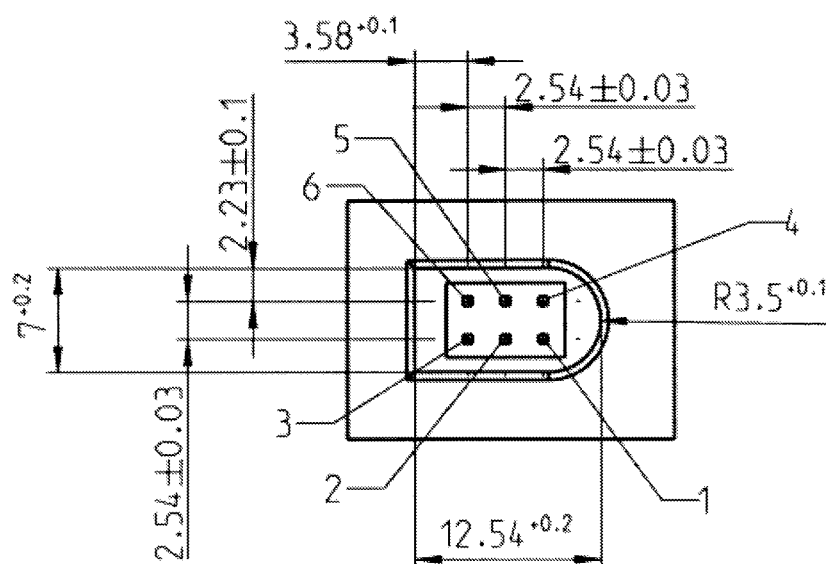
*Apendicele 6***INTERFEȚE EXTERNE****CUPRINS**

1.	Hardware	146
1.1.	Conector	146
1.2.	Alocarea contactelor	148
1.3.	Diagramă funcțională	148
2.	Interfață de descărcare	148
3.	Interfață de calibrare	149

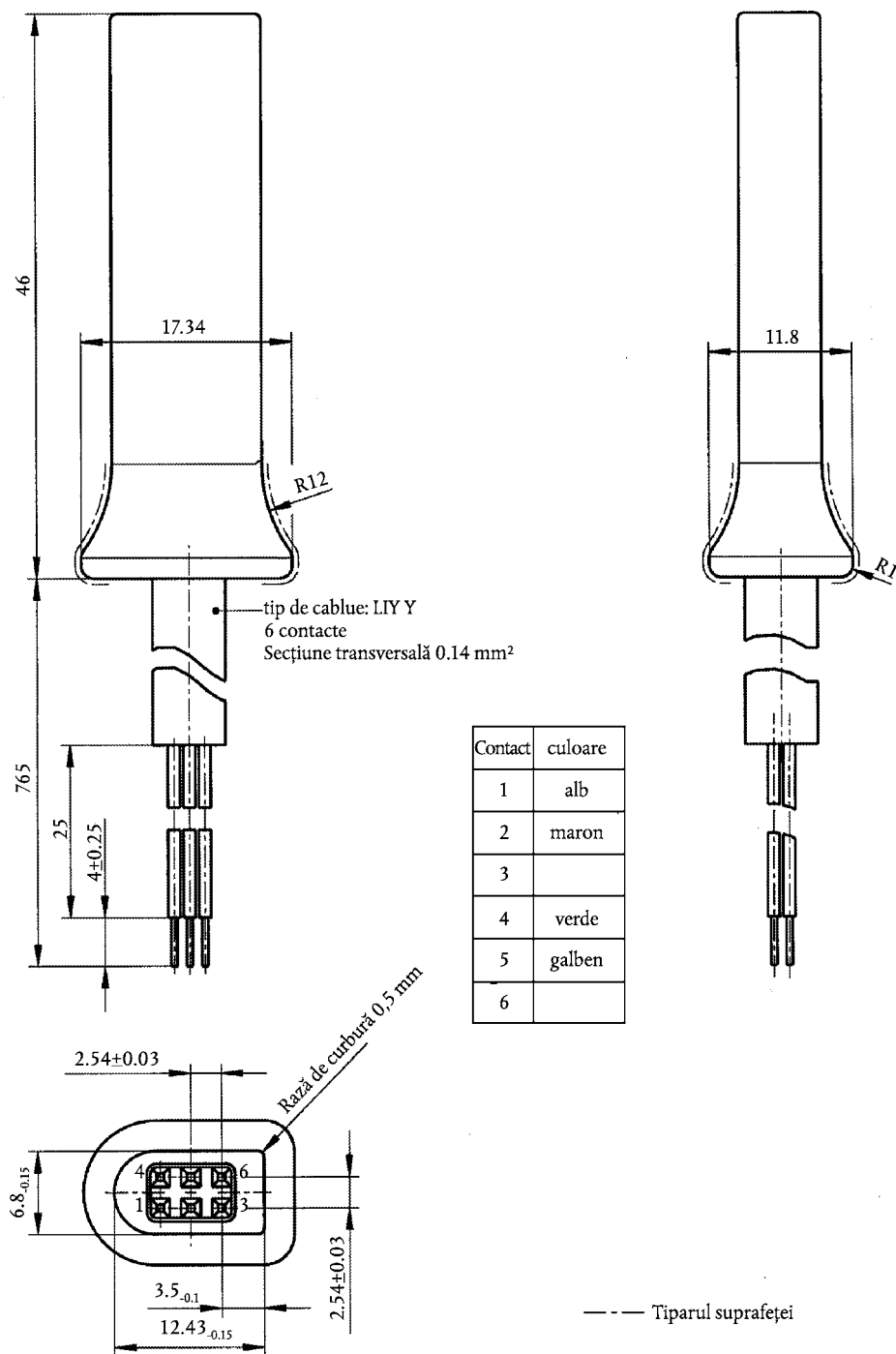
1. HARDWARE

1.1. Conector

INT_001 Conectorul de calibrare/descărcare trebuie să fie un conector cu șase contacte, care să poată fi accesat de la panoul frontal, fără a fi necesară deconectarea unei părți a aparatului de înregistrare, și trebuie să respecte următoarea schiță (toate dimensiunile sunt în milimetri):



În următoarea diagramă este prezentată o fișă obișnuită de conectare cu șase contacte:



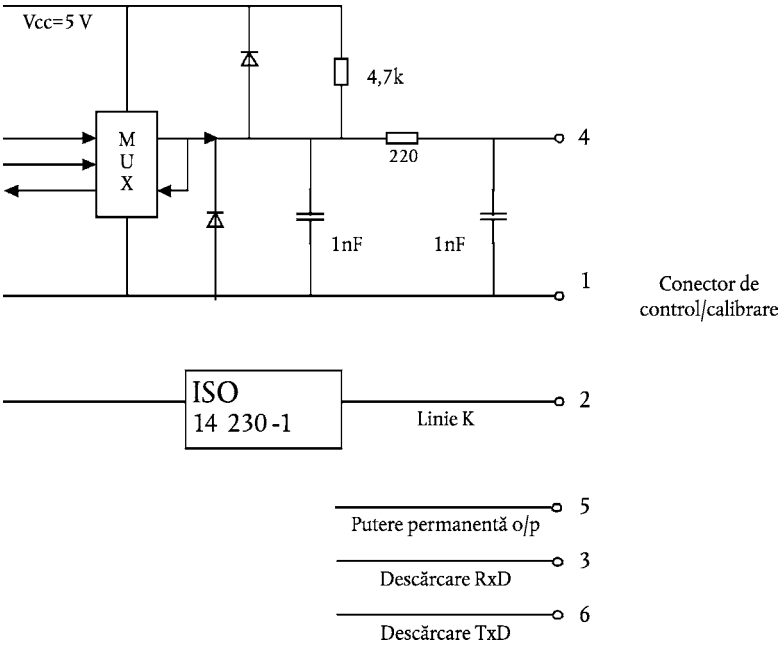
1.2. Alocarea contactelor

INT_002 Contactele se alocă în conformitate cu tabelul următor:

Contact	Descriere	Observații
1	Pol negativ al bateriei	Conectat la polul negativ al bateriei vehiculului
2	Comunicarea datelor	Linie K (ISO 14 230-1)
3	RxD – Descărcare	Introducerea datelor în aparatul de înregistrare
4	Semnal de intrare/ieșire	Calibrare
5	Putere de ieșire permanentă	Intervalul de tensiune trebuie să fie identic cu cel pentru alimentarea electrică a vehiculului minus 3 V pentru a lua în calcul căderea de tensiune din circuitele de protecție Ieșire de 40 mA
6	TxD – Descărcare	Ieșire de date din aparatul de înregistrare

1.3. Diagrama funcțională

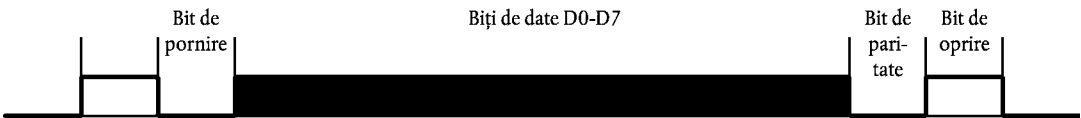
INT_003 Diagrama funcțională trebuie să respecte următoarele indicații:



2. INTERFAȚĂ DE DESCĂRCARE

INT_004 Interfața de descărcare trebuie să respecte specificațiile RS232.

INT_005 Interfața de descărcare folosește un bit de pornire, 8 biți de date, cu un BPI la început, un bit de paritate pară și un bit de oprire.



Organizarea octeților de informații

- Bit de pornire: un bit cu nivel logic 0
- Biți de date: transmis cu un BPI la început
- Bit de paritate: paritate pară
- Bit de oprire: un bit cu nivel logic 1

La transmisia datelor numerice compuse din mai mult de un octet, octetul cel mai important este transmis la început și octetul cel mai puțin important este transmis la sfârșit.

INT_006 Ratele binare pot fi reglate de la 9 600 bps la 115 200 bps. Transmisia se realizează la viteza cea mai mare posibilă, rata binară după începerea comunicării fiind stabilită la 9 600 bps.

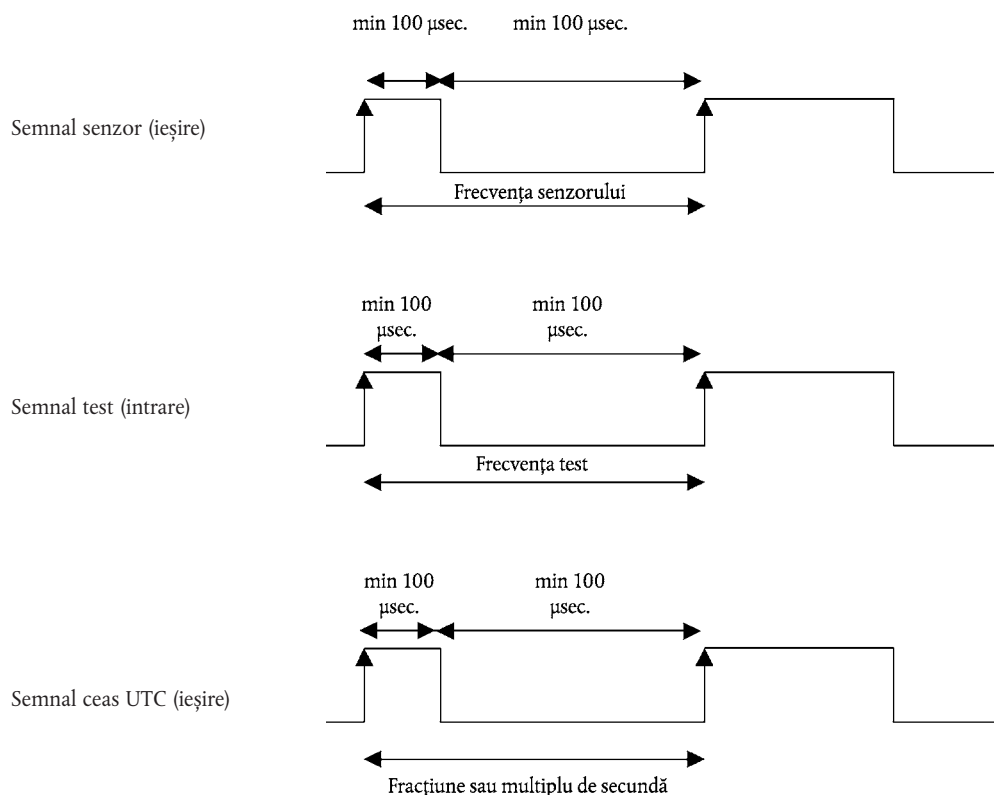
3. INTERFAȚĂ DE CALIBRARE

INT_007 Comunicările de date trebuie să respecte ISO 14 230-1 Vehicule rutiere – Sisteme de diagnostic – Protocol cu cuvinte cheie 2000 – Partea 1: Strat fizic, prima ediție: 1999.

INT_008 Semnalul de intrare/ieșire trebuie să respecte următoarele specificații electrice:

Parametru	Minim	Normal	Maxim	Observații
U_{low} (intrare)			1,0 V	$I = 750 \mu A$
U_{high} (intrare)	4 V			$I = 200 \mu A$
Frecvența			4 kHz	
U_{low} (ieșire)			1,0 V	$I = 1 \text{ mA}$
U_{high} (ieșire)	4 V			$I = 1 \text{ mA}$

INT_009 Semnalul de intrare/ieșire trebuie să respecte următoarele diagrame de timp:



Apendicele 7

PROTOCOL DE DESCĂRCARE A DATELOR

CUPRINS

1.	Introducere	152
1.1.	Domeniu de aplicare	152
1.2.	Acronime și notații	152
2.	Descărcarea datelor din UV	153
2.1.	Procedura de descărcare	153
2.2.	Protocolul de descărcare a datelor	153
2.2.1.	Structura mesajului	153
2.2.2.	Tipuri de mesaje	154
2.2.2.1.	Solicitare de inițiere a comunicării (SID 81)	156
2.2.2.2.	Răspuns pozitiv la solicitarea de inițiere a comunicării (SID C1)	156
2.2.2.3.	Solicitare de începere a sesiunii de diagnosticare (SID 10)	156
2.2.2.4.	Răspuns pozitiv la solicitarea de începere a sesiunii de diagnosticare (SID 50)	156
2.2.2.5.	Serviciu de control al legăturii (SID 87)	156
2.2.2.6.	Răspuns pozitiv la solicitarea serviciului de control al legăturii (SID C7)	156
2.2.2.7.	Solicitare de descărcare (SID 35)	156
2.2.2.8.	Răspuns pozitiv la solicitarea de descărcare (SID 75)	156
2.2.2.9.	Solicitare de transfer de date (SID 36)	156
2.2.2.10.	Răspuns pozitiv la solicitarea de transfer de date (SID 76)	157
2.2.2.11.	Solicitare de încheiere a transferului (SID 37)	157
2.2.2.12.	Răspuns pozitiv la solicitarea de încheiere a transferului (SID 77)	157
2.2.2.13.	Solicitare de încheiere a comunicării (SID 82)	157
2.2.2.14.	Răspuns pozitiv la solicitarea de încheiere a comunicării (SID C2)	157
2.2.2.15.	Confirmare de primire a unui submesaj (SID 83)	157
2.2.2.16.	Răspuns negativ (SID 7F)	157
2.2.3.	Fluxul mesajelor	158
2.2.4.	Sincronizare	159
2.2.5.	Gestionarea erorilor	159
2.2.5.1.	Etapa de inițiere a comunicării	159
2.2.5.2.	Etapa de comunicare	159
2.2.6.	Conținutul mesajelor de răspuns	162
2.2.6.1.	Răspuns pozitiv la un recapitulativ de transfer de date	162
2.2.6.2.	Răspuns pozitiv la solicitarea de transfer de date privind activitățile	163
2.2.6.3.	Răspuns pozitiv la solicitarea de transfer de date privind evenimentele și anomaliile	164

2.2.6.4.	Răspuns pozitiv la solicitarea de transfer de date privind viteza instantanee	165
2.2.6.5.	Răspuns pozitiv la solicitarea de transfer de date privind date tehnice	165
2.3.	Stocare de fișiere în SME	166
3.	Protocol de descărcare de pe cardurile de tahograf	166
3.1.	Domeniu de aplicare	166
3.2.	Definiții	166
3.3.	Descărcarea de pe card	166
3.3.1.	Secvență de inițializare	167
3.3.2.	Secvență de descărcare de fișiere de date nesemnate	167
3.3.3.	Secvență de descărcare de fișiere de date semnate	167
3.3.4.	Secvență de reinițializare a unui contor de calibrare	168
3.4.	Format de stocare a datelor	168
3.4.1.	Introducere	168
3.4.2.	Formatul fișierului	168
4.	Descărcarea unui card de tahograf prin intermediul unei unități montate pe vehicul	169

1. INTRODUCERE

Prezentul apendice cuprinde procedurile care trebuie urmate pentru a realiza diferite tipuri de descărcare de date într-un suport de memorie extern, precum și protocoalele care trebuie puse în aplicare pentru a asigura transferul corect de date și compatibilitatea deplină a formatului de date descărcate, pentru a permite oricărui controlor să inspecteze aceste date și să poată controla autenticitatea și integritatea acestora înainte de a le analiza.

1.1. Domeniu de aplicare

Datele pot fi descărcate într-un SME:

- dintr-o unitate montată pe vehicul, cu ajutorul unui echipament inteligent dedicat (EID) conectat la UV;
- de pe un card de tahograf, cu ajutorul unui EID conectat la un periferic de interfață pentru card (PIC);
- de pe un card de tahograf, cu ajutorul unei unități montate pe vehicul și prin intermediul unui EID conectat la UV.

Pentru a da posibilitatea de verificare a autenticității și integrității datelor descărcate stocate într-un SME, datele descărcate sunt însoțite de o semnătură în conformitate cu apendicele 11 la Mecanismele de securitate comune. Se descarcă, de asemenea, identificarea echipamentului sursă (UV sau cardul) și certificatele sale de securitate (stat membru și echipament). Cel care verifică datele trebuie să dețină o cheie publică europeană securizată.

DDP_001 Datele descărcate în cadrul unei sesiuni de descărcare trebuie să fie stocate în SME în același fișier.

1.2. Acronime și notații

În prezentul apendice sunt folosite următoarele acronime:

IDA	identificatorul aplicației
RLR	răspuns la resetare
TC	octet total de control
FD	fișier dedicat
SD_	sesiune de diagnosticare
FE	fișier elementar
SME	suport de memorie extern
IDF	identificatorul fișierului (ID fișier)
FMT	octet de format (primul octet al antetului mesajului)
CCI	card cu circuite integrate
EID	echipament inteligent dedicat: echipamentul folosit la efectuarea descărcării datelor în SME (de exemplu un calculator personal)
PIF	periferic de interfață
PCC	protocol cu cuvinte cheie 2000
LEN	octet de lungime (ultimul octet al antetului mesajului)
SPP	selecția parametrilor de protocol
PSO	efectuarea unei operațiuni de securitate
IDS	identificator al serviciului
SRC	octet sursă
TGT	octet țintă
VLM	valoarea unei lungimi de marcaj
PRT	parametru de răspuns la transfer
PST	parametru de solicitare de transfer
UV	unitate montată pe vehicul.

2. DESCĂRCAREA DATELOR DIN UV

2.1. Procedura de descărcare

Pentru a efectua o descărcare de date de pe UV, operatorul trebuie să realizeze următoarele operațiuni:

- să insereze cardul său de tahograf în lectorul de card al UV ⁽¹⁾;
- să conecteze EID la conectorul de descărcare al UV;
- să stabilească o conexiune între EID și UV;
- să selecteze în EID datele care trebuie descărcate și să trimită solicitarea la UV;
- să încheie sesiunea de descărcare.

2.2. Protocolul de descărcare a datelor

Protocolul este structurat pe baza unei relații stăpân-sclav, unde EID are rolul de stăpân și UV are rolul de sclav.

Structura, tipurile și fluxul mesajului se bazează în principal pe Protocolul cu cuvinte cheie 2000 (PCC) (ISO 14230-2 Vehicule rutiere – Sisteme de diagnosticare – Protocol cu cuvinte cheie 2000 – Partea 2: Stratul de legătură între date).

Stratul de aplicație se bazează în principal pe proiectul actual de normă ISO 14229-1 (Vehicule rutiere – Sisteme de diagnosticare – Partea 1: Servicii de diagnosticare, versiunea 6 din 22 februarie 2001).

2.2.1. Structura mesajului

DDP_002 Toate mesaje schimbate între EID și UV sunt caracterizate de un format alcătuit din trei părți:

- un antet compus dintr-un octet de format (FMT), un octet țintă (TGT), un octet sursă (SRC) și, eventual, un octet de lungime (LEN);
- un câmp de date compus dintr-un octet de identificare a serviciului (IDS) și un număr variabil de octeți de date care pot cuprinde un octet opțional de sesiune de diagnosticare (SD_) sau un octet opțional de parametru de transfer (PRT sau PST);
- o sumă de control compusă dintr-un octet total de control (TC).

Antet				Câmp de date					Sumă de control
FMT	TGT	SRC	LEN	IDS	DATA	...	...	...	TC
4 octeți				Maximum 255 octeți					1 octet

Octetul TGT și SRC reprezintă adresa fizică a destinatarului și a expeditorului mesajului. Valorile sunt F0 Hex pentru EID și EE Hex pentru UV.

Octetul LEN reprezintă lungimea câmpului de date.

Octetul total de control corespunde unei serii de sume de câte 8 biți modulo 256 care reprezintă toți octeții din mesaj cu excepția TC.

Octeții FMT, IDS, SD_, PRT și PST sunt definiți în continuare în prezentul document.

⁽¹⁾ Cardul inserat declanșează activarea drepturilor de acces corespunzătoare funcției de descărcare și datelor.

DDP_003 Dacă datele pe care mesajul urmează să le transporte sunt mai lungi decât spațiul disponibil în câmpul de date, mesajul este transmis practic sub forma mai multor submesaje. Fiecare submesaj are un antet, același IDS, PRT și un contor de submesaje de 2 octeți care indică numărul de ordine al submesajului în cadrul mesajului. Pentru a permite verificarea erorilor și un eventual abandon al schimbului de date, EID confirmă primirea fiecărui submesaj. EID poate accepta submesajul, poate solicita retransmiterea acestuia și poate solicita UV să reia sau să abandoneze transmisia.

DDP_004 Dacă ultimul submesaj conține exact 255 octeți în câmpul de date, trebuie să se adauge un câmp de date necompletat (cu excepția PRT, IDS și a contorului de submesaje) pentru a indica sfârșitul mesajului.

Exemplu:

Antet	IDS	PRT	Mesaj	TC
4 octeți	Mai mare de 255 octeți			

Se transmite astfel:

Antet	IDS	PRT	00	01	Submesaj 1	TC
4 octeți	255 octeți					

Antet	IDS	PRT	00	01	Submesaj 2	TC
4 octeți	255 octeți					

...

Antet	IDS	PRT	xx	yy	Submesaj n	TC
4 octeți	Mai puțin de 255 octeți					

sau astfel:

Antet	IDS	PRT	00	01	Submesaj 1	TC
4 octeți	255 octeți					

Antet	IDS	PRT	00	02	Submesaj 2	TC
4 octeți	255 octeți					

...

Antet	IDS	PRT	xx	yy	Submesaj n	TC
4 octeți	255 octeți					

Antet	IDS	PRT	xx	yy + 1	TC
4 octeți	4 octeți				

2.2.2. Tipuri de mesaje

Protocolul de comunicare pentru descărcarea de date între UV și EID impune schimbul a opt tipuri diferite de mesaje.

Aceste mesaje sunt prezentate în tabelul următor.

Structura mesajului		Antet de maximum 4 octeți				Date cu o lungime maximă de 255 octeți			Total de control de 1 octet
EID ->	<- UV	FMT	TGT	SRC	LEN	IDS	DS_/PST	DATA	TC
Solicitare de inițiere a comunicării		81	EE	F0		81			E0
Răspuns pozitiv la solicitarea de inițiere a comunicării		80	F0	EE	03	C1		8F, EA	9B
Solicitare de începere a sesiunii de diagnosticare		80	EE	F0	02	10	81		F1
Răspuns pozitiv la solicitarea de începere a sesiunii de diagnosticare		80	F0	EE	02	50	81		31
Legătura cu serviciul de control									
Verificarea ratei binare (etapa 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
Răspuns pozitiv la o solicitare de verificare a ratei binare		80	F0	EE	02	C7		01	28
Rata binară de tranziție (etapa 2)		80	EE	F0	03	87		02, 03	ED
Solicitare de descărcare								00,00, 00,00, 00,FF,FF, FF, FF	
		80	EE	F0	0A	35			99
Răspuns pozitiv la solicitarea de descărcare		80	F0	EE	03	75		00, FF	D5
Solicitare de transfer de date									
Rezumat		80	EE	F0	02	36	01		97
Activități		80	EE	F0	06	36	02	Data	TC
Evenimente și anomalii		80	EE	F0	02	36	03		99
Viteză detaliată		80	EE	F0	02	36	04		9A
Date tehnice		80	EE	F0	02	36	05		9B
Descărcare de pe card		80	EE	F0	02	36	06		9C
Răspuns pozitiv la solicitarea de transfer de date		80	F0	EE	Len	76	PRT	Data	TC
Solicitare de încheiere a transferului		80	EE	F0	01	37			96
Răspuns pozitiv la solicitarea de încheiere a transferului		80	F0	EE	01	77			D6
Solicitare de încheiere a comunicării		80	EE	F0	01	82			E1
Răspuns pozitiv la solicitarea de încheiere a comunicării		80	F0	EE	01	C2			21
Confirmare de primire a submesajului		80	EE	F0	Len	83		Data	TC
Răspunsuri negative									
Respingere generală		80	F0	EE	03	7F	Sid Req	10	TC
Serviciu incompatibil		80	F0	EE	03	7F	Sid Req	11	TC
Subfuncție incompatibilă		80	F0	EE	03	7F	Sid Req	12	TC
Lungime incorectă a mesajului		80	F0	EE	03	7F	Sid Req	13	TC
Condiții incorecte sau eroare a secvenței de interogare		80	F0	EE	03	7F	Sid Req	22	TC
Solicitare excesivă		80	F0	EE	03	7F	Sid Req	31	TC
Descărcare refuzată		80	F0	EE	03	7F	Sid Req	50	TC
Răspuns în așteptare		80	F0	EE	03	7F	Sid Req	78	TC
Datele nu sunt disponibile		80	F0	EE	03	7F	Sid Req	FA	TC

Note:

- Sid Req = Sid corespunzător solicitării.
- PRT = PST corespunzător solicitării.
- Rubricile marcate cu negru indică absența unei transmisii.
- Termenul «upload» (descărcare de la EID) – descărcare de pe satelit pe sistemul central – se folosește pentru a garanta compatibilitatea sistemului cu ISO 14229. Are aceeași semnificație ca și termenul «download» (descărcare de la UV) – descărcare din sistemul central pe satelit.
- În acest tabel nu se găsește nici un potențial contor de submesaje de 2 octeți.

2.2.2.1. Solicitare de inițiere a comunicării (SID 81)

DDP_005 Acest mesaj este emis de EID în vederea inițierii legăturii de comunicare cu UV. Comunicările inițiale sunt efectuate întotdeauna la rata binară 9 600 (până la eventuala schimbare a ratei binare cu ajutorul serviciilor adecvate de control al legăturilor).

2.2.2.2. Răspuns pozitiv la solicitarea de inițiere a comunicării (SID C1)

DDP_006 Acest mesaj este emis de UV ca răspuns pozitiv la solicitarea de inițiere a comunicării. Este compus din cei doi octeți cheie '8F' și 'EA' care indică faptul că unitatea este compatibilă cu protocolul în cauză și are un antet care include octeți sursă, țintă și de lungime.

2.2.2.3. Solicitare de începere a sesiunii de diagnosticare (SID 10)

DDP_007 EID emite un mesaj de solicitare de inițiere a sesiunii de diagnosticare pentru a solicita de la UV o nouă sesiune de diagnosticare. Subfuncția «sesiune implicită» (81 Hex) indică faptul că urmează să înceapă o sesiune de diagnosticare.

2.2.2.4. Răspuns pozitiv la solicitarea de începere a sesiunii de diagnosticare (SID 50)

DDP_008 Mesajul privind răspunsul pozitiv la solicitarea de începere a sesiunii de diagnosticare este trimis de UV ca răspuns pozitiv la solicitarea de începere a sesiunii de diagnosticare.

2.2.2.5. Serviciul de control al legăturii (SID 87)

DDP_052 Serviciul de control al legăturii este folosit de EID pentru a iniția o schimbare a ratei binare. Acest lucru se realizează în două etape. În prima etapă, EID propune schimbarea ratei binare, indicând rata nouă. La primirea mesajului cu răspuns pozitiv de la UV, EID trimite confirmarea privind modificarea ratei binare la UV (etapa a doua). În continuare, EID trece la noua rată binară. După primirea confirmării, UV trece la noua rată binară.

2.2.2.6. Răspuns pozitiv la solicitarea serviciului de control al legăturii (SID C7)

DDP_053 Răspunsul pozitiv la solicitarea serviciului de control al legăturii este emis de UV ca răspuns pozitiv la solicitarea serviciului de control al legăturii (prima etapă). Se poate observa că solicitarea de confirmare nu primește nici un răspuns (etapa a doua).

2.2.2.7. Solicitare de descărcare (SID 35)

DDP_009 Mesajul privind solicitarea de descărcare este emis de EID pentru a indica UV faptul că s-a solicitat o operațiune de descărcare. Pentru a respecta cerințele normei ISO 14229, datele incluse se referă la adresă, detalii privind dimensiunea și formatul datelor solicitate. Deoarece EID nu cunoaște aceste date înainte de descărcare, adresa memoriei este setată la 0, formatul este decriptat și decompimat și dimensiunea memoriei este setată la valoarea maximă.

2.2.2.8. Răspuns pozitiv la solicitarea de descărcare (SID 75)

DDP_010 Mesajul privind răspunsul pozitiv la solicitarea de descărcare este trimis de UV pentru a indica EID faptul că UV este pregătită pentru descărcarea datelor. Pentru a respecta cerințele normei ISO 14229, în acest mesaj privind răspunsul pozitiv sunt incluse date care indică EID că următoarele mesaje de răspuns pozitiv la solicitarea unui transfer de date vor fi compuse din cel mult 00FF hex octeți.

2.2.2.9. Solicitare de transfer de date (SID 36)

DDP_011 Solicitarea de transfer de date este trimisă de EID pentru a indica UV tipul de date care urmează să fie descărcate. Un parametru de solicitare de transfer (PST) de un octet indică tipul transferului.

Există șase tipuri de transfer de date:

- recapitulativ (PST 01);
- activitățile asociate unei anumite date (PST 02);
- evenimente și anomalii (PST 03);
- viteză instantanee (PST 04);
- date tehnice (PST 05);
- descărcare de pe card (PST 06).

DDP_054 Este obligatoriu pentru EID să solicite un transfer de date recapitulativ (PST 01) în timpul unei sesiuni de descărcare, deoarece este singurul lucru care garantează înregistrarea certificatelor UV în fișierul descărcat (și permite verificarea semnăturii digitale).

În al doilea caz (PST 02) mesajul de solicitare a transferului de date include indicația zilei calendaristice (format **TimeReal** care urmează să fie descărcată).

2.2.2.10. Răspuns pozitiv la solicitarea de transfer de date (SID 76)

DDP_012 Răspunsul pozitiv la solicitarea transferului de date este trimis de UV ca răspuns la solicitarea de transfer de date. Mesajul conține datele solicitate, cu un parametru de răspuns la solicitare de transfer (PRT) corespunzător PST al solicitării.

DDP_055 În primul caz (PST 01), UV trimite datele care să poată ajuta operatorul EID în alegerea datelor pe care dorește să le descarce în continuare. Informațiile incluse în acest mesaj sunt reprezentate de:

- certificate de securitate;
- identificarea vehiculului;
- data și ora actuale pentru UV;
- data de descărcare minimă și maximă (date UV);
- indicații privind prezența cardurilor în UV;
- descărcări precedente către o societate;
- blocări executate de societăți;
- controale anterioare.

2.2.2.11. Solicitare de încheiere a transferului (SID 37)

DDP_013 Mesajul de solicitare de încheiere a transferului este trimis de EID pentru a informa UV cu privire la faptul că sesiunea de descărcare s-a încheiat.

2.2.2.12. Răspuns pozitiv la solicitarea de încheiere a transferului (SID 77)

DDP_014 Mesajul de răspuns pozitiv la solicitarea de încheiere a transferului este trimis de UV pentru a confirma primirea solicitării de încheiere a transferului.

2.2.2.13. Solicitare de încheiere a comunicării (SID 82)

DDP_015 Mesajul de solicitare de încheiere a comunicării este trimis de EID cu scopul de a întrerupe legătura de comunicare cu UV.

2.2.2.14. Răspuns pozitiv la solicitarea de încheiere a comunicării (SID C2)

DDP_016 Mesajul de răspuns pozitiv la solicitarea de încheiere a comunicării este trimis de UV pentru a confirma primirea unei solicitări de încheiere a comunicării.

2.2.2.15. Confirmare de primire a unui submesaj (SID 83)

DDP_017 Confirmarea de primire a unui submesaj este trimisă de EID pentru a confirma primirea fiecărei părți a unui mesaj care este transmis sub formă de mai multe submesaje. Câmpul de date conține SID primit de la UV și un cod de 2 octeți după cum urmează:

- MsgC + 1 Confirmă primirea corectă a submesajului cu numărul MsgC.
Solicitare din partea EID către UV pentru a trimite submesajul următor;
- MsgC indică apariția unei probleme la primirea submesajului cu numărul MsgC.
Solicitare din partea EID către UV pentru a trimite din nou submesajul;
- FFFF solicită întreruperea mesajului aflat în curs de transmitere.

EID poate folosi acest cod pentru a întrerupe transmiterea mesajului UV, indiferent de motiv.

Primirea ultimului submesaj al unui mesaj (octetul LEN < 255) poate fi confirmată cu ajutorul unuia dintre aceste coduri sau poate să nu fie confirmată.

Răspunsurile din partea UV compuse din câteva submesaje sunt:

- răspuns pozitiv la o solicitare de transfer de date (SID 76)

2.2.2.16. Răspuns negativ (SID 7F)

DDP_018 Mesajul de răspuns negativ este trimis de UV ca răspuns la mesajele de solicitare menționate anterior în cazul în care UV nu poate da un răspuns solicitării. Câmpurile de date ale mesajului conțin SID al răspunsului (7F), SID al solicitării și un cod care precizează motivul răspunsului negativ. Se aplică următoarele coduri:

- 10 respingere generală
Acțiunea nu poate fi realizată dintr-un motiv care nu este menționat în continuare
- 11 serviciu incompatibil
SID al solicitării nu poate fi înțeles
- 12 subfuncție incompatibilă
SD_ sau PST al solicitării nu poate fi înțeles sau nu mai există alte submesaje de transmis
- 13 lungime incorectă a mesajului
Lungimea mesajului primit nu este cea corectă
- 22 condiții incorecte sau eroare a secvenței de interogare
Serviciul solicitat nu este disponibil sau secvența mesajelor de solicitare nu este corectă
- 31 solicitare în afara domeniului
Câmpul de date al parametrului solicitării nu este valid
- 50 descărcare refuzată
Solicitarea nu poate fi executată (UV nu se află în modul de funcționare corespunzător sau există o anomalie internă a UV)
- 78 răspuns în așteptare
Acțiunea solicitată nu poate fi finalizată în timp util și UV nu este pregătită să accepte o nouă solicitare
- datele FA nu sunt disponibile
Obiectul unei solicitări de transfer de date nu este disponibil în UV (de exemplu cardul nu este inserat, ...)

2.2.3. Fluxul mesajelor

Pe parcursul unei proceduri normale de descărcare de date, un flux de mesaje tipic se efectuează de obicei astfel:

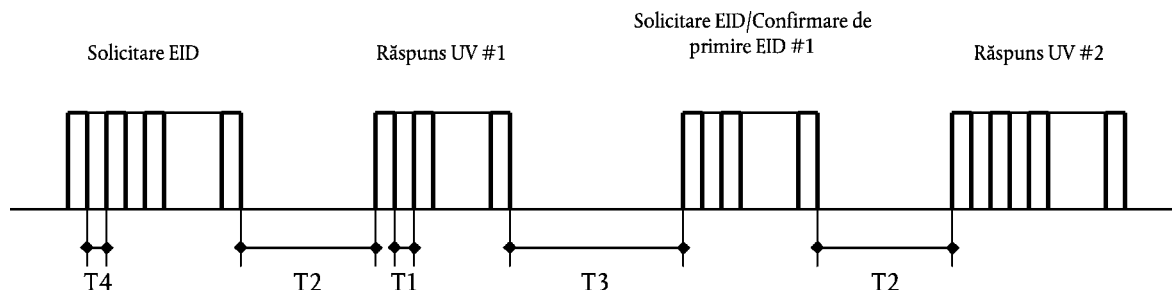
EID		UV
Solicitare de inițiere a comunicării	⇒ ⇐	Răspuns pozitiv
Solicitare de începere a serviciului de diagnosticare	⇒ ⇐	Răspuns pozitiv
Solicitare de descărcare	⇒ ⇐	Răspuns pozitiv
Solicitare de transfer de date recapitulativ	⇒ ⇐	Răspuns pozitiv
Solicitare de date #2	⇒ ⇐	Răspuns pozitiv #1
Confirmare de primire a submesajului #1	⇒ ⇐	Răspuns pozitiv #2
Confirmare de primire a submesajului #2	⇒ ⇐	Răspuns pozitiv #m
Confirmare de primire a submesajului #m	⇒ ⇐	Răspuns pozitiv (câmp de date < 255 octeți)
Confirmare de primire a submesajului (opțional)	⇒	
...		
Solicitare de transfer de date #n	⇒ ⇐	Răspuns pozitiv
Solicitare de încheiere a transferului	⇒ ⇐	Răspuns pozitiv
Solicitare de încheiere a comunicării	⇒ ⇐	Răspuns pozitiv

2.2.4. Sincronizare

DDP_019 În condiții de funcționare normale, se aplică parametrii de sincronizare indicați în figura următoare:

Figura 1

Fluxul mesajelor, sincronizare



Unde:

T1 = Timp interoctet pentru răspunsul UV.

T2 = Timp între încheierea solicitării EID și începerea răspunsului UV sau între încheierea confirmării de primire a EID și începerea următorului răspuns al UV.

T3 = Timp între încheierea răspunsului UV și începerea noii solicitări a EID sau între încheierea răspunsului UV și începerea confirmării de primire a EID sau între încheierea solicitării EID și începerea noii solicitări a EID, dacă UV nu reușește să răspundă.

T4 = Timp interoctet pentru solicitarea EID.

T5 = Valoarea extinsă a T3 pentru descărcare de pe card.

Valorile permise pentru parametrii de sincronizare sunt indicate în tabelul următor (setul de parametri de sincronizare ai PCC folosiți în caz de adresare fizică pentru o comunicare mai rapidă).

Parametru de sincronizare	Limita inferioară (ms)	Limita superioară (ms)
T1	0	20
T2	20	1 000 (*)
T3	10	5 000
T4	5	20
T5	10	20 de minute

(*) Dacă UV răspunde cu un răspuns negativ care conține codul cu semnificația «solicitare primită corect, răspuns în așteptare», această valoare este extinsă la limita superioară egală cu cea pentru T3.

2.2.5. Gestionarea erorilor

Dacă o eroare intervine în timpul schimbului de mesaje, planul de transmitere a mesajelor se modifică în funcție de echipamentul care a detectat eroarea și de mesajul care a generat eroarea.

În figura 2 și în figura 3 sunt prezentate procedurile de gestionare a erorilor folosite de UV și EID.

2.2.5.1. Etapa de inițiere a comunicării

DDP_020 Dacă EID detectează o eroare în timpul etapei de inițiere a comunicării, fie la nivelul sincronizării, fie la nivelul lanțului de biți, așteaptă o perioadă de T3 min înainte de a emite din nou solicitarea.

DDP_021 Dacă UV detectează o eroare în secvența primită de la EID, nu trimite nici un răspuns și așteaptă un alt mesaj de solicitare de inițiere a comunicării timp de T3 max.

2.2.5.2. Etapa de comunicare

Pot fi definite două proceduri diferite de gestionare a erorilor:

1. UV detectează o eroare de transmisie a EID

DDP_022 UV analizează fiecare mesaj primit pentru a detecta erori de sincronizare, erori de format al octeților (de exemplu încălcări ce afectează biții de pornire și oprire) și erorile de cadru (primirea unui număr greșit de octeți, octet total de control eronat).

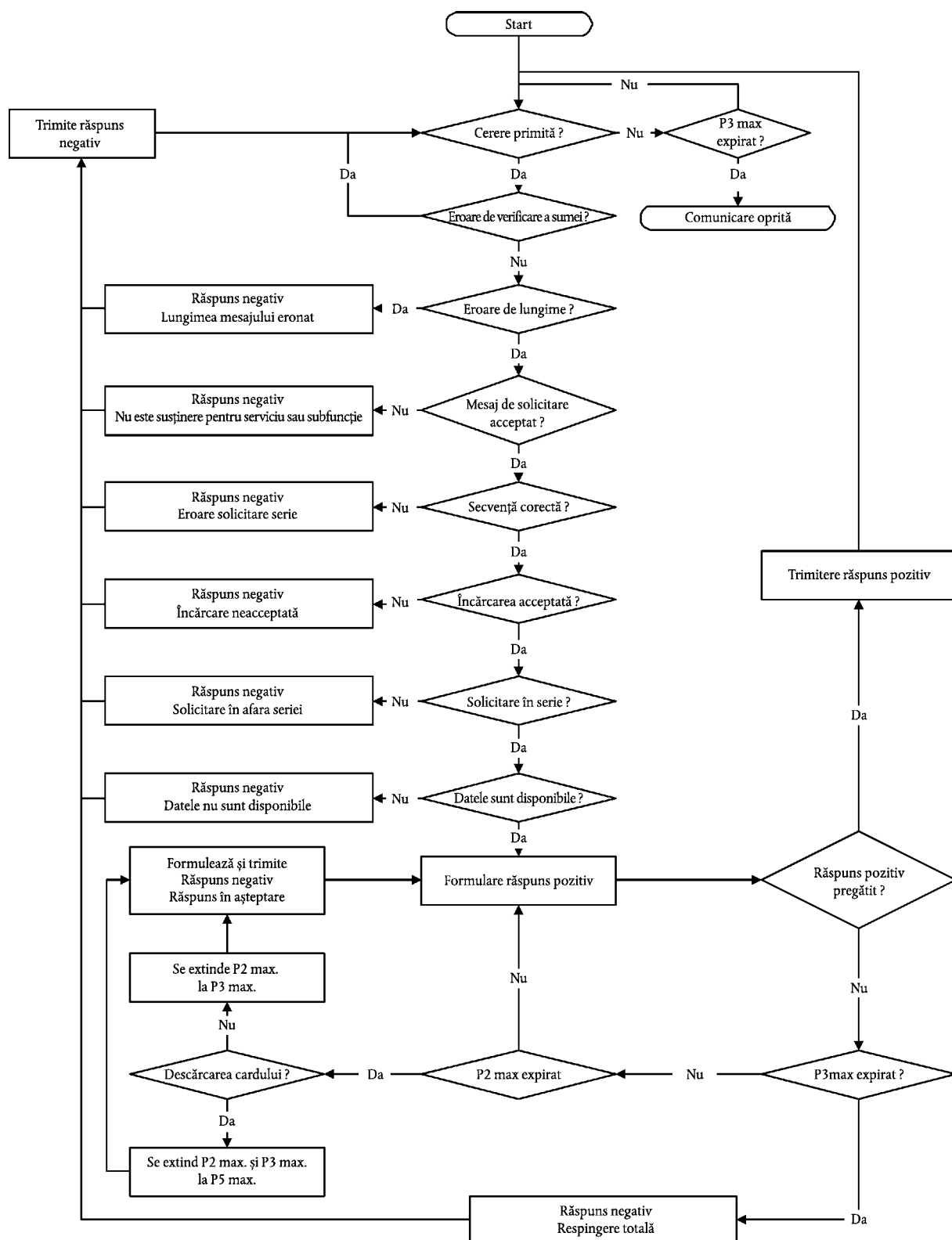
DDP_023 Dacă UV detectează una dintre erorile menționate anterior, nu trimite nici un răspuns și ignoră mesajul primit.

DDP_024

UV poate detecta alte erori ale formatului sau conținutului mesajului primit (de exemplu mesaj incompatibil) chiar dacă mesajul respectă cerințele de lungime și de total de control; în acest caz, UV îi răspunde unității EID cu un mesaj de răspuns negativ, indicând tipul erorii.

Figura 2

Gestionarea erorilor de către UV

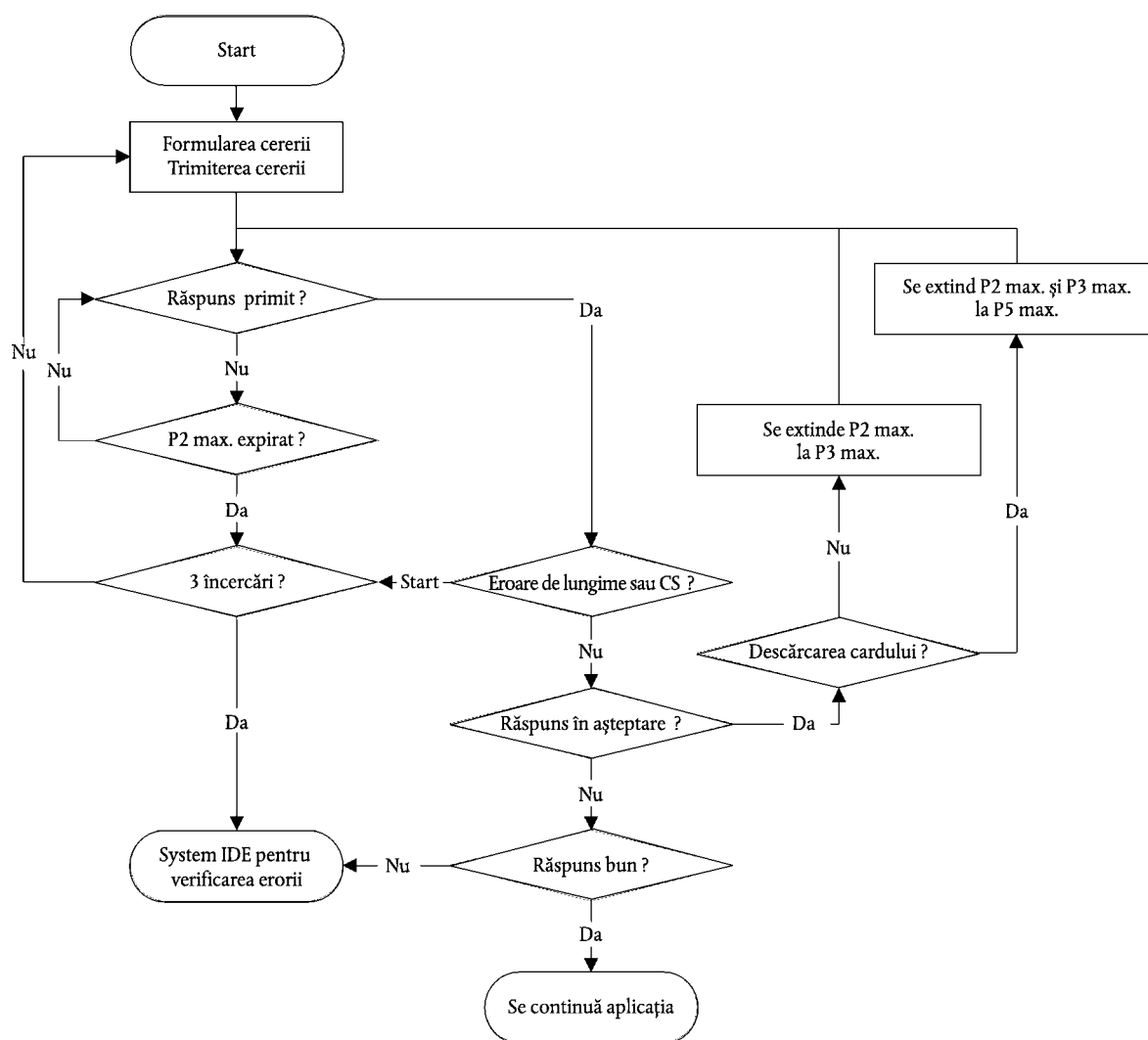


2. EID detectează o eroare de transmisie la UV

- DDP_025 EID analizează fiecare mesaj primit pentru a detecta erori de sincronizare, erori de format al octeților (de exemplu violări ce afectează biții de pornire și oprire) și erorile de cadru (primirea unui număr greșit de octeți, octet total de control eronat).
- DDP_026 EID detectează erorile de secvență, de exemplu incrementări greșite ale contorului de submesaje în mesaje succesive primite.
- DDP_027 Dacă EID detectează o eroare sau dacă nu primește nici un răspuns de la UV într-o perioadă T2 max, mesajul solicitării este trimis din nou destinatarului de cel mult trei ori. În scopul detectării acestei erori, o confirmare de primire a submesajului este considerată a fi o solicitare adresată UV.
- DDP_028 EID așteaptă o perioadă de T3 min înainte de începerea fiecărei transmisii; perioada de așteptare se măsoară de la ultima apariție calculată a unui bit de oprire după detectarea erorii în cauză.

Figura 3

Gestionarea erorilor de către EID



2.2.6. Conținutul mesajelor de răspuns

În acest paragraf este prezentat conținutul câmpurilor de date care cuprind diferite mesaje de răspuns pozitiv.

Elementele de date sunt definite în apendicele 1 – dicționar de date.

2.2.6.1. Răspuns pozitiv la un recapitulativ de transfer de date

DDP_029 Câmpul de date ale mesajului «răspuns pozitiv la recapitulativ de transfer de date» furnizează următoarele date în următoarea ordine în conformitate cu SID 76 Hex, PST 01 Hex și criteriile adecvate de separare și numărare a submesajelor.

Elemente de date	Lungime (octeți)	Comentariu
MemberStateCertificate	194	Certificate de securitate UV
VUCertificate	194	
VehicleIdentificationNumber	17	Identificarea vehiculului
VehicleRegistrationIdentification	1	
vehicleRegistrationNation vehicleRegistrationNumber	14	
CurrentDateTime	4	Ora și data curentă UV
VuDownloadablePeriod	4	Perioada de descărcare
minDownloadableTime maxDownloadableTime	4	
CardSlotsStatus	1	Tipul cardului inserat în UV
VuDownloadActivityData	4	Descărcarea anterioară de pe UV
downloadingTime	18	
fullCardNumber companyOrWorkshopName	36	
VuCompanyLocksData	1	Toate blocările efectuate de societate sunt stocate. Dacă secțiunea este necompletată, se trimite numai noOfLocks = 0
noOfLocks	(98)	
...		
Vu Company Locks Record	4	
lockInTime	4	
lockOutTime	36	
companyName companyAddress companyCardNumber	36	
...	18	
VuControlActivityData	1	Toate înregistrările de control sunt stocate în UV.
noOfControls	(31)	
...		
Vu Control Activity Record	1	
controlType	4	
controlTime	18	
controlCardNumber	4	
downloadPeriodBeginTime downloadPeriodEndTime	4	
...		Semnătura RSA a tuturor datelor (cu excepția certificatelor) de la numărul de identificare al vehiculului până la ultimul octet al ultimei înregistrări de activitate de control al UV.
Signature	128	

2.2.6.2. Răspuns pozitiv la solicitarea de transfer de date privind activitățile

DDP_030 Câmpul de date al mesajului «răspuns pozitiv la solicitarea de transfer de date privind activitățile» furnizează următoarele date în următoarea ordine în conformitate cu SID 76 Hex, PRT 02 Hex și criteriile adecvate de separare și numărare a submesajelor.

Elemente de date		Lungime (octeți)	Comentariu
TimeReal		4	Data zilei descărcate
OdometerValueMidnight		3	Contor kilometraj la sfârșitul zilei descărcate
VuCardIWData			
noOfVuCardIWRecords		2	Date privind ciclurile de introducere/ retragere a cardului
...		(129)	— Dacă această secțiune nu conține date disponibile, se trimite numai noOfVuCardIWRecords = 0 — Dacă un VuCardIWRecord acoperă o perioadă înainte de ora 00:00 (introducerea cardului în ziua anterioară) sau după ora 24:00 (retragerea cardului în ziua următoare), acesta apare integral pentru ambele zile în cauză.
VuCardIWRecord	cardHolderName	36	
	holderSurname	36	
	holderFirstNames	36	
	fullCardNumber	18	
	cardExpiryDate	4	
	cardInsertionTime	4	
	vehicleOdometerValueAtInsertion	3	
	cardSlotNumber	1	
	cardWithdrawalTime	4	
	vehicleOdometerValueAtWithdrawal	3	
	previousVehicleInfo		
	vehicleRegistrationIdentification	1	
	vehicleRegistrationNation	14	
	vehicleRegistrationNumber	4	
	cardWithdrawalTime	4	
	manualInputFlag	1	
...			
VuActivityDailyData			
noOfActivityChanges		2	Starea lectoarelor pentru carduri la ora 00:00 și modificările de activitate înregistrate în ziua descărcată.
...			
ActivityChangeInfo		2	
...			
VuPlaceDailyWorkPeriodData			
noOfPlaceRecords		1	Date privind locurile înregistrate în ziua descărcată. Dacă secțiunea este necompletată se trimite noOfPlaceRecords = 0.
...		(28)	
VuPlaceDailyWorkPeriodRecord	fullCardNumber	18	
	placeRecord		
	entryTime	4	
	entryTypeDailyWorkPeriod	1	
	dailyWorkPeriodCountry	1	
	dailyWorkPeriodRegion	1	
	vehicleOdometerValue	3	
...			
VuSpecificConditionData			
noOfSpecificConditionRecords		2	Date privind condițiile specifice înregistrate pentru ziua descărcată. Dacă secțiunea este necompletată, se trimite numai noOfSpecific-ConditionRecords = 0.
...		(5)	
SpecificConditionRecord			
EntryTime		4	
specificConditionType		1	
...			
Signature		128	Semnătură RSA a tuturor datelor, de la Timp real până la ultimul octet din ultima înregistrare privind condițiile specifice.

2.2.6.3. Răspuns pozitiv la solicitarea de transfer de date privind evenimentele și anomaliile

DDP_031 Câmpul de date al mesajului «răspuns pozitiv la solicitarea de transfer de date privind evenimentele și anomaliile» furnizează următoarele date în următoarea ordine în conformitate cu SID 76 Hex, PRT 03 Hex și criteriile adecvate de separare și numărare a submesajelor.

Elemente de date		Lungime (octeți)	Comentariu
VuFaultData			
NoOfVuFaults		1	Toate anomaliile stocate sau în desfășurare în UV. Dacă secțiunea este necompletată, se trimite numai noOfVuFaults = 0.
...		(82)	
VuFaultRecord	FaultType	1	
	FaultRecordPurpose	1	
	FaultBeginTime	4	
	FaultEndTime	4	
	CardNumberDriverSlotBegin	18	
	cardNumberCodriverSlotBegin	18	
	CardNumberDriverSlotEnd	18	
CardNumberCodriverSlotEnd	18		
...			
VuEventData			
NoOfVuEvents		1	Toate evenimentele (cu excepția depășirii vitezei autorizate) stocate sau în desfășurare în UV. Dacă secțiunea este necompletată, se trimite numai noOfVu Events = 0.
...		(83)	
VuEventRecord	EventType	1	
	EventRecordPurpose	1	
	EventBeginTime	4	
	EventEndTime	4	
	CardNumberDriverSlotBegin	18	
	cardNumberCodriverSlotBegin	18	
	CardNumberDriverSlotEnd	18	
	CardNumberCodriverSlotEnd	18	
	SimilarEventsNumber	1	
...			
VuOverSpeedingControlData			
LastOverspeedControlTime		4	Date referitoare la ultimul control privind depășirea vitezei autorizate (valoare implicită, în lipsa datelor).
FirstOverspeedSince		4	
NumberOfOverspeedSince		1	
VuOverSpeedingEventData			
NoOfVuOverSpeedingEvents		1	Toate evenimentele de depășire a vitezei autorizate stocate în UV. Dacă secțiunea este necompletată, se trimite numai noOfVuOver-SpeedingEvents = 0
...		(31)	
VuOverSpeedingEventRecord	EventType	1	
	EventRecordPurpose	1	
	EventBeginTime	4	
	EventEndTime	4	
	MaxSpeedValue	1	
	AverageSpeedValue	1	
	CardNumberDriverSlotBegin	18	
	SimilarEventsNumber	1	
...			
VuTimeAdjustmentData			
NoOfVuTimeAdjRecords		1	Toate evenimentele de reglare a orei stocate în UV (în afara cadrului de calibrare completă). Dacă secțiunea este necompletată, se trimite numai noOfVu – TimeAdjRecords = 0.
...		(98)	
VuTimeAdjustmentRecord	OldTimeValue	4	
	NewTimeValue	4	
	WorkshopName	36	
	WorkshopAddress	36	
	WorkshopCardNumber	18	
...			
Signature		128	Semnătură RSA a tuturor datelor, de la noOfVuFaults până la ultimul octet din ultima înregistrare privind reglarea orei.

2.2.6.4. Răspuns pozitiv la solicitarea de transfer de date privind viteza instantanee

DDP_032 Câmpul de date al mesajului «răspuns pozitiv la solicitarea de transfer de date privind viteza instantanee» furnizează următoarele date în următoarea ordine în conformitate cu SID 76 Hex, PRT 04 Hex și criteriile adecvate de separare și numărare a submesajelor.

Elemente de date		Lungime (octeți)	Comentariu
VuDetailedSpeedData			
NoOfSpeedBlocks		2	Toate datele referitoare la viteza instantanee stocate în UV (un bloc de viteză pe minut în timpul căruia vehiculul a fost în mișcare) 60 de valori ale vitezei instantanee pe minut (o valoare pe secundă)
VuDetailedSpeedBlock	...		
	SpeedBlockBeginDate	4	
	speedsPerSecond	60	
Signature		128	Semnătură RSA a tuturor datelor, de la numărul blocurilor de date până la ultimul octet din ultimul bloc de viteză.

2.2.6.5. Răspuns pozitiv la solicitarea de transfer de date privind date tehnice

DDP_033 Câmpul de date al mesajului «răspuns pozitiv la solicitarea de transfer de date privind datele tehnice» furnizează următoarele date în următoarea ordine în conformitate cu SID 76 Hex, PRT 05 Hex și criteriile adecvate de separare și numărare a submesajelor.

Elemente de date		Lungime (octeți)	Comentariu
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			
noOfVuCalibrationRecords		1	Toate înregistrările de calibrare stocate în UV.
...		(164)	
VuCalibrationRecord	calibrationPurpose	1	
	workshopName	36	
	workshopAddress	36	
	workshopCardNumber	18	
	workshopCardExpiryDate	4	
	vehicleIdentificationNumber	17	
	vehicleRegistrationIdentification		
	vehicleRegistrationNation	1	
	vehicleRegistrationNumber	14	
	wVehicleCharacteristicConstant	2	
	kConstantOfRecordingEquipment	2	
	lTyreCircumference	2	
	tyreSize	15	
	authorisedSpeed	1	
	oldOdometerValue	3	
	newOdometerValue	3	
	oldTimeValue	4	
	newTimeValue	4	
	nextCalibrationDate	4	
Signature		128	Semnătură RSA a tuturor datelor, de la vuManufacturerName până la ultimul octet din ultima înregistrare privind calibrarea UV.

2.3. Stocare de fișiere în SME

DDP_034 Dacă o sesiune de descărcare include un transfer de date de pe UV, EID stochează într-un singur fișier fizic toate datele primite de la UV în timpul unei sesiuni de descărcare în mesajele de răspuns pozitiv la solicitare de transfer de date. Datele stocate nu includ anteturi de mesaje, contoare de submesaje, submesaje necompletate și sume de control, dar includ SID și PRT (din primul submesaj, numai dacă există mai multe submesaje).

3. PROTOCOL DE DESCĂRCARE DE PE CARDURILE DE TAHOGRAF

3.1. Domeniu de aplicare

Acest paragraf cuprinde o descriere a descărcării datelor de pe un card de tahograf pe un EID. EID nu face parte dintr-un mediu securizat; prin urmare, nu se realizează nici o procedură de autentificare între card și EID.

3.2. Definiții

Sesiune de descărcare: De fiecare dată când sistemul efectuează o operațiune de descărcare de date de pe CCI. Sesiunea include întreaga procedură, de la resetarea CCI cu ajutorul unui PIF până la dezactivarea CCI (retragerea cardului sau următoarea resetare).

Fișier de date semnat: Un fișier din CCI. Fișierul este transferat în PIF sub formă de text. Pe CCI fișierul este distribuit și semnat, iar semnătura este transferată la PIF.

3.3. Descărcarea de pe card

DDP_035 Descărcarea de pe un card de tahograf include următoarele etape:

- descărcarea informațiilor comune stocate pe card în fișierele elementare (FE) ICC și IC. Aceste informații sunt opționale și nu sunt protejate de nici o semnătură digitală;
- descărcarea fișierelor FE Card_Certificate și CA_Certificate. Aceste informații nu sunt protejate de o semnătură digitală;

Descărcarea acestor fișiere este obligatorie în cadrul fiecărei sesiuni de descărcare.

- descărcarea celorlalte FE de date privind aplicația (în DF Tachograph cu excepția fișierului elementar Card_Download. Aceste informații sunt protejate de o semnătură digitală.

- trebuie să se descarce cel puțin FE Application_Identification și ID la fiecare sesiune de descărcare,

- La descărcarea de pe cardul șoferului, descărcarea următoarelor FE este obligatorie:

- Events_Data,
- Faults_Data,
- Driver_Activity_Data,
- Vehicles_Used,
- Places,
- Control_Activity_Data,
- Specific_Conditions.

- La descărcarea de pe un card al șoferului se impune actualizarea datei ultimei descărcări în Data ultimei descărcări în FE Card_Download;

- La descărcarea de pe un card al atelierului, se impune resetarea contorului de calibrare în FE Card_Download.

3.3.1. Secvență de inițializare

DDP_036 EID inițiază secvența după cum urmează:

Card	Direcție	EID/PIF	Semnificație/Observații
	↩	Resetare hardware	
RLR	↪		

Opțional, se poate folosi SPP pentru a trece la o rată binară mai mare dacă CCI este compatibil.

3.3.2. Secvență de descărcare de fișiere de date nesemnate

DDP_037 Secvența de descărcare ICC, IC, Card_Certificate și CA_Certificate se prezintă după cum urmează:

Card	Direcție	EID/PIF	Semnificație/Observații
	↩	Select file	Selectare cu ajutorul identificatorilor de fișier
OK	↪		
	↩	Read Binary	Dacă fișierul conține mai multe date decât capacitatea memoriei tampon a lectorului sau a cardului, comanda trebuie repetată până la citirea integrală a datelor din fișier.
Date OK	↪	Salvarea datelor în SME	conform punctului 3.4 (format de stocare a datelor)

Notă: Înainte de a selecta fișierul FE Card_Certificate, trebuie să selectați aplicația de tahograf (selecție cu IDA).

3.3.3. Secvență de descărcare de fișiere de date semnate

DDP_038 Următoarea secvență se folosește la fiecare dintre fișierele următoare care trebuie descărcate împreună cu semnătura lor:

Card	Direcție	EID/PIF	Semnificație/Observații
	↩	Select file	
OK	↪		
	↩	Perform hash of File	Calculează valoarea de distribuire în raport cu conținutul de date al fișierului selectat cu ajutorul algoritmului de distribuire indicat în conformitate cu apendicele 11. Această comandă nu este o ISO-Command.
Se calculează distribuția fișierului și se stochează temporar valoarea de distribuire			
OK	↪		
	↩	Read Binary	Dacă fișierul conține mai multe date decât capacitatea memoriei tampon a lectorului sau a cardului, comanda trebuie repetată până la citirea integrală a datelor din fișier.
Date OK	↪	Stocarea datelor primite în SME	conform punctului 3.4 (format de stocare a datelor)
	↩	PSO: Compute digital signature	
Executarea operațiunii de securitate «Calcularea semnăturii digitale» cu ajutorul valorii de distribuire stocate temporar			
Semnătură OK	↪	Adăugarea datelor la datele stocate deja în SME	conform punctului 3.4 (format de stocare a datelor)

3.3.4. Secvență de reinițializare a unui contor de calibrare

DDP_039 Secvența de resetare a contorului NoOfCalibrationsSinceDownload din FE Card_Download al unui card de atelier se prezintă după cum urmează:

Card	Direcție	EID/PIF	Semnificație/Observații
OK	↩	Select File EF Card_Download	Selectarea fișierului cu ajutorul identificatorilor de fișier
	↩		
	↩	Update Binary NoOfCalibrations- SinceDownload = '00 00'	
Resetează numărul de descărcări de pe card			
OK	⇒		

3.4. Format de stocare a datelor

3.4.1. Introducere

DDP_040 Datele descărcate trebuie stocate în conformitate cu următoarele condiții:

- stocarea datelor trebuie să fie transparentă. Acest lucru înseamnă că, pe parcursul stocării, trebuie să se mențină ordinea octeților, precum și ordinea biților din interiorul octeților care sunt transferați de pe card;
- toate fișierele de pe card descărcate în cadrul unei sesiuni de descărcare sunt stocate într-un fișier în SME.

3.4.2. Formatul fișierului

DDP_041 Formatul fișierului este o concatenare a anumitor obiecte VLM.

DDP_042 Marcajul pentru un FE este IDF însoțit de apendicele «00».

DDP_043 Marcajul pentru o semnătură a FE este IDF însoțit de apendicele «01».

DDP_044 Lungimea are o valoare de 2 octeți. Valoarea definește numărul de octeți din câmpul valorii. Valoarea «FF FF» din câmpul pentru lungime este rezervată unei utilizări ulterioare.

DDP_045 Dacă un fișier nu este descărcat, nu se stochează nici o informație privind fișierul (nici un marcaj și nici o lungime zero).

DDP_046 Semnăturile trebuie salvate sub formă de obiect VLM imediat după obiectul VLM care conține datele fișierului.

Definiție	Semnificație	Lungime
IDF (2 octeți) «00»	Marcajul pentru FE (IDF)	3 octeți
IDF (2 octeți) «01»	Marcajul pentru semnătura FE (IDF)	3 octeți
xx xx	Lungimea câmpului pentru valoare	3 octeți

Exemplu de date dintr-un fișier de descărcare în SME:

Marcaj	Lungime	Valoare
00 02 00	00 11	Date din FE ICC
C1 00 00	00 C2	Date din FE Card_Certificate
		...
05 05 00	0A 2E	Date din FE Vehicles_Used
05 05 01	00 80	Semnătura FE Vehicles_Used

4. DESCĂRCAREA UNUI CARD DE TAHOGRAPH PRIN INTERMEDIUL UNEI UNITĂȚI MONTATE PE VEHICUL

DDP_047 UV trebuie să permită descărcarea conținutului unui card al șoferului inserat într-un EID conectat.

DDP_048 EID trimite un mesaj de «solicitare de transfer de date privind descărcarea de pe card» către UV pentru a iniția acest mod (vezi 2.2.2.9).

DDP_049 În această etapă, UV trebuie să descarce integral cardul, fișier cu fișier, în conformitate cu protocolul de descărcare definit în paragraful 3, și să trimită toate datele primite de pe card către EID folosind formatul de fișier VLM adecvat (vezi 3.4.2) și încapsulate într-un mesaj de «răspuns pozitiv la solicitarea de transfer de date».

DDP_050 EID preia datele de pe card din mesajul «răspuns pozitiv la solicitarea de transfer de date» (eliminând toate anteturile, IDS, PRT, contoarele de submesaje și sumele de control) și le stochează într-un singur fișier fizic conform descrierii din paragraful 2.3.

DDP_051 În continuare, UV actualizează, dacă este cazul, fișierul `Control_Activity_Data` sau `Card_Download` de pe cardul șoferului.

Apendicele 8

PROTOCOL DE CALIBRARE

CUPRINS

1.	Introducere	172
2.	Terminologie, definiții și trimiteri	172
3.	Prezentare generală a serviciilor	172
3.1.	Servicii disponibile	172
3.2.	Coduri de răspuns	173
4.	Servicii de comunicare.....	173
4.1.	Serviciul StartCommunication	173
4.2.	Serviciul StopCommunication	175
4.2.1.	Descrierea mesajului	175
4.2.2.	Formatul mesajului	176
4.2.3.	Definirea parametrilor	177
4.3.	Serviciul TesterPresent	177
4.3.1.	Descrierea mesajului	177
4.3.2.	Formatul mesajului	177
5.	Servicii de gestionare	178
5.1.	Serviciul StartDiagnosticSession	178
5.1.1.	Descrierea mesajului	178
5.1.2.	Formatul mesajului	179
5.1.3.	Definirea parametrilor	180
5.2.	Serviciul SecurityAccess	180
5.2.1.	Descrierea mesajului	180
5.2.2.	Formatul mesajului – SecurityAccess – requestSeed	181
5.2.3.	Formatul mesajului – SecurityAccess – sendKey	182
6.	Servicii de transmisie de date	183
6.1.	Serviciul DataByIdentifier	183
6.1.1.	Descrierea mesajului	183
6.1.2.	Formatul mesajului	183
6.1.3.	Definirea parametrilor	184
6.2.	Serviciul WriteDataByIdentifier	185
6.2.1.	Descrierea mesajului	185
6.2.2.	Formatul mesajului	185
6.2.3.	Definirea parametrilor	186
7.	Controlul impulsurilor de test – unitatea funcțională de control al intrărilor/ieșirilor	186
7.1.	Serviciul InputOutputControlByIdentifier	186

7.1.1.	Descrierea mesajului	186
7.1.2.	Formatul mesajului	187
7.1.3.	Definirea parametrilor	188
8.	Formate de înregistrări de date	189
8.1.	Intervale de parametri transmiși	189
8.2.	Formate de înregistrări de date	190

1. INTRODUCERE

Prezentul apendice descrie modul în care are loc schimbul de date între o unitate montată pe vehicul și un aparat de probă prin intermediul unei linii K ce face parte dintr-o interfață de calibrare descrisă în apendicele 6. De asemenea, este inclusă descrierea controlului liniei de semnalizare de intrare/ieșire efectuat asupra conectorului de calibrare.

Inițierea comunicărilor pe linia K este descrisă în secțiunea 4 «Servicii de comunicare».

În prezentul apendice se folosește ideea de «sesiuni» de diagnosticare pentru a determina sfera de aplicare a controlului liniei K în diferite condiții. Sesiunea implicită este «StandardDiagnosticSession», în cadrul căreia pot fi extrase toate datele de pe o unitate montată pe vehicul, dar nu se pot înregistra date pe o unitate montată pe vehicul.

Selectarea sesiunii de diagnosticare este descrisă în secțiunea 5 «Servicii de gestionare».

CPR_001 Sesiunea «ECUProgrammingSession» permite introducerea datelor în unitatea montată pe vehicul. În cazul introducerii datelor de calibrare (cerințele 097 și 098), unitatea montată pe vehicul trebuie să se afle în modul de funcționare CALIBRARE.

Transferul de date prin intermediul liniei K este descris în secțiunea 6 «Servicii de transmisie a datelor». Formatele pentru datele transferate sunt descrise în detaliu în secțiunea 8 «Formate de înregistrare a datelor».

CPR_002 Sesiunea «ECUAdjustmentSession» permite selectarea modului liniei de semnalizare de intrare/ieșire de calibrare prin intermediul interfeței liniei K. Controlul liniei de semnal de intrare/ieșire de calibrare este descris în secțiunea 7 «Controlul impulsurilor de test – unitatea funcțională de control al intrărilor/ieșirilor».

CPR_003 În cadrul prezentului document adresa aparatului de probă este notată cu «tt». Cu toate că este posibil să existe adrese privilegiate pentru aparatele de probă, UV răspunde corect la orice adresă a aparatului de probă. Adresa fizică a UV este 0xEE.

2. TERMINOLOGIE, DEFINIȚII ȘI TRIMITERI

Protocoalele, mesajele și codurile de eroare se bazează în principal pe proiectul actual de norme ISO 14229-1 (Vehicule rutiere – Sisteme de diagnosticare – Partea 1: Servicii de diagnosticare, versiunea 6 din 22 februarie 2001).

Codificările octeților și alte valori hexazecimale sunt folosite la definirea identificatorilor de servicii, la elaborarea solicitărilor și a răspunsurilor de servicii și la configurarea parametrilor standard.

Termenul «aparat de probă» se referă la echipamentul folosit la introducerea datelor de programare/calibrare în UV.

Termenii «client» și «server» se referă la aparatul de probă, respectiv la UV.

Termenul ECU înseamnă «Unitate de control electronică» și se referă la UV.

Trimiteri:

ISO 14230-2: Vehicule rutiere – Sisteme de diagnosticare – Protocol cu cuvinte cheie 2000 – Partea 2: Strat de legătură a datelor. Prima ediție: 1999. Vehicule – Sisteme de diagnosticare.

3. PREZENTARE GENERALĂ A SERVICIILOR

3.1. Servicii disponibile

Următorul tabel cuprinde o prezentare generală a serviciilor care sunt disponibile în aparatul de înregistrare și sunt definite în prezentul document.

CPR_004 Tabelul prezintă serviciile disponibile în cadrul unei sesiuni de diagnosticare active.

— Prima coloană cuprinde serviciile disponibile;

— a doua coloană include numărul secțiunii care prezintă o descriere detaliată a serviciului în cauză în cadrul prezentului apendice;

- a treia coloană indică valoarea atribuită identificatorului de serviciu pentru mesajele de solicitare de serviciu;
- a patra coloană precizează serviciile sesiunii «StandardDiagnosticSession» (SD) care trebuie aplicate în cadrul fiecărei UV;
- a cincea coloană precizează serviciile sesiunii «ECUAdjustmentSession» (ECUAS) care trebuie aplicate pentru a permite controlul liniei de semnalizare intrare/ieșire în conectorul de calibrare din panoul frontal al UV;
- a șasea coloană precizează serviciile sesiunii «ECUProgrammingSession» (ECUPS) care trebuie aplicate pentru a permite programarea parametrilor în UV.

Tabelul 1

Tabel de prezentare a valorilor identificatorilor de serviciu

Denumirea serviciului de diagnosticare	Nr. secțiune	Valoarea atribuită identificatorilor de serviciu	Sesiuni de diagnosticare		
			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		■	

■ Acest simbol indică faptul că serviciul în cauză este obligatoriu în respectiva sesiune de diagnosticare.
 Absența simbolului indică faptul că serviciul în cauză nu este permis în cadrul respectivei sesiuni de diagnosticare.

3.2. Coduri de răspuns

Codurile de răspuns sunt definite pentru fiecare serviciu în parte.

4. SERVICII DE COMUNICARE

Există anumite servicii care sunt necesare pentru inițierea și menținerea comunicării. Acestea nu apar în stratul de aplicație. Serviciile disponibile sunt prezentate în detaliu în tabelul următor:

Tabelul 2

Servicii de comunicare

Denumirea serviciului	Descriere
StartCommunication	Clientul solicită inițierea unei sesiuni de comunicare cu unul sau mai multe servere
StopCommunication	Clientul solicită încheierea sesiunii de comunicare în curs de desfășurare
TesterPresent	Clientul indică serverului faptul că este încă prezent

CPR_005 Serviciul StartCommunication este folosit pentru inițierea unei comunicări. Pentru a efectua un serviciu, trebuie să se inițializeze comunicarea, iar parametrii de comunicare selectați trebuie să fie adaptați modului de funcționare dorit.

4.1. Serviciul StartCommunication

CPR_006 La primirea unui primitiv de indicare StartCommunication, UV verifică dacă legătura de comunicare solicitată poate fi inițializată în condițiile existente. Condițiile necesare inițializării unei comunicări sunt descrise în documentul ISO 14230-2.

CPR_007 În continuare, UV realizează toate acțiunile necesare pentru a inițializa o legătură de comunicare și trimite un primitiv de răspuns StartCommunication împreună cu parametrii de răspuns pozitiv selectați.

CPR_008 Dacă o UV inițializată deja (și care a început o sesiune de diagnosticare) primește o nouă solicitare StartCommunication (de exemplu datorită unei remedieri a erorii la nivel de aparat de probă), solicitarea este acceptată și UV este reinițializată.

CPR_009 Dacă legătura de comunicare nu poate fi inițializată, indiferent din ce motiv, UV continuă să funcționeze în aceleași condiții care existau imediat înainte de inițializarea legăturii de comunicare.

CPR_010 Mesajul de solicitare a StartCommunication trebuie să aibă o adresă fizică.

CPR_011 Inițializarea UV pentru servicii se realizează cu ajutorul unei metode de «inițializare rapidă».

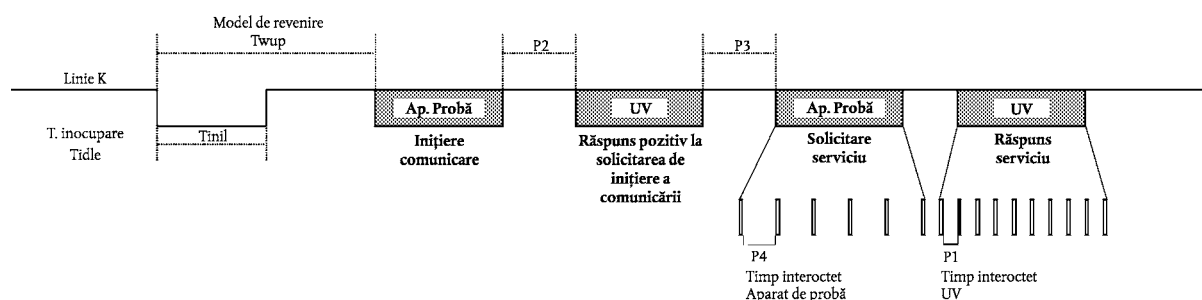
- timpul de ocupare/inocupare anterior oricărei activități;
- în continuare, aparatul de probă trimite o configurare de inițializare;
- toate informațiile necesare inițializării comunicării sunt incluse în răspunsul UV.

CPR_012 După finalizarea inițializării:

- tuturor parametrilor de comunicare le sunt atribuite valorile definite în tabelul 4 în funcție de octeții – cheie;
- UV așteaptă prima solicitare din partea aparatului de probă;
- UV se află în modul de diagnosticare implicit, adică StandardDiagnosticSession;
- linia de semnalizare a intrărilor/ieșirilor de calibrare este în starea implicită, adică inactivă.

CPR_014 Rata de transmisie a datelor pe linia K este de CPR_01 410 400 baudzi.

CPR_016 Inițializarea rapidă este lansată de aparatul de probă prin transmiterea unui model de revenire (Wup) pe linia K. Modelul începe la sfârșitul unui timp de inocupare al liniei K și este urmat de un timp de Tinil. Aparatul de probă transmite primul bit al serviciului StartCommunication după un timp Twup, după prima linie descendentă.



CPR_017 Valorile de sincronizare ale inițializării rapide și ale comunicării în general sunt descrise în detaliu în tabelele prezentate în continuare. Pentru timpul de inocupare există posibilități diferite:

- prima transmisie după alimentare, $T_{inoc} = 300 \text{ ms}$;
- după finalizarea unui serviciu StopCommunication, $T_{inoc} = P3 \text{ min}$;
- după încheierea comunicării prin depășirea timpului alocat P3 max, $T_{inoc} = 0$.

Tabelul 3

Valori de sincronizare pentru inițializarea rapidă

Parametru		valoare minimă	valoare maximă
Tinil	$25 \pm 1 \text{ ms}$	24 ms	26 ms
Twup	$50 \pm 1 \text{ ms}$	49 ms	51 ms

Tabelul 4

Valorile parametrilor de sincronizare ai comunicărilor

Parametru de sincronizare	Descrierea parametrului	Valori minime admise (ms)	Valori maxime admise (ms)
		minim	maxim
P1	Timpul interoctet pentru răspunsul UV	0	20
P2	Timpul dintre solicitarea aparatului de probă și răspunsul UV sau dintre două răspunsuri UV	25	250
P3	Timpul dintre sfârșitul răspunsurilor UV și începutul noii solicitări a aparatului de probă	55	5 000
P4	Timpul interoctet pentru solicitarea aparatului de probă	5	20

CPR_018 Formatul mesajului pentru inițializarea rapidă este prezentat în detaliu în tabelele următoare:

Tabelul 5

Mesaj de solicitare a inițierii comunicării

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
# 1	Octet de format – adresare fizică	81	FMT
# 2	Octet țintă de adresă	EE	TGT
# 3	Octet sursă de adresă	tt	SRC
# 4	Serviciu de solicitare StartCommunication	81	SCR
# 5	Sumă de control	00-FF	TC

Tabelul 6

Mesaj de răspuns pozitiv la solicitarea de inițiere a comunicării

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
# 1	Octet de format – adresare fizică	80	FMT
# 2	Octet țintă de adresă	tt	TGT
# 3	Octet sursă de adresă	EE	SRC
# 4	Octet de lungime suplimentar	03	LEN
# 5	ID al serviciului de răspuns pozitiv la o solicitare de inițiere a comunicării	C1	SCRPR
# 6	Octet – cheie 1	EA	OC1
# 7	Octet – cheie 2	8F	OC2
# 8	Sumă de control	00-FF	TC

CPR_019 Nu există nici un răspuns negativ la mesajul de solicitare de inițiere a comunicării. Dacă nu există un mesaj de răspuns pozitiv de transmis, UV nu este inițializată, nu se transmite nimic și rămâne în modul său normal de funcționare.

4.2. Serviciul StopCommunication

4.2.1. Descrierea mesajului

Scopul acestui serviciu privind stratul de comunicare este de a încheia o sesiune de comunicare.

CPR_020 La primirea unui primitiv de indicare StopCommunication, UV verifică dacă condițiile în vigoare permit încheierea comunicării în cauză. În acest caz, UV realizează toate acțiunile necesare pentru a încheia comunicarea în cauză.

CPR_021 Dacă încheierea comunicării este posibilă, UV emite un primitiv de răspuns StopCommunication împreună cu parametrii de răspuns pozitiv selectați, înainte de încheierea comunicării.

CPR_022 Dacă încheierea comunicării nu este posibilă, indiferent de motiv, UV emite un primitiv de răspuns StopCommunication împreună cu parametrii de răspuns negativ selectați.

CPR_023 Dacă UV detectează depășirea timpului alocat P3 max, comunicarea este încheiată fără a se emite un primitiv de răspuns.

4.2.2. **Formatul mesajului**

CPR_024 Formatele de mesaje pentru primitivele StopCommunication sunt prezentate în detaliu în tabelele următoare:

Tabelul 7

Mesaj de solicitare a încheierii comunicării

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
# 1	Octet de format – adresare fizică	80	FMT
# 2	Octet țintă de adresă	EE	TGT
# 3	Octet sursă de adresă	tt	SRC
# 4	Octet de lungime suplimentar	01	LEN
# 5	ID al serviciului de solicitare de încheiere a comunicării	82	SPR
# 6	Sumă de control	00-FF	TC

Tabelul 8

Mesaj de răspuns pozitiv la solicitarea de încheiere a comunicării

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
# 1	Octet de format – adresare fizică	80	FMT
# 2	Octet țintă de adresă	tt	TGT
# 3	Octet sursă de adresă	EE	SRC
# 4	Octet de lungime suplimentar	01	LEN
# 5	ID al serviciului de răspuns pozitiv la solicitarea de încheiere a comunicării	C2	SPRPR
# 6	Sumă de control	00-FF	TC

Tabelul 9

Mesaj de răspuns negativ la solicitarea de încheiere a comunicării

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
# 1	Octet de format – adresare fizică	80	FMT
# 2	Octet țintă de adresă	tt	TGT
# 3	Octet sursă de adresă	EE	SRC
# 4	Octet de lungime suplimentar	03	LEN
# 5	ID al serviciului de răspuns negativ	7F	RN
# 6	ID al serviciului de solicitare de încheiere a comunicării	82	SPR
# 7	Cod de răspuns = generalReject	10	CR_RG
# 8	Sumă de control	00-FF	TC

4.2.3. Definirea parametrilor

Acest serviciu nu necesită definirea nici unui parametru.

4.3. Serviciul TesterPresent

4.3.1. Descrierea mesajului

Serviciul TesterPresent este folosit de aparatul de probă pentru a indica serverului că este încă prezent, astfel încât să nu permită serverului să revină automat la modul de funcționare normal și să întrerupă astfel comunicarea. Acest serviciu, trimis periodic, menține sesiunea de diagnosticare/comunicare activă prin resetarea contorului P3 de fiecare dată când se primește o solicitare pentru acest serviciu.

4.3.2. Formatul mesajului

CPR_079 Formatele de mesaje pentru primitivele TesterPresent sunt prezentate în detaliu în tabelele următoare.

Tabelul 10

Mesaj de solicitare a indicatorului de prezență a aparatului de probă

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
# 1	Octet de format – adresare fizică	80	FMT
# 2	Octet țintă de adresă	EE	TGT
# 3	Octet sursă de adresă	tt	SRC
# 4	Octet de lungime suplimentar	02	LEN
# 5	ID al serviciului de solicitare TesterPresent	3E	TP
# 6	Subfuncție = responseRequired = [yes – da no] – nu	01	RESPREQ_Y
		02	RESPREQ_NO
# 7	Sumă de control	00-FF	TC

CPR_080 Dacă parametrul responseRequired are valoarea «yes» (da), serverul răspunde cu următorul mesaj de răspuns pozitiv. Dacă valoarea este «no» (nu), serverul nu trimite nici un răspuns.

Tabelul 11

Mesaj de răspuns pozitiv la solicitarea de indicator de prezență a aparatului de probă

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
# 1	Octet de format – adresare fizică	80	FMT
# 2	Octet țintă de adresă	tt	TGT
# 3	Octet sursă de adresă	EE	SRC
# 4	Octet de lungime suplimentar	01	LEN
# 5	ID al serviciului de răspuns pozitiv la solicitarea indicatorului de prezență a aparatului de probă	7E	TPPR
# 6	Sumă de control	00-FF	TC

CPR_081 Serviciul acceptă următoarele coduri de răspuns negativ:

Tabelul 12

Mesaj de răspuns negativ la TesterPresent

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
# 1	Octet de format – adresare fizică	80	FMT
# 2	Octet țintă de adresă	tt	TGT
# 3	Octet sursă de adresă	EE	SRC
# 4	Octet de lungime suplimentar	03	LEN
# 5	ID al serviciului de răspuns negativ	7F	RN
# 6	ID al serviciului de solicitare a indicatorului de prezență a aparatului de probă	3E	TP
# 7	ResponseCode = [SubfunctionNotSupported– InvalidFormatincorrectMessageLength] (subfuncție incompatibilă – format nevalid – lungime incorectă a mesajului)	12	RC_SFNS_IF
		13	RC_IML
# 8	Sumă de control	00-FF	TC

5. SERVICII DE GESTIONARE

Serviciile disponibile sunt prezentate în detaliu în tabelul următor:

Tabelul 13

Servicii de gestionare

Denumirea serviciului	Descriere
StartDiagnosticSession	Clientul solicită inițierea unei sesiuni de diagnosticare la o UV
SecurityAccess	Clientul solicită accesul la funcții rezervate utilizatorilor autorizați

5.1. Serviciul StartDiagnosticSession

5.1.1. Descrierea mesajului

CPR_025 Serviciul StartDiagnosticSession este folosit pentru a activa diferite sesiuni de diagnosticare în server. O sesiune de diagnosticare activează un set de servicii specifice, conform tabelului 17. O sesiune poate activa servicii specifice producătorului vehiculului, care nu sunt incluse în prezentul document. Normele de punere în aplicare trebuie să respecte următoarele cerințe:

- trebuie să existe întotdeauna exact o sesiune de diagnosticare activă în UV;
- UV începe întotdeauna o sesiune de diagnosticare standard dacă este conectată la o sursă de alimentare. Dacă nu se inițiază o altă sesiune de diagnosticare, sesiunea de diagnosticare standard rămâne deschisă atâta timp cât UV este conectată la o sursă de alimentare;
- dacă o sesiune de diagnosticare în curs de desfășurare a fost solicitată de un aparat de probă, UV trimite un mesaj de răspuns pozitiv;
- de fiecare dată când un aparat de probă solicită o sesiune de diagnosticare nouă, UV trimite mai întâi un mesaj de răspuns pozitiv la solicitarea de inițiere a sesiunii de diagnosticare, înainte ca noua sesiune să devină activă în UV. Dacă UV nu poate deschide noua sesiune de diagnosticare solicitată, răspunde cu un mesaj de răspuns negativ la solicitarea de inițiere a sesiunii de diagnosticare, iar sesiunea aflată în desfășurare continuă.

CPR_026 Inițierea unei sesiuni de diagnosticare poate avea loc numai dacă între client și UV s-a stabilit o comunicare.

CPR_027 Parametrii de sincronizare definiți în tabelul 4 devin activi după realizarea cu succes a unui serviciu StartDiagnosticSession cu un parametru de sesiune de diagnosticare «StandardDiagnosticSession» în mesajul de solicitare în cazul în care o altă sesiune de diagnosticare a fost activă în prealabil.

5.1.2. **Formatul mesajului**

CPR_028 Formatele de mesaj pentru primitivele StartDiagnosticSession sunt prezentate în detaliu în tabelele următoare:

Tabelul 14

Mesaj de solicitare a inițierii unei sesiuni de diagnosticare

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
# 1	Octet de format – adresare fizică	80	FMT
# 2	Octet țintă de adresă	EE	TGT
# 3	Octet sursă de adresă	tt	SRC
# 4	Octet de lungime suplimentar	02	LEN
# 5	ID al serviciului de solicitare a inițierii unei sesiuni de diagnosticare	10	STDS
# 6	diagnosticSession = (o valoare din tabelul 17)	xx	DS_...
# 7	Sumă de control	00-FF	TC

Tabelul 15

Mesaj de răspuns pozitiv la solicitarea de inițiere a unei sesiuni de diagnosticare

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
# 1	Octet de format – adresare fizică	80	FMT
# 2	Octet țintă de adresă	tt	TGT
# 3	Octet sursă de adresă	EE	SRC
# 4	Octet de lungime suplimentar	02	LEN
# 5	ID al serviciului de răspuns pozitiv la solicitarea de inițiere a unei sesiuni de diagnosticare	50	STDSPR
# 6	DiagnosticSession = (aceeași valoare ca și la octetul #6 din Tabelul 14)	xx	DS_...
# 7	Sumă de control	00-FF	TC

Tabelul 16

Mesaj de răspuns negativ la solicitarea de inițiere a unei sesiuni de diagnosticare

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
# 1	Octet de format – adresare fizică	80	FMT
# 2	Octet țintă de adresă	tt	TGT
# 3	Octet sursă de adresă	EE	SRC
# 4	Octet de lungime suplimentar	03	LEN
# 5	ID al serviciului de răspuns negativ	7F	RN
# 6	ID al serviciului de solicitare TesterPresent	10	STDS
# 7	ResponseCode = (subfunctionNotSupported – subfuncție incompatibilă ^(a))	12	RC_SFNS
	IncorrectMessageLength – lungime incorectă a mesajului ^(b)	13	RC_IML
	conditionsNotCorrect – condiții incorecte ^(c)	22	RC_CNC
# 8	Sumă de control	00-FF	TC

^(a) Valoarea introdusă la octetul # 6 din mesajul de solicitare nu este compatibilă, adică nu se află în tabelul 17.

^(b) Lungimea mesajului este greșită.

^(c) Criteriile pentru solicitarea StartDiagnosticSession nu sunt îndeplinite.

5.1.3. Definirea parametrilor

CPR_029 Parametrul *diagnosticSession* (*DS_*) este folosit de serviciul *StartDiagnosticSession* pentru a selecta comportamentul specific al serverului (serverelor). În prezentul document sunt precizate următoarele sesiuni de diagnosticare:

Tabelul 17

Definirea valorilor atribuite sesiunii de diagnosticare

Hex	Descriere	Cod mnemonic
81	StandardDiagnosticSession Această sesiune de diagnosticare activează toate serviciile specificate în tabelul 1 coloana 4 «SD». Aceste servicii permit citirea datelor de pe un server (UV). Această sesiune de diagnosticare este activă după finalizarea cu succes a inițializării între client (aparat de probă) și server (UV). Această sesiune de diagnosticare poate fi suprapusă altor sesiuni de diagnosticare specificate în prezenta secțiune.	SD
85	ECUProgrammingSession Această sesiune de diagnosticare activează toate serviciile specificate în tabelul 1 coloana 6 «ECUPS». Aceste servicii sunt compatibile cu programarea memoriei unui server (UV). Această sesiune de diagnosticare poate fi suprapusă altor sesiuni de diagnosticare specificate în prezenta secțiune.	ECUPS
87	ECUAdjustmentSession Această sesiune de diagnosticare activează toate serviciile specificate în tabelul 1 coloana 5 «ECUAS». Aceste servicii sunt compatibile cu controlul intrărilor/ieșirilor unui server (UV). Această sesiune de diagnosticare poate fi suprapusă altor sesiuni de diagnosticare specificate în prezenta secțiune.	ECUAS

5.2. Serviciul SecurityAccess

Înregistrarea datelor privind calibrarea sau accesul la linia de intrare/ieșire de calibrare pot fi realizate doar dacă UV se află în mod CALIBRARE. Pe lângă inserarea unui card de atelier în UV, trebuie să se introducă PIN-ul corespunzător în UV înainte de acordarea accesului la modul CALIBRARE.

Serviciul SecurityAccess permite introducerea PIN-ului și indică aparatului de probă dacă UV se află sau nu în mod CALIBRARE.

Sistemul permite introducerea PIN-ului și prin intermediul altor metode.

5.2.1. Descrierea mesajului

Serviciul SecurityAccess constă dintr-un mesaj «requestSeed», urmat eventual de un mesaj SecurityAccess «sendKey». Serviciul SecurityAccess trebuie să fie executat după serviciul StartDiagnosticSession.

- CPR_033 Aparatul de probă folosește mesajul SecurityAccess «requestSeed» pentru a verifica dacă unitatea montată pe vehicul este pregătită să accepte un PIN.
- CPR_034 Dacă unitatea montată pe vehicul este deja în mod CALIBRARE, aceasta răspunde solicitării prin trimiterea unui «germen» de 0x0000 cu ajutorul serviciului de răspuns pozitiv la solicitarea SecurityAccess.
- CPR_035 Dacă unitatea montată pe vehicul este pregătită să accepte un PIN pentru verificarea cu un card de atelier, aceasta răspunde solicitării prin trimiterea unui «germen» mai mare de 0x0000 cu ajutorul serviciului de răspuns pozitiv la solicitarea SecurityAccess.
- CPR_036 Dacă unitatea montată pe vehicul nu este pregătită să accepte un PIN de la aparatul de probă, fie deoarece cardul de atelier inserat nu este valabil, fie deoarece cardul de atelier nu a fost inserat sau deoarece unitatea montată pe vehicul așteaptă transmiterea unui PIN printr-o altă metodă, aceasta răspunde solicitării cu un răspuns negativ având un cod de răspuns setat pe conditionsNotCorrectOrRequestSequenceError.
- CPR_037 În cele din urmă, aparatul de probă folosește mesajul SecurityAccess «sendKey» pentru a transmite un PIN unității montate pe vehicul. Pentru a avea timpul necesar realizării procesului de autentificare a cardului, UV folosește codul de răspuns negativ requestCorrectlyReceived-ResponsePending pentru a prelungi timpul de răspuns. Totuși, timpul maxim de răspuns nu trebuie să depășească cinci minute. După finalizarea serviciului solicitat, UV trimite un mesaj de răspuns pozitiv sau un mesaj de răspuns negativ cu un cod de răspuns diferit de acesta. Codul de răspuns negativ requestCorrectlyReceived-ResponsePending poate fi repetat de UV până la finalizarea serviciului solicitat și trimiterea mesajului de răspuns final.

CPR_038 Unitatea montată pe vehicul răspunde acestei solicitări cu ajutorul serviciului de răspuns pozitiv la solicitarea SecurityAccess numai în modul CALIBRARE.

CPR_039 În următoarele cazuri, unitatea montată pe vehicul răspunde acestei solicitări cu un răspuns negativ însoțit de un cod de răspuns cu valoarea:

- subFunctionNotSupported: format nevalid pentru parametrul subfuncției (accessType);
- conditionsNotCorrectOrRequestSequenceError: unitatea montată pe vehicul nu este pregătită să accepte introducerea unui PIN;
- invalidKey: PIN nevalid fără depășirea numărului de încercări de verificare a PIN;
- exceededNumberOfAttempts: PIN nevalid cu depășirea numărului de încercări de verificare a PIN;
- generalReject: PIN corect, dar tentativă nereușită de autentificare reciprocă cu cardul de atelier.

5.2.2. **Formatul mesajului – SecurityAccess – requestSeed**

CPR_040 Formatele mesajului pentru primitivele «requestSeed» SecurityAccess sunt prezentate în detaliu în tabelele următoare:

Tabelul 18

Mesaj de solicitare SecurityAccess – requestSeed

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
# 1	Octet de format – adresare fizică	80	FMT
# 2	Octet țintă de adresă	EE	TGT
# 3	Octet sursă de adresă	tt	SRC
# 4	Octet de lungime suplimentar	02	LEN
# 5	ID al serviciului de solicitare SecurityAccess	27	SA
# 6	accessType – requestSeed	7D	AT_RSD
# 7	Sumă de control	00-FF	TC

Tabelul 19

Mesaj de răspuns pozitiv la o solicitare de SecurityAccess – requestSeed

Octet #	Denumirea parametrului	Valoarea Hex	Mnemonic
# 1	Octet de format – adresare fizică	80	FMT
# 2	Octet țintă de adresă	tt	TGT
# 3	Octet sursă de adresă	EE	SRC
# 4	Octet de lungime suplimentar	04	LEN
# 5	ID al serviciului de răspuns pozitiv la o solicitare de SecurityAccess	67	SAPR
# 6	accessType – requestSeed	7D	AT_RSD
# 7	Germen superior	00-FF	SEEDH
# 8	Germen inferior	00-FF	SEEDL
# 9	Sumă de control	00-FF	TC

Tabelul 20

Mesaj de răspuns negativ la o solicitare de SecurityAccess

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
# 1	Octet de format – adresare fizică	80	FMT
# 2	Octet țintă de adresă	tt	TGT
# 3	Octet sursă de adresă	EE	SRC
# 4	Octet de lungime suplimentar	03	LEN
# 5	ID al serviciului de răspuns negativ	7F	NR
# 6	ID al serviciului de solicitare SecurityAccess	27	SA
# 7	ResponseCode = (conditionsNotCorrectOr RequestSequenceError incorrectMessageLength)	22	RC_CNC
		13	RC_IML
# 8	Sumă de control	00-FF	TC

5.2.3. **Formatul mesajului – SecurityAccess – sendKey**

CPR_041 Formatele mesajului pentru primitivele «sendKey» SecurityAccess sunt prezentate în detaliu în tabelele următoare:

Tabelul 21

Mesaj de solicitare SecurityAccess – sendKey

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
# 1	Octet de format – adresare fizică	80	FMT
# 2	Octet țintă de adresă	EE	TGT
# 3	Octet sursă de adresă	tt	SRC
# 4	Octet de lungime suplimentar	m + 2	LEN
# 5	ID al serviciului de solicitare a SecurityAccess	27	SA
# 6	accessType – sendKey	7E	AT_SK
# 7 - #m + 6	Cheie # 1 (superior)	xx	KEY
	...	...	
	Cheie # m (inferior, m trebuie să fie cuprins între 4 și 8, inclusiv)	xx	
# m + 7	Sumă de control	00-FF	TC

Tabelul 22

Mesaj de răspuns pozitiv la o solicitare de SecurityAccess – sendKey

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
# 1	Octet de format – adresare fizică	80	FMT
# 2	Octet țintă de adresă	tt	TGT
# 3	Octet sursă de adresă	EE	SRC
# 4	Octet de lungime suplimentar	02	LEN
# 5	ID al serviciului de răspuns pozitiv la o solicitare de SecurityAccess	67	SAPR
# 6	accessType – sendKey	7E	AT_SK
# 7	Sumă de control	00-FF	TC

Tabelul 23

Mesaj de răspuns negativ la o solicitare de SecurityAccess

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
# 1	Octet de format – adresare fizică	80	FMT
# 2	Octet țintă de adresă	tt	TGT
# 3	Octet sursă de adresă	EE	SRC
# 4	Octet de lungime suplimentar	03	LEN
# 5	ID al serviciului de răspuns negativ	7F	NR
# 6	ID al serviciului de solicitare SecurityAccess	27	SA
# 7	reponseCode = (generalReject	10	RC_GR
	subFunctionNotSupported	12	RC_SFNS
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrectOrRequest-SequenceError	22	RC_CNC
	invalidKey	35	RC_IK
	exceededNumberOfAttempts	36	RC_ENA
	requestCorrectlyReceived-ResponsePending	78	RC_RCR_RP
# 8	Sumă de control	00-FF	TC

6. SERVICII DE TRANSMISIE DE DATE

Aceste servicii sunt prezentate în detaliu în tabelul următor:

Tabelul 24

Servicii de transmisie de date

Denumire serviciu	Descriere
ReadDataByIdentifier	Clientul solicită transmisia valorii curente a unei înregistrări care poate fi accesată prin recordDataIdentifier
WriteDataByIdentifier	Clientul solicită introducerea unei înregistrări care poate fi accesată prin recordDataIdentifier

6.1. Serviciul ReadDataByIdentifier

6.1.1. Descrierea mesajului

CPR_050 Serviciul ReadDataByIdentifier este folosit de client pentru a solicita valorile datelor înregistrate pe un server. Datele sunt identificate de un recordDataIdentifier. Producătorul UV trebuie să se asigure că, la efectuarea acestui serviciu, condițiile privind serverul sunt îndeplinite.

6.1.2. Formatul mesajului

CPR_051 Formatele mesajului pentru primitivele ReadDataByIdentifier sunt prezentate în detaliu în tabelele următoare:

Tabelul 25

Mesaj de solicitare ReadDataByIdentifier

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
# 1	Octet de format – adresare fizică	80	FMT
# 2	Octet țintă de adresă	EE	TGT
# 3	Octet sursă de adresă	tt	SRC
# 4	Octet de lungime suplimentar	03	LEN
# 5	ID al serviciului de solicitare ReadDataByIdentifier	22	RDBI
# 6 și # 7	recordDataIdentifier = (o valoare din tabelul 28)	xxxx	RDI_...
# 8	Sumă de control	00-FF	TC

Tabelul 26

Răspuns pozitiv la mesajul de solicitare ReadDataByIdentifier

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
# 1	Octet de format – adresare fizică	80	FMT
# 2	Octet țintă de adresă	tt	TGT
# 3	Octet sursă de adresă	EE	SRC
# 4	Octet de lungime suplimentar	m + 3	LEN
# 5	ID al serviciului de răspuns pozitiv la o solicitare a ReadDataByIdentifier	62	RDBIPR
# 6 și # 7	recordDataIdentifier = (aceeași valoare ca și pentru octeții #6 și #7 din tabelul 25)	xxxx	RDI_...
# 8 - #m + 7	dataRecord () = (valoarea # 1 : valoarea # m)	xx : xx	DREC_DATA1 : DREC_DATAm
# m + 8	Sumă de control	00-FF	TC

Tabelul 27

Răspuns negativ la mesaj de solicitare ReadDataByIdentifier

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
# 1	Octet de format – adresare fizică	80	FMT
# 2	Octet țintă de adresă	tt	TGT
# 3	Octet sursă de adresă	EE	SRC
# 4	Octet de lungime suplimentar	03	LEN
# 5	ID al serviciului de răspuns negativ	7F	NR
# 6	ID al serviciului de solicitare a ReadDataByIdentifier	22	RDBI
# 7	ResponseCode = (requestOutOfRange incorrectMessageLength conditionsNotCorrect)	31 13 22	RC_ROOR RC_IML RC_CNC
# 8	Sumă de control	00-FF	TC

6.1.3. Definirea parametrilor

CPR_052 Parametrul recordDataIdentifier (RDI_) din mesajul de solicitare a ReadDataByIdentifier identifică o înregistrare de date.

CPR_053 Valorile recordDataIdentifier definite în prezentul document sunt indicate în tabelul menționat în continuare.

Tabelul recordDataIdentifier este format din patru coloane și mai multe linii.

- Prima coloană (Hex) cuprinde «valoarea Hex» atribuită recordDataIdentifier specificat în coloana a treia.
- A doua coloană (element de date) precizează elementul de date din apendicele 1 pe care se bazează recordDataIdentifier (uneori este necesară transcodarea).
- A treia coloană (descriere) specifică denumirea recordDataIdentifier corespunzătoare.
- A patra coloană (cod mnemonic) indică mnemonicul recordDataIdentifier în cauză.

Tabelul 28

Definiția valorilor recordDataIdentifier

Hex	Element de date	Denumirea recordDataIdentifier (vezi format în secțiunea 8.2)	Cod mnemoni-
F90B	CurrentDateTime	Data și ora	RDI_TD
F912	HighResOdometer	Kilometrajul total al vehiculului de înaltă definiție	RDI_HRTVD
F918	K-ConstantOfRecordingEquipment	Factor K	RDI_KF
F91C	L-TyreCircumference	Circumferința pneurilor factor L	RDI_LF
F91D	W-VehicleCharacteristicConstant	Coeficientul W caracteristic al vehiculului	RDI_WVCF
F921	TyreSize	Dimensiunea pneurilor	RDI_TS
F922	nextCalibrationDate	Data următoarei calibrări	RDI_NCD
F92C	SpeedAuthorised	Viteza autorizată	RDI_SA
F97D	vehicleRegistrationNation	Statul membru de înmatriculare	RDI_RMS
F97E	VehicleRegistrationNumber	Numărul de înmatriculare al vehiculului	RDI_VRN
F190	VehicleIdentificationNumber	VIN	RDI_VIN

CPR_054 Parametrul dataRecord (DREC_) este folosit de mesajul de răspuns pozitiv la solicitarea ReadDataByIdentifier pentru a furniza clientului (aparatură de probă) înregistrarea de date identificată de recordDataIdentifier. Formatele de date sunt specificate în secțiunea 8. Utilizatorul poate obține înregistrări de date opționale, precum date de intrare și ieșire specifice pentru UV, dar acestea nu sunt definite în prezentul document.

6.2. Serviciul WriteDataByIdentifier**6.2.1. Descrierea mesajului**

CPR_056 Serviciul WriteDataByIdentifier este folosit de client pentru a introduce valorile datelor înregistrate pe un server. Datele sunt identificate de un recordDataIdentifier. Producătorul UV trebuie să se asigure că, la efectuarea acestui serviciu, condițiile privind serverul sunt îndeplinite. Pentru a actualiza parametrii enumerați în tabelul 28, UV trebuie să se afle în modul CALIBRARE.

6.2.2. Formatul mesajului

CPR_057 Formatele mesajului pentru primitivele WriteDataByIdentifier sunt prezentate în detaliu în tabelele următoare:

Tabelul 29

Mesaj de solicitare a scrierii de date în funcție de un identificator

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
# 1	Octet de format – adresare fizică	80	FMT
# 2	Octet țintă de adresă	EE	TGT
# 3	Octet sursă de adresă	tt	SRC
# 4	Octet de lungime suplimentar	m + 3	LEN
# 5	ID al serviciului de solicitare WriteDataByIdentifier	2E	WDBI
# 6 și # 7	recordDataIdentifier = (o valoare din tabelul 28)	xxxx	RDI_...
#8 – #m + 7	dataRecord () = valoare # 1 : valoare # m)	xx : xx	DREC_DATA1 : DREC_DATAm
# m + 8	Sumă de control	00-FF	TC

Tabelul 30

Răspuns pozitiv la un mesaj de solicitare a scrierii de date în funcție de un identificator

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
# 1	Octet de format – adresare fizică	80	FMT
# 2	Octet țintă de adresă	tt	TGT
# 3	Octet sursă de adresă	EE	SRC
# 4	Octet de lungime suplimentar	03	LEN
# 5	ID al serviciului de răspuns pozitiv la o solicitare a WriteDataByIdentifier	6E	WDBIPR
# 6 și # 7	recordDataIdentifier = (aceeași valoare ca și pentru octeții #6 și #7 din tabelul 29)	xxxx	RDI_...
# 8	Sumă de control	00-FF	TC

Tabelul 31

Răspuns negativ la un mesaj de solicitare a scrierii de date în funcție de un identificator

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
# 1	Octet de format – adresare fizică	80	FMT
# 2	Octet țintă de adresă	tt	TGT
# 3	Octet sursă de adresă	EE	SRC
# 4	Octet de lungime suplimentar	03	LEN
# 5	ID al serviciului de răspuns negativ	7F	NR
# 6	ID al serviciului de solicitare a WriteDataByIdentifier	2E	WDBI
# 7	ResponseCode = (requestOutOfRange incorrectMessageLength conditionsNotCorrect)	31	RC_ROOR
		13	RC_IML
		22	RC_CNC
# 8	Sumă de control	00-FF	TC

6.2.3. Definirea parametrilor

Parametrul recordDataIdentifier (RDI_) este definit în tabelul 28.

Parametrul dataRecord (DREC_) este folosit de mesajul de solicitare a WriteDataByIdentifier pentru a furniza valorile înregistrărilor de date identificate de recordDataIdentifier pe server (UV). Formatele de date sunt specificate în secțiunea 8.

7. CONTROLUL IMPULSURILOR DE TEST – UNITATEA FUNCȚIONALĂ DE CONTROL AL INTRĂRILOR/IEȘIRILOR

Serviciile disponibile sunt prezentate în detaliu în tabelul următor:

Tabelul 32

Unitatea funcțională de control al intrărilor/ieșirilor

Denumire serviciu	Descriere
InputOutputControlByIdentifier	Clientul solicită controlul intrărilor/ieșirilor specifice serverului

7.1. Serviciul InputOutputControlByIdentifier**7.1.1. Descrierea mesajului**

Conexiunea realizată cu ajutorul conectorului frontal permite controlul sau monitorizarea impulsurilor de testare folosind aparatul de probă corespunzător.

CPR_058 Linia de semnalizare de intrare/ieșire de calibrare poate fi configurată cu ajutorul comenzii pe linie K folosind serviciul InputOutputControlByIdentifier pentru a selecta funcția de intrare sau ieșire pentru linie. Stările disponibile pentru linie sunt următoarele:

- inactivă;
- speedSignalInput, dacă se folosește linia de semnalizare a intrărilor/ieșirilor pentru a introduce un semnal de viteză (semnal de test) care să înlocuiască un semnal de viteză al senzorului de mișcare;
- realTimeSpeedSignalOutputSensor, dacă se folosește linia de semnalizare a intrărilor/ieșirilor pentru ieșirea unui semnal de viteză al senzorului de mișcare;
- RTCTOutput, dacă se folosește linia de semnalizare a intrărilor/ieșirilor pentru ieșirea unui semnal de ceas UTC.

CPR_059 Unitatea montată pe vehicul trebuie să se afle într-o sesiune de reglare și în modul CALIBRARE pentru a configura starea liniei. La ieșirea din sesiunea de reglare sau din modul CALIBRARE unitatea montată pe vehicul trebuie să se asigure că linia de semnalizare a intrărilor/ieșirilor de calibrare a revenit la starea «inactivă» (implicită).

CPR_060 Dacă impulsurile de viteză sunt primite pe linia de intrare a semnalului de viteză instantanee a UV în timp ce linia de semnalizare a intrărilor/ieșirilor este în modul intrare, linia de semnalizare a intrărilor/ieșirilor trece în modul ieșire sau revine la starea inactivă.

CPR_061 Ordinea operațiunilor este următoarea:

- inițierea comunicărilor cu ajutorul serviciului StartCommunication;
- intrarea într-o sesiune de reglare cu ajutorul serviciului StartDiagnosticSession și trecerea în modul CALIBRARE (ordinea acestor două operațiuni nu este importantă);
- modificarea stării ieșirii cu ajutorul serviciului InputOutputControlByIdentifier.

7.1.2. **Formatul mesajului**

CPR_062 Formatele mesajului pentru primitivele InputOutputControlByIdentifier sunt prezentate în detaliu în tabelele următoare:

Tabelul 33

Mesaj de solicitare InputOutputControlByIdentifier

Octet #	Denumirea parametrului	Valoare Hex	Cod mnemonic
# 1	Octet de format – adresare fizică	80	FMT
# 2	Octet țintă de adresă	EE	TGT
# 3	Octet sursă de adresă	tt	SRC
# 4	Octet de lungime suplimentar	xx	LEN
# 5	ID al serviciului de solicitare InputOutputControlByIdentifier	2F	IOCBI
# 6 și # 7	InputOutputIdentifier = (CalibrationInputOutput)	F960	IOI_CIO
# 8 sau # 8 - # 9	ControlOptionRecord = [inputOutputControlParameter – o valoare din tabelul 36 controlState – o valoare din tabelul 38 (vezi nota de mai jos)]	xx xx	COR_... IOCP_... CS_...
# 9 sau # 10	Sumă de control	00-FF	TC

Notă: Parametrul controlState este prezent numai în anumite cazuri (vezi 7.1.3).

Tabelul 34

Răspuns pozitiv la mesaj de solicitare a unui control de intrare/ieșire prin identificator

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
# 1	Octet de format – adresare fizică	80	FMT
# 2	Octet țintă de adresă	tt	TGT
# 3	Octet sursă de adresă	EE	SRC
# 4	Octet de lungime suplimentar	xx	LEN
# 5	ID al serviciului de răspuns pozitiv la o solicitare de inputOutputControlByIdentifier	6F	IOCBIPR
# 6 și # 7	inputOutputIdentifier = (CalibrationInputOutput)	F960	IOI_CIO
# 8 sau # 8 - # 9	controlStatusRecord =[inputOutputControlParameter (aceeași valoare ca și cea a octetului #8 din tabelul 33) controlState – aceeași valoare ca și cea a octetului #9 din tabelul 33)] (dacă este cazul)	xx xx	CSR_... IOCP_... CS_...
#9 sau #10	Sumă de control	00-FF	TC

Tabelul 35

Răspuns negativ la mesaj de solicitare a unui control de intrare/ieșire prin identificator

Octet #	Denumirea parametrului	Valoarea Hex	Cod mnemonic
# 1	Octet de format – adresare fizică	80	FMT
# 2	Octet țintă de adresă	tt	TGT
# 3	Octet sursă de adresă	EE	SRC
# 4	Octet de lungime suplimentar	03	LEN
# 5	ID al serviciului de răspuns negativ	7F	NR
# 6	ID al serviciului de solicitare a inputOutputControlByIdentifier	2F	IOCB
# 7	responseCode =(incorrectMessageLength conditionsNotCorrect requestOutOfRange deviceControlLimitsExceeded)	13 22 31 7A	RC_IML RC_CNC RC_ROOR RC_DCLE
# 8	Sumă de control	00-FF	TC

7.1.3. Definirea parametrilor

CPR_064 Parametrul inputOutputControlParameter (IOCP_) este definit în tabelul următor:

Tabelul 36

Definirea valorilor atribuite parametrilor de control de intrare/ieșire

Hex	Descriere	Cod mnemonic
00	ReturnControlToECU Această valoare indică serverului (UV) faptul că aparatul de probă nu mai are controlul asupra liniei de semnalizare a intrărilor/ieșirilor de calibrare.	RCTECU
01	ResetToDefault Această valoare indică serverului (UV) faptul că s-a solicitat resetarea liniei de semnalizare a intrărilor/ieșirilor de calibrare la starea implicită.	RTD
03	ShortTermAdjustment Această valoare indică serverului (UV) faptul că s-a solicitat ajustarea liniei de semnalizare a intrărilor/ieșirilor de calibrare la valoarea inclusă în parametrul controlState.	STA

CPR_065 Parametrul controlState este prezent numai dacă inputOutputControlParameter are configurare identică celei a parametrului ShortTermAdjustment și este definit în tabelul următor:

Tabelul 37

Definiția valorilor atribuite parametrului stat de control

Mod	Valoare Hex	Descriere
Inactiv	00	Linia de intrări/ieșiri este inactivă (stare implicită)
Activ	01	Linia de intrări/ieșiri este activă pentru intrarea speedSignalInput
Activ	02	Linia de intrări/ieșiri este activă pentru ieșirea realTimeSpeedSignalOutputSensor
Activ	03	Linia de intrări/ieșiri este activă pentru RTCOutput

8. FORMATE DE ÎNREGISTRĂRI DE DATE

Această secțiune prezintă în detaliu:

- normele generale care se aplică intervalelor de parametri transmiși de unitatea montată pe vehicul către aparatul de probă;
- formatele care se folosesc pentru datele transferate cu ajutorul serviciilor de transmisie de date descrise în secțiunea 6.

CPR_067 Toți parametrii identificați sunt compatibili cu UV.

CPR_068 Datele transmise de UV către aparatul de probă ca răspuns la un mesaj de solicitare sunt de tip cuantificabil (adică valoarea activă a parametrului solicitat, măsurat sau observat de UV).

8.1. Intervale de parametri transmiși

CPR_069 Tabelul 38 definește intervalele folosite la determinarea valabilității unui parametru transmis.

CPR_070 Valorile din intervalul «indicator de eroare» permit unității montate pe vehicul să indice imediat faptul că nici o dată parametrică nu este valabilă din cauza unui tip de eroare la nivelul aparatului de înregistrare.

CPR_071 Valorile din intervalul «nu sunt disponibile» permit unității montate pe vehicul să transmită un mesaj ce conține parametrul care nu este disponibil sau nu este compatibil cu modulul în cauză. Valorile din intervalul «nu sunt solicitate» permit transmiterea unui mesaj de comandă și identifică parametrii pentru care echipamentul de recepție nu așteaptă nici un răspuns.

CPR_072 Dacă defectarea unei componente împiedică transmiterea de date valabile pentru un parametru, în locul parametrului în cauză se folosește indicatorul de eroare, conform descrierii din tabelul 38. Totuși, dacă datele măsurate sau calculate dau ca rezultat o valoare valabilă care depășește intervalul parametrului definit, nu se folosește indicatorul de eroare. Datele trebuie să fie transmise folosind valoarea minimă sau maximă adecvată a parametrului.

Tabelul 38

Intervalele de înregistrări de date

Denumirea intervalului	1 octet (valoarea Hex)	2 octeți (valoarea Hex)	4 octeți (valoarea Hex)	ASCII
Semnal valabil	00-FA	0000-FAFF	00000000-FAFFFFFF	1-254
Indicator specific parametrului	FB	FB00-FBFF	FB000000-FBFFFFFF	nul
Interval rezervat pentru viitorii biți ai indicatorului	FC-FD	FC00-FDFF	FC000000-FDFFFFFF	nul
Indicator de eroare	FE	FE00-FEFF	FE000000-FEFFFFFF	0
Nu sunt disponibile sau nu sunt solicitate	FF	FF00-FFFF	FF000000-FFFFFF	FF

CPR_073 Pentru parametrii codificați în ASCII, caracterul ASCII «*» este rezervat ca delimitator.

8.2. Formate de înregistrări de date

În tabelele 40-44 sunt prezentate în detaliu formatele care trebuie folosite prin intermediul serviciilor ReadDataByIdentifier și WriteDataByIdentifier.

CPR_074 Tabelul 40 prezintă lungimea, rezoluția și domeniul de valori al fiecărui parametru identificat de recordDataIdentifier:

Tabelul 39

Formatul înregistrărilor de date

Denumirea parametrului	Lungimea datelor (octeți)	Rezoluție	Domeniu de valori
Data și ora	8	Vezi detalii în tabelul 40	
Kilometrajul total al vehiculului de înaltă definiție	4	amplificare 5 m/bit, decalaj 0 m	de la 0 până la + 21 055 406 km
Factor K	2	amplificare 0,001 impulsuri/m/bit, decalaj 0	0-64,255 impulsuri/m
Circumferința pneurilor factor L	2	amplificare 0,125 10 ⁻³ m/bit, decalaj 0	0-8,031 m
Coeficientul W caracteristic al vehiculului	2	amplificare 0,001 impulsuri/m/bit, decalaj 0	0-64,255 impulsuri/m
Dimensiunea pneurilor	15	ASCII	ASCII
Data următoarei calibrări	3	Vezi detalii în tabelul 41	
Viteza autorizată	2	amplificare 1/256 km/h/bit, decalaj 0	0-250,996 km/h
Statul membru de înmatriculare	3	ASCII	ASCII
Numărul de înmatriculare al vehiculului	14	Vezi detalii în tabelul 42	
VIN	17	ASCII	ASCII

CPR_075 Tabelul 40 prezintă în detaliu formatele diferiților octeți ai parametrului TimeDate:

Tabelul 40

Format detaliat al parametrului data și ora (valoarea identificatorului înregistrării de date # F00B)

Octet	Definiția parametrului	Rezoluția	Domeniu de valori
1	Secunde	amplificare 0,25 s/bit, decalaj 0 s	0-59,75 s
2	Minute	amplificare 1 min/bit, decalaj 0 min	0-59 min
3	Ore	amplificare 1 h/bit, decalaj 0 h	0-23 h
4	Lună	amplificare 1 lună/bit, decalaj 0 lună	1-12 luni
5	Zi	amplificare 0,25 zile/bit, decalaj 0 zile (vezi nota din tabelul 41)	0,25-31,75 zile
6	An	amplificare 1 an/bit, decalaj + anul 1985 (vezi nota din tabelul 41)	anul 1985-anul 2235
7	Decalaj local minute	amplificare 1 min/bit, decalaj – 125 min	între – 59 și 59 min
8	Decalaj orar local	amplificare 1 h/bit, decalaj – 125	între – 23 și + 23 h

CPR_076 Tabelul 41 prezintă în detaliu formatele diferiților octeți ai parametrului NextCalibrationDate:

Tabelul 41

Format detaliat al parametrului data următoarei calibrări (valoarea identificatorului înregistrării de date # F022)

Octet	Definiția parametrului	Rezoluție	Domeniu de valori
1	Lună	amplificare 1 lună/bit, decalaj 0 luni	1-12 luni
2	Zi	amplificare 0,25 zile/bit, decalaj 0 zile (vezi nota menționată în continuare)	0,25-31,75 zile
3	An	amplificare 1 an/bit, decalaj + anul 1985 (vezi nota menționată în continuare)	anul 1985-anul 2235

Notă privind folosirea parametrului «zi»:

1. Valoarea 0 pentru dată este o valoare nulă. Valorile 1, 2, 3 și 4 sunt folosite pentru a identifica prima zi a lunii; 5, 6, 7 și 8 indică a doua zi a lunii etc.
2. Acest parametru nu influențează și nici nu modifică parametrul pentru oră menționat anterior.

Notă privind folosirea parametrului «an»:

Valoarea 0 pentru an identifică anul 1985, valoarea 1 indică anul 1986 etc.

CPR_078 Tabelul 42 prezintă în detaliu formatele diferiților octeți ai parametrului VehicleRegistrationNumber:

Tabelul 42

Format detaliat al parametrului numărul de înmatriculare al vehiculului (valoarea identificatorului înregistrării de date # F07E)

Octet	Definiția parametrului	Rezoluție	Domeniu de valori
1	Pagină de cod (conform definiției din apendicele 1)	ASCII	01-0A
2-14	Numărul de înmatriculare al vehiculului (conform definiției din apendicele 1)	ASCII	ASCII

Apendicele 9

OMOLOGARE – LISTA TESTELOR MINIME OBLIGATORII

CUPRINS

1.	Introducere	193
1.1.	Omologare	193
1.2.	Trimiteri	193
2.	Teste de funcționare pentru unitatea montată pe vehicul	194
3.	Teste de funcționare pentru senzorul de mișcare	197
4.	Teste de funcționare pentru cardurile de tahograf	199
5.	Teste de interoperare	200

1. INTRODUCERE

1.1. Omologare

Omologarea CEE pentru aparatul de înregistrare (sau componentele acestuia) sau pentru un card de tahograf se bazează pe următoarele:

- certificarea securității, efectuată de o autoritate ITSEC, în raport cu un obiectiv de securitate care respectă în totalitate apendicele 10 la prezenta anexă;
- certificarea funcționării, efectuată de o autoritate a unui stat membru, care atestă faptul că articolul testat respectă cerințele prezentei anexe, din punctul de vedere al funcțiilor îndeplinite, preciziei măsurărilor și caracteristicilor de mediu;
- certificarea interoperării, efectuată de un organ competent, care atestă faptul că aparatul de înregistrare (sau cardul de tahograf) sunt în întregime interoperabile cu modelele compatibile de card de tahograf (sau de aparat de înregistrare) (vezi capitolul VIII din prezenta anexă).

Prezenta anexă enumeră testele minime care trebuie efectuate de către o autoritate a unui stat membru în cadrul testelor de funcționare, precum și testele minime care trebuie efectuate de organul competent în cadrul testelor de interoperare. Procedurile care vor fi urmate pentru efectuarea testelor sau tipul testelor nu sunt specificate în cuprinsul prezentului document.

Această anexă nu se referă la aspecte privind certificarea securității. Dacă anumite teste necesare pentru omologare sunt efectuate și în cadrul procesului de evaluare și de certificare a securității, ele nu mai trebuie repetate. Într-un asemenea caz, este suficientă inspectarea rezultatelor acestor teste de securitate. În scop informativ, cerințele care trebuie testate (sau cele strâns legate de testele care trebuie efectuate) în timpul certificării securității sunt marcate cu caracterul «*» în cuprinsul prezentului apendice.

Prezentul apendice tratează separat omologarea senzorului de mișcare și a unității montate pe vehicul, în calitate de componente ale aparatului de înregistrare. Nu este obligatoriu ca fiecare model de senzor de mișcare să fie interoperabil cu toate modelele de unități montate pe vehicule, drept pentru care omologarea unui anumit senzor de mișcare poate fi acordată numai în combinație cu omologarea unei anumite unități montate pe vehicul și viceversa.

1.2. Trimiteri

În cuprinsul prezentului apendice se utilizează următoarele trimiteri:

IEC 68-2-1	Testare în mediu – Partea 2: Teste – Teste A: Frig. 1990 + Amendamentul 2: 1994.
IEC 68-2-2	Testare în mediu – Partea 2: Teste – Teste B: Căldură uscată. 1974 + Amendamentul 2: 1994.
IEC 68-2-6	Proceduri de bază de testare în mediu – Metode de testare – Test Fc și linii directoare: Vibrație (sinusoidală). Ediția a VI-a: 1985.
IEC 68-2-14	Proceduri de bază de testare în mediu – Metode de testare – Test N: Modificări de temperatură. Modificarea 1: 1986.
IEC 68-2-27	Proceduri de bază de testare în mediu – Metode de testare – Test Ea și linii directoare: Șoc. Ediția a III-a: 1987.
IEC 68-2-30	Proceduri de bază de testare în mediu – Metode de testare – Test Db și linii directoare: Căldură umedă, ciclică (cicluri de 12 + 12 ore). Modificarea 1: 1985.
IEC 68-2-35	Proceduri de bază de testare în mediu – Metode de testare – Test Fda: Bandă largă de frecvență pentru vibrații aleatorii – Valoare maximă de reproductibilitate. Modificarea 1: 1983.
IEC 529	Grade de protecție oferite de incinte (Cod IP). Ediția a II-a: 1989.
IEC 61000-4-2	Compatibilitate electromagnetică (EMC) – Tehnici de testare și măsurare – Test de imunitate la descărcări electrostatice: 1995/Amendamentul 1: 1998.
ISO 7637-1	Vehicule rutiere – Avarii electrice prin conducție și cuplare – Partea 1: Automobile și vehicule comerciale ușoare cu tensiune nominală de alimentare de 12 V – Conducție electrică tranzitorie numai prin liniile de alimentare. Ediția a II-a: 1990.

- ISO 7637-2 Vehicule rutiere – Avarii electrice prin conducție și cuplare – Partea 1: Vehicule comerciale cu tensiune nominală de alimentare de 12 V – Conducție electrică tranzitorie numai prin liniile de alimentare. Ediția a II-a: 1990.
- ISO 7637-3 Vehicule rutiere – Avarii electrice prin conducție și cuplare – Partea 3: Vehicule cu tensiune nominală de alimentare de 12 sau 24 V – Transmisie electrică tranzitorie prin cuplare capacitivă și inductivă prin alte linii decât cele de alimentare. Ediția I: 1995 + Cor 1: 1995.
- ISO/IEC 7816-1 Carduri de identificare – Carduri cu circuite integrate cu contacte – Partea 1: Caracteristici fizice. Ediția I: 1998.
- ISO/IEC 7816-2 Tehnologia informației – Carduri de identificare – Carduri cu circuite integrate cu contacte – Partea 2: Dimensiunile și localizarea contactelor. Ediția I: 1999.
- ISO/IEC 7816-3 Tehnologia informației – Carduri de identificare – Carduri cu circuite integrate cu contacte – Partea 3: Semnale electronice și protocol de transmisie. Ediția a II-a: 1997.
- ISO/IEC 10373 Carduri de identificare – Metode de testare. Ediția I: 1993.

2. TESTE DE FUNCȚIONARE PENTRU UNITATEA MONTATĂ PE VEHICUL

Nr.	Test	Descriere	Cerințe asociate
1.	Examinare administrativă		
1.1.	Documentație	Corectitudinea documentației	
1.2.	Rezultate test producător	Rezultatele testului producătorului efectuate în cursul integrării. Demonstrații pe suport hârtie	070, 071, 073
2.	Inspecție vizuală		
2.1.	Respectarea documentației		
2.2.	Identificare/marcaje		168, 169
2.3.	Materiale		163-167
2.4.	Sigilare		251
2.5.	Interfețe externe		
3.	Teste de funcționare		
3.1.	Funcții oferite		002, 004, 244
3.2.	Moduri de funcționare		006*, 007*, 008*, 009*, 106, 107
3.3.	Funcții și drepturi de acces la date		010*, 011*, 240, 246, 247
3.4.	Monitorizarea introducerii și retragerii cardurilor		013, 014, 015*, 016*, 106
3.5.	Măsurarea vitezei și a distanței		017-026
3.6.	Măsurarea timpului (teste efectuate la 20 °C)		027-032
3.7.	Monitorizarea activităților șoferului		033-043, 106
3.8.	Monitorizarea stării activității de conducere		044, 045, 106
3.9.	Înregistrări manuale		046-050b
3.10.	Gestionarea blocărilor efectuate de societate		051-055
3.11.	Monitorizarea activităților de control		056, 057
3.12.	Detectarea evenimentelor și/sau a anomaliilor		059-069, 106

Nr.	Test	Descriere	Cerințe asociate
3.13.	Date de identificare a echipamentului		075*, 076*, 079
3.14.	Date privind introducerea și retragerea cardului șoferului		081*-083*
3.15.	Date privind activitatea șoferului		084*-086*
3.16.	Date privind locurile		087*-089*
3.17.	Date privind contorul de parcurs		090*-092*
3.18.	Date detaliate privind viteza		093*
3.19.	Date privind evenimentele		094*, 095
3.20.	Date privind anomaliiile		096*
3.21.	Date privind calibrarea		097*, 098*
3.22.	Date privind reglarea orei		100*, 101*
3.23.	Date privind activitatea de control		102*, 103*
3.24.	Date privind blocările efectuate de societate		104*
3.25.	Date privind activitatea de descărcare		105*
3.26.	Date privind condițiile specifice		105a*, 105b*
3.27.	Înregistrarea și stocarea informațiilor pe cardul de tahograf		108, 109*, 109a*, 110*, 111, 112
3.28.	Afișare		072, 106, 113-128, PIC_001, DIS_001
3.29.	Tipărire		072, 106, 129-138, PIC_001, PRT_001-PRT_012
3.30.	Avertisment		106, 139-148, PIC_001
3.31.	Descărcarea datelor pe suporturi externe		072, 106, 149-151
3.32.	Date de ieșire transmise unor dispozitive externe suplimentare		152, 153
3.33.	Calibrare		154*, 155*, 156*, 245
3.34.	Reglarea orei		157*, 158*
3.35.	Neinterferența cu funcțiile suplimentare		003, 269

Nr.	Test	Descriere	Cerințe asociate
4.	Teste în mediu		
4.1.	Temperatură	Verificarea funcționalității prin: — IEC 68-2-1, test Ad, cu o durată a testului de 72 de ore la temperatură scăzută (-20°C), o oră de funcționare, o oră de nefuncționare. — IEC 68-2-2, test Bd, cu o durată a testului de 72 de ore la temperatură ridicată ($+70^{\circ}\text{C}$), o oră de funcționare, o oră de nefuncționare. Cicluri de temperatură: se verifică, prin intermediul testului Na IEC 68-2-14, dacă unitatea montată pe vehicul poate suporta modificări rapide ale temperaturii mediului ambiant, la 20 de cicluri, în cursul fiecărui ciclu înregistrându-se o variație a temperaturii între valoarea minimă (-20°C) și cea maximă ($+70^{\circ}\text{C}$) și cu 2 ore de menținere atât la temperatura minimă, cât și la cea maximă Un set redus de teste (din cadrul celor definite la secțiunea 3 din acest tabel) poate fi efectuat la temperatură scăzută, la temperatură ridicată și pe parcursul ciclurilor de temperatură	159
4.2.	Umiditate	Se verifică, prin intermediul testului Db IEC 68-2-30, dacă unitatea montată pe vehicul poate suporta un ciclu de căldură umedă (testul de căldură), prin șase cicluri de câte 24 de ore fiecare, cu temperaturi variind între $+25^{\circ}\text{C}$ și $+55^{\circ}\text{C}$ la o umiditate relativă de 97 % la $+25^{\circ}\text{C}$ și egală cu 93 % la $+55^{\circ}\text{C}$	160
4.3.	Vibrație	1. Vibrații sinusoidale: se verifică dacă unitatea montată pe vehicul poate suporta vibrații sinusoidale cu următoarele caracteristici: deplasare constantă la frecvențe între 5 și 11 Hz: valoare maximă 10 mm acelerație constantă între 11 și 300 Hz: 5 g Această cerință este verificată prin intermediul testului Fc IEC 68-2-6, cu o durată minimă a testului de 3×12 ore (12 ore pe osie) 2. Vibrații aleatorii: se verifică dacă unitatea montată pe vehicul poate suporta vibrații aleatorii cu următoarele caracteristici: Frecvență 5-150 Hz, nivel $0,02 \text{ g}^2/\text{Hz}$ Această cerință este verificată prin IEC 68-2-35, testul Ffda, cu o durată minimă a testului de 3×12 ore (12 ore pe osie), cu o oră de funcționare, o oră de nefuncționare Cele două teste descrise anterior se efectuează pe două mostre diferite ale echipamentului testat	163
4.4.	Protecție împotriva apei și corpurilor străine	Se verifică dacă indicele de protecție al unității montate pe vehicul, conform IEC 529, este de cel puțin IP 40, atunci când unitatea este montată într-un vehicul în condiții de funcționare	164, 165
4.5.	Protecție împotriva supratensiunii	Se verifică dacă unitatea montată pe vehicul poate suporta următoarele tensiuni:	161
		Pentru versiunile de 24 V: 34 V la $+40^{\circ}\text{C}$ timp de o oră	
		Pentru versiunile de 12 V: 17 V la $+40^{\circ}\text{C}$ timp de o oră	
4.6.	Protecție împotriva inversării de polaritate	Se verifică dacă unitatea montată pe vehicul poate suporta o inversare a polarității la sursa de alimentare	161

Nr.	Test	Descriere	Cerințe asociate
4.7.	Protecție împotriva scurtcircuitelor	Se verifică dacă semnalele de intrare/ieșire sunt protejate împotriva scurtcircuitelor la sursa de alimentare și la masă	161
5.	Teste privind compatibilitatea electromagnetică		
5.1.	Emisii de radiații și susceptibilitate de radiații	Respectarea Directivei 95/54/CEE	162
5.2.	Descărcări electrostatice	Respectarea IEC 61000-4-2, $\pm 2\text{kV}$ (nivelul 1)	162
5.3.	Susceptibilitate de conducție tranzitorie pe liniile de alimentare	Pentru versiunile de 24 V: respectarea ISO 7637-2: puls 1a: $V_s = -100\text{ V}$, $R_i = 10\text{ ohmi}$ puls 2: $V_s = +100\text{ V}$, $R_i = 10\text{ ohmi}$ puls 3a: $V_s = -100\text{ V}$, $R_i = 50\text{ ohmi}$ puls 3b: $V_s = +100\text{ V}$, $R_i = 50\text{ ohmi}$ puls 4: $V_s = -16\text{ V}$, $V_a = -12\text{ V}$, $t_6 = 100\text{ ms}$ puls 5: $V_s = +120\text{ V}$, $R_i = 2,2\text{ ohmi}$, $t_d = 250\text{ ms}$ Pentru versiunile de 12 V: respectarea ISO 7637-1: puls 1: $V_s = -100\text{ V}$, $R_i = 10\text{ ohmi}$ puls 2: $V_s = +100\text{ V}$, $R_i = 10\text{ ohmi}$ puls 3a: $V_s = -100\text{ V}$, $R_i = 50\text{ ohmi}$ puls 3b: $V_s = +100\text{ V}$, $R_i = 50\text{ ohmi}$ puls 4: $V_s = -6\text{ V}$, $V_a = -5\text{ V}$, $t_6 = 15\text{ ms}$ puls 5: $V_s = +65\text{ V}$, $R_i = 3\text{ ohmi}$, $t_d = 100\text{ ms}$ Pulsul 5 se testează numai pentru unitățile montate pe vehicule care sunt concepute pentru a fi instalate în vehicule pentru care nu există o protecție externă obișnuită împotriva căderii încărcăturii transportate	162

3. TESTE DE FUNCȚIONARE PENTRU SENZORUL DE MIȘCARE

Nr.	Test	Descriere	Cerințe asociate
1.	Examinare administrativă		
1.1.	Documentație	Corectitudinea documentației	
2.	Inspecție vizuală		
2.1.	Respectarea documentației		
2.2.	Identificare/marcaje		169, 170
2.3.	Materiale		163-167
2.4.	Sigilare		251
3.	Teste de funcționare		
3.1.	Date de identificare a senzorului		077*
3.2.	Cuplarea senzorului de mișcare cu unitatea montată pe vehicul		099*, 155
3.3.	Detectarea mișcării		
	Precizia măsurării mișcării		022-026

Nr.	Test	Descriere	Cerințe asociate
4.	Teste în mediu		
4.1.	Temperatura de funcționare	Se verifică funcționalitatea (conform definiției din testul nr. 3.3) pentru intervalul de temperatură (– 40 °C; + 135 °C) prin: — IEC 68-2-1 test Ad, cu o durată de 96 de ore a testului la temperatura minimă $T_{o_{min}}$ — IEC 68-2-2 test Bd, cu o durată a testului de 96 de ore la temperatura maximă $T_{o_{max}}$	159
4.2.	Cicluri de temperatură	Se verifică funcționalitatea (conform definiției din testul nr. 3.3) prin testul Na IEC 68-2-14, 20 de cicluri, fiecare cu temperatura variind între valoarea minimă (– 40 °C) și cea maximă (+ 135 °C) și 2 ore de menținere la temperatura minimă și apoi la cea maximă Un set redus de teste (din cadrul celor definite la testul 3.3) poate fi efectuat la temperatură minimă, maximă și pe parcursul unor cicluri de temperatură	159
4.3.	Cicluri de umiditate	Se verifică funcționalitatea (conform definiției din testul nr. 3.3) prin testul Db, IEC 68-2-30, prin șase cicluri de câte 24 de ore fiecare, temperatura variind în cadrul fiecărui ciclu între + 25 °C și + 55 °C, la o umiditate relativă de 97 % la + 25 °C și de 93 % la + 55 °C	160
4.4.	Vibrație	Se verifică funcționalitatea (conform definiției din testul nr. 3.3) prin testul Fc IEC 68-2-6, la o durată a testului de 100 de cicluri de frecvență: deplasare constantă între 10 și 57 Hz; valoarea maximă 1,5 mm accelerație constantă între 57 și 500 Hz: 20 g	163
4.5.	Șoc mecanic	Se verifică funcționalitatea (conform definiției din testul nr. 3.3) prin testul Ea IEC 68-2-27, prin 3 șocuri în ambele direcții ale celor 3 axe de referință perpendiculare	163
4.6.	Protecție împotriva apei și corpurilor străine	Se verifică dacă indicele de protecție al senzorului de mișcare, conform IEC 529, este de cel puțin IP 64, atunci când acesta este montat într-un vehicul în condiții de funcționare	165
4.7.	Protecție împotriva inversării de polaritate	Se verifică dacă senzorul de mișcare poate suporta o inversare a polarității la alimentare	161
4.8.	Protecție împotriva scurtcircuitelor	Se verifică dacă semnalele de intrare/ieșire sunt protejate împotriva scurtcircuitelor la sursa de alimentare și la masă	161
5.	Compatibilitate electromagnetică		
5.1.	Emisii de radiații și susceptibilitate de radiații	Respectarea Directivei 95/54/CEE	162
5.2.	Descărcări electrostatice	Respectarea IEC 61000-4-2, ± 2kV (nivelul 1)	162
5.3.	Susceptibilitate de conducție tranzitorie pe liniile de alimentare	Respectarea ISO 7637-3 (nivelul III)	162

4. TESTE DE FUNCȚIONARE PENTRU CARDURILE DE TAHOGRAPH

Nr.	Test	Descriere	Cerințe asociate
1.	Examinare administrativă		
1.1.	Documentație	Corectitudinea documentației	
2.	Inspecție vizuală		
2.1.		Se verifică dacă toate caracteristicile care asigură protecția și datele vizibile sunt tipărite corect pe card și respectate	171-181
3.	Teste fizice		
3.1.		Se verifică dimensiunea cardului și localizarea contactelor	184 ISO/IEC 7816-1 ISO/IEC 7816-2
4.	Teste privind protocoalele		
4.1.	RLR	Se verifică dacă RLR este conform	ISO/IEC 7816-3 TCS 304, 307, 308
4.2.	T = 0	Se verifică dacă protocolul T = 0 este conform	ISO/IEC 7816-3 TCS 302, 303, 305
4.3.	SPT	Se verifică funcționarea comenzii SPT prin setarea valorii T = 1 în locul valorii inițiale T = 0	ISO/IEC 7816-3 TCS 309-311
4.4.	T = 1	Se verifică funcționarea protocolului T = 1	ISO/IEC 7816-3 TCS 303, 306
5.	Structura cardului		
5.1.		Se testează integritatea structurii de fișiere de pe card, verificându-se prezența pe card a fișierelor obligatorii și a condițiilor de acces la aceste fișiere	TCS 312 TCS 400*, 401, 402, 403*, 404, 405*, 406, 407, 408*, 409, 410*, 411, 412, 413*, 414, 415*, 416, 417, 418*, 419
6.	Teste de funcționare		
6.1.	Funcționare normală	Se testează cel puțin o dată utilizarea autorizată a tuturor comenzilor (de exemplu se testează comanda UPDATE BINARY la CLA = «00», CLA = «0C» și la valori diferite ale parametrilor P1, P2 și Lc) Se verifică dacă operațiunile au fost efectuate pe card (de exemplu prin citirea fișierului asupra căruia s-a executat comanda)	TCS 313-TCS 379
6.2.	Mesaje de eroare	Se testează cel puțin o dată fiecare mesaj de eroare (conform anexei 2) pentru fiecare comandă. Se testează cel puțin o dată fiecare eroare generică (cu excepția erorilor de integritate «6400» verificate în cursul certificării de securitate)	
7.	Teste în mediu		
7.1.		Se verifică funcționarea cardurilor în condițiile limită definite în conformitate cu ISO/IEC 10373	185-188 ISO/IEC 7816-1

5. TESTE DE INTEROPERARE

Nr.	Test	Descriere
1.	Autentificare reciprocă	Se verifică dacă autentificarea reciprocă dintre unitatea montată pe vehicul și cardul de tahograf se produce normal
2.	Teste de scriere/citire	Se rulează un scenariu tipic de activitate asupra unității montate pe vehicul. Scenariul este adaptat tipului de card supus testării și implică scrierea pe card într-un număr cât mai mare de fișiere elementare. Se verifică, prin descărcarea informațiilor de pe card, dacă toate înregistrările au fost efectuate corect. Se verifică, prin tipărirea zilnică a informațiilor de pe card, dacă toate înregistrările corespundente pot fi citite în bune condiții.

Apendicele 10

OBIECTIVE GENERALE DE SECURITATE

Prezenta anexă specifică conținutul minim obligatoriu al obiectivelor de securitate privind senzorul de mișcare, unitatea montată pe vehicul și cardul de tahograf.

Pentru a defini obiectivele de securitate pe baza cărora urmează să solicite certificarea securității, producătorii detaliază și completează documentele în funcție de necesități, fără a modifica sau a elimina specificațiile referitoare la pericole, obiective, mijloace procedurale și funcții de garantare a securității.

CUPRINS

Obiectivul general de securitate pentru senzorul de mișcare

1.	Introducere	206
2.	Abrevieri, definiții și trimiteri	206
2.1.	Abrevieri	206
2.2.	Definiții	206
2.3.	Trimiteri	207
3.	Prezentarea produsului	207
3.1.	Descrierea și modul de utilizare a senzorului de mișcare	207
3.2.	Ciclul de viață al senzorului de mișcare	208
3.3.	Pericole	208
3.3.1.	Pericole privind politicile de control al accesului	208
3.3.2.	Pericole privind concepția	209
3.3.3.	Pericole privind funcționarea	209
3.4.	Obiective de securitate	209
3.5.	Obiective de securitate privind tehnologia informației	209
3.6.	Mijloace fizice, de personal sau procedurale	210
3.6.1.	Concepția echipamentului	210
3.6.2.	Livrarea echipamentului	210
3.6.3.	Generarea și furnizarea datelor privind securitatea	210
3.6.4.	Instalarea, calibrarea și inspectarea aparatului de înregistrare	210
3.6.5.	Controlul respectării legii	210
3.6.6.	Perfecționarea	210
4.	Funcții de garantare a securității	210
4.1.	Identificare și autentificare	210
4.2.	Controlul accesului	211
4.2.1.	Politica de control al accesului	211
4.2.2.	Drepturi de acces la date	211
4.2.3.	Structura de fișiere și condiții de acces	211
4.3.	Responsabilitate	211

4.4.	Audit	212
4.5.	Precizie	212
4.5.1.	Politica de control al fluxului de informații	212
4.5.2.	Transferuri interne de date	212
4.5.3.	Integritatea datelor stocate	212
4.6.	Fiabilitatea serviciului	212
4.6.1.	Teste	212
4.6.2.	Software	213
4.6.3.	Protecție fizică	213
4.6.4.	Întreruperi în alimentarea cu energie electrică	213
4.6.5.	Condiții de resetare	213
4.6.6.	Disponibilitatea datelor	213
4.6.7.	Aplicații multiple	213
4.7.	Schimb de date.....	213
4.8.	Suport criptografic	213
5.	Definirea mecanismelor de securitate	214
6.	Protecția minimă oferită de mecanismele de securitate	214
7.	Nivelul de garanție	214
8.	Prezentare.....	214

Obiectivul general de securitate pentru unitatea montată pe vehicul

1.	Introducere	216
2.	Abrevieri, definiții și trimiteri	216
2.1.	Abrevieri	216
2.2.	Definiții.....	216
2.3.	Trimiteri	216
3.	Prezentarea produsului	216
3.1.	Descrierea și modul de utilizare a unității montate pe vehicul	216
3.2.	Ciclul de viață al unității montate pe vehicul	218
3.3.	Pericole	218
3.3.1.	Pericole privind politicile de identificare și de control al accesului	218
3.3.2.	Pericole privind concepția	219
3.3.3.	Pericole privind funcționarea	219
3.4.	Obiective de securitate.....	219
3.5.	Obiective de securitate privind tehnologia informației	220
3.6.	Mijloace fizice, de personal sau procedurale	220
3.6.1.	Proiectarea echipamentului	220
3.6.2.	Livrarea și activarea echipamentului	220

3.6.3.	Generarea și furnizarea datelor privind securitatea	220
3.6.4.	Livrarea cardurilor	221
3.6.5.	Instalarea, calibrarea și inspectarea aparatului de înregistrare	221
3.6.6.	Funcționarea echipamentului	221
3.6.7.	Controlul respectării legii	221
3.6.8.	Perfecționarea software-ului	221
4.	Funcții de garantare a securității	221
4.1.	Identificare și autentificare	221
4.1.1.	Identificarea și autentificarea senzorului de mișcare	221
4.1.2.	Identificarea și autentificarea utilizatorului.....	222
4.1.3.	Identificarea și autentificarea societății conectate la distanță.....	223
4.1.4.	Identificarea și autentificarea dispozitivului de gestionare	223
4.2.	Controlul accesului	223
4.2.1.	Politica de control al accesului	223
4.2.2.	Drepturi de acces la funcții	223
4.2.3.	Drepturi de acces la date	223
4.2.4.	Structura de fișiere și condiții de acces	224
4.3.	Responsabilitate	224
4.4.	Audit.....	224
4.5.	Refolosirea obiectului	225
4.6.	Precizie	225
4.6.1.	Politica de control al fluxului de informații	225
4.6.2.	Transferuri interne de date	225
4.6.3.	Integritatea datelor stocate	225
4.7.	Fiabilitatea serviciului	225
4.7.1.	Teste	225
4.7.2.	Software	226
4.7.3.	Protecție fizică	226
4.7.4.	Întreruperi în alimentare	226
4.7.5.	Condiții de resetare	226
4.7.6.	Disponibilitatea datelor	226
4.7.7.	Aplicații multiple	226
4.8.	Schimb de date.....	226
4.8.1.	Schimbul de date cu senzorul de mișcare	226
4.8.2.	Schimbul de date cu cardurile de tahograf.....	227
4.8.3.	Schimbul de date cu suporturile de memorie externe (funcția descărcare)	227
4.9.	Suport criptografic	227

5.	Definirea mecanismelor de securitate	227
6.	Protecția minimă oferită de mecanismele de securitate	227
7.	Nivelul de garanție	227
8.	Prezentare	228

Obiectivul general de securitate pentru cardul de tahograf

1.	Introducere	232
2.	Abrevieri, definiții și trimiteri	232
2.1.	Abrevieri	232
2.2.	Definiții	232
2.3.	Trimiteri	233
3.	Prezentarea produsului	233
3.1.	Descrierea și modul de utilizare a cardului de tahograf	233
3.2.	Ciclul de viață al cardului de tahograf	233
3.3.	Pericole	234
3.3.1.	Scopuri finale	234
3.3.2.	Căi de atac	234
3.4.	Obiective de securitate	234
3.5.	Obiective de securitate privind tehnologia informației	234
3.6.	Mijloace fizice, de personal sau procedurale	234
4.	Funcții de garantare a securității	235
4.1.	Respectarea profilului de protecție	235
4.2.	Identificarea și autentificarea utilizatorului	235
4.2.1.	Identificarea utilizatorului	235
4.2.2.	Autentificarea utilizatorului	235
4.2.3.	Eșecul autentificării	235
4.3.	Controlul accesului	236
4.3.1.	Politica de control al accesului	236
4.3.2.	Funcții de control al accesului	236
4.4.	Responsabilitate	236
4.5.	Audit	236
4.6.	Precizie	236
4.6.1.	Integritatea datelor stocate	236
4.6.2.	Autentificarea datelor de bază	236
4.7.	Fiabilitatea serviciului	237
4.7.1.	Teste	237
4.7.2.	Software	237
4.7.3.	Alimentarea cu energie electrică	237

4.7.4.	Condiții de resetare	237
4.8.	Schimb de date	237
4.8.1.	Schimbul de date cu unitatea montată pe vehicul	237
4.8.2.	Exportul de date către o unitate exterioară vehiculului (funcția descărcare)	237
4.9.	Suport criptografic	237
5.	Definirea mecanismelor de securitate	237
6.	Nivelul minim solicitat de protecție al mecanismelor	238
7.	Nivelul de garanție	238
8.	Prezentare	238

OBIECTIVUL GENERAL DE SECURITATE PENTRU SENZORUL DE MIȘCARE

1. Introducere

Acest document conține o descriere a senzorului de mișcare, a pericolelor pe care acesta trebuie să le contracareze și a obiectivelor de securitate pe care trebuie să le atingă. Conține și funcțiile obligatorii de garantare a securității. Documentul precizează nivelul de protecție minim solicitat pentru mecanismele de securitate, precum și nivelul minim de garanție pentru dezvoltare și evaluare.

Cerințele menționate în prezentul document sunt cele cuprinse în anexa I B. Pentru a facilita citirea, uneori apare o duplicare a cerințelor din anexa I B și a celor privind obiectivul de securitate. În caz de ambiguitate între o cerință privind un obiectiv de securitate și o cerință din cadrul anexei I B inclusă în obiectivul de securitate respectiv, cerința din cadrul anexei I B are prioritate.

Cerințele din anexa I B cărora nu li se asociază obiective de securitate nu fac obiectul funcțiilor de garantare a securității.

Pericolelor, obiectivelor, mijloacelor procedurale și specificațiilor funcțiilor de garantare a securității le-au fost asociate etichete unice pentru a asigura o mai bună urmărire a lor în cadrul documentației de dezvoltare și de evaluare.

2. Abrevieri, definiții și trimiteri

2.1. Abrevieri

ROM Memorie fixă

SEF Funcție de garantare a securității

TBD De definit

TOE Obiectiv de evaluare

UV Unitate montată pe vehicul

2.2. Definiții

Tahograf digital	Aparat de înregistrare
Dispozitiv periferic	Un dispozitiv conectat la senzorul de mișcare
Date privind mișcarea	Date schimbate cu UV, reprezentând viteza și distanța parcursă
Componente separate fizic	Componente fizice ale senzorului de mișcare distribuite în interiorul vehiculului, spre deosebire de componentele fizice reunite în interiorul carcasei senzorului de mișcare
Date privind securitatea	Date specifice necesare pentru susținerea funcțiilor de garantare a securității (de exemplu cheile criptografice)
Sistem	Echipamentul, persoanele sau organizațiile care interacționează în orice fel cu aparatul de înregistrare
Utilizator	Un utilizator uman al senzorului de mișcare (atunci când nu este folosit în expresia «date privind utilizatorul»)
Date privind utilizatorul	Orice date, diferite de cele referitoare la mișcare și la securitate, înregistrate sau stocate de către senzorul de mișcare.

2.3. Trimiteri

ITSEC Criterii de evaluare a securității în tehnologia informației ITSEC 1991.

3. Prezentarea produsului

3.1. Descrierea și modul de utilizare a senzorului de mișcare

Senzorul de mișcare se instalează în interiorul vehiculelor de transport rutier. Scopul său este să ofere unității montate pe vehicul date protejate privind mișcarea, care să redea viteza vehiculului și distanța parcursă de acesta.

Senzorul de mișcare dispune de o interfață mecanică cu o parte mobilă a vehiculului, a cărei mișcare poate fi reprezentativă pentru viteza vehiculului și distanța parcursă de acesta. Poate fi localizat în cutia de viteze sau în orice altă parte a vehiculului.

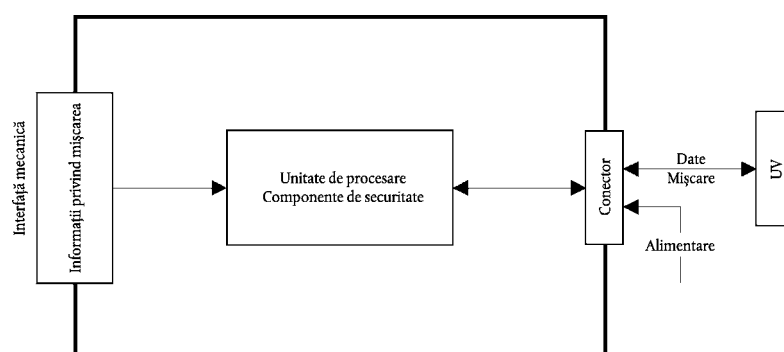
În modul de funcționare, senzorul de mișcare este conectat la o unitate montată pe vehicul.

Poate să fie, de asemenea, conectat la un aparat distinct, în scopuri de gestionare (TBD de către producător).

Figura de mai jos prezintă un senzor de mișcare tipic:

Figura 1

Senzor de mișcare tipic

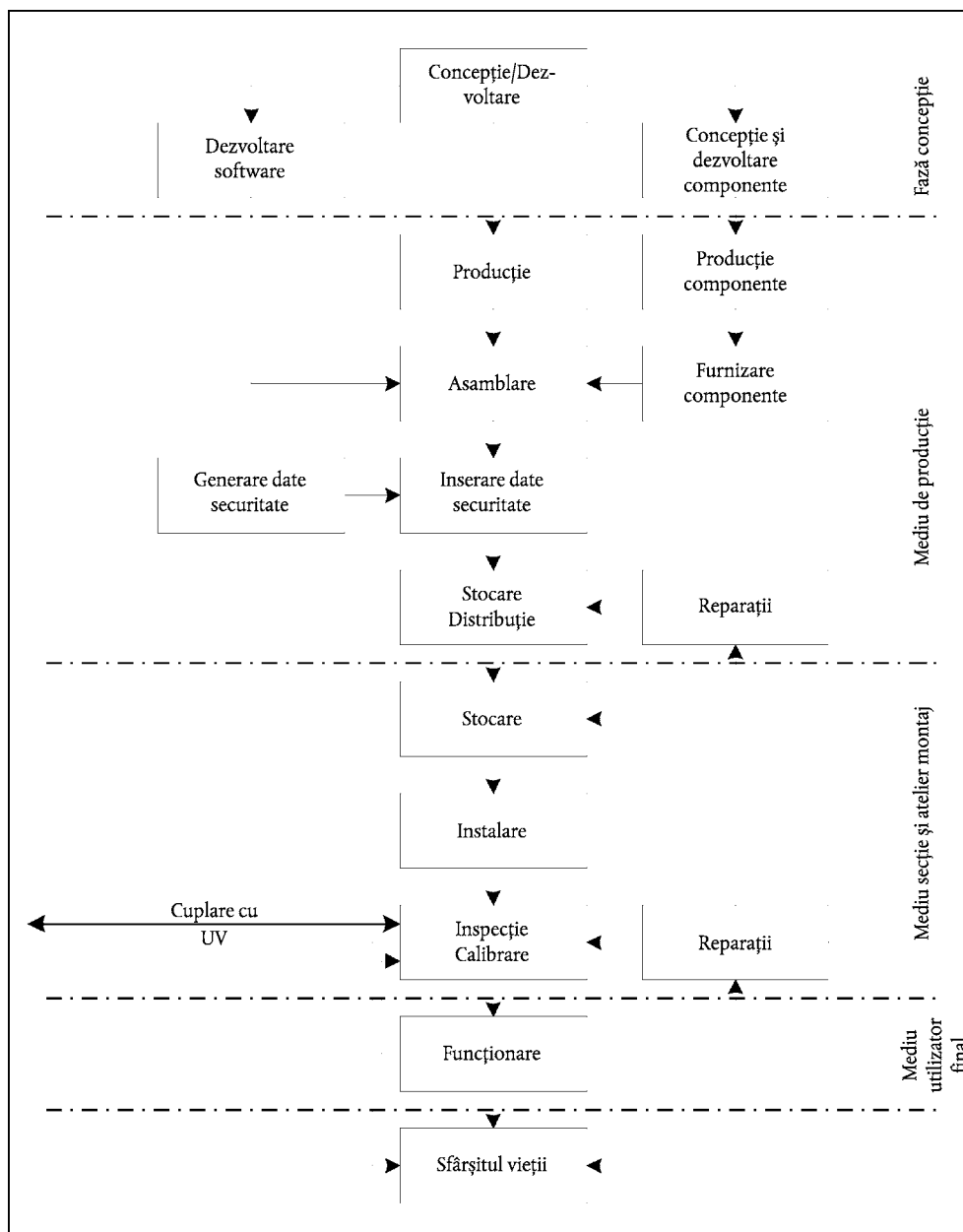


3.2. Ciclul de viață al senzorului de mișcare

Ciclul de viață tipic al senzorului de mișcare este descris în figura următoare:

Figura 2

Ciclul de viață tipic al unui senzor de mișcare



3.3. Pericole

Prezentul punct descrie pericolele cu care se poate confrunta senzorul de mișcare.

3.3.1. Pericole privind politicile de control al accesului

P.Acces Utilizatorii pot încerca să acceseze funcții la care nu le este permis accesul.

3.3.2. Pericole privind concepția

P.Anomalii	Anomaliile care afectează hardware-ul, software-ul și procedurile de comunicare pot plasa senzorul de mișcare în condiții neprevăzute, compromițându-i securitatea
P.Teste	Folosirea unor moduri de testare nevalidate sau a ușilor auxiliare poate compromite securitatea senzorului de mișcare
P.Concepție	Utilizatorii pot încerca să dobândească cunoștințe ilicite privind concepția senzorului, fie pe baza materialelor producătorului (obținute prin furt, mită, ...), fie prin proiectare inversă.

3.3.3. Pericole privind funcționarea

P.Mediu	Utilizatorii pot compromite securitatea senzorului de mișcare, provocând atacuri de mediu (termice, electromagnetice, optice, chimice, mecanice, ...)
P.Hardware	Utilizatorii pot încerca să modifice hardware-ul senzorului de mișcare
P.Origine_Mecanică	Utilizatorii pot încerca să manipuleze dispozitivul de transmitere a datelor către senzorul de mișcare (de exemplu prin deșurubarea de la cutia de viteze, ...)
P.Date_Mișcare	Utilizatorii pot încerca să modifice datele privind mișcarea vehiculului (adăugare, modificare, ștergere, repetare a semnalului)
P.Alimentare	Utilizatorii pot încerca să compromită obiectivele de securitate ale senzorului de mișcare afectând alimentarea acestuia cu energie electrică (prin întrerupere, reducere, creștere a alimentării)
P.Date_Securitate	Utilizatorii pot încerca să dobândească cunoștințe ilicite privind datele de securitate în cursul generării, transmiterii sau stocării datelor de securitate în interiorul aparatului
P.Software	Utilizatorii pot încerca să modifice software-ul senzorului de mișcare
P.Date_Stocate	Utilizatorii pot încerca să modifice datele stocate (privind securitatea sau utilizatorul).

3.4. Obiective de securitate

Principalul obiectiv de securitate al sistemului tahografului digital este următorul:

O.Principal	Datele care urmează să fie verificate de către autoritățile de control trebuie să fie disponibile și să reflecte integral și cu precizie activitățile șoferilor și ale vehiculelor, controlate din punctul de vedere al conducerii, al activității, disponibilității și perioadelor de repaus, precum și din punctul de vedere al vitezei vehiculului
-------------	---

În consecință, obiectivul de securitate al senzorului de mișcare, care contribuie la obiectivul de securitate global, este:

O.Senzor_Principal	Datele transmise de senzorul de mișcare trebuie să fie disponibile pentru unitatea montată pe vehicul, astfel încât să îi permită acestuia din urmă să determine cu precizie întreaga deplasare a vehiculului, din punctul de vedere al vitezei și distanței parcurse.
--------------------	--

3.5. Obiective de securitate privind tehnologia informației

Obiectivele de securitate ale senzorului de mișcare, legate de tehnologia informației și care contribuie la obiectivul său principal de securitate, sunt următoarele:

O.Acces	Senzorul de mișcare trebuie să controleze accesul dispozitivelor conectate la funcții și date
O.Audit	Senzorul de mișcare trebuie să auditeze încercările de subminare a securității sale și să le urmărească în relație cu dispozitivele asociate
O.Autentificare	Senzorul de mișcare trebuie să autentifice dispozitivele conectate

O.Procesare	Senzorul de mișcare trebuie să garanteze faptul că procesarea datelor de intrare, pe baza cărora sunt generate datele privind mișcarea, este corectă
O.Fiabilitate	Senzorul de mișcare trebuie să ofere un serviciu fiabil
O.Schimb _Protejat_Date	Senzorul de mișcare trebuie să protejeze schimburile de date cu unitatea montată pe vehicul.

3.6. **Mijloace fizice, de personal sau procedurale**

Prezentul punct descrie cerințele fizice, de personal sau procedurale care contribuie la securitatea senzorului de mișcare.

3.6.1. *Concepția echipamentului*

M.Proiectare	Proiectanții senzorului de mișcare trebuie să se asigure că repartizarea responsabilităților în timpul fazei de proiectare se face cu respectarea securității IT
M.Producție	Producătorii senzorului de mișcare trebuie să se asigure că repartizarea responsabilităților în timpul fazei de producție se face cu respectarea securității IT și că în timpul procesului de producție senzorul de mișcare este protejat împotriva atacurilor fizice care ar putea compromite securitatea IT.

3.6.2. *Livrarea echipamentului*

M.Livrare	Producătorii senzorului de mișcare, producătorii vehiculelor și secțiile sau atelierele de montaj trebuie să se asigure că senzorul de mișcare este manipulat într-un mod care nu îi afectează securitatea IT.
-----------	--

3.6.3. *Generarea și furnizarea datelor privind securitatea*

M.Generare_Date_Sec	Algoritmii de generare a datelor privind securitatea trebuie să fie accesibili numai persoanelor autorizate și de încredere
M.Transmitere_Date_Sec	Datele privind securitatea trebuie să fie generate, transmise și introduse în senzorul de mișcare astfel încât să nu le fie afectate confidențialitatea și integritatea.

3.6.4. *Instalarea, calibrarea și inspectarea aparatului de înregistrare*

M.Ateliere_Agreate	Instalarea, calibrarea și repararea aparatului de înregistrare trebuie efectuate de secții sau ateliere de montaj de încredere și agreate
M.Interfață_Mecanică	Trebuie asigurate mijloace de detectare a alterării fizice a interfeței mecanice (de exemplu sigilii)
M.Inspecții_Periodice	Aparatul de înregistrare trebuie să fie periodic inspectat și calibrat.

3.6.5. *Controlul respectării legii*

M.Controale	Controalele respectării legii se fac atât periodic, cât și inopinat și trebuie să includă audituri ale securității.
-------------	---

3.6.6. *Perfecționarea software-ului*

M.Perfecționare_Software	Modificările software-ului trebuie certificate din punctul de vedere al securității înainte de a putea fi implementate într-un senzor de mișcare.
--------------------------	---

4. **Funcții de garantare a securității**

4.1. **Identificare și autentificare**

UIA_101	Senzorul de mișcare este capabil să stabilească, în cursul fiecărei interacțiuni, identitatea perifericului la care este conectat.
---------	--

UIA_102 Identitatea unui periferic conectat poate fi:

- un grup de periferice:
- unitatea montată pe vehicul;
- un dispozitiv de gestionare;
- altul;
- un ID de dispozitiv (numai pentru UV).

UIA_103 ID-ul de dispozitiv al unei UV conectate este compus din numărul de omologare UV și numărul de serie UV.

UIA_104 Senzorul de mișcare este capabil să autentifice orice UV sau dispozitiv de gestionare la care este conectat:

- în momentul conectării cu dispozitivul respectiv;
- la reluarea alimentării.

UIA_105 Senzorul de mișcare este capabil să reautentifice periodic orice UV la care este conectat.

UIA_106 Senzorul de mișcare detectează și împiedică folosirea datelor de autentificare care au fost copiate și repetate.

UIA_107 După detectarea unui număr (TBD de către producător și care să nu depășească 20) de încercări consecutive de autentificare eșuate, funcția de garantare a securității procedează astfel:

- generează o înregistrare de audit a evenimentului;
- avertizează perifericul;
- continuă să exporte într-un mod neprotejat date privind mișcarea.

4.2. Controlul accesului

Controalele accesului garantează faptul că informația este citită, creată și modificată în cadrul obiectivului de evaluare numai de către persoanele autorizate.

4.2.1. Politica de control al accesului

ACC_101 Senzorul de mișcare controlează drepturile de acces la funcții și date.

4.2.2. Drepturi de acces la date

ACC_102 Senzorul de mișcare garantează faptul că datele sale de identificare pot fi scrise o singură dată (cerința 078).

ACC_103 Senzorul de mișcare acceptă și/sau stochează date privind utilizatorul provenite numai de la dispozitive autentificate.

ACC_104 Senzorul de mișcare garantează drepturi adecvate de acces de scriere și citire la datele privind securitatea.

4.2.3. Structura de fișiere și condiții de acces

ACC_105 Structura fișierelor aplicației și a fișierelor de date, precum și condițiile de acces sunt create în timpul procesului de producție, după care este blocată orice modificare sau ștergere a acestora.

4.3. Responsabilitate

ACT_101 Senzorul de mișcare păstrează în memorie datele sale de identificare (cerința 077).

ACT_102 Senzorul de mișcare păstrează în memorie datele de instalare (cerința 099).

ACT_103 Senzorul de mișcare are capacitatea de a produce date de ieșire privind responsabilitatea, pe care să le pună la dispoziția dispozitivelor autentificate, la cererea acestora.

4.4. **Audit**

AUD_101 În cazul evenimentelor care îi afectează securitatea, senzorul de mișcare generează înregistrări de audit ale evenimentelor respective.

AUD_102 Evenimentele care afectează securitatea senzorului de mișcare sunt următoarele:

- încercări de încălcare a securității;
- eșecuri de autentificare;
- erori care afectează integritatea datelor stocate;
- erori privind transferul intern de date;
- deschiderea neautorizată a carcasei;
- sabotarea hardware-ului;
- anomalia senzorului.

AUD_103 Înregistrările de audit includ următoarele date:

- data și ora evenimentului;
- tipul evenimentului;
- identitatea dispozitivului periferic conectat.

dacă datele solicitate nu sunt disponibile, este furnizată o indicație prestabilită adecvată (TBD de către producător).

AUD_104 Senzorul de mișcare trimite unității montate pe vehicul înregistrările de audit generate în momentul producerii lor, putând, de asemenea, să le stocheze în memorie.

AUD_105 În cazul în care memorează înregistrări de audit, senzorul de mișcare păstrează în memorie 20 de înregistrări de audit independent de epuizarea spațiului de stocare alocat acestora și are capacitatea de a transmite înregistrările de audit stocate către perifericele autorizate, la cererea perifericelor respective.

4.5. **Precizie**

4.5.1. *Politica de control al fluxului de informații*

ACR_101 Senzorul de mișcare garantează faptul că datele privind mișcarea pot fi procesate și derivate numai din punctele de contact ale senzorului cu periferice mecanice.

4.5.2. *Transferuri interne de date*

Cerințele enunțate în acest paragraf sunt valabile numai dacă senzorul de mișcare utilizează componente separate fizic.

ACR_102 Dacă au loc transferuri de date între componentele separate fizic ale senzorului de mișcare, datele trebuie protejate împotriva modificărilor.

ACR_103 La detectarea unei erori de transfer de date în cursul unui transfer intern, transmisia se repetă, iar funcția de garantare a securității generează o înregistrare de audit a evenimentului.

4.5.3. *Integritatea datelor stocate*

ACR_104 Senzorul de mișcare verifică datele privind utilizatorul stocate în memorie, pentru a detecta eventualele erori de integritate.

ACR_105 La detectarea unei erori de integritate a datelor privind utilizatorul, funcția de garantare a securității generează o înregistrare de audit a evenimentului.

4.6. **Fiabilitatea serviciului**

4.6.1. *Teste*

RLB_101 Toate comenzile, acțiunile sau punctele de testare, corespunzătoare nevoilor de testare din faza de producție, sunt dezactivate sau eliminate înaintea finalizării fazei de producție. Nu mai pot fi reintroduse în vederea utilizării ulterioare.

RLB_102 Senzorul de mișcare rulează autoteste în momentul primei puneri în funcțiune, precum și în cursul funcționării normale, pentru a-și verifica funcționarea corectă. Autotestele efectuate de senzorul de mișcare includ verificarea integrității datelor privind securitatea, precum și verificarea integrității codului executabilelor stocate (dacă nu sunt în ROM).

RLB_103 La detectarea unei anomalii interne în cursul unui autotest, funcția de garantare a securității generează o înregistrare de audit (anomalie senzor).

4.6.2. Software

RLB_104 Nu există nici un mod de analizare sau de depanare a software-ului senzorului de mișcare în condiții de teren.

RLB_105 Datele preluate din surse externe ca date de intrare nu sunt acceptate drept cod executabil.

4.6.3. Protecție fizică

RLB_106 Dacă este conceput astfel încât să poată fi deschis, senzorul de mișcare detectează orice deschidere a carcasei sale, chiar și atunci când alimentarea sa este întreruptă, timp de minimum 6 luni. Într-un astfel de caz, funcția de garantare a securității generează o înregistrare de audit a evenimentului (se acceptă ca înregistrarea de audit să fie generată și stocată după reluarea alimentării).

Dacă este conceput astfel încât să nu poată fi deschis, senzorul de mișcare trebuie să permită detectarea cu ușurință a tuturor încercărilor de avariere fizică (de exemplu prin inspecție vizuală).

RLB_107 Senzorul de mișcare detectează aspecte precise privind sabotarea hardware-ului (TBD de către producător).

RLB_108 În cazul anterior, funcția de garantare a securității generează o înregistrare de audit a evenimentului, iar senzorul de mișcare acționează astfel: (TBD de către producător).

4.6.4. Întreruperi în alimentarea cu energie electrică

RLB_109 Senzorul de mișcare se menține stabil în timpul întreruperilor sau variațiilor de alimentare.

4.6.5. Condiții de resetare

RLB_110 În cazul unei întreruperi în alimentare, dacă o tranzacție este întreruptă înaintea finalizării sau a oricăror alte condiții de resetare, senzorul de mișcare este resetat fără a suferi defecțiuni.

4.6.6. Disponibilitatea datelor

RLB_111 Senzorul de mișcare garantează faptul că accesul la resurse este asigurat oricând este necesar și că resursele nu sunt solicitate sau reținute inutil.

4.6.7. Aplicații multiple

RLB_112 Dacă senzorul de mișcare include aplicații diferite de cea pentru tahograf, toate aplicațiile sunt separate fizic și/sau logic. Aceste aplicații nu partajează date de securitate. O singură sarcină este activă o dată.

4.7. Schimb de date

DEX_101 Senzorul de mișcare exportă către unitatea montată pe vehicul date privind mișcarea împreună cu atributele de securitate ale acestora, astfel încât UV să le poată verifica integritatea și autenticitatea.

4.8. Suport criptografic

Cerințele enunțate în acest paragraf sunt aplicabile numai acolo unde este cazul, în funcție de mecanismele de securitate utilizate și de soluțiile producătorului.

CSP_101 Orice operație criptografică efectuată de senzorul de mișcare respectă un algoritm și o dimensiune a cheii specificate.

CSP_102 Dacă senzorul de mișcare generează chei criptografice, acest lucru se realizează în conformitate cu algoritmi de generare a cheilor criptografice preciși și cu dimensiuni precise ale cheilor criptografice.

CSP_103 Dacă senzorul de mișcare distribuie chei criptografice, acest lucru se realizează în conformitate cu metode precise de distribuție a cheilor criptografice.

CSP_104 Dacă senzorul de mișcare accesează chei criptografice, acest lucru se realizează în conformitate cu metode precise de accesare a cheilor criptografice.

CSP_105 Dacă senzorul de mișcare distruge chei criptografice, acest lucru se realizează în conformitate cu metode precise de distrugere a cheilor criptografice.

5. Definirea mecanismelor de securitate

Mecanismele de securitate, care îndeplinesc funcțiile de garantare a securității pentru senzorul de mișcare, sunt definite de către producătorii acestuia.

6. Protecția minimă oferită de mecanismele de securitate

Protecția minimă oferită de mecanismele de securitate are valoarea Ridicăta, conform definiției (ITSEC).

7. Nivelul de garanție

Nivelul-țintă de garanție pentru senzorul de mișcare este nivelul E3 ITSEC, conform definiției (ITSEC).

8. Prezentare

Următoarele matrici oferă o prezentare a funcțiilor de garantare a securității, precizând:

- ce pericole sunt contracarate de fiecare funcție sau mijloc de garantare a securității;
- ce obiective de securitate privind tehnologia informației sunt protejate de fiecare funcție de garantare a securității.

	Pericole													Obiective IT				
	Acces	Anomalii	Teste	Concepție	Mediu	Hardware	Origine_Mecanică	Date_Mișcare	Alimentare_energie	Date_Securitate	Software	Date_Stocate	Acces	Audit	Autentificare	Procesare	Fiabilitate	Schimb_Protejat_Date
Mijloace fizice, de personal sau procedurale																		
Dezvoltare		x	x	x														
Producție			x	x														
Livrare						x					x	x						
Generarea datelor privind securitatea										x								
Transferul datelor privind securitatea										x								
Ateliere agreate							x											
Interfață mecanică							x											
Inspecție periodică						x	x		x		x							
Controlul respectării legii					x	x	x		x	x	x							
Perfecționarea software-ului											x							
Funcții de garantare a securității																		
Identificare și autentificare																		
UIA_101 Identificare dispozitive	x							x					x		x			x
UIA_102 Identitate dispozitive	x												x		x			
UIA_103 Identitate UV														x				
UIA_104 Autentificare dispozitive	x							x					x		x			x
UIA_105 Reautentificare	x							x					x		x			x
UIA_106 Autentificare nefalsificabilă	x							x					x		x			
UIA_107 Eșec autentificare								x						x			x	
Controlul accesului																		
ACC_101 Politică de control acces	x									x		x	x					
ACC_102 ID senzor de mișcare												x	x					

OBIECTIVUL GENERAL DE SECURITATE PENTRU UNITATEA MONTATĂ PE VEHICUL

1. Introducere

Acest document conține o descriere a unității montate pe vehicul, a pericolelor pe care aceasta trebuie să le contracareze și a obiectivelor de securitate pe care trebuie să le atingă. Conține și funcțiile obligatorii de garantare a securității. Documentul precizează nivelul de protecție minim solicitat pentru mecanismele de securitate, precum și nivelul minim de garanție pentru dezvoltare și evaluare.

Cerințele menționate în prezentul document sunt cele cuprinse în anexa I B. Pentru a facilita citirea, uneori apare o duplicare a cerințelor din anexa I B și a celor privind obiectivul de securitate. În caz de ambiguitate între o cerință privind un obiectiv de securitate și o cerință din cadrul anexei I B cuprinsă în cerința privind obiectivul de securitate respectiv, cerința din cadrul anexei I B are prioritate.

Cerințele din cuprinsul anexei I B cărora nu li se asociază obiective de securitate nu fac obiectul funcțiilor de garantare a securității.

Pericolelor, obiectivelor, mijloacelor procedurale și specificațiilor funcțiilor de garantare a securității le-au fost asociate etichete unice pentru a asigura o mai bună urmărire a lor în cuprinsul documentației de dezvoltare și evaluare.

2. Abrevieri, definiții și trimiteri

2.1. Abrevieri

PIN	Număr de identificare personal
ROM	Memorie fixă
SEF	Funcție de garantare a securității
TBD	De definit
TOE	Obiectiv de evaluare
UV	Unitate montată pe vehicul

2.2. Definiții

Tahograf digital	Aparat de înregistrare
Date privind mișcarea	Date schimbate cu senzorul de mișcare, reprezentând viteza și distanța parcursă
Componente separate fizic	Componente fizice ale unității montate pe vehicul, distribuite în interiorul vehiculului, spre deosebire de componentele fizice reunite în interiorul carcasei unității montate pe vehicul
Date privind securitatea	Date specifice necesare pentru susținerea funcțiilor de garantare a securității (de exemplu cheile criptografice)
Sistem	Echipamentul, persoanele sau organizațiile care interacționează în orice fel cu aparatul de înregistrare
Utilizator	Un utilizator uman al aparatului. Utilizatorii normali ai unității montate pe vehicul sunt șoferii, controlorii, atelierile și societățile.
Date privind utilizatorul	Orice date, diferite de cele referitoare la securitate, înregistrate sau stocate de către unitatea montată pe vehicul, necesare în conformitate cu capitolul III punctul 12.

2.3. Trimiteri

ITSEC Criterii de evaluare a securității în tehnologia informației ITSEC 1991.

3. Prezentarea produsului

3.1. Descrierea și modul de utilizare a unității montate pe vehicul

Unitatea montată pe vehicul se instalează în interiorul vehiculelor de transport rutier. Scopul său este să înregistreze, să stocheze, să afișeze, să tipărească și să furnizeze date privind activitățile șoferului.

Este conectată la un senzor de mișcare cu care schimbă date privind mișcarea vehiculului.

Utilizatorii se identifică la unitatea montată pe vehicul folosind carduri de tahograf.

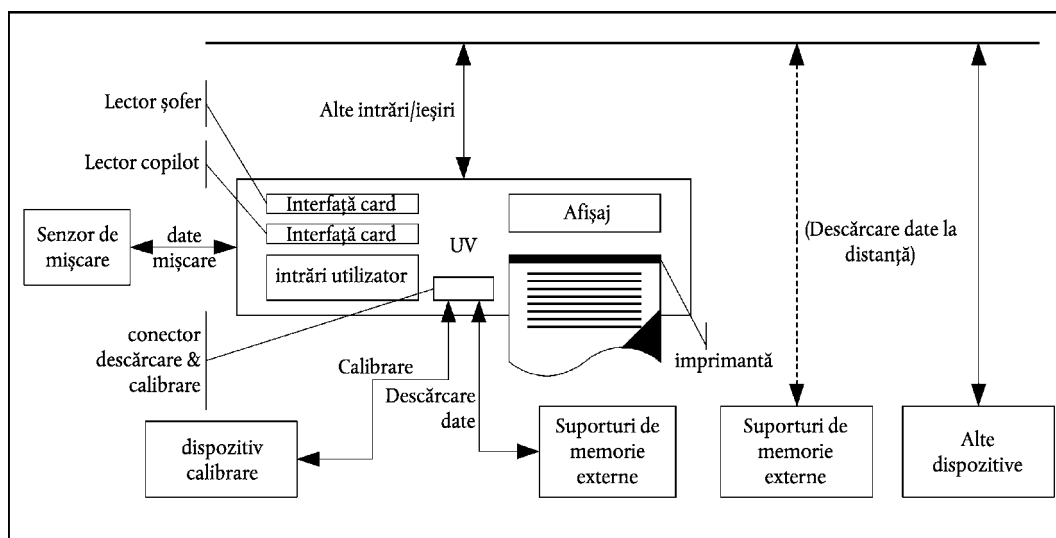
Unitatea montată pe vehicul înregistrează și stochează date privind activitățile utilizatorilor atât în memoria sa de date, cât și pe cardurile de tahograf.

Unitatea montată pe vehicul produce date de ieșire care pot fi vizualizate, tipărite sau preluate de dispozitive exterioare.

Figura de mai jos prezintă mediul de funcționare al unității montate pe vehicul, atunci când aceasta este instalată într-un vehicul:

Figura 1

Mediul de funcționare al unității montate pe vehicul



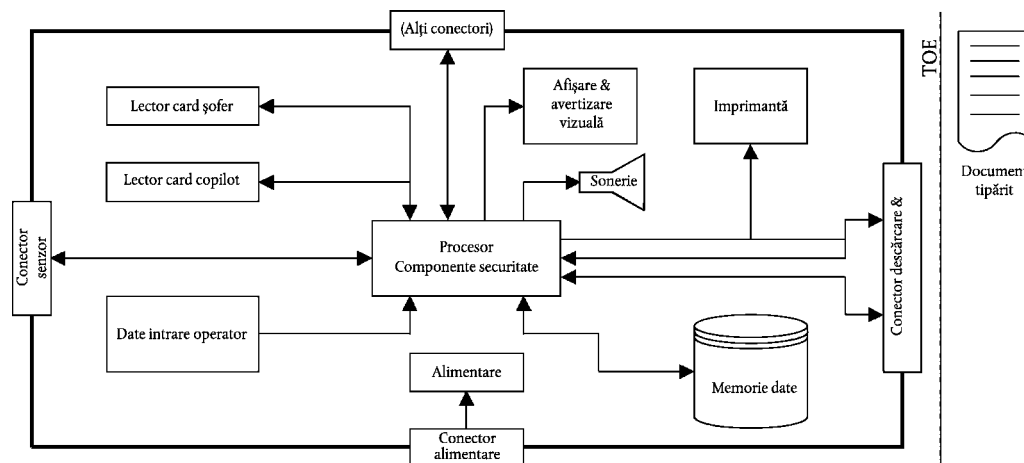
Caracteristicile generale, funcțiile și modul de funcționare ale unității montate pe vehicul sunt descrise în capitolul II din anexa I B.

Cerințele funcționale ale unității montate pe vehicul sunt specificate în capitolul III din anexa I B.

Figura de mai jos prezintă o unitate montată pe vehicul tipică:

Figura 2

Unitate montată pe vehicul tipică (...) opțional



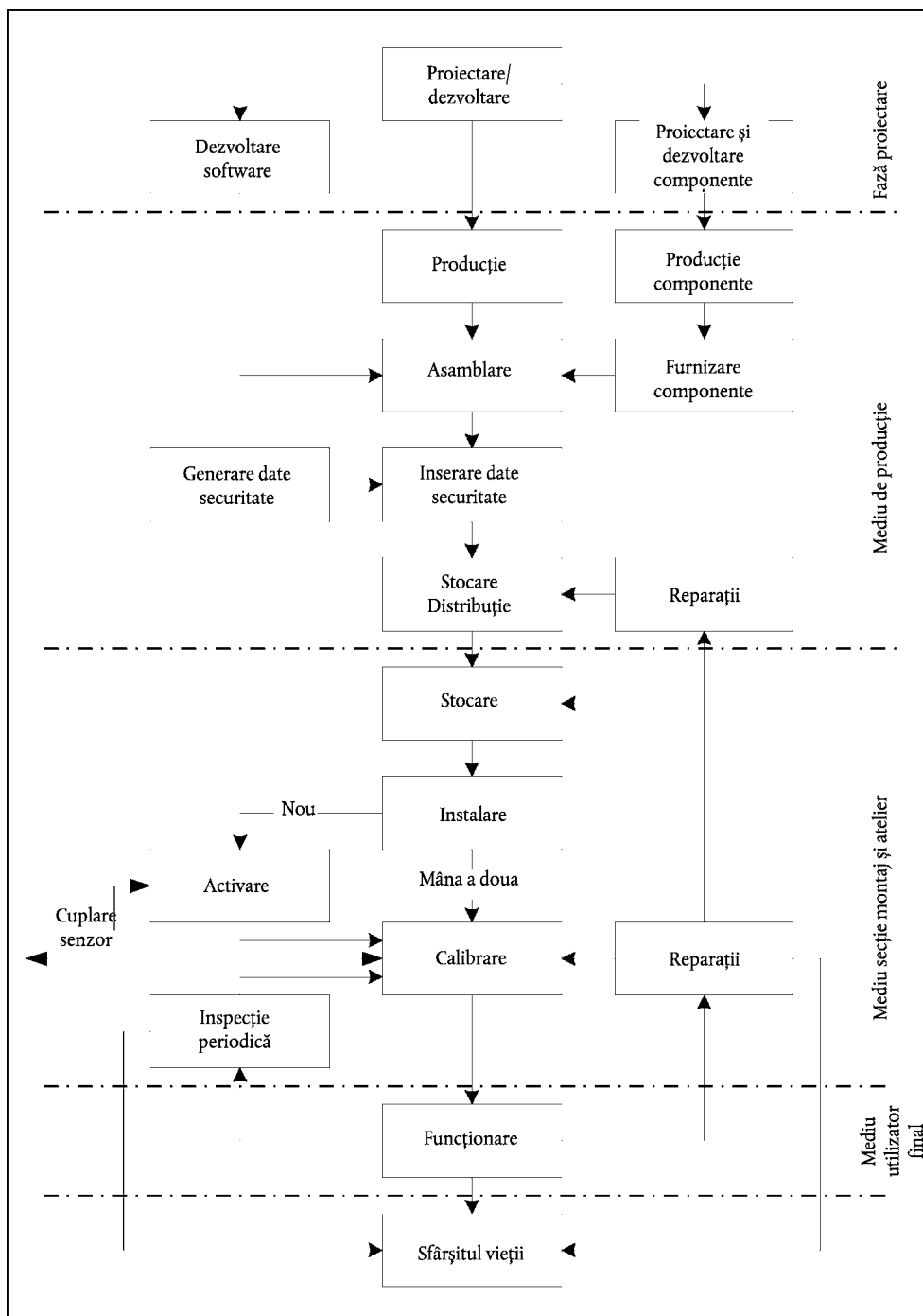
Se remarcă faptul că, deși mecanismul imprimantei face parte din TOE, documentul, odată tipărit, nu mai face parte din TOE.

3.2. Ciclul de viață al unității montate pe vehicul

Ciclul de viață tipic al unității montate pe vehicul este descris în figura următoare:

Figura 3

Ciclul de viață tipic al unei unități montate pe vehicul



3.3. Pericole

Acest paragraf descrie pericolele cu care se poate confrunta unitatea montată pe vehicul.

3.3.1. Pericole privind politicile de identificare și de control al accesului

- P.Acces Utilizatorii pot încerca să acceseze funcții nepermise (de exemplu șoferii pot încerca să acceseze funcția de calibrare)
- P.Identificare Utilizatorii pot încerca să folosească mai multe identificări sau nici o identificare.

3.3.2. *Pericole privind concepția*

P.Anomalii	Anomaliile care afectează hardware-ul, software-ul și procedurile de comunicare pot plasa unitatea montată pe vehicul în condiții neprevăzute, compromițându-i securitatea
P.Teste	Folosirea unor moduri de testare nevalidate sau a ușilelor auxiliare poate compromite securitatea unității montate pe vehicul
P.Proiectare	Utilizatorii pot încerca să dobândească cunoștințe ilicite privind concepția unității montate pe vehicul, fie pe baza materialelor producătorului (obținute prin furt, mită, ...), fie prin proiectare inversă.

3.3.3. *Pericole privind funcționarea*

P.Parametri_Calibrare	Utilizatorii pot încerca să utilizeze aparatură calibrată greșit (prin modificarea datelor de calibrare sau speculând slăbiciunile organizației)
P.Schimb_Date_Card	Utilizatorii pot încerca să modifice datele, atunci când acestea sunt schimbate între UV și cardurile de tahograf (prin adăugare, modificare, ștergere, repetarea semnalului)
P.Ceas	Utilizatorii pot încerca să modifice ceasul intern
P.Mediu	Utilizatorii pot compromite securitatea unității montate pe vehicul provocând atacuri de mediu (termice, electromagnetice, optice, chimice, mecanice, ...)
P.Dispozitive_Fictive	Utilizatorii pot încerca să conecteze la UV dispozitive fictive (senzor de mișcare, carduri cu memorie)
P.Hardware	Utilizatorii pot încerca să modifice hardware-ul unității montate pe vehicul
P.Date_Mișcare	Utilizatorii pot încerca să modifice datele privind mișcarea vehiculului (prin adăugare, modificare, ștergere, repetarea semnalului)
P.Neactivat	Utilizatorii pot folosi aparatură neactivată
P.Date_Ieșire	Utilizatorii pot încerca să modifice datele de ieșire (tipărite, afișate sau descărcate)
P.Alimentare	Utilizatorii pot încerca să compromită obiectivele de securitate ale unității montate pe vehicul afectând alimentarea acestora cu energie electrică (prin întrerupere, reducere, creștere a alimentării)
P.Date_Securitate	Utilizatorii pot încerca să dobândească cunoștințe ilicite privind datele de securitate în cursul generării, transmiterii sau stocării datelor de securitate în interiorul aparatului
P.Software	Utilizatorii pot încerca să modifice software-ul unității montate pe vehicul
P.Date_Stocate	Utilizatorii pot încerca să modifice datele stocate (privind securitatea sau utilizatorul).

3.4. **Obiective de securitate**

Principalul obiectiv de securitate al sistemului tahografului digital este următorul:

O.Principal	Datele care urmează să fie verificate de către autoritățile de control trebuie să fie disponibile și să reflecte integral și cu precizie activitățile șoferilor și ale vehiculelor, controlate din punctul de vedere al conducerii, activității, disponibilității și perioadelor de odihnă, precum și din punctul de vedere al vitezei vehiculului.
-------------	---

În consecință, obiectivele de securitate ale unității montate pe vehicul, care contribuie la obiectivul de securitate global, sunt:

O.UV_Principal	Datele care urmează să fie măsurate și înregistrate, iar apoi verificate de autoritățile de control trebuie să fie disponibile și să reflecte fidel activitățile șoferilor și ale vehiculelor, controlate din punctul de vedere al conducerii, activității, perioadelor de odihnă, precum și din punctul de vedere al vitezei vehiculului
O.UV_Export	Unitatea montată pe vehicul trebuie să poată exporta date către suporturi de memorie externe într-un mod care să permită verificarea integrității și autenticității datelor respective.

3.5. Obiective de securitate privind tehnologia informației

Obiectivele de securitate ale unității montate pe vehicul, legate de tehnologia informației și care contribuie la obiectivele sale principale de securitate, sunt următoarele:

O.Acces	Unitatea montată pe vehicul trebuie să controleze accesul utilizatorilor la funcții și date
O.Responsabilitate	Unitatea montată pe vehicul trebuie să colecteze date corecte privind responsabilitatea
O.Audit	Unitatea montată pe vehicul trebuie să auditeze încercările de subminare a securității sistemului și să le coreleze cu utilizatorii implicați
O.Autentificare	Unitatea montată pe vehicul trebuie să autentifice utilizatorii și dispozitivele conectate (atunci când e necesară stabilirea unei căi de încredere între dispozitive)
O.Integritate	Unitatea montată pe vehicul trebuie să mențină integritatea datelor stocate
O.Ieșire	Unitatea montată pe vehicul trebuie să garanteze faptul că datele finale produse reflectă fidel datele măsurate sau stocate
O.Procesare	Unitatea montată pe vehicul trebuie să garanteze faptul că procesarea datelor de intrare, pe baza cărora sunt generate datele privind utilizatorul, este corectă
O.Fiabilitate	Unitatea montată pe vehicul trebuie să ofere un serviciu fiabil
O.Schimb_Protejat_Date	Unitatea montată pe vehicul trebuie să protejeze schimburile de date cu senzorul de mișcare și cu cardurile de tahograf.

3.6. Mijloace fizice, de personal sau procedurale

Prezentul punct descrie cerințele fizice, de personal sau procedurale care contribuie la securitatea unității montate pe vehicul.

3.6.1. Proiectarea echipamentului

M.Dezvoltare	Proiectanții unității montate pe vehicul trebuie să se asigure că repartizarea responsabilităților în timpul fazei de proiectare se face cu respectarea securității IT
M.Producție	Producătorii unității montate pe vehicul trebuie să se asigure că repartizarea responsabilităților în timpul fazei de producție se face cu respectarea securității IT și că în timpul procesului de producție unitatea montată pe vehicul este protejată împotriva atacurilor fizice care ar putea compromite securitatea IT.

3.6.2. Livrarea și activarea echipamentului

M.Livrare	Producătorii unității montate pe vehicul, producătorii vehiculelor și secțiile sau atelierele de montaj trebuie să se asigure că unitățile neactivate sunt manipulate într-un mod care nu le afectează securitatea IT.
M.Activare	Producătorii vehiculelor și secțiile sau atelierele de montaj trebuie să activeze unitatea după instalarea acesteia și înainte ca vehiculul să părăsească locul unde s-a făcut instalarea.

3.6.3. Generarea și furnizarea datelor privind securitatea

M.Generare_Date_Sec	Algoritmii de generare a datelor privind securitatea trebuie să fie accesibili numai persoanelor autorizate și de încredere
M.Transmitere_Date_Sec	Datele privind securitatea trebuie să fie generate, transmise și introduse în unitatea montată pe vehicul, astfel încât să nu le fie afectate confidențialitatea și integritatea.

3.6.4. *Livrarea cardurilor*

M.Disponibilitate_Card	Cardurile de tahograf trebuie să fie disponibile și să fie livrate numai persoanelor autorizate
M.Unicitate_Card_Șofer	Șoferii trebuie să posede un singur card de șofer valabil.
M.Urmărire_Card	Livrarea cardurilor trebuie să poată fi urmărită (prin liste albe, liste negre), iar listele negre trebuie folosite în cadrul auditurilor de securitate.

3.6.5. *Instalarea, calibrarea și inspectarea aparatului de înregistrare*

M.Ateliere_Agreate	Instalarea, calibrarea și repararea aparatului de înregistrare trebuie efectuate de secții sau ateliere de montaj de încredere și agreate
M.Inspecții_Periodice	Aparatul de înregistrare trebuie să fie periodic inspectat și calibrat
M.Calibrare_Corectă	Secțiile sau atelierele de montaj agreate trebuie să introducă în aparatul de înregistrare parametrii corecți ai vehiculului în timpul calibrării.

3.6.6. *Funcționarea echipamentului*

M.Șoferi_Responsabili	Șoferii trebuie să respecte regulile și să se comporte responsabil (de exemplu să utilizeze cardurile personale de șofer, să selecteze corect activitatea în cazul activităților selectate manual,...).
-----------------------	---

3.6.7. *Controlul respectării legii*

M.Controale	Controalele respectării legii se fac atât periodic, cât și inopinat și trebuie să includă audituri ale securității.
-------------	---

3.6.8. *Perfecționarea software-ului*

M.Perfecționare_Software	Modificările software-ului trebuie certificate din punctul de vedere al securității înainte de a putea fi implementate într-o unitate montată pe vehicul.
--------------------------	---

4. **Funcții de garantare a securității**

4.1. *Identificare și autentificare*

4.1.1. *Identificarea și autentificarea senzorului de mișcare*

UIA_201 Unitatea montată pe vehicul este capabilă să stabilească, în cursul fiecărei interacțiuni, identitatea senzorului de mișcare la care este conectată.

UIA_202 Identitatea senzorului de mișcare cuprinde numărul de omologare și numărul de serie ale senzorului.

UIA_203 Unitatea montată pe vehicul autentifică senzorul de mișcare la care este conectată:

- în momentul conectării la senzorul de mișcare;
- la fiecare calibrare a aparatului de înregistrare;
- la reluarea alimentării.

Autentificarea este reciprocă și inițiată de UV.

UIA_204 Unitatea montată pe vehicul reidentifică și reautentifică periodic (la intervale TBD de către producător și de mai multe ori pe oră) senzorul de mișcare la care este conectată și garantează faptul că senzorul de mișcare identificat în cursul ultimei calibrări a aparatului de înregistrare nu a fost schimbat.

UIA_205 Unitatea montată pe vehicul detectează și împiedică folosirea datelor de autentificare care au fost copiate și repetate.

UIA_206 După detectarea unui număr (TBD de către producător și care să nu depășească 20) de încercări de autentificare consecutive eșuate și/sau după detectarea modificării neautorizate a identității senzorului de mișcare (de exemplu nu în cursul calibrării aparatului de înregistrare) funcția de garantare a securității procedează astfel:

- generează o înregistrare de audit a evenimentului;
- atenționează utilizatorul;
- continuă să accepte și să utilizeze date neprotejate privind mișcarea, trimise de senzorul de mișcare.

4.1.2. Identificarea și autentificarea utilizatorului

UIA_207 Unitatea montată pe vehicul detectează permanent și selectiv identitatea a doi utilizatori, prin monitorizarea cardurilor de tahograf inserate în lectorul șoferului și, respectiv, cel al copilotului.

UIA_208 Identitatea utilizatorului este:

- un grup de utilizatori:
 - ȘOFER (cardul șoferului)
 - CONTROLOR (card de control)
 - ATELIER (card de atelier)
 - SOCIETATE (cardul societății)
 - NECUNOSCUȚ (nu este introdus nici un card);
- un ID de utilizator, compus din:
 - codul statului membru care a emis cardul și numărul cardului
 - NECUNOSCUȚ dacă grupul de utilizatori este necunoscut.

Identitățile de tipul NECUNOSCUȚ pot fi cunoscute implicit sau explicit.

UIA_209 UV autentifică utilizatorii la introducerea cardului.

UIA_210 UV reautentifică utilizatorii:

- la reluarea alimentării;
- periodic sau după producerea anumitor evenimente (TBD de către producător și de mai multe ori pe zi)

UIA_211 Prin autentificare se demonstrează valabilitatea cardului de tahograf introdus, card care conține date privind securitatea pe care numai sistemul le-ar fi putut distribui. Autentificarea este reciprocă și inițiată de UV.

UIA_212 Pe lângă cele de mai sus, atelierele trebuie autentificate prin verificarea codului PIN. Codurile PIN trebuie să conțină cel puțin 4 caractere.

Notă: în cazul în care codul PIN este transferat către unitatea montată pe vehicul de la un echipament exterior situat în apropierea unității, confidențialitatea codului PIN nu trebuie protejată în timpul transferului.

UIA_213 UV detectează și împiedică utilizarea datelor de autentificare copiate și repetate.

UIA_214 După 5 încercări succesive de autentificare eșuate, funcția de garantare a securității:

- generează o înregistrare de audit a evenimentului;
- avertizează utilizatorul;
- presupune că utilizatorul este NECUNOSCUȚ și cardul nu este valid [definiția (z) și cerința 007].

4.1.3. *Identificarea și autentificarea societății conectate la distanță*

Facilitatea de conectare la distanță a societății este opțională. În consecință, acest paragraf este aplicabil numai în cazurile în care această facilitare este implementată.

- UIA_215 La fiecare interacțiune cu o societate conectată la distanță, UV poate stabili identitatea societății respective.
- UIA_216 Identitatea societății conectate la distanță este reprezentată de codul statului membru care a emis cardul de societate și de numărul cardului de societate.
- UIA_217 UV trebuie să autentifice cu succes societatea conectată la distanță înainte de a permite orice exporturi de date către aceasta.
- UIA_218 Autentificarea constă în dovedirea faptului că societatea deține un card de societate valid, care conține date privind securitatea pe care numai sistemul le-ar fi putut distribui.
- UIA_219 UV detectează și împiedică utilizarea datelor de autentificare copiate și repetate.
- UIA_220 După detectarea unui număr de 5 încercări succesive de autentificare eșuate, UV
- avertizează societatea conectată la distanță.

4.1.4. *Identificarea și autentificarea dispozitivului de gestionare*

Producătorii de unități montate pe vehicule pot prevedea dispozitive dedicate pentru funcții de gestiune suplimentare ale unității montate pe vehicul (de exemplu perfecționarea software-ului, reîncărcarea datelor privind securitatea, ...). În consecință, acest paragraf este valabil numai în cazurile în care această facilitare este implementată.

- UIA_221 La fiecare interacțiune cu un dispozitiv de gestionare, unitatea montată pe vehicul stabilește identitatea dispozitivului.
- UIA_222 Înainte de a permite orice altă interacțiune, unitatea montată pe vehicul trebuie să autentifice cu succes dispozitivul de gestionare.
- UIA_223 UV detectează și împiedică utilizarea datelor de autentificare copiate și repetate.

4.2. **Controlul accesului**

Controalele accesului garantează faptul că informația este citită, creată și modificată în cadrul obiectivului de evaluare numai de către persoanele autorizate.

Se remarcă faptul că datele privind utilizatorul înregistrate cu ajutorul unității montate pe vehicul, deși prezintă aspecte sensibile din punct de vedere comercial sau al confidențialității utilizatorului, nu sunt de natură confidențială. În consecință, cerințele funcționale legate de drepturile de acces de citire a datelor (cerința 011) nu fac obiectul unei funcții de garantare a securității.

4.2.1. *Politica de control al accesului*

- ACC_201 Unitatea montată pe vehicul gestionează și verifică drepturile de control al accesului la funcții și date.

4.2.2. *Drepturi de acces la funcții*

- ACC_202 Unitatea montată pe vehicul susține regulile de selectare a modurilor de funcționare (cerințele 006-009).
- ACC_203 Unitatea montată pe vehicul folosește modul de operare pentru a susține regulile de control al accesului la funcții (cerința 010).

4.2.3. *Drepturi de acces la date*

- ACC_204 Unitatea montată pe vehicul susține regulile de acces la scrierea datelor sale de identificare (cerința 076).
- ACC_205 Unitatea montată pe vehicul susține regulile de acces la scrierea datelor de identificare ale senzorului de mișcare cuplat (cerințele 079 și 155).
- ACC_206 După activarea unității montate pe vehicul, aceasta garantează faptul că datele de calibrare pot fi introduse în unitatea montată pe vehicul și stocate în memoria sa numai în mod calibrare (cerințele 154 și 156).
- ACC_207 După activarea unității montate pe vehicul, aceasta susține regulile de acces la scrierea și ștergerea datelor de calibrare (cerința 097).

ACC_208 După activarea unității montate pe vehicul, aceasta garantează faptul că datele de modificare a orei pot fi introduse în unitatea montată pe vehicul și stocate în memoria sa numai în mod calibrare. (Această cerință nu se aplică modificărilor minore ale orei permise de cerințele 157 și 158).

ACC_209 După activarea unității montate pe vehicul, aceasta susține regulile de acces la scrierea și ștergerea datelor privind modificarea orei (cerința 100).

ACC_210 Unitatea montată pe vehicul susține drepturile adecvate de acces la scrierea și ștergerea datelor privind securitatea (cerința 080).

4.2.4. Structura de fișiere și condiții de acces

ACC_211 Structura fișierelor aplicației și a fișierelor de date, precum și condițiile de acces sunt create în timpul procesului de producție, după care este blocată orice modificare sau ștergere a acestora.

4.3. Responsabilitate

ACT_201 Unitatea montată pe vehicul garantează faptul că șoferii sunt responsabili pentru activitățile lor (cerințele 081, 084, 087, 105a, 105b, 109 și 109a).

ACT_202 Unitatea montată pe vehicul păstrează datele de identificare permanente (cerința 075).

ACT_203 Unitatea montată pe vehicul garantează faptul că atelierele sunt responsabile pentru activitățile lor (cerințele 098, 101 și 109).

ACT_204 Unitatea montată pe vehicul garantează faptul că controlorii sunt responsabili pentru activitățile lor (cerințele 102, 103 și 109).

ACT_205 Unitatea montată pe vehicul înregistrează datele contorului de parcurs (cerința 090), precum și date detaliate privind viteza (cerința 093).

ACT_206 Unitatea montată pe vehicul garantează faptul că datele privind utilizatorul prevăzute în cerințele 081-093 și 102-105b inclusiv nu sunt modificate odată ce au fost înregistrate, cu excepția cazului când devin cea mai veche înregistrare și sunt înlocuite cu date noi.

ACT_207 Unitatea montată pe vehicul garantează faptul că nu modifică datele deja stocate pe cardul de tahograf (cerințele 109 și 109a), decât pentru a înlocui cele mai vechi date cu altele noi (cerința 110) sau în cazul descris în anexa 1 alineatul 2.1, notă.

4.4. Audit

Serviciile de audit sunt necesare numai pentru acele evenimente care pot indica o încercare de manipulare sau de violare a securității. Ele nu sunt necesare în cazul exercitării normale a drepturilor, chiar dacă aceasta este relevantă pentru securitate.

AUD_201 În cazul evenimentelor care îi afectează securitatea, UV înregistrează evenimentele respective împreună cu datele aferente (cerințele 094, 096 și 109).

AUD_202 Evenimentele care afectează securitatea unității montate pe vehicul sunt următoarele:

- Încercări de încălcare a securității:
 - eșecul autentificării senzorului de mișcare;
 - eșecul autentificării cardului de tahograf;
 - înlocuirea neautorizată a senzorului de mișcare;
 - eroare de integritate a datelor de intrare preluate de pe card;
 - eroare de integritate a datelor stocate privind utilizatorul;
 - eroare de transfer intern de date;
 - deschidere neautorizată a carcasei;
 - sabotarea hardware-ului;

- ultima sesiune închisă incorect;
- eveniment de eroare în cazul datelor privind mișcarea;
- eveniment de întrerupere a alimentării;
- anomalie internă a unității montate pe vehicul.

AUD_203 Unitatea montată pe vehicul susține regulile de stocare a înregistrărilor de audit (cerințele 094 și 096).

AUD_204 Unitatea montată pe vehicul stochează în memoria sa înregistrările de audit generate de senzorul de mișcare.

AUD_205 Înregistrările de audit pot fi tipărite, afișate și descărcate.

4.5. **Refolosirea obiectului**

REU_201 Unitatea montată pe vehicul garantează faptul că obiectele stocate temporar pot fi reutilizate, fără ca acest lucru să producă un flux nepermis de informații.

4.6. **Precizie**

4.6.1. *Politica de control al fluxului de informații*

ACR_201 Unitatea montată pe vehicul garantează faptul că datele privind utilizatorul prevăzute în cerințele 081, 084, 087, 090, 093, 102, 104, 105, 105a și 109 pot fi procesate numai când sunt preluate din surse corecte, respectiv:

- datele privind mișcarea vehiculului;
- ceasul unității montate pe vehicul, indicând timpul real;
- parametrii de calibrare ai aparatului de înregistrare;
- cardurile de tahograf;
- datele introduse de utilizator.

ACR_201a Unitatea montată pe vehicul garantează faptul că datele privind utilizatorul prevăzute în cerința 109a pot fi introduse numai pentru perioada dintre ultima retragere a cardului și introducerea curentă a acestuia (cerința 050a).

4.6.2. *Transferuri interne de date*

Cerințele enunțate în acest paragraf sunt valabile numai dacă unitatea montată pe vehicul utilizează componente separate fizic.

ACR_202 Dacă au loc transferuri de date între componentele separate fizic ale unității montate pe vehicul, datele trebuie protejate împotriva modificărilor

ACR_203 La detectarea unei erori de transfer al datelor în cursul unui transfer intern, transmisia se repetă, iar funcția de garantare a securității generează o înregistrare de audit a evenimentului.

4.6.3. *Integritatea datelor stocate*

ACR_204 Unitatea montată pe vehicul verifică datele privind utilizatorul stocate în memorie, pentru a detecta eventualele erori de integritate.

ACR_205 La detectarea unei erori de integritate a datelor privind utilizatorul, funcția de garantare a securității generează o înregistrare de audit.

4.7. **Fiabilitatea serviciului**

4.7.1. *Teste*

RLB_201 Toate comenzile, acțiunile sau punctele de testare, corespunzătoare nevoilor de testare din faza de producție a UV, sunt dezactivate sau eliminate înaintea activării UV. Nu mai pot fi reintroduse în vederea utilizării ulterioare.

RLB_202 Unitatea montată pe vehicul rulează autoteste în momentul primei puneri în funcțiune, precum și în cursul funcționării normale, pentru a verifica dacă funcționează corect. Autotestele efectuate de UV includ verificarea integrității datelor privind securitatea, precum și verificarea integrității codului executabilelor stocate (dacă nu sunt în ROM).

RLB_203 La detectarea unei anomalii interne în cursul unui autotest, funcția de garantare a securității procedează astfel:

- generează o înregistrare de audit (dacă nu este în modul calibrare) (anomalie internă UV);
- păstrează integritatea datelor stocate.

4.7.2. *Software*

RLB_204 Nu există nici un mod de analizare sau depanare a unității montate pe vehicul în condiții de teren, după activarea acesteia.

RLB_205 Datele preluate din surse externe ca date de intrare nu sunt acceptate drept cod executabil.

4.7.3. *Protecție fizică*

RLB_206 Dacă este concepută astfel încât să poată fi deschisă, UV detectează orice deschidere a carcasei sale, chiar și atunci când alimentarea sa este întreruptă, cu excepția cazului când se află în modul calibrare, timp de minimum 6 luni. Într-un astfel de caz, funcția de garantare a securității generează o înregistrare de audit (se acceptă ca înregistrarea de audit să fie generată și stocată după reluarea alimentării).

Dacă este concepută astfel încât să nu poată fi deschisă, UV trebuie să permită detectarea cu ușurință a tuturor încercărilor de avariere fizică (de exemplu prin inspecție vizuală).

RLB_207 După activare, UV detectează aspecte precise privind sabotarea hardware-ului (TBD de către producător).

RLB_208 În cazul anterior, funcția de garantare a securității generează o înregistrare de audit, iar UV acționează astfel: (TBD de către producător).

4.7.4. *Întreruperi în alimentare*

RLB_209 UV detectează devierile de la valorile normale de la alimentare, inclusiv întreruperile în alimentare.

RLB_210 În cazul descris anterior, funcția de garantare a securității:

- generează o înregistrare de audit (dacă nu este în modul calibrare);
- păstrează stabilă starea UV;
- menține funcțiile de securitate legate de componentele sau de procesele active;
- păstrează integritatea datelor stocate.

4.7.5. *Condiții de resetare*

RLB_211 În cazul unei întreruperi în alimentare, dacă o tranzacție este întreruptă înaintea finalizării, sau în oricare alte condiții de resetare, unitatea montată pe vehicul este resetată fără probleme.

4.7.6. *Disponibilitatea datelor*

RLB_212 UV garantează faptul că accesul la resurse este asigurat oricând este nevoie și că resursele nu sunt solicitate sau reținute inutil.

RLB_213 UV garantează eliberarea cardurilor numai după ce s-au stocat pe ele date relevante (cerințele 015 și 016).

RLB_214 În cazul descris anterior, funcția de garantare a securității generează o înregistrare de audit a evenimentului.

4.7.7. *Aplicații multiple*

RLB_215 Dacă UV include aplicații diferite de cea pentru tahograf, toate aplicațiile sunt separate fizic și/sau logic. Aceste aplicații nu partajează date de securitate. O singură sarcină este activă la un moment dat.

4.8. *Schimb de date*

Acest paragraf se referă la schimbul de date dintre UV și dispozitivele conectate la aceasta.

4.8.1. *Schimbul de date cu senzorul de mișcare*

DEX_201 UV verifică integritatea și autenticitatea datelor privind mișcarea importate de la senzorul de mișcare.

DEX_202 La detectarea unei erori care afectează integritatea sau autenticitatea datelor privind mișcarea, funcția de garantare a securității:

- generează o înregistrare de audit;
- continuă să utilizeze datele importate.

4.8.2. Schimbul de date cu cardurile de tahograf

DEX_203 UV verifică integritatea și autenticitatea datelor importate de pe cardurile de tahograf.

DEX_204 La detectarea unei erori care afectează integritatea sau autenticitatea datelor de pe card, UV

- generează o înregistrare de audit;
- nu folosește datele.

DEX_205 UV exportă date către carduri de tahograf cu memorie, împreună cu atributele de securitate asociate, astfel încât cardul să poată verifica integritatea și autenticitatea datelor.

4.8.3. Schimbul de date cu suporturile externe de stocare (funcția descărcare)

DEX_206 UV generează o dovadă a originii datelor descărcate pe suporturi externe.

DEX_207 UV oferă receptorului posibilitatea de a verifica dovada de origine în cazul datelor descărcate.

DEX_208 UV descarcă date pe suporturi de stocare externe, împreună cu atributele de securitate asociate, astfel încât integritatea și autenticitatea datelor descărcate să poată fi verificată.

4.9. Suport criptografic

Cerințele enunțate în acest paragraf sunt aplicabile numai acolo unde este cazul, în funcție de mecanismele de securitate utilizate și de soluțiile producătorului.

CSP_201 Orice operație criptografică efectuată de senzorul de mișcare respectă un algoritm și o dimensiune a cheii specificate.

CSP_202 Dacă senzorul de mișcare generează chei criptografice, acest lucru se realizează în conformitate cu algoritmi preciși de generare a cheilor criptografice și a dimensiunilor specificate ale cheilor criptografice.

CSP_203 Dacă senzorul de mișcare distribuie chei criptografice, acest lucru se realizează în conformitate cu metode precise de distribuție a cheilor criptografice.

CSP_204 Dacă senzorul de mișcare accesează chei criptografice, acest lucru se realizează în conformitate cu metode precise de accesare a cheilor criptografice.

CSP_205 Dacă senzorul de mișcare distruge chei criptografice, acest lucru se realizează în conformitate cu metode precise de distrugere a cheilor criptografice.

5. Definirea mecanismelor de securitate

Mecanismele de securitate necesare sunt specificate în apendicele 11.

Toate celelalte mecanisme de securitate trebuie definite de către producător.

6. Protecția minimă oferită de mecanismele de securitate

Protecția minimă oferită de mecanismele de securitate ale unității montate pe vehicul are valoarea Ridică, conform definiției (ITSEC).

7. Nivelul de garanție

Obiectivul pentru nivelul de garanție pentru unitatea montată pe vehicul este nivelul E3 ITSEC, conform definiției (ITSEC).

8. Prezentare

Următoarele matrice oferă o prezentare a funcțiilor de garantare a securității, precizând:

- ce pericole sunt contracarate de fiecare funcție sau mijloc de garantare a securității;
- ce obiective de securitate privind tehnologia informației sunt protejate de fiecare funcție de garantare a securității.

	Pericole																	Obiective IT									
	Acces	Identificare	Anomali	Teste	Proiectare	Parametri_Calibrare	Schimb_Date_Card	Ceas	Mediu	Dispozitive_Fictive	Hardware	Date_Miscare	Neactivat	Date_Ieșire	Alimentare	Date_Securitate	Software	Date_Stocate	Acces	Responsabilitate	Audit	Autentificare	Integritate	Ieșire	Procesare	Fiabilitate	Schimb_Protejat_Date
Mijloace fizice, de personal și procedurale																											
Dezvoltare			x	x	x																						
Producție				x	x																						
Livrare													x														
Activare	x											x															
Generare date privind securitatea																x											
Transmitere date privind securitatea																x											
Disponibilitate card		x																									
Unicitate card șofer		x																									
Urmărire card		x																									
Ateliere agreate						x		x																			
Calibrare cu ocazia inspecțiilor periodice						x		x				x	x			x											
Ateliere de încredere						x		x																			
Șoferi de încredere		x																									
Controlul respectării legii		x				x		x	x		x		x		x		x	x									
Perfecționare software																		x									
Funcții de garantare a securității																											
Identificare și autentificare																											
UIA_201 Identificare senzor										x		x										x					x
UIA_202 Identitate senzor										x		x										x					x
UIA_203 Autentificare senzor										x		x										x					x
UIA_204 Reidentificare și reautentificare senzor										x		x										x					x
UIA_205 Autentificare nefalsificabilă										x		x										x					
UIA_206 Eșec autentificare										x		x									x					x	
UIA_207 Identificare utilizatori	x	x								x									x			x					x
UIA_208 Identitate utilizator	x	x								x									x			x					x
UIA_209 Autentificare utilizator	x	x								x									x			x					x
UIA_210 Reautentificare utilizator	x	x								x									x			x					x
UIA_211 Mijloace autentificare	x	x								x									x			x					
UIA_212 Verificări PIN	x	x				x		x											x			x					
UIA_213 Autentificare nefalsificabilă	x	x								x									x			x					

	Pericole																		Obiective IT										
	Acces	Identificare	Anomalii	Teste	Proiectare	Parametri_Calibrare	Schimb_Date_Card	Ceas	Mediu	Dispozitive_Fictive	Hardware	Date_Miscare	Neactivat	Date_Iesire	Alimentare		Date_Securitate	Software	Date_Stocate	Acces	Responsabilitate	Audit	Autentificare	Integritate	Iesire	Procesare	Fiabilitate	Schimb_Proteiat_Date	
UIA_214 Eșec autentificare	x	x								x												x							
UIA_215 Identificare utilizator la distanță	x	x																		x			x						x
UIA_216 Identitate utilizator la distanță	x	x																		x			x						
UIA_217 Autentificare utilizator la distanță	x	x																		x			x						x
UIA_218 Mijloace de autentificare	x	x																		x			x						
UIA_219 Autentificare nefalsificabilă	x	x																		x			x						
UIA_220 Eșec autentificare	x	x																											
UIA_221 Identificare dispozitiv de gestionare	x	x																		x			x						
UIA_222 Autentificare dispozitiv de gestionare	x	x																		x			x						
UIA_223 Autentificare nefalsificabilă	x	x																		x			x						
Control acces																													
ACC_201 Politică de control al accesului	x					x		x										x		x	x								
ACC_202 Drepturi de acces la funcții	x					x		x												x									
ACC_203 Drepturi de acces la funcții	x					x		x												x									
ACC_204 ID UV																			x	x									
ACC_205 ID senzor conectat										x									x	x									
ACC_206 Date calibrare	x					x													x	x									
ACC_207 Date calibrare						x													x	x									
ACC_208 Date privind reglarea orei								x											x	x									
ACC_209 Date privind reglarea orei								x											x	x									
ACC_210 Date privind securitatea																		x	x	x									
ACC_211 Structură fișiere și condiții acces	x					x												x	x	x									
Responsabilitate																													
ACT_201 Responsabilitate șoferi																					x								
ACT_202 Date ID UV																					x	x							
ACT_203 Responsabilitate ateliere																					x								
ACT_204 Responsabilitate controlori																					x								
ACT_205 Responsabilitate privind deplasările vehiculului																					x								
ACT_206 Modificare date privind responsabilitatea																			x					x				x	
ACT_207 Modificare date privind responsabilitatea																			x					x				x	

[illegible]

OBJECTIVE GENERALE DE SECURITATE PENTRU CARDUL DE TAHOGRAF

1. Introducere

Acest document conține o descriere a cardului de tahograf, a pericolelor pe care acesta trebuie să le contracareze și a obiectivelor de securitate pe care trebuie să le atingă. Conține și funcțiile obligatorii de garantare a securității. Documentul precizează nivelul de protecție minim solicitat pentru mecanismele de securitate, precum și nivelul minim de garanție pentru dezvoltare și evaluare.

Cerințele menționate în prezentul document sunt cele cuprinse în anexa I B. Pentru a facilita citirea, uneori apare o duplicare a cerințelor din anexa I B și a celor privind obiectivul de securitate. În caz de ambiguitate între o cerință privind un obiectiv de securitate și o cerință din cadrul anexei I B menționată în obiectivul de securitate respectiv, cerința din cadrul anexei I B are prioritate.

Cerințele din anexa I B cărora nu li se asociază obiective de securitate nu fac obiectul funcțiilor de garantare a securității.

Un card de tahograf este un card standard cu memorie care include o aplicație de tahograf dedicată și îndeplinește cerințele actuale de securitate funcționale și de garanție aplicabile cardurilor cu memorie. De aceea, prezentul obiectiv de securitate încorporează numai cerințele de securitate suplimentare necesare pentru aplicația de tahograf.

Au fost atribuite etichete unice pentru pericole, obiective, mijloace procedurale și specificațiile funcțiilor de garantare a securității în scopul urmăririi documentației de dezvoltare și de evaluare.

2. Abrevieri, definiții și trimiteri

2.1. Abrevieri

CI	Circuit integrat (component electronic proiectat pentru a realiza funcții de procesare și/sau de memorare)
SO	Sistem de operare
PIN	Număr personal de identificare
ROM	Memorie fixă
PFS	Politică de funcții de securitate
TBD	De definit
TOE	Obiectiv de evaluare
TSF	Funcție de securitate a TOE
UV	Unitate montată pe vehicul

2.2. Definiții

Tahograf digital	Aparat de înregistrare.
Date sensibile	Date stocate de cardul de tahograf a căror integritate și confidențialitate (dacă este cazul pentru datele privind securitatea) trebuie să fie protejate, evitându-se și modificarea neautorizată. Datele sensibile includ datele privind securitatea și datele privind utilizatorul.
Date privind securitatea	Datele specifice necesare pentru a aplica funcțiile de garantare a securității (de exemplu cheile criptografice).
Sistem	Echipament, persoane sau organizații care au o legătură cu aparatul de înregistrare.
Utilizator	Orice entitate (utilizator uman sau entitate informatică externă) independentă de obiectivul de evaluare care interacționează cu obiectivul de evaluare (atunci când nu este folosit în expresia «date privind utilizatorul»).

Date privind utilizatorul	Date sensibile stocate pe cardul de tahograf, diferite de datele privind securitatea. Datele privind utilizatorul includ datele de identificare și datele privind activitatea.
Date de identificare	Datele de identificare includ datele de identificare a cardului și datele de identificare a titularului cardului.
Date de identificare a cardului	Date privind utilizatorul care au legătură cu identificarea cardului așa cum sunt definite în cerințele 190, 191, 192, 194, 215, 231 și 235.
Date de identificare a titularului cardului	Date privind utilizatorul care au legătură cu identificarea titularului cardului așa cum sunt definite în cerințele 195, 196, 216, 232 și 236.
Date privind activitatea	Datele privind activitatea includ datele privind activitatea titularului, date privind evenimentele și anomaliiile și datele privind activitățile de control.
Date privind activitatea titularului	Date privind utilizatorul care au legătură cu activitățile efectuate de titularul cardului așa cum sunt definite în cerințele 197, 199, 202, 212, 212a, 217, 219, 221, 226, 227, 229, 230a, 233 și 237.
Date privind evenimentele și anomaliiile	Date privind utilizatorul care au legătură cu evenimentele sau anomaliiile așa cum sunt definite în cerințele 204, 205, 207, 208 și 223.
Date privind activitățile de control	Date privind utilizatorul care au legătură cu controalele de aplicare a legii așa cum sunt definite în cerințele 210 și 225.

2.3. Trimiteri

ITSEC ITSEC Criterii de evaluare a securității în tehnologia informației 1991

IC PP Profil de protecție a circuitelor integrate pe carduri cu memorie – versiunea 2.0 – din septembrie 1998. Înregistrat la organismul francez de certificare cu numărul PP/9806.

ES PP Profil de protecție a circuitelor integrate pe carduri cu memorie cu software încorporat – versiunea 2.0 – din iunie 1999. Înregistrat la organismul francez de certificare cu numărul PP/9911.

3. Prezentarea produsului

3.1. Descrierea și metoda de utilizare a cardului de tahograf

Un card de tahograf este un card cu memorie, așa cum este descris în (IC PP) și (ES PP), care include o aplicație prevăzută pentru utilizarea lui cu aparatul de înregistrare.

Funcțiile de bază ale cardului de tahograf sunt:

- să stocheze datele de identificare a cardului și datele de identificare a titularului cardului. Aceste date sunt folosite de unitatea montată pe vehicul pentru a identifica titularul cardului și a oferi funcții și drepturi adecvate de acces la date și a asigura responsabilitatea titularului cardului pentru activitățile sale;
- să stocheze datele privind activitățile titularului cardului, datele privind evenimentele și anomaliiile și datele privind activitățile de control, referitoare la titularul cardului.

Un card de tahograf este proiectat să fie folosit de dispozitivul de interfață pentru card al unei unități montate pe vehicul. El poate fi folosit și de orice lector de carduri (de exemplu un calculator personal) care are drepturi de acces de citire integrale asupra datelor privind utilizatorul.

În timpul fazei de utilizare finală din ciclul de viață al cardului de tahograf [faza 7 din ciclul de viață descris în (ES PP)], numai unitățile montate pe vehicul pot scrie date privind utilizatorul pe card.

Cerințele funcționale pentru un card de tahograf sunt specificate în textul corpului anexei I B și în apendicele 2.

3.2. Ciclul de viață al cardului de tahograf

Ciclul de viață al cardului de tahograf corespunde ciclului de viață al unui card cu memorie descris în (ES PP).

3.3. **Pericole**

Pe lângă pericolele generale pentru cardurile cu memorie prezentate în (ES PP) și (IC PP), cardul de tahograf se mai poate confrunta cu următoarele amenințări:

3.3.1. *Scopuri finale*

Scopul final al atacurilor este să modifice datele privind utilizatorul stocate în cadrul obiectivului de evaluare.

- P.Date_Identificare O modificare reușită a datelor de identificare păstrate de obiectivul de evaluare (de exemplu tipul de card sau data de expirare a cardului sau date privind titularul cardului) permite utilizarea frauduloasă a obiectivului de evaluare și constituie un pericol major pentru obiectivul de securitate globală a sistemului.
- P.Date_Activitate O modificare reușită a datelor privind activitatea memorate în obiectivul de evaluare constituie un pericol pentru securitatea obiectivului de evaluare.
- P.Date_Schimb O modificare reușită a datelor privind activitatea (adăugare, ștergere, modificare) în timpul importului sau exportului constituie o amenințare pentru securitatea obiectivului de evaluare.

3.3.2. *Căi de atac*

Activele obiectivului de evaluare pot fi atacate prin:

- încercarea de a obține cunoștințe ilicite despre proiectarea hardware și software a obiectivului de evaluare și în special despre funcțiile sale de securitate sau datele de securitate. Cunoștințele ilicite pot fi obținute prin atacuri asupra materialelor proiectantului sau ale producătorului (furt, mită etc.) sau prin examinarea directă a obiectivului de evaluare (sondare fizică, analiză inferențială etc.);
- exploatarea slăbiciunilor din proiectarea sau realizarea obiectivului de evaluare (exploatarea erorilor hardware, a erorilor software, a anomaliilor de transmitere, a erorilor induse în obiectivul de evaluare de agresiunile mediului, exploatarea slăbiciunilor din funcțiile de securitate cum ar fi procedurile de autentificare, controlul accesului la date, operațiunile criptografice etc.);
- modificarea obiectivului de evaluare sau a funcțiilor sale de securitate prin atacuri fizice, electrice sau logice sau o combinație a acestora.

3.4. **Obiective de securitate**

Obiectivul principal de securitate al întregului sistem digital de tahograf este următorul:

- O.Principal Datele pe care le verifică autoritățile de control trebuie să fie disponibile și să reflecte integral și exact activitatea șoferilor și a vehiculelor controlate cu privire la perioadele de conducere, muncă, disponibilitate și odihnă și la viteza vehiculului.

De aceea, obiectivele principale de securitate pentru obiectivul de evaluare, care contribuie la acest obiectiv de securitate globală, sunt următoarele:

- O.Date_Identificare_Card Obiectivul de evaluare trebuie să păstreze datele de identificare a cardului și datele de identificare a titularului cardului stocate în timpul procesului de personalizare a cardului.
- O.Stocare_Activitate_Card Obiectivul de evaluare trebuie să păstreze datele privind utilizatorul stocate pe card de unitățile montate pe vehicul.

3.5. **Obiective de securitate privind tehnologia informației**

Pe lângă obiectivele de securitate generale pentru cardurile cu memorie prezentate în (ES PP) și (IC PP), obiectivele de securitate specifice tehnologiei informațiilor ale obiectivului de evaluare care contribuie la obiectivele principale de securitate în timpul fazei de utilizare finală din ciclul de viață sunt următoarele:

- O.Acces_Date Obiectivul de evaluare trebuie să limiteze drepturile de acces și scriere a datelor privind utilizatorul numai la unitățile montate pe vehicul autentificate.
- O.Comunicații_Securizate Obiectivul de evaluare trebuie să recunoască protocoalele și procedurile de comunicare securizată între card și dispozitivul de interfață pentru card atunci când acest lucru este solicitat de aplicație.

3.6. **Mijloace fizice, de personal sau procedurale**

Cerințele fizice, de personal sau procedurale care contribuie la securitatea obiectivului de evaluare sunt prezentate în (ES PP) și (IC PP) (capitolele obiective de securitate pentru mediul înconjurător).

4. Funcții de garantare a securității

Acest paragraf detaliază unele dintre operațiile permise cum ar fi atribuirea sau selectarea de (ES PP) și oferă cerințe funcționale suplimentare privind funcțiile de garantare a securității.

4.1. Respectarea profilurilor de protecție

CPP_301 Obiectivul de evaluare trebuie să respecte (IC PP).

CPP_302 Obiectivul de evaluare trebuie să respecte (ES PP) după cum se detaliază mai jos.

4.2. Identificarea și autentificarea utilizatorului

Cardul trebuie să identifice entitatea în care este introdus și să cunoască dacă este un vehicul autentificat sau nu. Cardul poate exporta orice date privind utilizatorul, indiferent de entitatea la care este conectat, cu excepția cardului de control care poate exporta date de identificare a titularului numai către unități montate pe vehicul autentificate (astfel încât un controlor să fie sigur că unitatea montată pe vehicul nu este o unitate falsă văzându-și numele pe ecran sau pe listări).

4.2.1. Identificarea utilizatorului

Misiunea (FIA_UID.1.1) *Lista acțiunilor moderate de TSF:* nici una.

Misiunea (FIA_ATD.1.1) *Lista atributelor de securitate:*

GRUP_UTILIZATORI UNITATE_VEHICUL, UNITATE_FĂRĂ_VEHICUL,

ID_UTILIZATOR: Numărul de înmatriculare a vehiculului (VRN) și codul statului membru în care este înmatriculat vehiculul (ID_UTILIZATOR este cunoscut numai pentru GRUP_UTILIZATORI = UNITATE_VEHICUL).

4.2.2. Autentificarea utilizatorului

Misiunea (FIA_UAU.1.1) *Lista acțiunilor moderate de TSF:*

- Cardurile șoferului și ale atelierului: exportă datele privind utilizatorul cu atributele de securitate (funcția de descărcare a datelor de pe card);
- Cardul de control: exportă datele privind utilizatorul fără atributele de securitate, cu excepția datelor de identificare a titularului.

UIA_301 Autentificarea unei unități montate pe vehicul se realizează prin dovedirea faptului că posedă date de securitate pe care numai sistemul le putea distribui.

Selecția (FIA_UAU.3.1 și FIA_UAU.3.2): prevenire.

Misiunea (FIA_UAU.4.1) *Mecanism(e) identificat(e) de autentificare:* orice mecanism de autentificare.

UIA_302 Cardul atelierului trebuie să ofere un mecanism de autentificare suplimentar prin verificarea unui cod PIN (Acest mecanism este destinat unității montate pe vehicul pentru a asigura identitatea titularului cardului, nu este prevăzut pentru a proteja conținutul cardului atelierului).

4.2.3. Eșecul autentificării

Următoarele misiuni descriu reacția cardului pentru fiecare eșec de autentificare a unui utilizator.

Misiunea (FIA_AFL.1.1) *Număr: 1, lista de evenimente de autentificare:* autentificarea unui dispozitiv de interfață pentru card.

Misiunea (FIA_AFL.1.2) *Lista acțiunilor:*

- avertizează entitatea conectată;
- consideră utilizatorul ca pe o UNITATE_FĂRĂ_VEHICUL;

Următoarele misiuni descriu reacția cardului în cazul eșecului mecanismului de autentificare suplimentar cerut în UIA_302.

Misiunea (FIA_AFL.1.1) *Număr: 5, lista de evenimente de autentificare:* verificări ale codului PIN (cardul atelierului).

Misiunea (FIA_AFL.1.2) *Lista acțiunilor:*

- avertizează entitatea conectată,
- blochează procedura de verificare a codului PIN astfel încât orice încercare ulterioară de verificare a codului PIN va eșua,
- poate indica utilizatorilor următorii motivul blocării.

4.3. **Controlul accesului**

4.3.1. *Politica de control al accesului*

În timpul fazei de utilizare finală din ciclul său de viață, cardul de tahograf este subiectul unei singure politici de funcții de securitate privind controlul accesului (PFS) denumită AC_SFP.

Misiunea (FDP_ACC.2.1) *PFS privind controlul accesului:* AC_SFP.

4.3.2. *Funcții de control al accesului*

Misiunea (FDP_ACF.1.1) *PFS privind controlul accesului:* AC_SFP.

Misiunea (FDP_ACF.1.1) *Grupul numit de atribute de securitate:* GRUP_UTILIZATORI.

Misiunea (FDP_ACF.1.2) *Regulile care reglementează accesul la subiectele și obiectele controlate utilizând operațiuni controlate asupra obiectelor controlate:*

- CITIRE_GENERALĂ: Datele privind utilizatorul pot fi citite din obiectivul de evaluare de către orice utilizator, cu excepția datelor de identificare a titularului care pot fi citite de pe cardurile de control numai de către UNITATE_VEHICUL.
- SCRIERE_IDENTIFICARE: Datele de identificare pot fi scrise o singură dată și înainte de terminarea fazei 6 din ciclul de viață al cardului. Nici un utilizator nu poate scrie sau modifica datele de identificare în timpul fazei de utilizare finală din ciclul de viață al cardului.
- SCRIERE_ACTIVITATE: Datele privind activitatea pot fi scrise în obiectivul de evaluare numai de UNITATE_VEHICUL.
- PERFECTIONARE_SOFT: Nici un utilizator nu poate perfecționa software-ul obiectivului de evaluare.
- STRUCTURĂ_FIȘIERE: Structura fișierelor și condițiile de acces sunt create înainte de terminarea fazei 6 din ciclul de viață al obiectivului de evaluare și apoi orice modificare sau ștergere ulterioară de către orice utilizator este blocată.

4.4. **Responsabilitate**

ACT_301 Obiectivul de evaluare păstrează date de identificare permanente.

ACT_302 Există o indicație a datei și orei personalizării obiectivului de evaluare. Această indicație nu poate fi modificată.

4.5. **Audit**

Obiectivul de evaluare trebuie să monitorizeze evenimentele care indică o posibilă violare a securității lui.

Misiunea (FAU_SAA.1.2) *Subset de evenimente analizabile definite:*

- eșec de autentificare a titularului cardului (5 verificări consecutive nereușite ale codului PIN);
- eroare de testare automată;
- eroare de integritate a datelor stocate;
- eroare de integritate a datelor introduse privind activitățile.

4.6. **Precizie**

4.6.1. *Integritatea datelor stocate*

Misiunea (FDP_SDI.2.2) *Acțiuni de efectuat:* avertizarea entității conectate.

4.6.2. *Autentificarea datelor de bază*

Misiunea (FDP_DAU.1.1) *Lista tipurilor de obiecte sau informații:* date privind activitățile.

Misiunea (FDP_DAU.1.2) *Lista subiectelor:* oricare.

4.7. **Fiabilitatea serviciului**

4.7.1. *TesteSelecția*

(FPT_TST.1.1): în timpul primei puneri în funcțiune, apoi periodic în timpul funcționării normale.

Notă: în timpul primei puneri în funcțiune înseamnă înainte de executarea codului [și nu neapărat în timpul procedurii Răspuns la reinițializare (Answer To Reset)]

RLB_301 Testele automate ale obiectivului de evaluare includ verificarea integrității oricărui cod software care nu este stocat în ROM.

RLB_302 La detectarea unei erori de testare automată TSF avertizează entitatea conectată.

RLB_303 După terminarea testării sistemului de operare, toate comenzile și acțiunile specifice testării sunt dezactivate sau eliminate. Nu este posibil să se înlocuiască aceste comenzi sau să se reactiveze pentru utilizare. Comenzile asociate exclusiv cu o stare din ciclul de viață nu sunt niciodată accesate în timpul unei alte stări.

4.7.2. *Software*

RLB_304 Nu există nici o metodă de analiză, depanare sau modificare pe teren a software-ului obiectivului de evaluare.

RLB_305 Intrările din surse externe nu sunt acceptate drept cod executabil.

4.7.3. *Alimentarea cu energie electrică*

RLB_306 Obiectivul de evaluare trebuie să își mențină o stare sigură în timpul întreruperii sau variațiilor alimentării cu energie.

4.7.4. *Condiții de resetare*

RLB_307 Dacă alimentarea este întreruptă (sau dacă apar variații de alimentare cu energie) la obiectivul de evaluare sau dacă o tranzacție este oprită înainte de terminare ori în orice alte condiții de reinițializare, obiectivul de evaluare trebuie să fie reinițializat fără probleme.

4.8. **Schimb de date**

4.8.1. *Schimbul de date cu o unitate montată pe vehicul*

DEX_301 Obiectivul de evaluare trebuie să verifice integritatea și autenticitatea datelor importate de la o unitate montată pe vehicul.

DEX_302 La detectarea unei erori de integritate a datelor importate, obiectivul de evaluare:

- avertizează entitatea care trimite datele;
- nu utilizează datele.

DEX_303 Obiectivul de evaluare exportă datele privind utilizatorul către unitatea montată pe vehicul împreună cu atributele de securitate asociate, astfel încât unitatea montată pe vehicul să poată verifica integritatea și autenticitatea datelor primite.

4.8.2. *Exportul de date către o unitate exterioară vehiculului (funcția descărcare)*

DEX_304 Obiectivul de evaluare trebuie să poată genera o dovadă de origine pentru datele descărcate pe suporturi externe.

DEX_305 Obiectivul de evaluare trebuie să ofere o funcție de verificare a dovezii de origine a datelor descărcate pentru destinatar.

DEX_306 Obiectivul de evaluare trebuie să poată descărca datele pe un suport de memorie extern, împreună cu atributele de securitate asociate, astfel încât integritatea datelor descărcate să poată fi verificată.

4.9. **Suport criptografic**

CSP_301 Dacă funcția de securitate a obiectivului de evaluare generează chei criptografice, acestea corespund unor algoritmi preciși de generare a cheilor criptografice și unor dimensiuni specificate ale cheilor criptografice. Cheile criptografice de sesiune generate au un număr limitat de utilizări posibile (TBD de către producător, dar nu mai multe de 240).

CSP_302 Dacă funcția de securitate a obiectivului de evaluare distribuie chei criptografice, acestea corespund unor metode specificate de distribuire a cheilor criptografice.

5. **Definirea mecanismelor de securitate**

Mecanisme de securitate necesare sunt specificate în apendicele 11.

Toate celelalte mecanisme de securitate sunt definite de producătorul obiectivului de evaluare.

6. Nivelul minim solicitat de protecție al mecanismelor

Puterea minimă a mecanismelor pentru cardul de tahograf este **Ridicată** conform definiției din (ITSEC).

7. Nivelul de garanție

Nivelul de garanție vizat pentru cardul de tahograf este nivelul ITSEC **E3**, conform definiției din (ITSEC).

8. Prezentare

Matricele următoare prezintă o analiză pentru funcțiile suplimentare de garantare a securității indicând:

- funcțiile de garantare a securității capabile să neutralizeze diverse pericole;
- funcțiile de garantare a securității care îndeplinesc diverse obiective de securitate a tehnologiei informației.

	Amenințări										Obiective de tehnologia informației									
	T.CLON*	T.DIS_ES2	T.T_ES	T.T_CMD	T.MOD_SOFT*	T.MOD_LOAD	T.MOD_EXE	T.MOD_SHARE	Date_Identificare	Date_activitate	Schimb_Date	O.TAMPER_ES	O.CLON*	O.OPERATE*	O.FLAW*	O.DIS_MECHANISM2	O.DIS_MEMORY*	O.MOD_MEMORY*	Acces_Date	Comunicații_Securizate
UIA_301 Mijloace de autentificare																			x	
UIA_302 Verificări PIN																			x	
ACT_301 Date de identificare																				
ACT_302 Date de personalizare																				
RLB_301 Integritate software												x		x						
RLB_302 Autoteste												x		x						
RLB_303 Teste de fabricație					x	x						x		x						
RLB_304 Analiză software					x		x	x				x		x						
RLB_305 Intrări software					x	x		x				x		x						
RLB_306 Alimentarea cu energie									x	x		x		x						
RLB_307 Resetarea												x		x						
DEX_301 Import de date securizate											x									x
DEX_302 Import de date securizate											x									x
DEX_303 Export de date securizate către UV											x									x
DEX_304 Dovada de origine											x									x
DEX_305 Dovada de origine											x									x
DEX_306 Export securizat pe suporturi externe											x									x
CSP_301 Generare de chei												x								x
CSP_302 Distribuie de chei												x								x

Apendicele 11

MECANISME DE SECURITATE COMUNE

CUPRINS

1.	Generalități	240
1.1.	Trimiteri	240
1.2.	Notății și termeni prescurtați	241
2.	Sisteme și algoritmi criptografici.....	242
2.1.	Sisteme criptografice	242
2.2.	Algoritmi criptografici.....	242
2.2.1.	Algoritmul RSA	242
2.2.2.	Algoritmul de distribuire	242
2.2.3.	Algoritmul de criptare a datelor	242
3.	Chei și certificate	242
3.1.	Generarea și distribuirea cheilor	242
3.1.1.	Generarea și distribuirea cheilor RSA	242
3.1.2.	Chei de test RSA	244
3.1.3.	Cheile senzorului de mișcare	244
3.1.4.	Generarea și distribuția cheilor de sesiune T-DES	244
3.2.	Chei	244
3.3.	Certificate	244
3.3.1.	Conținutul certificatelor	245
3.3.2.	Certificate emise	246
3.3.3.	Verificarea și dezvăluirea certificatelor	247
4.	Mecanismul de autentificare reciprocă	247
5.	Confidențialitatea, integritatea și mecanismul de autentificare a transferului de date dintre unitățile montate pe vehicul și carduri	250
5.1.	Mesageria securizată	250
5.2.	Tratarea erorilor de mesagerie securizată	251
5.3.	Algoritmul de calcul al sumelor de control criptografic	252
5.4.	Algoritmul de calcul al criptogramelor pentru DO confidențiale.....	252
6.	Mecanismele de semnare digitală a datelor descărcate	253
6.1.	Generarea semnăturilor	253
6.2.	Verificarea semnăturilor	253

1. GENERALITĂȚI

Prezentul apendice precizează mecanismele de securitate care asigură:

- autentificarea reciprocă între unitățile montate pe vehicul și cardurile de tahograf, inclusiv acordul privind cheia de sesiune;
- confidențialitatea, integritatea și autentificarea datelor transferate între unitățile montate pe vehicul și cardurile de tahograf;
- integritatea și autentificarea datelor descărcate din unitățile montate pe vehicul pe suporturi de memorie externe;
- integritatea și autentificarea datelor descărcate de pe cardurile de tahograf pe suporturi de memorie externe.

1.1. Trimiteri

În prezentul apendice se folosesc următoarele trimiteri:

SHA-1	National Institute of Standards and Technology (NIST). FIPS Publication 180-1: Secure Hash Standard. Aprilie 1995
PKCS1	RSA Laboratories. PKCS # 1: RSA Encryption Standard. Version 2.0. Octombrie 1998
TDES	National Institute of Standards and Technology (NIST). FIPS Publication 46-3: Data Encryption Standard. Proiect de normă 1999
TDES-OP	ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation. 1998
ISO/IEC 7816-4	Tehnologia informației – Carduri de identificare – Carduri cu circuite integrate și cu contacte – Partea 4: Comenzile intersectoriale pentru schimburi. Prima ediție: 1995 + Amendamentul 1: 1997
ISO/IEC 7816-6	Tehnologia informației – Carduri de identificare – Carduri cu circuite integrate și cu contacte – Partea 6: Elemente de date intersectoriale. Prima ediție: 1996 + Cor 1: 1998
ISO/IEC 7816-8	Tehnologia informației – Carduri de identificare – Carduri cu circuite integrate și cu contacte – Partea 8: Comenzi intersectoriale privind securitatea. Prima ediție: 1999
ISO/IEC 9796-2	Tehnologia informației – Tehnici de securitate – Schițe de semnătură digitală pentru recuperarea mesajelor – Partea 2: Mecanisme care utilizează o funcție de distribuire. Prima ediție: 1997
ISO/IEC 9798-3	Tehnologia informației – Tehnici de securitate – Mecanisme de autentificare a perifericelor – Partea 3: Autentificarea perifericelor utilizând un algoritm cu cheie publică. Ediția a doua: 1998
ISO 16844-3	Vehicule rutiere – Sisteme de tahograf – Partea 3: Interfața senzorului de mișcare.

1.2. Notății și termeni prescurțați

În prezentul apendice sunt folosite următoarele notații și termeni prescurțați:

(K_a, K_b, K_c)	Un grup de chei utilizat de algoritmul triplu de criptare a datelor
CA	Autoritate de certificare
CAR	Trimitere la autoritatea de certificare
CC	Sumă de control criptografică
CG	Criptogramă
CH	Antet de comandă
CHA	Autorizarea titularului certificatului
CHR	Trimitere la titularul certificatului
D()	Decriptare cu DES (Data Encryption Standard)
DE	Element de date
DO	Obiect de date
d	Cheie privată, exponent privat RSA
e	Cheie publică, exponent public RSA
E()	Criptare cu DES
EQT	Echipament
$Hash()$	Valoare de distribuire, rezultatul funcției <i>hash</i>
<i>Hash</i>	Funcție de distribuire
KID	Identificator de cheie
Km	Cheie TDES. Cheie principală definită în ISO 16844-3
Km_{VU}	Cheie TDES introdusă în unitățile montate pe vehicul
Km_{WC}	Cheie TDES introdusă în cardurile atelierelor
m	Reprezentant pentru mesaj, număr întreg cuprins între 0 și $n - 1$
n	Chei RSA, modulo
PB	Octeți de completare
PI	Octet indicator de completare (utilizat în criptograme pentru confidențialitatea DO)
PV	Valoare normală
s	Reprezentant pentru semnătură, număr întreg cuprins între 0 și $n - 1$
SSC	Contor de secvențe trimise
SM	Mesagerie securizată
TCBC	Mod de funcționare prin înlănțuirea blocurilor de cifru TDEA
TDEA	Algoritm triplu de criptare a datelor
TLV	Valoarea unei lungimi de marcat
VU	Unitate montată pe vehicul
X.C	Certificatul utilizatorului X eliberat de o autoritate de certificare
X.CA	O autoritate de certificare a utilizatorului X
X.CA.PK ₀ X.C	Operația de dezvăluire a unui certificat pentru a extrage o cheie publică. Este un operator infix, al cărui operand stâng este cheia publică a unei autorități de certificare, iar operandul drept este certificatul eliberat de acea autoritate de certificare. Rezultatul este cheia publică a utilizatorului X al cărui certificat este operandul drept.

X.PK	Cheia publică a utilizatorului X
X.PK[I]	Cifrarea RSA a unor informații I, folosind cheia publică a utilizatorului X
X.SK	Cheia privată RSA a utilizatorului X
X.SK[I]	Cifrarea RSA a unor informații I, folosind cheia privată a utilizatorului X
«xx»	O valoare hexazecimală
	Operatorul de concatenare

2. SISTEME ȘI ALGORITMI CRIPTOGRAFICI

2.1. Sisteme criptografice

CSM_001 Unitățile montate pe vehicule și cardurile de tahograf utilizează un sistem criptografic cu cheie publică RSA clasic pentru a oferi următoarele mecanisme de securitate:

- autentificare între unitățile montate pe vehicule și carduri;
- transportul cheilor de sesiune DES triple între unitățile montate pe vehicule și cardurile de tahograf;
- semnătura digitală a datelor descărcate din unitățile montate pe vehicule și din cardurile de tahograf pe suporturi externe.

CSM_002 Unitățile montate pe vehicule și cardurile de tahograf utilizează un sistem criptografic simetric DES triplu pentru a asigura un mecanism pentru integritatea datelor în timpul schimburilor de date privind utilizatorul dintre unitățile montate pe vehicul și cardurile de tahograf și pentru a asigura, unde este cazul, confidențialitatea schimburilor de date dintre unitățile montate pe vehicule și cardurile de tahograf.

2.2. Algoritmi criptografici

2.2.1. Algoritmul RSA

CSM_003 Algoritmul RSA este definit integral prin următoarele relații:

$$\begin{aligned} X.SK[m] &= s = m^d \bmod n \\ X.PK[s] &= m = s^e \bmod n \end{aligned}$$

O descriere mai completă a funcției RSA poate fi găsită în referința (PKCS1).

Exponentul public, e, pentru calculele RSA este diferit de 2 în toate cheile RSA generate.

2.2.2. Algoritmul de distribuire

CSM_004 Mecanismele de semnătură digitală utilizează algoritmul de distribuire SHA-1 așa cum este definit în referința (SHA-1).

2.2.3. Algoritmul de criptare a datelor

CSM_005 Algoritmii pe baza DES sunt utilizați în modul de funcționare prin înlănțuirea blocurilor de cifru.

3. CHEI ȘI CERTIFICATE

3.1. Generarea și distribuția cheilor

3.1.1. Generarea și distribuția cheilor RSA

CSM_006 Cheile RSA sunt generate prin trei niveluri ierarhice funcționale:

- nivelul european;
- nivelul statului membru;
- nivelul echipamentului.

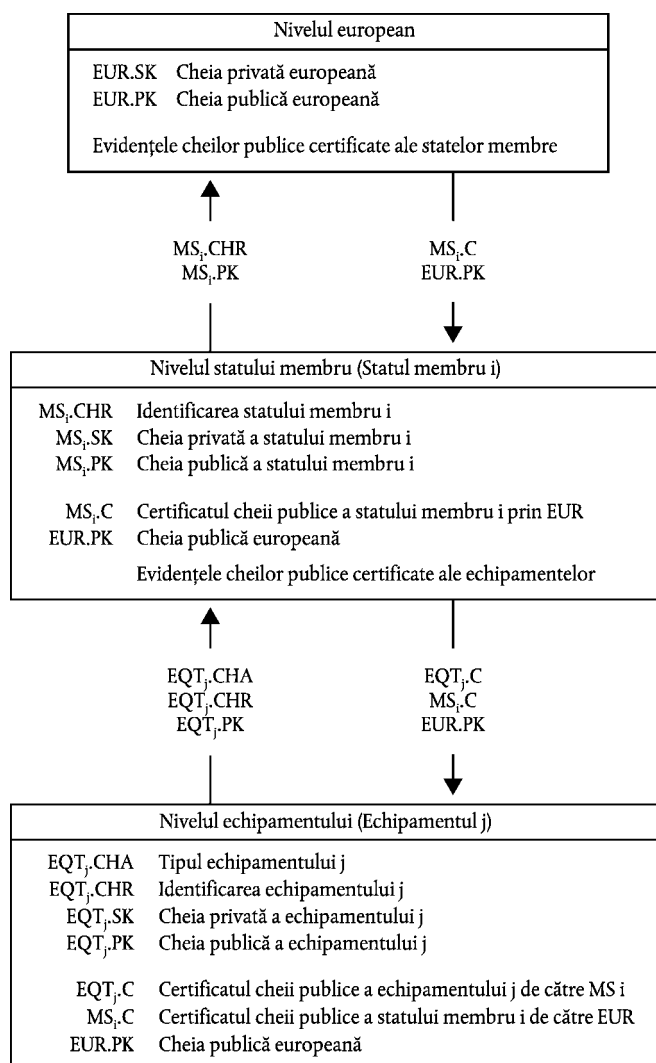
CSM_007 La nivelul european, se generează o singură pereche de chei europene (EUR.SK și EUR.PK). Cheia privată europeană se utilizează pentru certificarea cheilor publice ale statelor membre. Se ține evidența tuturor cheilor certificate. Aceste sarcini sunt îndeplinite de o autoritate de certificare europeană, sub autoritatea și responsabilitatea Comisiei Europene.

CSM_008 La nivelul statului membru, se generează o pereche de chei ale statului membru (MS.SK și MS.PK). Cheile publice ale statelor membre sunt certificate de Autoritatea de certificare europeană. Cheile private ale statelor membre se utilizează pentru certificarea cheilor publice care se introduc în echipament (unitate montată pe vehicul sau card de tahograf). Se ține evidența tuturor cheilor publice certificate împreună cu identificarea echipamentului pentru care se folosesc. Aceste sarcini sunt îndeplinite de o autoritate de certificare a statului membru. Un stat membru își poate schimba periodic perechea de chei.

CSM_009 La nivelul echipamentului, se generează o singură pereche de chei (EQT.SK și EQT.PK) și se introduce în fiecare echipament. Cheile publice ale echipamentelor sunt certificate de o autoritate de certificare a statului membru. Aceste sarcini pot fi îndeplinite de producătorii de echipamente, de personalizatorii de echipamente sau de autoritățile statelor membre. Această pereche de chei se folosește pentru serviciile de autentificare, semnătură digitală și cifrare.

CSM_010 Confidențialitatea cheilor private trebuie menținută în timpul generării, transportului (dacă este cazul) și stocării.

Ilustrația următoare sintetizează fluxul de date al acestui proces.



3.1.2. *Chei de test RSA*

CSM_011 Pentru testarea echipamentelor (inclusiv testele de interoperare) autoritatea de certificare europeană generează o pereche unică diferită de chei de test europene și cel puțin două perechi de chei de test ale statelor membre, ale căror chei publice sunt certificate cu cheia de test privată europeană. Producătorii introduc, în echipamentele supuse testelor pentru omologarea de tip, chei de test certificate cu una dintre aceste chei de test ale statelor membre.

3.1.3. *Cheile senzorului de mișcare*

Confidențialitatea celor trei chei TDES descrise mai jos trebuie menținută corespunzător în timpul generării, transportului (dacă este cazul) și stocării.

Pentru a asigura suportul pentru aparatele de înregistrare compatibile ISO 16844, autoritatea de certificare europeană și autoritățile de certificare din statele membre asigură, în plus, următoarele:

CSM_036 Autoritatea de certificare europeană generează $K_{m_{VU}}$ și $K_{m_{WC}}$, două chei DES triple independente și unice, și generează K_m ca fiind:

$$K_m = K_{m_{VU}} \text{ XOR } K_{m_{WC}}$$

Autoritatea de certificare europeană trimite aceste chei, prin proceduri securizate corespunzătoare, autorităților de certificare ale statelor membre la cererea acestora.

CSM_037 Autoritățile de certificare ale statelor membre:

- folosesc K_m pentru a cripta datele senzorului de mișcare solicitate de producătorii de senzori de mișcare (datele care trebuie criptate cu K_m sunt definite în ISO 16844-3);
- trimit $K_{m_{VU}}$ producătorilor de unități montate pe vehicule, prin proceduri securizate corespunzătoare, pentru introducere în unitățile montate pe vehicule;
- se asigură că $K_{m_{WC}}$ este introdus în toate cardurile atelierelor (`SensorInstallationSecData`) în fișierul elementar `Sensor_Installation_Data` în timpul personalizării cardului.

3.1.4. *Generarea și distribuția cheilor de sesiune T-DES*

CSM_012 Unitățile montate pe vehicule și cardurile de tahograf generează și schimbă datele necesare pentru elaborarea unei chei de sesiune T-DES triple comune, ca parte a procesului de autentificare reciprocă. Confidențialitatea acestui schimb de date trebuie să fie protejată printr-un mecanism de criptare RSA.

CSM_013 Această cheie se utilizează pentru toate operațiunile criptografice ulterioare folosind mesageria securizată. Valabilitatea ei expiră la terminarea sesiunii (retragerea cardului sau reinițializarea cardului) și/sau după 240 de utilizări (o utilizare a cheii = o comandă trimisă cardului folosind mesageria securizată și răspunsul asociat).

3.2. *Chei*

CSM_014 Cheile RSA au (indiferent de nivel) următoarele lungimi: modulo n 1024 biți, exponentul public e maxim 64 biți, exponentul privat d 1024 biți.

CSM_015 Cheile DES triple au forma (K_a, K_b, K_a) unde K_a și K_b sunt chei independente cu o lungime de 64 biți. Nu se fixează nici un bit de detectare a erorilor de paritate.

3.3. *Certificate*

CSM_016 Certificatele cheilor publice RSA sunt certificate de tip «non self-descriptive» și «Card Verifiable» (Ref.: ISO/IEC 7816-8)

3.3.1. **Conținutul certificatelor**

CSM_017 Certificatele cheilor publice RSA sunt alcătuite din datele următoare în ordinea indicată:

Date	Format	Ocțeți	Observații
CPI	ÎNTREG	1	Identificator de profil al certificatului ('01' pentru această versiune)
CAR	ȘIR DE OCTEȚI	8	Referința autorității de certificare
CHA	ȘIR DE OCTEȚI	7	Autorizația titularului certificatului
EOV	Timp Real	4	Termenul de expirare a valabilității certificatului. Opțional, umplut cu 'FF' dacă nu este folosit
CHR	ȘIR DE OCTEȚI	8	Referința titularului certificatului
<i>n</i>	ȘIR DE OCTEȚI	128	Cheie publică (modulo)
<i>e</i>	ȘIR DE OCTEȚI	8	Cheie publică (exponent public)
		164	

Note:

1. «Indicatorul de profil al certificatului» (CPI) determină structura precisă a unui certificat de autentificare. El poate fi folosit ca identificator intern al echipamentului pentru o listă antet relevantă care descrie concatenarea elementelor de date în cadrul certificatului.

Lista antet asociată cu acest conținut al certificatului este următoarea:

'4D'	'16'	'5F 29'	'01'	'42'	'08'	'5F 4B'	'07'	'5F 24'	'04'	'5F 20'	'08'	'7F 49'	'05'	'81'	'81 80'	'82'	'08'
Marcaj listă antet extinsă	Lungimea listei antet	Marcaj CPI	Lungime CPI	Marcaj CAR	Lungime CAR	Marcaj CHA	Lungime CHA	Marcaj EOv	Lungime EOv	Marcaj CHR	Lungime CHR	Marcaj cheie publică (construită)	Lungimea DO următoare	Marcaj modulo	Lungime modulo	Marcaj exponent public	Lungime exponent public

2. «Referința autorității de certificare» (CAR) are scopul de a identifica autoritatea de certificare care a emis certificatul, astfel încât elementul de date să poată fi folosit în același timp și ca un identificator al cheii de autoritate pentru a trimite la cheia publică a autorității de certificare (pentru codificare, vezi mai jos identificatorul de cheie).
3. «Autorizația titularului certificatului» (CHA) este folosită pentru a identifica drepturile titularului certificatului. Ea se compune din Identificatorul aplicației tahografului și din tipul de echipament pentru care este destinat certificatul (în conformitate cu elementul de date EquipmentType, «00» pentru un stat membru).
4. «Referința titularului certificatului» (CHR) are scopul de a identifica în mod unic titularul certificatului, astfel încât elementul de date să poată fi folosit în același timp ca identificator al cheii subiect pentru a trimite la cheia publică a titularului certificatului.
5. Identificatoarele cheii identifică în mod unic titularul certificatului sau autoritatea de certificare. Acestea sunt codificate după cum urmează:

5.1. Echipament (UV sau card):

Date	Numărul de serie al echipamentului	Date	Tip	Producător
Lungime	4 ocțeți	2 ocțeți	1 octet	1 octet
Valoare	Întreg	11 aa codare BCD	Specific producătorului	Codul producătorului

În cazul unei unități montate pe vehicul, când producătorul solicită certificate, el poate sau nu să cunoască identificatorul echipamentului în care vor fi introduse cheile.

În primul caz, producătorul trimite identificatorul echipamentului împreună cu cheia publică la autoritatea din statul membru respectiv pentru certificare. Certificatul va conține atunci identificatorul echipamentului, iar producătorul trebuie să se asigure că cheile și certificatele sunt introduse în echipamentele prevăzute. Identificatorul cheii are forma indicată mai sus.

În al doilea caz, producătorul trebuie să identifice în mod unic fiecare cerere de certificare și să trimită acest identificator împreună cu cheia publică la autoritatea din statul membru respectiv pentru certificare. Certificatul conține identificatorul cererii. Producătorul trebuie să informeze autoritatea de certificare din statul membru cu privire la atribuirea cheii echipamentului (adică identificatorul cererii de certificare, identificatorul echipamentului) după instalarea cheii în echipament. Identificatorul cheii are forma următoare:

Date	Numărul de serie al cererii de certificare	Date	Tip	Producător
Lungime	4 octeți	2 octeți	1 octet	1 octet
Valoare	Codare BCD	11 aa codare BCD	'FF'	Codul producătorului

5.2. Autoritatea de certificare

Date	Identificatorul autorității	Numărul de serie al cheii	Informații suplimentare	Identificator
Lungime	4 octeți	1 octet	2 octeți	1 octet
Valoare	Codul numeric național 1 octet Codul alfanumeric național 3 octeți	Întreg	Cod suplimentar (specific CA) 'FF FF' dacă nu este folosit	'01'

Numărul de serie al cheii este folosit pentru a distinge cheile diferite ale unui stat membru, în cazul în care cheia este schimbată.

6. Verificatorii certificatelor știu implicit că cheia publică certificată este o cheie RSA relevantă pentru autentificarea, verificarea semnăturii digitale și cifrarea pentru serviciile de confidențialitate (certificatul nu conține nici un identificator de obiect care să specifice acest lucru).

3.3.2. Certificate emise

CSM_018 Certificatul emis este o semnătură digitală cu recuperarea parțială a conținutului certificatului în conformitate cu ISO/IEC 9796-2, cu «Referința autorității de certificare» adăugată.

$$X.C = X.CA.SK[6A] || C_r || Hash(Cc) || BC || C_n || X.CAR$$

Cu conținutul certificatului = Cc = $\begin{matrix} C_r \\ 106 \text{ Bytes} \end{matrix} || \begin{matrix} C_n \\ 58 \text{ Bytes} \end{matrix}$

Note:

1. Acest certificat are o lungime de 194 octeți.
2. CAR, fiind ascuns de semnătură, este în același timp adăugat la semnătură, astfel încât cheia publică a autorității de certificare să poată fi selectată pentru verificarea certificatului.
3. Verificatorul certificatului cunoaște implicit algoritmul folosit de autoritatea de certificare pentru semnarea certificatului.

4. Lista antet asociată cu acest certificat emis este după cum urmează:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
Marcaj certificat CV (Construit)	Lungimea DO următoare	Marcaj semnătură	Lungime semnătură	Marcaj rest	Lungime rest	Marcaj CAR	Lungime CAR

3.3.3. Verificarea și dezvăluirea certificatelor

Verificarea și dezvăluirea certificatelor constă în verificarea semnăturii în conformitate cu ISO/IEC 9796-2, extrăgând conținutul certificatului și cheia publică conținută: $X.PK = X.CA.Pk_o.X.C$ și verificarea valabilității certificatului.

CSM_019 Aceasta implică următoarele etape:

Verificarea semnăturii și extragerea conținutului:

- din $X.C$ extrage Semn, C_n' și CAR' : $X.C = \begin{matrix} \text{Sign} \\ 128 \text{ Bytes} \end{matrix} \parallel \begin{matrix} C_n' \\ 58 \text{ Bytes} \end{matrix} \parallel \begin{matrix} CAR' \\ 8 \text{ Bytes} \end{matrix}$
- din CAR' selectează cheia publică a autorității de certificare corespunzătoare (dacă nu s-a efectuat anterior prin alte metode)
- deschide Semn cu Cheia publică a CA: $Sr' = X.CA.PK [Semn]$,
- verifică dacă Sr' începe cu '6A' și se termină cu 'BC'
- calculează Cr' și H' din: $Sr' = \begin{matrix} '6A' \\ 106 \text{ Bytes} \end{matrix} \parallel \begin{matrix} C_r' \\ 20 \text{ Bytes} \end{matrix} \parallel \begin{matrix} H' \\ 20 \text{ Bytes} \end{matrix} \parallel \begin{matrix} 'BC' \end{matrix}$
- recuperează conținutul certificatului $C' = C_r' \parallel C_n$
- verifică $Hash(C') = H'$

Dacă verificările sunt în regulă, certificatul este original, având conținutul C.

Verificarea valabilității. Din C:

- dacă este cazul, verifică termenul de expirare a valabilității

Extrage și stochează cheia publică, identificatorul cheii, autorizarea titularului certificatului și data de expirare a valabilității din C:

- $X.PK = n \parallel e$
- $X.KID = CHR$
- $X.CHA = CHA$
- $X.EOV = EOV$

4. MECANISMUL DE AUTENTIFICARE RECIPROCĂ

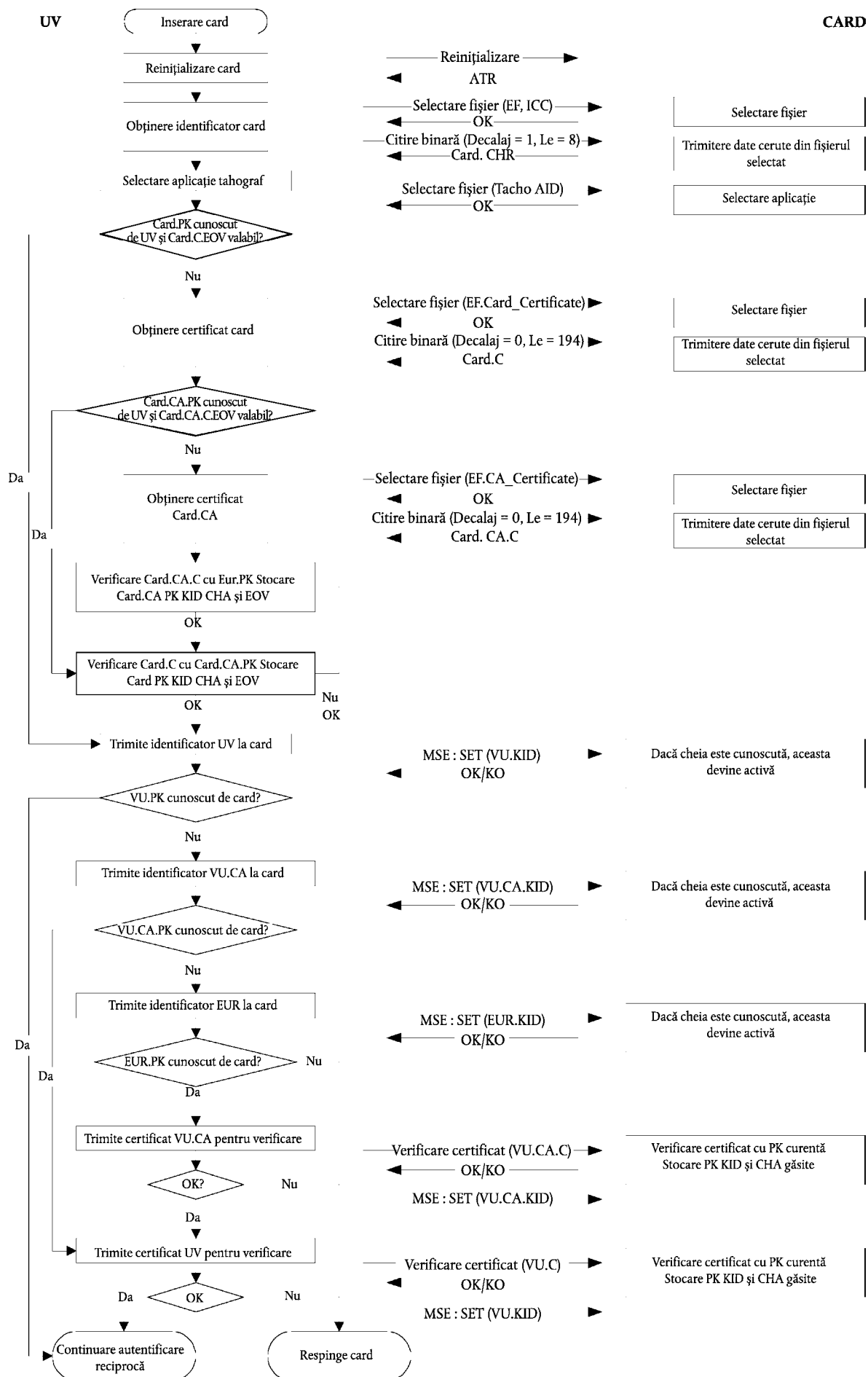
Autentificarea reciprocă între carduri și unitățile montate pe vehicule se bazează pe principiul următor:

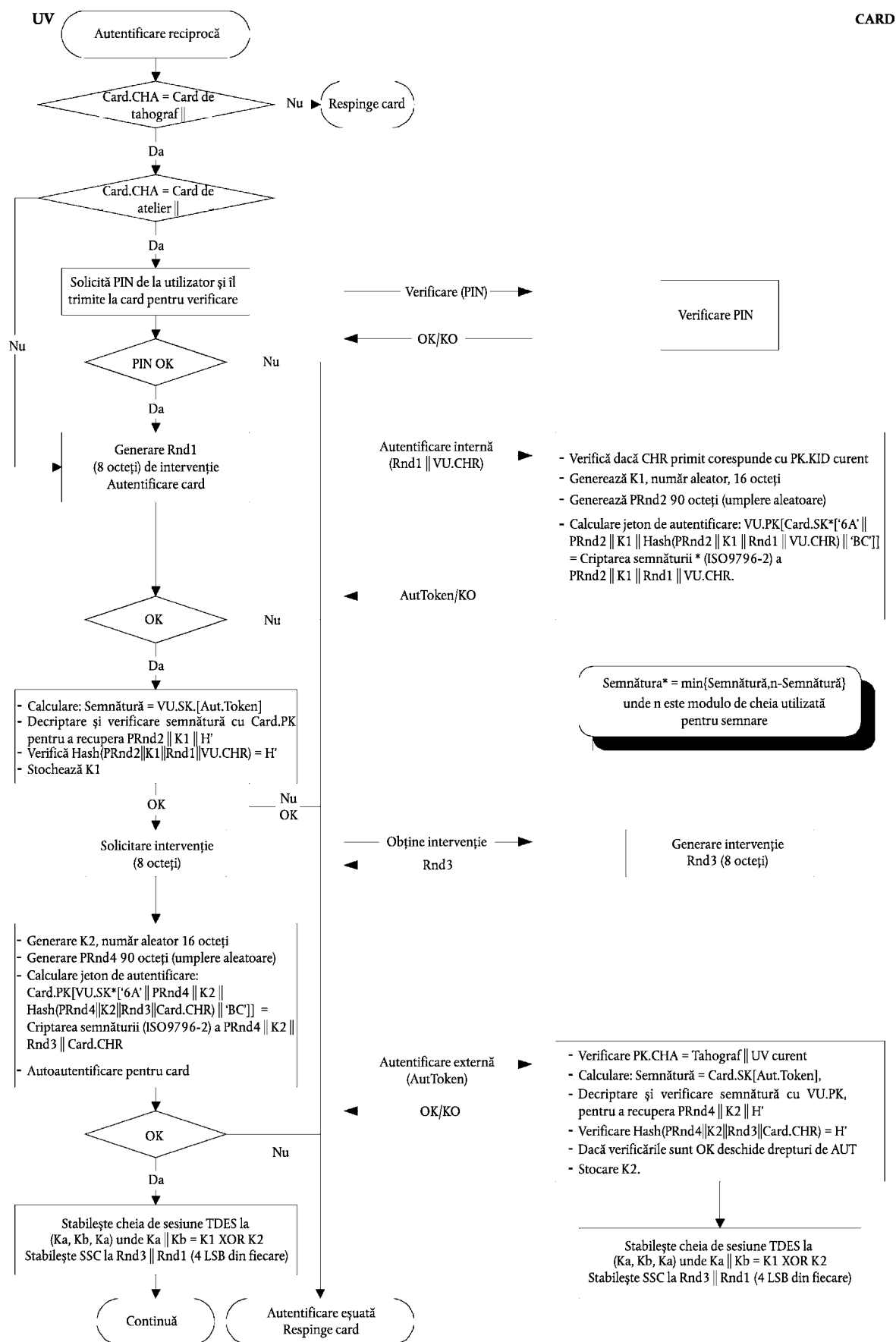
Fiecare parte îi demonstrează celeilalte că deține o pereche valabilă de chei, a cărei cheie publică a fost certificată de o autoritate de certificare a statului membru, care la rândul ei a fost certificată de autoritatea de certificare europeană.

Demonstrația se face prin semnarea cu cheia privată a unui număr aleatoriu trimis de cealaltă parte, care trebuie să recupereze numărul aleatoriu trimis în momentul verificării acestei semnături.

Mecanismul este declanșat la introducerea cardului de către unitatea montată pe vehicul. Începe cu schimbul de certificate și dezvăluirea cheilor publice și se termină cu stabilirea unei chei de sesiune.

CSM_020 Trebuie utilizat următorul protocol [săgețile indică comenzile și datele schimbate (vezi apendicele 2)]:





5. CONFIDENȚIALITATEA, INTEGRITATEA ȘI MECANISMUL DE AUTENTIFICARE A TRANSFERULUI DE DATE DINTRE UNITĂȚILE MONTATE PE VEHICUL ȘI CARDURI

5.1. Mesageria securizată

- CSM_021 Integritatea transferurilor de date dintre unitățile montate pe vehicul și carduri trebuie protejată prin mesagerie securizată în conformitate cu referințele (ISO/IEC 7816-4) și (ISO/IEC 7816-8).
- CSM_022 Atunci când datele trebuie să fie protejate în timpul transferului, se adaugă un obiect de date sumă de control criptografică la obiectele de date trimise în cadrul comenzii sau al răspunsului. Suma de control criptografică este verificată de receptor.
- CSM_023 Suma de control criptografică a datelor trimise în cadrul unei comenzi integrează antetul comenzii și toate obiectele de date trimise (= > CLA = '0C' și toate obiectele de date sunt încapsulate cu marcaje în care b1 = 1).
- CSM_024 Octeții de stare-informații ai răspunsului sunt protejați printr-o sumă de control criptografică atunci când răspunsul nu conține nici un câmp de date.
- CSM_025 Sumele de control criptografice au o lungime de patru octeți.

Structura comenzilor și răspunsurilor când se utilizează mesageria securizată este următoarea:

Obiectele de date utilizate sunt un set parțial din obiectele de date de mesagerie securizată descrise în ISO/IEC 7816-4:

Marcaj	Cod mnemonic	Semnificație
'81'	T _{PV}	Valoare normală necodată prin BER-TLV (de protejat prin CC)
'97'	T _{LE}	Valoarea Le din comanda nesecurizată (de protejat prin CC)
'99'	T _{SW}	Informații de stare (de protejat prin CC)
'8E'	T _{CC}	Sumă de onrol criptografică
'87'	T _{PI CG}	Octet indicator de umplere Criptogramă (valoare normală necodată prin BER-TLV)

Fiind dată o pereche comandă-răspuns nesecurizată:

Antetul comenzii	Corpul comenzii
CLA INS P1 P2	(câmp L _c) (câmp de date) (câmp L _c)
patru octeți	L octeți, indicați prin B ₁ -B _L

Corpul răspunsului	Coda răspunsului
(Câmp de date)	SW1 SW2
Octeți de date L _r	Doi octeți

Perechea corespunzătoare comandă-răspuns securizată este:

Comanda securizată:

Antetul comenzii (CH)	Corpul comenzii										
CLA INS P1 P2	(Câmp L _c nou)	(Câmp de date nou)									(Câmp L _c nou)
'0C'	Lungimea noului câmp de date	T _{PV}	L _{PV}	PV	T _{LE}	L _{LE}	L _c	T _{CC}	L _{CC}	CC	'00'
		'81'	L _c	Câmp de date	'97'	'01'	L _c	'8E'	'04'	CC	

Datele care trebuie integrate în suma de control = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB

PB = octeți de umplere (80..00) în conformitate cu ISO-IEC 7816-4 și ISO 9797 metoda 2.

Obiectele de date PV și LE sunt prezente numai dacă există date corespondente și în comanda nesecurizată.

Răspunsul securizat:

1. Cazul în care câmpul de date răspuns nu este gol și nu este nevoie să fie protejat pentru confidențialitate:

Corpul răspunsului						Coda răspunsului
(Câmp de date nou)						SW1 SW2 nou
T _{PV}	L _{PV}	PV	T _{CC}	L _{CC}	CC	
'81'	L _r	Câmp de date	'8E'	'04'	CC	

Datele care se integrează în suma de control = T_{PV} || L_{PV} || PV || PB

2. Cazul în care câmpul de date răspuns nu este gol și este nevoie să fie protejat pentru confidențialitate:

Corpul răspunsului						Coda răspunsului
(Câmp de date nou)						SW1 SW2 nou
T _{PI CG}	L _{PI CG}	PI CG	T _{CC}	L _{CC}	CC	
'87'		PI CG	'8E'	'04'	CC	

Datele care sunt transportate prin CG: date necodate prin BER-TLV și octeții de umplere.

Datele care se integrează în suma de control = T_{PI CG} || L_{PI CG} || PI CG || PB

3. Cazul în care câmpul de date răspuns este gol:

Corpul răspunsului						Coda răspunsului
(Câmp de date nou)						SW1 SW2 nou
T _{SW}	L _{SW}	SW	T _{CC}	L _{CC}	CC	
'99'	'02'	SW1 SW2 nou	'8E'	'04'	CC	

Datele care se integrează în suma de control = T_{SW} || L_{SW} || SW || PB

5.2. Tratarea erorilor de mesagerie securizată

CSM_026 Atunci când cardul de tahograf recunoaște o eroare de SM în timpul interpretării unei comenzi, octeții de stare trebuie să fie returnați fără SM. În conformitate cu ISO/IEC 7816-4, sunt definiți următorii octeți de stare pentru a indica erorile SM:

'66 88' verificarea sumei de control criptografice care eșuase;

'69 87' obiectul de date SM așteptat lipsește;

'69 88' obiectele de date SM sunt incorecte.

CSM_027 Atunci când cardul de tahograf returnează octeții de stare fără obiectele de date ale SM sau cu un obiect de date SM eronat, sesiunea trebuie să fie terminată de unitatea montată pe vehicul.

5.3. Algoritmul de calcul al sumelor de control criptografic

CSM_028 Sumele de control criptografice sunt construite folosind controale de acces la suport (MAC) detaliate în conformitate cu ANSI X9.19 cu DES:

- etapa inițială: blocul de verificare inițial y_0 este $E(K_a, SSC)$;
- etapa secvențială: blocurile de verificare $y_1, \dots, y_n$ sunt calculate folosind K_a ;
- etapa finală: suma de control criptografică este calculată din ultimul bloc de control y_n după cum urmează: $E(K_a, D(K_b, y_n))$.

Unde $E()$ este criptarea cu DES, iar $D()$ este decriptarea cu DES.

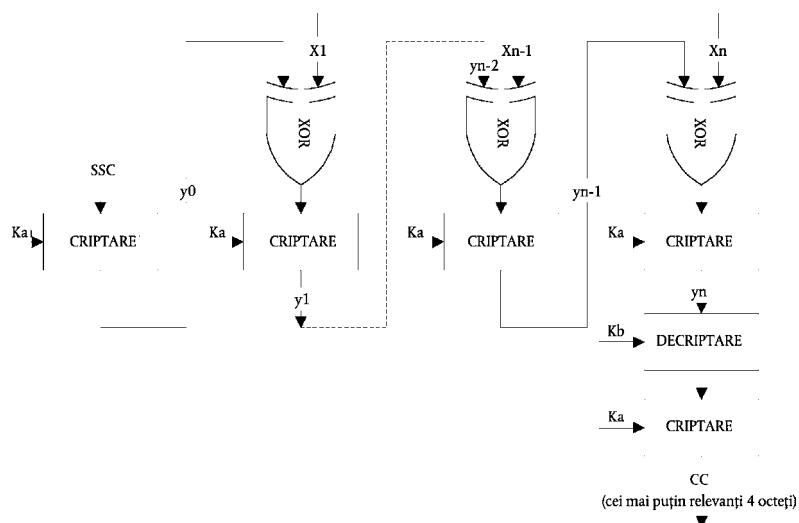
Cei mai relevanți patru octeți ai sumei de control criptografice sunt transferați.

CSM_029 Contorul de secvențe trimise (SSC) este inițializat în timpul procedurii de acord asupra cheii la:

SSC inițial: $Rnd3$ (cei mai puțin relevanți 4 octeți) || $Rnd1$ (cei mai puțin relevanți 4 octeți).

CSM_030 Contorul de secvențe trimise este incrementat cu 1 de fiecare dată înainte de calcularea unui MAC (de exemplu SSC pentru prima comandă este SSC inițial + 1, SSC pentru primul răspuns este SSC inițial + 2).

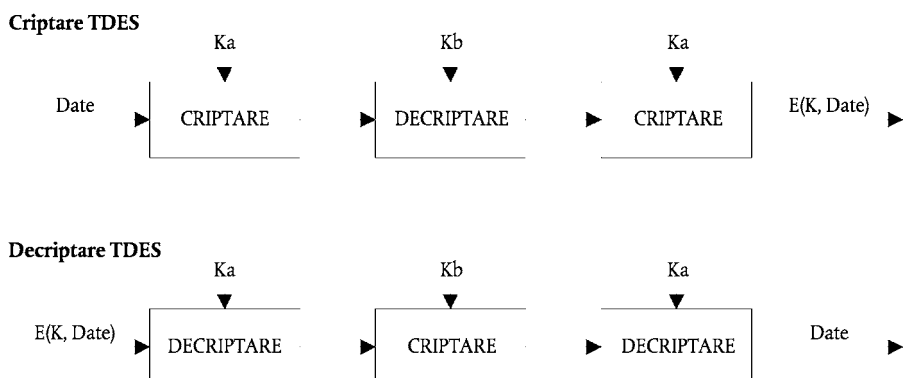
Figura următoare ilustrează calcularea MAC detaliat:



5.4. Algoritmul de calcul al criptogramelor pentru DO confidențiale

CSM_031 Criptogramele sunt calculate folosind TDEA în modul de funcționare TCBC în conformitate cu referințele (TDES) și (TDES-OP) și cu vectorul nul ca bloc de valoare inițial.

Figura următoare ilustrează aplicarea cheilor în TDES:



6. MECANISMELE DE SEMNARE DIGITALĂ A DATELOR DESCĂRCATE

CSM_032 Echipamentul inteligent dedicat (EID) stochează datele recepționate de la un echipament (UV sau card) în timpul unei sesiuni de descărcare într-un singur fișier fizic de date. Acest fișier trebuie să conțină certificatele MS_iC și EQT.C. Fișierul conține semnăturile digitale ale blocurilor de date așa cum se specifică în apendicele 7 Protocoale de descărcare a datelor.

CSM_033 Semnăturile digitale ale datelor descărcate utilizează o schemă de semnătură digitală cu apendice astfel încât datele descărcate să poată fi citite fără nici o descifrare dacă se dorește.

6.1. Generarea semnăturilor

CSM_034 Generarea semnăturilor de date de către echipament trebuie să respecte schema de semnătură cu apendice definită în referința (PKCS1) cu funcția de distribuire SHA-1:

$$\text{Semnătură} = \text{EQT.SK}\{\text{'00' || '01' || PS || '00' || DER[SHA-1(Date)]}\}$$

PS Șir de octeți de umplere cu valoarea 'FF' astfel încât lungimea să fie 128.

DER(SHA-1(M)) este codarea identificatorului algoritmului pentru funcția de distribuire și valoarea de distribuire într-o valoare ASN.1 de tip *DigestInfo* (reguli de codare distincte):

'30' || '21' || '30' || '09' || '06' || '05' || '2B' || '0E' || '03' || '02' || '1A' || '05' || '00' || '04' || '14' || Valoare de distribuire.

6.2. Verificarea semnăturilor

CSM_035 Verificarea semnăturii datelor la datele descărcate trebuie să respecte schema de semnătură cu apendice definită în referința (PKCS1) cu funcția de distribuire SHA-1:

Cheia publică europeană EUR.PK trebuie să fie cunoscută independent (și aprobată) de vericator.

Tabelul următor ilustrează protocolul pe care îl respectă un EID dotat cu un card de control pentru a verifica integritatea datelor descărcate și stocate pe ESM (suport de memorie extern). Cardul de control este folosit pentru a efectua descifrarea semnăturilor digitale. Această funcție poate în acest caz să nu fie implementată în EID.

Echipamentul care a descărcat și semnat datele de analizat este denumit EQT.

