

32002R1360

5.8.2002

DZIENNIK URZĘDOWY WSPÓLNOT EUROPEJSKICH

L 207/1

ROZPORZĄDZENIE KOMISJI (WE) NR 1360/2002**z dnia 13 czerwca 2002 r.****dostosowujące po raz siódmy do postępu technicznego rozporządzenie Rady (EWG) nr 3821/85 w sprawie urządzeń rejestrujących stosowanych w transporcie drogowym****(Tekst mający znaczenie dla EOG)**

KOMISJA WSPÓLNOT EUROPEJSKICH,

uwzględniając Traktat ustanawiający Wspólnotę Europejską,

uwzględniając rozporządzenie Rady (EWG) nr 3821/85 z dnia 20 grudnia 1985 r. w sprawie urządzeń rejestrujących stosowanych w transporcie drogowym ⁽¹⁾, ostatnio zmienione rozporządzeniem (WE) nr 2135/98 ⁽²⁾, w szczególności jego art. 17 i 18,

a także mając na uwadze, co następuje:

- (1) Wymagania techniczne określone w załączniku I B do rozporządzenia (EWG) nr 3821/85 należy dostosować do postępu technicznego zwracając uwagę, w szczególności, na całkowite bezpieczeństwo systemu i współdziałanie urządzeń rejestrujących z kartami kierowcy.
- (2) Dostosowanie urządzeń wymaga też dostosowania załącznika II do rozporządzenia (EWG) nr 3821/85, w którym zdefiniowano znaki i świadectwa homologacji.
- (3) Komitet powołany na mocy art. 18 rozporządzenia (EWG) nr 3821/85 nie wydał opinii o środkach przewidzianych we wniosku i dlatego też Komisja złożyła do Rady wnioski dotyczące tych środków.
- (4) Do końca okresu ustanowionego w art. 18 ust. 5 lit. b) rozporządzenia (EWG) nr 3821/85 Rada nie wykonała czynności i w związku z tym na Komisji spoczywa zadanie przyjęcia tych środków,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Załącznik do rozporządzenia (WE) nr 2135/98 zastępuje się Załącznikiem do niniejszego rozporządzenia.

Artykuł 2

W załączniku II do rozporządzenia (EWG) nr 3821/85 wprowadza się następujące zmiany:

1. W rozdziale I pozycja 1 akapit pierwszy wprowadza się następujące zmiany:
 - konwencjonalny znak państwa dla Grecji „GR” zastępuje się liczbą „23”,
 - konwencjonalny znak państwa dla Irlandii „IRL” zastępuje się liczbą „24”,
 - dodaje się znak państwa „12” dla Austrii,
 - dodaje się znak państwa „17” dla Finlandii,
 - dodaje się znak państwa „5” dla Szwecji.
2. W rozdziale I pozycja 1 akapit drugi wprowadza się następujące zmiany:
 - wyrazy „lub karcie do tachografów” dodaje się po wyrazie „wykresówce”.
3. W rozdziale I pozycja 2 wprowadza się następujące zmiany:
 - wyrazy „i na każdej karcie do tachografów” dodaje się po wyrazie „wykresówce”.
4. W rozdziale II do tytułu dodaje się następujące wyrazy „DLA PRODUKTÓW ZGODNYCH Z ZAŁĄCZNIKIEM I”.

⁽¹⁾ Dz.U. L 370 z 31.12.1985, str. 8.⁽²⁾ Dz.U. L 274 z 9.10.1998, str. 1.

5. Dodaje się rozdział III w brzmieniu:

„III. ŚWIADECTWO HOMOLOGACJI TYPU DLA PRODUKTÓW ZGODNYCH Z ZAŁĄCZNIKIEM B

Państwo, wydając homologację, wydaje wnioskodawcy świadectwo homologacji typu, zgodnie ze wzorem zamieszczonym poniżej. Informując Państwa Członkowskie o wydanych homologacjach lub, zależnie od okoliczności, o ich wycofaniu, Państwo Członkowskie używa kopii tego świadectwa.

ŚWIADECTWO HOMOLOGACJI TYPU DLA PRODUKTÓW ZGODNYCH Z ZAŁĄCZNIKIEM I B

Nazwa właściwego organu administracyjnego

Zawiadomienie dotyczy ⁽³⁾:

- ☐ homologacji
- ☐ cofnięcia homologacji
- ☐ typu urządzenia rejestrującego
- ☐ elementu urządzenia rejestrującego ⁽⁴⁾
- ☐ karty kierowcy
- ☐ karty kierowcy
- ☐ karty firmowej
- ☐ karty kontrolnej

nr homologacji

1. Znak fabryczny lub towarowy
2. Nazwa typu
3. Nazwa producenta
4. Adres producenta
5. Zgłoszono do homologacji
6. Laboratorium(-a)
7. Data i liczba testu(-ów)
8. Data homologacji
9. Data wycofania homologacji
10. Typ lub typy elementów urządzeń rejestrujących, do których element jest przeznaczony
11. Miejscowość
12. Data
13. Załączone dokumenty opisowe
14. Uwagi, (gdy dotyczy także miejsce założenia plomby)

(podpis)

⁽³⁾ Zaznaczyć odpowiednie rubryki.

⁽⁴⁾ Określić element, którego dotyczy zawiadomienie.”

Artykuł 3

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Wspólnot Europejskich*.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich Państwach Członkowskich.

Sporządzono w Brukseli, dnia 13 czerwca 2002 r.

W imieniu Komisji
Loyola DE PALACIO
Wiceprzewodniczący

ZAŁĄCZNIK

„ZAŁĄCZNIK I B

WYMAGANIA DOTYCZĄCE BUDOWY, BADAŃ, INSTALACJI I KONTROLI

SPIS TREŚCI

I.	DEFINICJE	286
II.	CHARAKTERYSTYKI OGÓLNE I FUNKCJE URZĄDZENIA REJESTRUJĄCEGO	290
1.	Charakterystyki ogólne	290
2.	Funkcje	290
3.	Tryby pracy	291
4.	Zabezpieczenie	292
III.	WYMAGANIA ODNOŚNIE DO KONSTRUKCJI I FUNKCJONALNOŚCI URZĄDZENIA REJESTRUJĄCEGO	292
1.	Monitorowanie wkładania i wyjmowania kart	292
2.	Pomiar prędkości i odległości	292
2.1.	Pomiar przebytej drogi	293
2.2.	Pomiar prędkości	293
3.	Pomiar czasu	293
4.	Monitorowanie czynności wykonywanych przez kierowcę	294
5.	Monitorowanie stanu prowadzenia pojazdu	294
6.	Dane wprowadzane ręcznie przez kierowcę	294
6.1.	Wprowadzanie miejsca rozpoczęcia i/lub zakończenia okresu pracy	294
6.2.	Ręczne wprowadzanie czynności wykonywanych przez kierowcę	294
6.3.	Stany szczególne	296
7.	Zarządzanie blokadami firmowymi	296
8.	Monitorowanie czynności kontrolnych	296
9.	Wykrywanie zdarzeń i/lub usterek	296
9.1.	Zdarzenie — włożenie nieważnej karty	296
9.2.	Zdarzenie — »Konflikt kart«	297
9.3.	Zdarzenie — »Nakładające się czasy«	297
9.4.	Zdarzenie — »Prowadzenie bez prawidłowej karty«	297
9.5.	Zdarzenie — »Włożenie karty podczas jazdy«	297
9.6.	Zdarzenie — »Sesja ostatniej karty nie zamknięta prawidłowo«	297
9.7.	Zdarzenie — »Przekroczenie prędkości«	297

9.8.	Zdarzenie — »Przerwa zasilania«	298
9.9.	Zdarzenie — »Błąd danych dotyczących ruchu«	298
9.10.	Zdarzenie — »Próba naruszenia zabezpieczenia«	298
9.11.	Usterka — »Karta«	298
9.12.	Usterka — »Urządzenie rejestrujące«	298
10.	Testy wbudowane i auto testy	298
11.	Odczyt z pamięci danych	298
12.	Zapisywanie i przechowywanie w pamięci danych	299
12.1.	Dane identyfikujące sprzęt	299
12.1.1.	Dane identyfikujące przyrząd rejestrujący	299
12.1.2.	Dane identyfikujące czujnik ruchu	299
12.2.	Elementy zabezpieczenia	300
12.3.	Dane rejestrowane przy wkładaniu i wyjmowaniu karty kierowcy	300
12.4.	Dane dotyczące czynności kierowcy	301
12.5.	Miejsca rozpoczęcia i/lub zakończenia dziennego okresu pracy	301
12.6.	Dane dotyczące licznika kilometrów	301
12.7.	Dane szczegółowe dotyczące prędkości	301
12.8.	Dane dotyczące zdarzeń	301
12.9.	Dane dotyczące usterek	303
12.10.	Dane kalibracyjne	304
12.11.	Dane dotyczące regulacji czasu	304
12.12.	Dane dotyczące kontroli	304
12.13.	Dane dotyczące blokad firmowych	305
12.14.	Dane dotyczące wczytywania danych	305
12.15.	Dane dotyczące warunków szczególnych	305
13.	Odczyt kart do tachografów	305
14.	Rejestrowania i przechowywanie danych na kartach do tachografów	305
15.	Wyświetlanie	306
15.1.	Informacje na wyświetlaczu w warunkach normalnych	306
15.2.	Ostrzeżenia	307
15.3.	Dostęp do menu	307
15.4.	Inne informacje	307
16.	Drukowanie	307
17.	Ostrzeżenia	308
18.	Przesyłanie danych do nośnika zewnętrznego	309
19.	Wyjście danych dla dodatkowych urządzeń zewnętrznych	309
20.	Kalibracja	310
21.	Regulacja czasu	310

22.	Charakterystyki pracy	310
23.	Materiały	310
24.	Oznakowania	311
IV.	WYMAGANIA KONSTRUKCYJNE I FUNKCYJONALNE KART DO TACHOGRAFÓW	311
1.	Dane widzialne	311
2.	Zabezpieczenie	314
3.	Normy	314
4.	Specyfikacje środowiskowe i elektryczne	314
5.	Gromadzenie danych	314
5.1.	Identyfikacja kart i bezpieczeństwo danych	315
5.1.1.	Identyfikacja aplikacji	315
5.1.2.	Identyfikacja układu scalonego	315
5.1.3.	Identyfikacja kart mikroprocesorowych	315
5.1.4.	Zabezpieczenia	315
5.2.	Karta kierowcy	315
5.2.1.	Identyfikacja karty	315
5.2.2.	Identyfikacja posiadacza karty	316
5.2.3.	Dane dotyczące prawa jazdy	316
5.2.4.	Dane dotyczące używanego pojazdu	316
5.2.5.	Dane dotyczące czynności kierowcy	316
5.2.6.	Miejsca rozpoczęcia i/lub zakończenia dziennego okresu pracy	317
5.2.7.	Dane dotyczące zdarzeń	317
5.2.8.	Dane dotyczące usterek	318
5.2.9.	Dane dotyczące czynności kontrolnej	318
5.2.10.	Dane sesji karty	318
5.2.11.	Dane dotyczące warunków szczególnych	318
5.3.	Karta warsztatowa	319
5.3.1.	Zabezpieczenia	319
5.3.2.	Identyfikacja karty	319
5.3.3.	Identyfikacja posiadacza karty	319
5.3.4.	Dane dotyczące używanego pojazdu	319
5.3.5.	Dane dotyczące czynności kierowcy	319
5.3.6.	Dane dotyczące rozpoczęcia i/lub zakończenia dziennego okresu pracy	319
5.3.7.	Dane dotyczące zdarzeń i usterek	319
5.3.8.	Dane dotyczące czynności kontrolnej	319
5.3.9.	Dane dotyczące kalibracji i regulacji czasu	320
5.3.10.	Dane dotyczące warunków szczególnych	320
5.4.	Karta kontrolna.	320

5.4.1.	Identyfikacja karty	320
5.4.2.	Identyfikacja posiadacza karty	320
5.4.3.	Dane dotyczące czynności kontrolnej	320
5.5.	Karta firmowa	321
5.5.1.	Identyfikacja karty	321
5.5.2.	Identyfikacja posiadacza karty	321
5.5.3.	Dane dotyczące czynności wykonywanych przez firmę	321
V.	INSTALACJA URZĄDZENIA REJESTRUJĄCEGO	321
1.	Instalacja	321
2.	Tabliczka instalacyjna	322
3.	Plombowanie	322
VI.	SPRAWDZENIA, INSPEKCJE I NAPRAWY	323
1.	Zatwierdzenie instalatorów lub warsztatów	323
2.	Kontrola techniczna przyrządów nowych i po naprawie	323
3.	Kontrola techniczna po instalacji	323
4.	Przeglądy okresowe	323
5.	Pomiar błędów	324
6.	Naprawy	324
VII.	WYDAWANIE KART	324
VIII.	HOMOLOGACJA TYPU DLA URZĄDZENIA REJESTRUJĄCEGO I KART DO TACHOGRAFÓW	324
1.	Uwagi ogólne	324
2.	Świadectwo bezpieczeństwa	325
3.	Świadectwo funkcjonalności	325
4.	Świadectwa współdziałania	325
5.	Świadectwo homologacji typu	320
6.	Procedura szczególna: pierwsze świadectwa współdziałania	320
Dodatek 1.	Słownik danych	
Dodatek 2.	Wymagania dla kart tachografów	
Dodatek 3.	Piktogramy	
Dodatek 4.	Wydruki	
Dodatek 5.	Wyświetlacz	
Dodatek 6.	Interfejsy zewnętrzne	
Dodatek 7.	Protokół wczytywania danych	
Dodatek 8.	Protokół kalibracyjny	
Dodatek 9.	HOMOLOGACJA TYPU — WYKAZ MINIMUM WYMAGANYCH TESTÓW	
Dodatek 10.	OGÓLNE CELE ZABEZPIECZENIA	
Dodatek 11.	WSPÓLNE MECHANIZMY ZABEZPIECZENIA	

I. DEFINICJE

Ilekroć użyte w niniejszym załączniku:

a) **»aktywacja« oznacza:**

fazę, gdy urządzenie rejestrujące uzyskuje pełną funkcjonalność i uruchamia wszystkie funkcje, włącznie z funkcjami zabezpieczającymi;

Aktywowanie urządzenia rejestrującego wymaga użycia karty warsztatowej i wprowadzenia kodu PIN tej karty;

b) **»uwierzytelnienie« oznacza:**

funkcję przeznaczoną do ustanowienia i kontroli tożsamości;

c) **»autentyczność« oznacza:**

właściwość polegającą na tym, że informacje pochodzą od strony, której tożsamość można zweryfikować;

d) **»test wbudowany (BIT)« oznacza:**

testy wykonywane na żądanie, uruchamiane przez operatora lub urządzenia zewnętrzne;

e) **»dzień kalendarzowy« oznacza:**

dzień zaczynający się o godzinie 00:00 i kończący o godzinie 24:00. Wszystkie dni kalendarzowe odnoszą się do czasu UTC (uniwersalny czas skoordynowany);

f) **»kalibracja« oznacza:**

aktualizację lub potwierdzenie parametrów pojazdu przechowywanych w pamięci danych. Parametry pojazdu obejmują identyfikację pojazdu (numery VIN, VRN i kod rejestrującego Państwa Członkowskiego) i charakterystyki pojazdu, (w, k, l, wielkość opon, ustawienie ogranicznika prędkości, (gdy dotyczy), bieżący czas UTC, bieżąca wartość licznika kilometrów);

do kalibracji urządzenia rejestrującego potrzebna jest karta warsztatowa;

g) **»numer karty« oznacza:**

numer składający się z 16 znaków alfanumerycznych, który jednoznacznie identyfikuje kartę do tachografów w Państwie Członkowskim. Numer karty zawiera numer kolejny, (gdy dotyczy), numer zastąpienia i numer odświeżenia;

tym samym karta jest jednoznacznie zidentyfikowana przez kod Państwa Członkowskiego wydającego i numer karty;

h) **»numer kolejny karty« oznacza:**

numer składający się z 14 znaków alfanumerycznych, który umożliwia rozróżnianie różnych kart wydanych przez firmę lub organ uprawniony do wydawania kilku kart do tachografów. Firmę lub organ jednoznacznie identyfikuje pierwszych 13 znaków numeru karty;

i) **»numer odświeżenia karty« oznacza:**

kod w numerze karty składający się z 16 znaków alfanumerycznych, który jest zmieniany przyrostowo przy każdym odświeżeniu karty do tachografów;

j) **»numer wymiany karty« oznacza:**

kod w numerze karty składający się z 15 znaków alfanumerycznych, który jest zmieniany przyrostowo przy każdej wymianie karty do tachografów;

k) **»współczynnik charakterystyczny pojazdu« oznacza:**

wielkość liczbowa określającą liczbę sygnałów dostarczanych przez część pojazdu podłączoną do urządzenia rejestrującego (wał główny skrzyni biegów lub oś) w czasie, gdy pojazd przebywa drogę o długości jednego kilometra mierzoną w warunkach normalnych (patrz: rozdział VI, pkt 5). Współczynnik charakterystyczny pojazdu podaje się w impulsach na kilometr (w =... imp/km);

l) **»karta firmowa« oznacza:**

kartę do tachografów wydaną przez organy Państwa Członkowskiego właścicielowi lub posiadaczowi pojazdów silnikowych wyposażonych w urządzenie rejestrujące;

karta firmowa identyfikuje przedsiębiorstwo i umożliwia odczytywanie, wczytywanie i drukowanie danych zapamiętanych w urządzeniu rejestrującym, które zostały wprowadzone przez to przedsiębiorstwo;

m) **»stała urządzenia rejestrującego« oznacza:**

wielkość liczbowa określającą wartość sygnału wejściowego niezbędną do wskazania i zarejestrowania przejechanej odległości jednego kilometra; stała ta jest wyrażona w impulsach na kilometr ($k = \dots \text{imp/km}$);

n) **»nieprzerwany czas prowadzenia pojazdu« obliczany jest przez urządzenie rejestrujące w następujący sposób ⁽¹⁾:**

nieprzerwany czas prowadzenia pojazdu obliczany jest jako bieżące, zakumulowane czasy prowadzenia pojazdu przez danego kierowcę od końca jego ostatniego 45-minutowego lub dłuższego okresu DYSPOZYCYJNOŚCI lub PRZERWY/ODPOCZYNKU lub NIEOKREŚLONEGO ⁽²⁾ (okres ten może być rozbity na kilka 15-minutowych lub dłuższych okresów). W obliczeniach uwzględnia się, stosownie do okoliczności, ostatnie czynności zapisane na karcie kierowcy. Jeżeli kierowca nie włoży swojej karty, obliczenia wykonuje się na podstawie znajdujących się w pamięci danych zapisów dla bieżącego okresu, w którym nie było włożonej karty i dla stosownego czytnika;

o) **»karta kontrolna« oznacza:**

kartę do tachografów wydaną przez organ Państwa Członkowskiego, właściwego krajowego organu kontrolnego;

karta kontrolna identyfikuje organ kontrolny i, w miarę możliwości, odpowiedzialnego funkcjonariusza oraz umożliwia dostęp do danych zapisanych w pamięci danych lub na karcie kierowcy w celu odczytania, wydrukowania i/lub wczytania danych;

p) **»skumulowany czas przerwy« obliczany jest przez urządzenie rejestrujące w następujący sposób ⁽¹⁾:**

skumulowany czas przerwy w prowadzeniu pojazdu obliczany jest jako bieżące, zakumulowane, 15-minutowe lub dłuższe czasy DYSPOZYCYJNOŚCI lub PRZERWY/ODPOCZYNKU lub NIEOKREŚLONE ⁽²⁾ dla danego kierowcy, od końca jego ostatniego 45-minutowego lub dłuższego okresu DYSPOZYCYJNOŚCI lub PRZERWY/ODPOCZYNKU lub NIEOKREŚLONEGO ⁽²⁾ (okres ten może być rozbity na kilka 15-minutowych lub dłuższych okresów).

W obliczeniach uwzględnia się, stosownie do okoliczności, ostatnie czynności zapisane na karcie kierowcy. Do obliczeń nie bierze się nieznanego czasu trwania (początek nieznanego okresu > końca nieznanego okresu) wynikłych z nakładania się czasów z dwóch różnych urządzeń rejestrujących.

Jeżeli kierowca nie włoży swojej karty, obliczenia wykonuje się na podstawie znajdujących się w pamięci danych zapisów dla bieżącego okresu, w którym nie było włożonej karty i dla stosownego czytnika;

q) **»pamięć danych« oznacza:**

elektroniczne urządzenie gromadzenia danych wbudowane w urządzenie rejestrujące;

r) **»podpis cyfrowy« oznacza:**

dane dołączone lub kryptograficzne przekształcenie bloku danych, które umożliwia odbiorcy sprawdzenie autentyczności oraz integralności tego bloku danych;

s) **»wczytywanie danych« oznacza:**

kopiowanie wraz z podpisem cyfrowym części lub całego zbioru danych zapisanego w pamięci danych pojazdu lub w pamięci karty do tachografów;

wczytywanie danych nie może zmienić ani skasować zapisanych danych;

⁽¹⁾ Ten sposób obliczania nieprzerwanego czasu prowadzenia pojazdu oraz łącznego czasu przerwy służy do obliczenia ostrzeżenia nieprzerwanego czasu prowadzenia. Nie przesądza to prawnej interpretacji tych czasów.

⁽²⁾ Nieznane okresy odpowiadają okresom, gdy karta kierowcy nie jest włożona do urządzenia rejestrującego oraz dla których nie dokonano ręcznego włożenia karty.

- t) **»karta kierowcy« oznacza:**
- kartę do tachografów wydaną konkretnemu kierowcy przez organy Państwa Członkowskiego;
- karta kierowcy identyfikuje kierowcę i umożliwia gromadzenie danych dotyczących czynności kierowcy;*
- u) **»skuteczny obwód opon« oznacza:**
- wartość średnią długości drogi przebytej przez każde z kół (napędowych) poruszającego się pojazdu podczas jednego pełnego obrotu. Pomiar tych długości drogi jest wykonywany w warunkach normalnych (patrz: rozdział VI, pkt 5 niniejszego Załącznika) i wyrażony jest w postaci: »l =... mm«. Producenci pojazdów mogą zastąpić pomiar tej odległości obliczeniem teoretycznym, w którym uwzględnia się rozkład ciężaru na osie dla niezaladowanego pojazdu w normalnych warunkach ruchu ⁽¹⁾. Metody takich obliczeń teoretycznych zatwierdzają właściwe organy Państw Członkowskich;
- v) **»zdarzenie« oznacza:**
- nieprawidłową pracę wykrytą przez urządzenie rejestrujące, której źródłem może być próba dokonania nadużycia finansowego;
- w) **»usterka« oznacza:**
- nieprawidłową pracę wykrytą przez urządzenie rejestrujące, której źródłem może być wadliwa praca lub awaria urządzeń;
- x) **»instalacja« oznacza:**
- montaż urządzenia rejestrującego w pojeździe;
- y) **»czujnik ruchu« oznacza:**
- część urządzenia rejestrującego dostarczającą sygnał przedstawiający prędkość pojazdu i/lub przebytą drogę;
- z) **»karta nieważna« oznacza:**
- wykryta karta jest wadliwa, lub nie jest możliwe wstępne uwierzytelnienie karty, lub okres ważności jeszcze się nie rozpoczął lub już upłynął;
- aa) **»poza zakresem« oznacza:**
- że zgodnie z przepisami rozporządzenia Rady (EWG) nr 3820/85 użycie urządzenia rejestrującego nie jest wymagane;
- bb) **»przekroczenie prędkości« oznacza:**
- przekroczenie dozwolonej prędkości pojazdu definiowane jako dowolny przynajmniej 60-sekundowy okres, w którym zmierzona prędkość pojazdu przekracza wartość ograniczenia dla urządzenia ograniczenia prędkości ustanowioną w dyrektywie Rady 92/6/EWG z dnia 10 lutego 1992 r. w sprawie montowania i zastosowania urządzeń ograniczenia prędkości w niektórych kategoriach pojazdów silnikowych we Wspólnocie ⁽²⁾;
- cc) **»przegląd okresowy« oznacza:**
- zespół czynności wykonywanych w celu skontrolowania czy urządzenie rejestrujące pracuje prawidłowo i czy jego ustawienia odpowiadają parametrom pojazdu;
- dd) **»drukarka« oznacza:**
- element urządzenia rejestrującego wykonujący wydruki danych zapisanych w pamięci;
- ee) **»urządzenie rejestrujące« oznacza:**
- całość urządzeń zamierzonych do instalowania w pojazdach drogowych w celu automatycznego lub półautomatycznego pokazywania, rejestrowania i zapamiętywania szczegółowych danych o ruchu takich pojazdów i o pewnych okresach pracy osób kierujących tymi pojazdami;

⁽¹⁾ Dyrektywa 97/27/WE z dnia 22 lipca 1997 r. odnosząca się do wagi i wymiarów niektórych kategorii pojazdów silnikowych i ich przyrządy oraz zmieniająca dyrektywę 70/156/EWG (Dz.U. L 233 z 25.8.1997, str. 1).

⁽²⁾ Dz.U. nr L 57 z 2.3.1992, str. 27.

ff) **»odświeżenie« oznacza:**

wydanie nowej karty do tachografów po upływie terminu ważności dotychczasowej karty lub w przypadku nieprawidłowego działania karty i zwrócenia jej organowi, który wydał kartę. Odświeżenie zawsze wiąże się z pewnością, że nie współistnieją dwie ważne karty;

gg) **»naprawa« oznacza:**

wszelką naprawę czujnika ruchu lub przyrządu rejestrującego wymagającą odłączenia ich zasilania lub odłączenia od innych elementów urządzenia rejestrującego lub otwarcia go;

hh) **»zastąpienie« oznacza:**

wydanie karty do tachografów w celu zastąpienia dotychczasowej karty, której utratę, kradzież lub wadliwe działanie zgłoszono i której nie zwrócono organowi, który wydał kartę. Zastąpienie zawsze wiąże się z ryzykiem, że mogą współistnieć dwie ważne karty;

ii) **»świadectwo zabezpieczenia« oznacza:**

urzędowy dokument wydany przez jednostkę certyfikującą ITSEC ⁽¹⁾ zaświadczający, że badane urządzenie rejestrujące (lub jego element) lub karta do tachografów spełnia wymagania zabezpieczenia określone w dodatku 10 »Generyczne cele zabezpieczenia«;

jj) **»auto test« oznacza:**

testy wykonywane okresowo i automatycznie przez urządzenie rejestrujące w celu wykrycia usterek;

kk) **»karta do tachografów« oznacza:**

kartę inteligentną przeznaczoną do użycia w urządzeniu rejestrującym. Karty do tachografów umożliwiają urządzeniu rejestrującemu identyfikację tożsamości (lub grupy tożsamości) posiadacza karty i umożliwiają przekazywanie i gromadzenie danych dotyczących posiadacza karty. Rozróżnia się następujące typy kart do tachografów:

- karta kierowcy,
- karta kontrolna,
- karta warsztatowa,
- karta firmowa;

ll) **»homologacja typu« oznacza:**

urzędowy dokument wydany przez Państwo Członkowskie i zaświadczający, że dane urządzenie rejestrujące (lub jego element) lub karta do tachografów spełnia wymagania niniejszego rozporządzenia;

mm) **»rozmiar opon« oznacza:**

oznaczenie wymiarów opon (na zewnętrznych kołach napędowych) zgodne z dyrektywą 92/23/EWG z dnia 31 marca 1992 r. ⁽²⁾;

nn) **»identyfikacja pojazdu« oznacza:**

numery identyfikujące pojazd: numer rejestracyjny pojazdu (VRN) z oznaczeniem Państwa Członkowskiego i numer identyfikacyjny pojazdu (VIN) ⁽³⁾;

oo) **»przyrząd rejestrujący (VU)« oznacza:**

urządzenie rejestrujące bez czujnika ruchu i przewodów do przyłączenia czujnika ruchu. Przyrząd rejestrujący może być zarówno pojedynczą jednostką jak i kilkoma jednostkami rozmieszczonymi w pojeździe, o ile tylko spełnia wymagania zabezpieczenia określone w niniejszym rozporządzeniu;

⁽¹⁾ Zalecenie Rady 95/144/WE z dnia 7 kwietnia 1995 r. w sprawie wspólnych kryteriów oceny zabezpieczenia informatycznego (Dz.U. L 93 z 26.4.1995, str. 27).

⁽²⁾ Dz.U. nr L 129 z 14.5.1992, str. 95.

⁽³⁾ Dyrektywa 76/114/EWG z dnia 18 grudnia 1975 r. w sprawie zbliżenia ustawodawstw Państw Członkowskich odnoszących się do tabliczek znamionowych i oznakowania identyfikacyjnego pojazdów silnikowych i ich przyczep oraz sposobu i miejsca ich umieszczenia (Dz.U. L 24 z 30.1.1976, str. 1).

pp) **dla potrzeb obliczeniowych w urządzeniu rejestrującym »tydzień« oznacza:**

okres zawarty między godziną 00:00 UTC w poniedziałek a 24:00 UTC w niedzielę;

qq) **»karta warsztatowa« oznacza:**

kartę do tachografu wydaną przez organ Państwa Członkowskiego producentowi urządzenia rejestrującego, instalatorowi, producentowi pojazdu lub warsztatowi zatwierdzonemu przez to Państwo Członkowskie.

Karta warsztatowa identyfikuje posiadacza karty i umożliwia testowanie, kalibrację i/lub wczytywanie danych do urządzenia rejestrującego;

II. CHARAKTERYSTYKI OGÓLNE I FUNKCJE URZĄDZENIA REJESTRUJĄCEGO

000 Pojazd wyposażony w urządzenie rejestrujące spełniające wymagania niniejszego załącznika musi mieć prędkościomierz i licznik kilometrów. Funkcje te może spełniać urządzenie rejestrujące.

1. Charakterystyki ogólne

Celem urządzenia rejestrującego jest rejestrowanie, przechowywanie, wyświetlanie, drukowanie i wyprowadzanie danych związanych z czynnościami wykonywanymi przez kierowcę.

001 Urządzenie rejestrujące składa się z przewodów, czujnika ruchu i przyrządu rejestrującego.

002 Przyrząd rejestrujący składa się z jednostki przetwarzającej, pamięci danych, zegara czasu rzeczywistego, dwóch czytników kart inteligentnych (dla kierowcy i współkierowcy), drukarki, wyświetlacza, ostrzeżenia wizualnego, gniazda do kalibracji/wczytywania danych i urządzeń do wprowadzania danych przez użytkownika.

Urządzenie rejestrujące można przyłączać do innych urządzeń poprzez dodatkowe gniazda.

003 Zawarcie w urządzeniu rejestrującym lub przyłączenie do niego jakiejkolwiek funkcji, urządzenia lub urządzeń, zatwierdzonych lub nie, nie może zakłócać, ani potencjalnie zakłócać, prawidłowego i bezpiecznego działania urządzenia rejestrującego ani uchybiać przepisom niniejszego rozporządzenia.

Użytkowników urządzenia rejestrującego identyfikują w sprzęcie ich karty do tachografów.

004 Urządzenie rejestrujące zapewnia selektywne prawa dostępu do danych i funkcji, odpowiednio do i/lub tożsamości użytkownika.

Urządzenie rejestrujące rejestruje i przechowuje dane w swojej pamięci danych i na kartach do tachografów.

Odbywa się to zgodnie z dyrektywą 95/46/WE z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych ⁽¹⁾.

2. Funkcje

005 Urządzenie rejestrujące realizuje następujące funkcje:

- monitorowanie wkładania i wyjmowania kart,
- pomiar prędkości i odległości,
- pomiar czasu,
- monitorowanie czynności wykonywanych przez kierowcę,
- monitorowanie stanu prowadzenia pojazdu,
- dane wprowadzane ręcznie przez kierowcę:
 - wprowadzanie miejsca rozpoczęcia i/lub zakończenia okresu pracy,
 - ręcznie wprowadzane dane o czynnościach kierowcy,
 - warunki szczególne,

⁽¹⁾ Dz.U. L 281 z 23.11.1995, str. 31.

- zarządzanie blokadami firmowymi,
- monitorowanie czynności kontrolnych,
- wykrywanie zdarzeń i/lub usterek,
- testy wbudowane i auto testy,
- odczyt z pamięci danych,
- rejestrowanie i przechowywanie w pamięci danych,
- odczyt z kart do tachografów,
- rejestrowanie i przechowywanie na kartach do tachografów,
- wyświetlanie,
- drukowanie,
- ostrzeganie,
- przysyłanie danych do nośników zewnętrznych,
- wyprowadzanie danych do dodatkowych urządzeń zewnętrznych,
- kalibracja,
- nastawianie czasu.

3. Tryby pracy

006 Urządzenie rejestrujące może pracować w czterech trybach pracy:

- tryb eksploatacyjny,
- tryb kontrolny,
- tryb kalibracyjny,
- tryb firmowy.

007 Urządzenie rejestrujące przełącza się do następujących trybów pracy odpowiednio do tego, jakie karty do tachografów są włożone do czytników kart:

Tryb pracy		Szczelina karty współkierowcy				
		Brak karty	Karta kierowcy	Karta kontrolna	Karta warsztatowa	Karta firmowa
Szczelina karty kierowcy	Brak karty	Operacyjny	Operacyjny	Kontrolny	Kalibracyjny	Firmowy
	Karta kierowcy	Operacyjny	Operacyjny	Kontrolny	Kalibracyjny	Firmowy
	Karta kontrolna	Kontrolny	Kontrolny	Kontrolny (*)	Operacyjny	Operacyjny
	Karta warsztatowa	Kalibracyjny	Kalibracyjny	Operacyjny	Kalibracyjny (*)	Operacyjny
	Karta firmowa	Firmowy	Firmowy	Operacyjny	Operacyjny	Firmowy (*)

008 (*) W tych sytuacjach urządzenie rejestrujące korzysta tylko z karty do tachografów włożonej do szczeliny karty kierowcy.

- 009 Urządzenie rejestrujące ignoruje karty nieważne, z wyjątkiem tego, że możliwe jest wyświetlanie, drukowanie lub wczytywanie danych zgromadzonych na kartach, których termin ważności minął.
- 010 Wszystkie funkcje wymienione w pkt II.2. działają w każdym trybie pracy z następującymi wyjątkami:
- funkcja kalibracji dostępna jest tylko w trybie kalibracyjnym,
 - funkcja nastawiania czasu dostępna poza trybem kalibracyjnym działa tylko w ograniczonym zakresie,
 - funkcje ręcznego wprowadzania danych przez kierowcę dostępne są tylko w trybach eksploatacyjnym i kalibracyjnym,
 - funkcja zarządzania blokadami firmowymi dostępna jest tylko w trybie firmowym,
 - funkcja monitorowania czynności kontrolnych dostępna jest tylko w trybie kontrolnym,
 - funkcja wczytywania danych dostępna jest tylko w trybie eksploatacyjnym (wyjąwszy jak przewidziano w wymaganiu 150).
- 011 Urządzenie rejestrujące może wyprowadzać dane na wyświetlacz, do drukarki lub interfejsów zewnętrznych z następującymi wyjątkami:
- w trybie eksploatacyjnym — wszystkie dane identyfikujące osoby (nazwisko i imię/imiona) nieodpowiadające włożonej karcie do tachografu są wygaszone a numer karty, nieodpowiadający włożonej karcie do tachografu jest częściowo wygaszony (wszystkie nieparzyste znaki od lewej do prawej są wygaszone),
 - w trybie firmowym — dane dotyczące kierowcy (wymagania 081, 084 i 087) mogą być wyprowadzane tylko w okresach niezablokowanych przez inną firmę (identyfikowaną pierwszymi 13 cyframi numeru karty firmowej),
 - przy braku karty w czytniku urządzenia rejestrującego dane dotyczące kierowcy mogą być wyprowadzane tylko dla obecnego i ośmiu poprzednich dni kalendarzowych.

4. Zabezpieczenie

Celem zabezpieczenia systemu jest taka ochrona pamięci danych, by uniemożliwić nieautoryzowany dostęp i manipulowanie danymi oraz wykrycie wszelkich takich prób, ochrona integralności i autentyczności danych wymienianych między czujnikiem ruchu a przyrządem rejestrującym, ochrona integralności i autentyczności danych wymienianych między urządzeniem rejestrującym a kartami do tachografów oraz sprawdzenie integralności i autentyczności wczytywanych danych.

- 012 W celu uzyskania zabezpieczenia systemu urządzenie rejestrujące musi spełniać wymagania dotyczące bezpieczeństwa ustanowione dla czujnika ruchu i przyrządu rejestrującego ogólne cele zabezpieczenia (dodatek 10).

III. WYMAGANIA ODNOŚNIE DO KONSTRUKCJI I FUNKCJONALNOŚCI URZĄDZENIA REJESTRUJĄCEGO

1. Monitorowanie wkładania i wyjmowania kart

- 013 Urządzenie rejestrujące monitoruje urządzenia interfejsu kart w celu wykrycia wkładania i wyjmowania kart.
- 014 Po włożeniu karty urządzenie rejestrujące sprawdza czy włożona karta jest ważną kartą do tachografów i w przypadku takiej karty sprawdza, jakiego typu jest to karta.
- 015 Urządzenie rejestrujące musi być tak skonstruowane, aby po prawidłowym włożeniu do urządzenia interfejsu kart karty do tachografów były blokowane we właściwej pozycji.
- 016 Odblokowanie kart do tachografów w celu wyjęcia jest możliwe tylko przy zatrzymanym pojeździe i po zapisaniu odpowiednich danych na kartach. Odblokowanie karty wymaga wykonania przez użytkownika odpowiedniej czynności.

2. Pomiar prędkości i odległości

- 017 Funkcja ta nieprzerwanie mierzy i dostarcza wartość stanu licznika kilometrów odpowiadającą całkowitej drodze przebytej przez pojazd.
- 018 Funkcja ta nieprzerwanie mierzy i dostarcza wartość prędkości pojazdu.

- 019 Funkcja pomiaru prędkości podaje także informacje o tym, czy pojazd porusza się czy stoi. Uważa się, że pojazd porusza się, gdy tylko funkcja pomiaru prędkości wykrywa więcej niż 1 impuls na sekundę z czujnika ruchu przez przynajmniej pięć sekund, w przeciwnym razie uważa się, że pojazd stoi.

Urządzenia do pokazywania prędkości (prędkościomierz) i łącznej drogi przebytej (licznik kilometrów) zainstalowane w pojeździe wyposażonym w urządzenie rejestrujące, spełniające wymagania niniejszego rozporządzenia, spełniają wymagania odnośnie maksymalnych tolerancji ustanowione w niniejszym załączniku (rozdział III pkt 2.1 i 2.2).

2.1. *Pomiar przebytej drogi*

- 020 Długość przebytej drogi może być mierzona, gdy pojazd porusza się:
- do przodu i do tyłu, albo
 - tylko do przodu.
- 021 Urządzenie rejestrujące mierzy odległość w zakresie 0-9 999 999,9 km.
- 022 Pomiar odległości jest wykonywany z następującą dokładnością (odległości przynajmniej 1 000 m):
- $\pm 1\%$ przed instalacją,
 - $\pm 2\%$ po instalacji i przeglądzie okresowym,
 - $\pm 4\%$ podczas eksploatacji.
- 023 Pomiar odległości jest wykonywany z rozdzielczością przynajmniej 0,1 km lub lepszą.

2.2. *Pomiar prędkości*

- 024 Urządzenie rejestrujące mierzy prędkość w zakresie od 0 do 220 km/godz.
- 025 W celu zapewnienia maksymalnej tolerancji wskazywanej prędkości ± 6 km/godz podczas eksploatacji i uwzględniając:
- tolerancję ± 2 km/godz. na zmiany sygnału wejściowego (zmiany opon, etc.),
 - tolerancję ± 1 km/godz. dla pomiarów wykonywanych w czasie instalacji lub przeglądów okresowych,
- urządzenie rejestrujące, dla zakresu prędkości między 20 a 180 km/godz. i dla współczynników charakterystycznych pojazdu między 4 000 a 25 000 impulsów na km, mierzy szybkość z dokładnością ± 1 km/godz. (przy stałej szybkości).
- Uwaga: Rozdzielczość gromadzenia danych wprowadza dodatkową tolerancję $\pm 0,5$ km/godz. do prędkości zapisanej przez urządzenie rejestrujące.

- 025a Prędkość jest mierzona prawidłowo w zakresie normalnych tolerancji po czasie nie dłuższym niż 2 sekundy od zakończenia zmiany prędkości, gdy tempo zmiany prędkości jest maksymalne 2 m/s^2 .
- 026 Pomiar prędkości jest wykonywany z rozdzielczością przynajmniej 1 km/godz. lub lepszą.

3. *Pomiar czasu*

- 027 Funkcja pomiaru czasu mierzy czas nieprzerwanie i cyfrowo podaje datę i czas UTC.
- 028 Do datowania w urządzeniu rejestrującym (rejestracja, wydruki, wymiana danych, prezentacje, etc.) używane są data i czas UTC.
- 029 W celu wizualizacji czasu lokalnego możliwe jest przesuwanie pokazywanego czasu w stopniach półgodzinnych.
- 030 Dryft czasu mieści się w granicach ± 2 sekundy dziennie w warunkach zgodnych z homologacją typu.
- 031 Pomiar czasu jest wykonywany z rozdzielczością przynajmniej 1 sekundy lub lepszą.
- 032 Odcięcie zewnętrznego źródła zasilania na czas nie krótszy niż 12 miesięcy w warunkach zgodnych z homologacją typu nie wpływa na pomiar czasu.

4. Monitorowanie czynności wykonywanych przez kierowcę

- 033 Funkcja ta nieprzerwanie i odrębnie monitoruje czynności wykonywane przez jednego kierowcę i jednego współkierowcę.
- 034 Czynnościami kierowcy są PROWADZENIE, PRACA, DYSPOZYCYJNOŚĆ lub PRZERWA/ODPOCZYNEK.
- 035 Kierowca i/lub współkierowca mogą ręcznie wybierać PRACĘ, DYSPOZYCYJNOŚĆ lub PRZERWĘ/ODPOCZYNEK.
- 036 Gdy pojazd porusza się następuje automatyczne wybranie PROWADZENIE dla kierowcy i DYSPOZYCYJNOŚĆ dla współkierowcy.
- 037 Gdy pojazd zatrzymuje się następuje automatyczne wybranie PRACY dla kierowcy.
- 038 Jeżeli w czasie 120 sekund od automatycznej zmiany na PRACĘ, wskutek zatrzymania pojazdu, nastąpi zmiana czynności, to przyjmuje się, że pierwsza taka zmiana zaistniała w czasie postoju pojazdu (w ten sposób można anulować zmianę na PRACĘ).
- 039 Funkcja ta przekazuje zmiany czynności do funkcji rejestrującej w odstępach co jedną minutę.
- 040 W danej minucie zegarowej, jeżeli w tym okresie nastąpi czynność PROWADZENIE, to cała ta minuta liczy się jako PROWADZENIE.
- 041 W danej minucie zegarowej, jeżeli czynność PROWADZENIE następuje zarówno w minucie bezpośrednio poprzedzającej, jak i bezpośrednio następującej, to cała ta minuta liczy się jako PROWADZENIE.
- 042 W danej minucie zegarowej, niezaliczonej jako PROWADZENIE, zgodnie z poprzednimi wymaganiami, cała taka minuta liczy się jako jedna czynność, która trwała najdłużej w ciągu tej minuty (lub późniejsza w przypadku czynności o jednakowym czasie trwania).
- 043 Funkcja ta także nieprzerwanie monitoruje zarówno nieprzerwany czas prowadzenia pojazdu jak i skumulowany czas przerwy dla kierowcy.

5. Monitorowanie stanu prowadzenia pojazdu

- 044 Funkcja ta nieprzerwanie i automatycznie monitoruje stan prowadzenia pojazdu.
- 045 Po włożeniu dwóch ważnych kart kierowcy wybierany jest stan prowadzenia pojazdu ZAŁOGA, w każdym innym przypadku wybierany jest stan prowadzenia pojazdu JEDEN KIEROWCA.

6. Dane wprowadzane ręcznie przez kierowcę**6.1. Wprowadzanie miejsca rozpoczęcia i/lub zakończenia okresu pracy**

- 046 Funkcja ta umożliwia wprowadzanie miejsc rozpoczęcia i/lub zakończenia okresu pracy dla kierowcy i/lub współkierowcy.
- 047 Miejsca definiuje się jako kraj i dodatkowo, gdy stosowne, region.
- 048 W chwili wyjścia karty kierowcy (lub warsztatowej), urządzenie rejestrujące sygnalizuje, że oczekuje od (współ)kierowcy wprowadzenia »miejsca zakończenia dziennego okresu pracy«.
- 049 Urządzenie rejestrujące umożliwia zignorowanie tego żądania.
- 050 Wprowadzenie miejsca rozpoczęcia i/lub zakończenia dziennego okresu pracy jest możliwe bez włożonej karty lub w innym czasie niż przy wkładaniu lub wyjmowaniu karty.

6.2. Ręczne wprowadzanie czynności wykonywanych przez kierowcę

- 050a Po włożeniu karty kierowcy (lub warsztatowej) i tylko w tym czasie, urządzenie rejestrujące:
- przypomina posiadaczowi karty datę i godzinę ostatniego wyjścia jego karty, i
 - pyta posiadacza karty, czy obecne włożenie karty stanowi kontynuację bieżącego dziennego okresu pracy.

Urządzenie rejestrujące umożliwia posiadaczowi karty zignorowanie tego pytania i pozostawienie go bez odpowiedzi lub udzielenie odpowiedzi potwierdzającej lub zaprzeczającej:

- w przypadku, gdy posiadacz karty zignoruje pytanie, urządzenie rejestrujące sygnalizuje, że oczekuje od posiadacza karty wprowadzenia »miejsc rozpoczęcia dziennego okresu pracy«. Urządzenie rejestrujące umożliwia zignorowanie tego pytania. W przypadku wprowadzenia miejsca jest ono rejestrowane w pamięci danych i na karcie do tachografów, oraz powiązane z godziną włożenia karty,
- w przypadku odpowiedzi potwierdzającej lub zaprzeczającej urządzenie rejestrujące zachęca posiadacza karty do ręcznego wprowadzenia czynności wybranych tylko spośród PRACA, DYSPOZYCYJNOŚĆ lub PRZERWA/ODPOCZYNEK, razem z datami i godzinami rozpoczęcia i zakończenia, ściśle zawartych wyłącznie w okresie między ostatnim wyjęciem a obecnym włożeniem karty i bez możliwości nakładania się okresów wykonywania tych czynności. Odbyna się to zgodnie z następującą procedurą:
- w przypadku odpowiedzi potwierdzającej urządzenie rejestrujące zachęca posiadacza karty do ręcznego wprowadzenia czynności, w porządku chronologicznym, za okres między ostatnim wyjęciem a obecnym włożeniem karty. Procedura kończy się, jeśli godzina zakończenia ręcznie wprowadzanej czynności pokrywa się z godziną włożenia karty.
- w przypadku odpowiedzi zaprzeczającej urządzenie rejestrujące:

- zachęca posiadacza karty do ręcznego wprowadzenia czynności, w porządku chronologicznym, za okres od ostatniego wyjęcia karty do godziny zakończenia związanego dziennego okresu pracy (lub czynności związanych z tym pojazdem, w przypadku gdy w rejestrze kontynuowany jest dzienny okres pracy). Dlatego też urządzenie rejestrujące, przed umożliwieniem posiadaczowi karty ręcznego wprowadzenia czynności, zachęca posiadacza karty do określenia, czy godzina zakończenia ostatniej zarejestrowanej czynności odpowiada zakończeniu poprzedniego okresu pracy (patrz uwaga poniżej),

uwagi: w przypadku gdy posiadacz karty nie zadeklaruje kiedy zakończył się poprzedni okres pracy i ręcznie wprowadzi czynność, której czas zakończenia pokrywa się z godziną włożenia karty, urządzenie rejestrujące:

- przyjmuje, że dzienny okres pracy zakończył się z rozpoczęciem pierwszego okresu ODPOCZYNEKU (lub czynność pozostaje NIEOKREŚLONA) po wyjęciu karty lub w czasie wyjęcia karty, jeżeli nie wprowadzono okresu odpoczynku (ani okres nie jest NIEOKREŚLONY),
- przyjmuje, że czas rozpoczęcia (patrz poniżej) równy jest godzinie włożenia karty,
- wykonuje kroki opisane poniżej;
- następnie, jeżeli godzina zakończenia związanego okresu pracy różni się od godziny wyjęcia karty, lub, gdy w tym czasie nie wprowadzono miejsca zakończenia dziennego okresu pracy, zachęca posiadacza karty do »potwierdzenia lub wprowadzenia miejsca zakończenia dziennego okresu pracy« (urządzenie rejestrujące pozwala na zignorowanie tego żądania). W przypadku wprowadzenia miejsca jest ono rejestrowane na karcie do tachografów wtedy i tylko wtedy, gdy różni się od tego wprowadzonego przy wyjęciu karty, (jeżeli zostało wprowadzone) i zostaje powiązane z godziną zakończenia okresu pracy,
- następnie zaprasza posiadacza karty do »potwierdzenia godziny rozpoczęcia« bieżącego dziennego okresu pracy (lub czynności związanych z tym pojazdem, w przypadku gdy posiadacz karty użył wcześniej arkusza rejestracyjnego w ciągu tego okresu) i zaprasza posiadacza karty do wprowadzenia »miejsc rozpoczęcia dziennego okresu pracy« (urządzenie rejestrujące pozwala na zignorowanie tego żądania). W przypadku wprowadzenia miejsca jest ono zarejestrowane na karcie do tachografów i powiązane z tą godziną rozpoczęcia. Jeżeli ta godzina rozpoczęcia pokrywa się z godziną włożenia karty, również miejsce jest rejestrowane w pamięci danych,
- następnie, jeżeli ta godzina rozpoczęcia różni się od godziny włożenia karty, prosi posiadacza karty o ręczne wprowadzenie czynności w kolejności chronologicznej od tej godziny rozpoczęcia do godziny włożenia karty. Procedura kończy się, jeśli godzina zakończenia ręcznie wprowadzanej czynności pokrywa się z godziną włożenia karty,
- następnie urządzenie rejestrujące umożliwia posiadaczowi karty zmodyfikowanie wprowadzonej ręcznie czynności, przeprowadzenie walidacji poprzez wybranie odpowiedniego polecenia i uniemożliwia wprowadzanie takich zmian w późniejszym czasie,
- takie odpowiedzi na początkowe pytanie, po których nie są wprowadzane czynności, urządzenie rejestrujące interpretuje tak jakby posiadacz karty zignorował pytanie.

W czasie całego tego procesu urządzenie rejestrujące oczekuje na wprowadzenie danych nie dłużej niż przez określone poniżej okresy oczekiwania:

- jedna minutę — jeżeli nie ma interakcji z interfejsem człowiek-maszyna (z optycznym i o ile możliwe akustycznym sygnałem ostrzegawczym po 30 sekundach) lub
- do wyjęcia karty kierowcy (lub warsztatowej) lub włożenia innej karty kierowcy (lub warsztatowej),
- do rozpoczęcia jazdy przez pojazd,

w tym przypadku urządzenie rejestrujące dokonuje walidacji wszystkich już wprowadzonych danych.

6.3. *Stany szczególne*

050b Urządzenie rejestrujące umożliwia kierowcy wprowadzanie w czasie rzeczywistym następujących dwóch stanów szczególnych:

- »POZA ZAKRESEM« (początek, koniec)
- »PRZEPRAWA PROMOWA/PRZEJAZD KOLEJOWY«

Przy rozpoczętym stanie »POZA ZAKRESEM« nie może być stanu »PRZEPRAWA PROMOWA/PRZEJAZD KOLEJOWY«.

Włożenie lub wyjęcie karty kierowcy automatycznie kończy rozpoczęty stan »POZA ZAKRESEM«.

7. Zarządzanie blokadami firmowymi

- 051 Funkcja ta umożliwia zarządzanie blokadami umieszczanymi przez firmę w celu ograniczenia dostępu do danych, gdy urządzenie pracuje w trybie firmowym.
- 052 Blokadę firmową polegają na ustawieniu daty/godziny rozpoczęcia (włączenie blokady) i daty/godziny zakończenia (zwolnienie blokady) związanych z identyfikacją firmy pobraną z numeru karty firmowej (przy włączeniu blokady).
- 053 Blokadę można włączać i zwalniać tylko w czasie rzeczywistym.
- 054 Blokadę może zwolnić tylko ta firma, która ją włączyła (identyfikowana na podstawie pierwszych 13 cyfr numeru karty firmowej) lub
- 055 zwolnienie następuje automatycznie po włączeniu blokady przez inną firmę.
- 055a W przypadku gdy firma włącza blokadę a poprzednia blokada była włączona przez tę samą firmę, przyjmuje się, że poprzednia blokada nie została zdjęta i nadal jest włączona.

8. Monitorowanie czynności kontrolnych

- 056 Funkcja ta monitoruje wykonywane w trybie kontrolnym operacje OBRAZOWANIA, DRUKOWANIA, WCZYTYWANIA DANYCH z przyrządu rejestrującego i karty.
- 057 Funkcja ta również monitoruje KONTROLE PRZEKROCZENIA PRĘDKOŚCI wykonywane w trybie kontrolnym. Uważa się, że kontrola przekroczenia prędkości została przeprowadzona gdy w trybie kontrolnym komunikat »przekroczenie prędkości« zostaje wysłany do drukarki lub wyświetlony na monitorze, lub gdy dane o »zdarzeniach i usterek« zostały wczytane z pamięci danych przyrządu rejestrującego.

9. Wykrywanie zdarzeń i/lub usterek

- 058 Funkcja ta wykrywa następujące zdarzenia i/lub usterek:

9.1. *Zdarzenie — włożenie nieważnej karty*

- 059 Zdarzenie to uruchamia włożenie nieważnej karty i/lub wygaśnięcie ważności włożonej, ważnej karty.

9.2. **Zdarzenie — »Konflikt kart«**

060 Zdarzenie to uruchamia każda kombinacja ważnych kart zaznaczona X w tabeli poniżej:

Konflikt kart		Szczelina karty współkierowcy				
		brak karty	karta kierowcy	karta kontrolna	karta warsztatowa	karta firmowa
Szczelina karty kierowcy	brak karty					
	karta kierowcy				X	
	karta kontrolna			X	X	X
	karta warsztatowa		X	X	X	X
	karta firmowa			X	X	X

9.3. **Zdarzenie — »Nakładające się czasy«**

061 Zdarzenie to uruchamia sytuacja, gdy data/godzina ostatniego wyjęcia karty kierowcy, odczytana z karty, jest późniejsza niż bieżąca data/godzina urządzenia rejestrującego, do którego karta jest wkładana.

9.4. **Zdarzenie — »Prowadzenie bez prawidłowej karty«**

062 Zdarzenie to uruchamia dowolna kombinacja kart do tachografów zaznaczonych X w poniższej tabeli, gdy czynność wykonywana przez kierowcę zmienia się na PROWADZENIE w przypadku zmiany trybu pracy, w czasie gdy czynnością wykonywaną przez kierowcę jest PROWADZENIE:

Prowadzenie bez prawidłowej karty		Szczelina karty współkierowcy				
		brak karty (lub karta nieważna)	karta kierowcy	karta kontrolna	karta warsztatowa	karta firmowa
Szczelina karty kierowcy	brak karty (lub karta nieważna)	X		X		X
	karta kierowcy	X		X	X	X
	karta kontrolna	X	X	X	X	X
	karta warsztatowa	X	X	X		X
	karta firmowa	X	X	X	X	X

9.5. **Zdarzenie — »Włożenie karty podczas jazdy«**

063 Zdarzenie to uruchamia się, gdy do dowolnej szczeliny wkładana jest karta do tachografów, w czasie gdy czynnością wykonywaną przez kierowcę jest PROWADZENIE.

9.6. **Zdarzenie — »Sesja ostatniej karty niezamknięta prawidłowo«**

064 Zdarzenie to uruchamia się, gdy przy wkładaniu karty urządzenie rejestrujące wykryje, że pomimo przepisów ustanowionych w rozdziale III pkt 1, sesja poprzedniej karty nie jest prawidłowo zamknięta (karta została wyjęta przed zapisaniem na karcie wszystkich wymaganych danych). Zdarzenie to uruchamiają tylko karty kierowcy i warsztatowe.

9.7. **Zdarzenie — »Przekroczenie prędkości«Przekroczenie prędkości«**

065 Zdarzenie to uruchamia się przy każdym przekroczeniu prędkości.

9.8. Zdarzenie — »Przerwa zasilania«

- 066 Zdarzenie to uruchamia się, z wyłączeniem pracy w trybie kalibracyjnym, w przypadku przekraczającej 200 ms przerwy w zasilaniu czujnika ruchu i/lub przyrządu rejestrującego. Wartość progową przerwy definiuje producent. Przerwa w zasilaniu spowodowana uruchamianiem silnika pojazdu nie może uruchamiać tego zdarzenia.

9.9. Zdarzenie — »Błąd danych dotyczących ruchu«

- 067 Zdarzenie to uruchamia się w przypadku przerwy normalnego przepływu danych między czujnikiem ruchu a przyrządem rejestrującym i/lub w przypadku błędu integralności danych lub błędu uwierzytelnienia danych wymienianych między czujnikiem ruchu a przyrządem rejestrującym.

9.10. Zdarzenie — »Próba naruszenia zabezpieczenia«

- 068 Zdarzenie to uruchamia każde inne zdarzenie naruszające zabezpieczenie czujnika ruchu i/lub przyrządu rejestrującego, określone w ogólnych celach zabezpieczenia tych elementów, z wyłączeniem pracy w trybie kalibracyjnym.

9.11. Usterka — »Karta«

- 069 Usterkę tę uruchamia usterka karty do tachografów powstała podczas pracy.

9.12. Usterka — »Urządzenie rejestrujące«

- 070 Usterkę tę uruchamia dowolna z następujących usterek, z wyłączeniem pracy w trybie kalibracyjnym:

- usterka wewnętrzna VU,
- usterka drukarki,
- usterka wyświetlacza,
- usterka wczytywania danych,
- usterka czujnika.

10. Testy wbudowane i auto testy

- 071 Urządzenie rejestrujące samoczynnie wykrywa usterki wykonując auto testy i testy wbudowane, zgodnie z poniższą tabelą:

Testowany podzespół	Auto test	Test wbudowany
Oprogramowanie		integralność
Testowany podzespół	Auto test	Test wbudowany
Pamięć danych	dostęp	dostęp, integralność danych
Czytniki kart	dostęp	dostęp
Klawiatura		sprawdzenie ręczne
Drukarka	(wg producenta)	wydruk
Wyświetlacz		sprawdzenie wizualne
Wczytywanie danych (wykonywane tylko podczas wczytywania danych)	prawidłowa praca	
Czujnik		prawidłowa praca prawidłowa praca

11. Odczyt z pamięci danych

- 072 Urządzenie rejestrujące umożliwia odczyt danych przechowywanych w jego pamięci danych.

12. Zapisywanie i przechowywanie w pamięci danych

Do celów niniejszego pkt,

— »365 dni« definiuje się jako 365 dni kalendarzowych przeciętnych czynności wykonywanych przez kierowców w pojeździe. Przeciętne czynności na dzień w pojeździe definiuje się jako przynajmniej sześciu kierowców lub współkierowców, sześć cykli wkładania wyjmowania karty i 256 zmian czynności. Tak więc »365 dni« obejmuje przynajmniej 2 190 współkierowców, 2 190 cykli wkładania wyjmowania karty i 93 440 zmian czynności,

— czasy rejestruje się z rozdzielczością jednej minuty, chyba że ustalono inaczej,

— stany licznika kilometrów rejestruje się z rozdzielczością jednego kilometra,

— prędkości rejestruje się z rozdzielczością 1 km/godz.

073 Odcięcie zewnętrznego źródła zasilania na czas krótszy niż 12 miesięcy, w warunkach zgodnych z homologacją typu, nie wpływa na dane przechowywane w pamięci danych.

074 Urządzenie rejestrujące umożliwia rejestrowanie, pośrednio lub bezpośrednio, w swojej pamięci danych następujących informacji:

12.1. Dane identyfikujące sprzęt

12.1.1. Dane identyfikujące przyrząd rejestrujący

075 Urządzenie rejestrujące umożliwia przechowywanie w swojej pamięci danych następujących danych identyfikujących przyrząd rejestrujący:

— nazwa producenta,

— adres producenta,

— numer części,

— numer fabryczny,

— numer wersji oprogramowania,

— data instalacji wersji oprogramowania,

— rok produkcji urządzenia,

— numer homologacji.

076 Dane identyfikujące przyrząd rejestrujący są rejestrowane i zapisywane w pamięci tylko raz i tylko przez producenta przyrządu rejestrującego, z wyłączeniem danych dotyczących oprogramowania i numeru homologacji, które mogą zmieniać się w przypadku aktualizacji oprogramowania.

12.1.2. Dane identyfikujące czujnik ruchu

077 Czujnik ruchu umożliwia przechowywanie w swojej pamięci następujących danych identyfikujących:

— nazwa producenta,

— numer części,

— numer fabryczny,

— numer homologacji,

— identyfikator wbudowanego elementu zabezpieczenia (np. numer części wewnętrznego chipu/procesora),

— identyfikator systemu operacyjnego (np. numer wersji oprogramowania).

078 Dane identyfikujące czujnik ruchu są rejestrowane i zapisywane w czujniku ruchu tylko raz i tylko przez producenta czujnika ruchu.

079 Przyrząd rejestrujący umożliwia przechowywanie w swojej pamięci danych następujących danych identyfikujących sparowany czujnik ruchu:

- numer fabryczny,
- numer homologacji,
- data pierwszego sparowania.

12.2. *Elementy zabezpieczenia*

080 Urządzenie rejestrujące umożliwia przechowywanie w pamięci następujących danych dotyczących elementów zabezpieczenia:

- europejski klucz publiczny,
- certyfikat Państwa Członkowskiego,
- certyfikat urządzenia,
- klucz prywatny urządzenia.

Elementy zabezpieczenia urządzenia rejestrującego wpisuje producent przyrządu rejestrującego.

12.3. *Dane rejestrowane przy wkładaniu i wyjmowaniu karty kierowcy*

081 Przy każdym cyklu wkładania/wyjmowania karty kierowcy lub warsztatowej do urządzenia, urządzenie rejestrujące rejestruje i przechowuje w swojej pamięci danych następujące informacje:

- nazwisko i imię(imiona) posiadacza karty zapisane na karcie,
- numer karty, Państwo Członkowskie, które wydało kartę i datę ważności zapisane na karcie,
- datę i godzinę włożenia karty,
- stan licznika kilometrów przy wkładaniu karty,
- szczelinę czytnika, do której karta jest wkładana,
- datę i godzinę wyjęcia karty,
- stan licznika kilometrów przy wyjęciu karty,
- następujące informacje o poprzednim pojeździe używanym przez kierowcę, zapisane na karcie:
 - numer VRN i Państwo Członkowskie rejestracji,
 - datę i godzinę wyjęcia karty,
- wskaźnik stanu pokazujący, czy przy wkładaniu karty posiadacz karty wprowadził ręcznie informacje o wykonywaniu czynności.

082 Pamięć danych wystarcza do przechowywania tych danych przez przynajmniej 365 dni.

083 W przypadku zapełnienia pamięci danych nowe dane zastępują najstarsze dane.

12.4. Dane dotyczące czynności kierowcy

084 Urządzenie rejestrujące rejestruje i przechowuje w swojej pamięci danych za każdym razem, kiedy następuje zmiana czynności kierowcy i/lub współkierowcy, i/lub za każdym razem, kiedy następuje zmiana stanu prowadzenia pojazdu, i/lub za każdym razem, kiedy następuje włożenie lub wyjęcie karty kierowcy lub karty warsztatowej:

- stan prowadzenia pojazdu (ZAŁOGA, JEDEN KIEROWCA),
- kartę w szczelinie czytnika (KIEROWCA, WSPÓLKIEROWCA),
- status karty w odpowiedniej szczelinie czytnika kart (WŁOŻONA, NIEWŁOŻONA) (patrz uwaga),
- czynność (PROWADZENIE, DYSPOZYCYJNOŚĆ, PRACA, PRZERWA/ODPOCZYNEK),
- datę i godzinę zmiany.

Uwaga: WŁOŻONA oznacza, że do szczeliny jest włożona ważna karta kierowcy lub warsztatowa. NIEWŁOŻONA oznacza sytuację przeciwną, tzn. że do szczeliny nie jest włożona ważna karta kierowcy lub warsztatowa (np. włożona jest karta firmowa lub brak karty).

Uwaga: Dane dotyczące czynności ręcznie wprowadzone przez kierowcę nie są rejestrowane w pamięci danych.

085 Pamięć danych wystarcza do przechowywania danych dotyczących czynności kierowcy przez przynajmniej 365 dni.

086 W przypadku zapelnienia pamięci danych nowe dane zastępują najstarsze dane.

12.5. Miejsca rozpoczęcia i/lub zakończenia dziennego okresu pracy

087 Urządzenie rejestrujące rejestruje i przechowuje w swojej pamięci danych za każdym razem gdy współkierowca wprowadza miejsce rozpoczęcia i/lub zakończenia dziennego okresu pracy:

- gdy dotyczy, numer karty (współ-)kierowcy i Państwo Członkowskie, które wydało kartę,
- datę i godzinę wprowadzenia danych (lub datę/godzinę odnoszące się do wpisu, jeżeli wpisu dokonano w ramach procedury ręcznego wprowadzania danych),
- typ wpisu (rozpoczęcia lub zakończenia, status wpisu),
- wprowadzone kraj i region,
- stan licznika kilometrów.

088 Pamięć danych wystarcza do przechowywania danych dotyczących rozpoczęcia i/lub zakończenia dziennego okresu pracy przez przynajmniej 365 dni (przy założeniu, że jeden kierowca wprowadza dwa zapisy dziennie).

089 W przypadku zapelnienia pamięci danych nowe dane zastępują najstarsze dane.

12.6. Dane dotyczące licznika kilometrów

090 Urządzenie rejestrujące rejestruje w swojej pamięci danych stan licznika kilometrów i odpowiadającą datę o północy każdego dnia kalendarzowego.

091 Pamięć danych wystarcza do przechowywania danych dotyczących stanu licznika o północy przez przynajmniej 365 dni kalendarzowych.

092 W przypadku zapelnienia pamięci danych nowe dane zastępują dane najstarsze.

12.7. Dane szczegółowe dotyczące prędkości

093 Urządzenie rejestrujące rejestruje i przechowuje w swojej pamięci danych prędkość chwilową pojazdu wraz z datą i godziną, rejestrowane co sekundę za okres przynajmniej ostatnich 24 godzin, w których pojazd był w ruchu.

12.8. Dane dotyczące zdarzeń

Do celów niniejszego punktu czas rejestruje się z rozdzielczością jednej sekundy.

094 Urządzenie rejestrujące rejestruje i przechowuje w swojej pamięci danych następujące dane dla każdego zdarzenia wykrytego zgodnie z poniższymi zasadami gromadzenia danych:

Zdarzenie	Zasady gromadzenia danych	Dane rejestrowane dla zdarzenia
Konflikt kart	— 10 ostatnich zdarzeń.	— data i godzina rozpoczęcia zdarzenia, — data i godzina zakończenia zdarzenia, — typ karty, numer karty i Państwo Członkowskie, które wydało kartę, dla obu kart powodujących konflikt.
Prowadzenie bez prawidłowej karty	— najdłuższe trwające zdarzenie dla każdego z 10 ostatnich dni od zaistnienia zdarzenia. — pięć najdłuższych trwających zdarzeń w okresie ostatnich 365 dni.	— data i godzina rozpoczęcia zdarzenia, — data i godzina zakończenia zdarzenia, — typ karty, numer karty i Państwo Członkowskie, które wydało kartę, dla obu kart powodujących konflikt. — liczba podobnych zdarzeń w tym dniu.
Włożenie karty podczas jazdy	— ostatnie zdarzenie dla każdego z 10 ostatnich dni od zaistnienia zdarzenia.	— data i godzina zdarzenia, — typ karty, numer karty i Państwo Członkowskie, które wydało kartę, — liczba podobnych zdarzeń w tym dniu.
Sesja ostatniej karty niezamknięta prawidłowo	— 10 ostatnich zdarzeń.	— data i godzina włożenia karty, — typ karty, numer karty i Państwo Członkowskie, które wydało kartę, — dane dotyczące ostatniej sesji odczytane z karty: — data i godzina włożenia karty, — numer VRN i Państwo Członkowskie rejestracji.
Przekroczenie prędkości ⁽¹⁾	— najpoważniejsze zdarzenie dla każdego z 10 ostatnich dni od zaistnienia zdarzenia (tzn. zdarzenie o najwyższej, przeciętnej prędkości), — pięć najpoważniejszych zdarzeń w okresie ostatnich 365 dni. — pierwsze zdarzenie zaistniałe po ostatniej kalibracji.	— data i godzina rozpoczęcia zdarzenia, — data i godzina zakończenia zdarzenia, — maksymalna prędkość pomierzona w czasie zdarzenia, — średnia arytmetyczna prędkość pomierzona w czasie zdarzenia, — typ karty, numer karty i Państwo Członkowskie, które wydało kartę kierowcy, (gdy dotyczy), — liczba podobnych zdarzeń w tym dniu.

Zdarzenie	Zasady gromadzenia danych	Dane rejestrowane dla zdarzenia
Przerwa zasilania ⁽²⁾	— najdłużej trwające zdarzenie dla każdego z 10 ostatnich dni od zaistnienia zdarzenia, — pięć najdłużej trwających zdarzeń w okresie ostatnich 365 dni.	— data i godzina rozpoczęcia zdarzenia, — data i godzina zakończenia zdarzenia, — typ karty, numer karty i Państwo Członkowskie, które wydało kartę, dla każdej karty włożonej na początku i/lub po zakończeniu zdarzenia, — liczba podobnych zdarzeń w tym dniu.
Błąd danych dotyczących ruchu	— najdłużej trwające zdarzenie dla każdego z 10 ostatnich dni od zaistnienia zdarzenia. — pięć najdłużej trwających zdarzeń w okresie ostatnich 365 dni.	— data i godzina rozpoczęcia zdarzenia, — data i godzina zakończenia zdarzenia — typ karty, numer karty i Państwo Członkowskie, które wydało kartę, dla każdej karty włożonej na początku i/lub po zakończeniu zdarzenia, — liczba podobnych zdarzeń w tym dniu.
Próba naruszenia zabezpieczenia	— 10 ostatnich zdarzeń wg typu zdarzenia.	— data i godzina rozpoczęcia zdarzenia, — data i godzina zakończenia zdarzenia, (gdy dotyczy), — typ karty, numer karty i Państwo Członkowskie, które wydało kartę, dla każdej karty włożonej na początku i/lub po zakończeniu zdarzenia, — typ zdarzenia.

095

⁽¹⁾ Urządzenie rejestrujące rejestruje również i przechowuje w swojej pamięci danych:

- datę i godzinę ostatniej KONTROLI PRZEKROCZENIA PRĘDKOŚCI,
- datę i godzinę pierwszego przekroczenia prędkości po tej KONTROLI PRZEKROCZENIA PRĘDKOŚCI,
- liczbę zdarzeń przekroczenia prędkości od ostatniej KONTROLI PRZEKROCZENIA PRĘDKOŚCI.

⁽²⁾ Dane te mogą być rejestrowane tylko po przywróceniu zasilania, godziny mogą być znane z dokładnością do minuty.

12.9. Dane dotyczące usterek

Do celów niniejszego pkt czas rejestruje się z rozdzielczością jednej sekundy.

096

A menetíró készülék az adatmemóriájában megkísérli rögzíteni és tárolni a következő tárolási szabályok szerint észlelt valamennyi hibát:

Usterka	Zasady gromadzenia danych	Dane rejestrowane dla usterek
Uszkodzenie karty	— 10 ostatnich uszkodzeń karty kierowcy	— data i godzina rozpoczęcia usterek, — data i godzina zakończenia usterek, — typ karty, numer karty i Państwo Członkowskie, które wydało kartę.
Usterki urządzenia rejestrującego	— 10 ostatnich usterek dla każdego typu usterek — pierwsza usterka po ostatniej kalibracji	— data i godzina rozpoczęcia usterek, — data i godzina rozpoczęcia usterek, — typ usterek, — typ karty, numer karty i Państwo Członkowskie, które wydało kartę, dla każdej karty włożonej na początku i/lub po zakończeniu usterek.

12.10. Dane kalibracyjne

- 097 Urządzenie rejestrujące rejestruje i przechowuje w swojej pamięci dane dotyczące:
- parametrów kalibracyjnych znanych w momencie aktywacji,
 - pierwszej kalibracji po aktywacji urządzenia,
 - pierwszej kalibracji w obecnym pojeździe (identyfikowanym numerem VIN),
 - pięciu ostatnich kalibracji, (jeżeli w czasie jednego dnia jest kilka kalibracji, zapamiętuje się tylko jedną, ostatnią z tego dnia).
- 098 Przy każdej z tych kalibracji rejestruje się następujące dane:
- rodzaj kalibracji (aktywacja, pierwsza instalacja, instalacja, przegląd okresowy),
 - nazwa (nazwisko) i adres warsztatu,
 - numer karty warsztatowej, Państwo Członkowskie wydające kartę i data ważności karty,
 - identyfikacja pojazdu,
 - parametry uaktualnione lub potwierdzone: w, k, l, rozmiar opon, nastawy urządzenia ograniczenia prędkości, licznik kilometrów (wartości stare i nowe), data i godzina (wartości stare i nowe).
- 099 Czujnik ruchu rejestruje i przechowuje w swojej pamięci następujące dane instalacyjne czujnika ruchu:
- pierwsze sparowanie z VU (data, godzina, numer homologacji VU, numer fabryczny VU),
 - ostatnie sparowanie z VU (data, godzina, numer homologacji VU, numer fabryczny VU).

12.11. Dane dotyczące regulacji czasu

- 100 Urządzenie rejestrujące rejestruje i przechowuje w swojej pamięci następujące dane:
- ostatnia regulacja czasu,
 - pięć największych regulacji czasu od ostatniej kalibracji,
- wykonane w trybie kalibracyjnym, poza ramami regularnej kalibracji (definicja f).
- 101 Przy każdej z tych regulacji czasu rejestruje się następujące dane:
- data i godzina, stara wartość,
 - data i godzina, nowa wartość,
 - nazwa (nazwisko) i adres warsztatu,
 - numer karty warsztatowej, Państwo Członkowskie wydające kartę i data ważności karty.

12.12. Dane dotyczące kontroli

- 102 Urządzenie rejestrujące rejestruje i przechowuje w swojej pamięci danych następujące dane dotyczące ostatnich 20 czynności kontrolnych:
- data i godzina kontroli,
 - numer karty kontrolnej i Państwo Członkowskie wydające kartę,
 - typ kontroli (wyświetlanie i/lub drukowanie i/lub wczytywanie danych z VU i/lub wczytywanie danych z karty).

- 103 W przypadku wczytywania danych rejestruje się także daty najbardziej oddalonych w czasie i najświeższych dni, z których dane są wczytywane.

12.13. *Dane dotyczące blokad firmowych*

- 104 Urządzenie rejestrujące rejestruje i przechowuje w swojej pamięci następujące dane dotyczące 20 ostatnich blokad firmowych:

- data i godzina założenia blokady,
- data i godzina zdjęcia blokady,
- numer karty firmowej i Państwo Członkowskie wydające kartę,
- nazwa (nazwisko) i adres firmy.

12.14. *Dane dotyczące wczytywania danych*

- 105 Urządzenie rejestrujące rejestruje i przechowuje w swojej pamięci danych następujące dane dotyczące ostatniego wczytywania danych z pamięci urządzenia na nośnik zewnętrzny, wykonanego w trybie firmowym lub kalibracyjnym:

- data i godzina wczytania danych,
- numer karty firmowej lub warsztatowej, Państwo Członkowskie wydające kartę,
- nazwa (nazwisko) firmy lub warsztatu.

12.15. *Dane dotyczące warunków szczególnych*

- 105a Urządzenie rejestrujące rejestruje i przechowuje w swojej pamięci danych następujące dane dotyczące stanów szczególnych:

- data i godzina wprowadzenia danych,
- typ stanu szczególnego.

- 105b Pamięć danych przechowuje dane dotyczące stanów szczególnych przez przynajmniej 365 dni (przy założeniu, że przeciętnie otwiera się i zamyka jeden stan dziennie). W przypadku zapelnienia pamięci danych nowe dane zastępują dane najstarsze.

13. *Odczyt kart do tachografów*

- 106 Urządzenie rejestrujące umożliwia odczyt z kart do tachografów, gdzie stosowne, danych niezbędnych do:

- rozpoznania typu karty, posiadacza karty, wcześniej używanego pojazdu, daty i godziny ostatniego wyjęcia karty i czynności wybranej dla tego czasu,
- sprawdzenia czy ostatnia sesja karty jest prawidłowo zamknięta,
- wyliczenia dla kierowcy: nieprzerwanego czasu prowadzenia pojazdu, skumulowanego czasu przerwy i skumulowanego czasu prowadzenia za poprzedni i obecny tydzień,
- wydrukowania żądanych wydruków związanych z danymi zarejestrowanymi na karcie kierowcy,
- przesłania danych z karty kierowcy do zewnętrznego nośnika.

- 107 W przypadku błędu odczytu urządzenie rejestrujące maksymalnie trzykrotnie powtarza to samo polecenie odczytu i w przypadku gdy odczyt nadal nie jest możliwy, uznaje kartę za uszkodzoną i nieważną.

14. *Rejestrowanie i przechowywanie danych na kartach do tachografów*

- 108 Urządzenie rejestrujące ustawia »dane sesji karty« na karcie kierowcy lub warsztatowej bezpośrednio po włożeniu karty.

- 109 Urządzenie rejestrujące aktualizuje dane zapisane na ważnej karcie kierowcy, warsztatowej i/lub kontrolnej wprowadzając wszystkie niezbędne dane odnośnie do okresu, w którym karta pozostaje włożona i odnośnie do posiadacza karty. Dane, które są przechowywane na tych kartach, określono w rozdziale IV.
- 109a Urządzenie rejestrujące aktualizuje dane dotyczące czynności kierowcy i umiejscowienia (określone w rozdziale IV, pkt 5.2.5 i 5.2.6), zapisane na ważnej karcie kierowcy i/lub warsztatowej, wpisując dane dotyczące czynności i umiejscowienia wprowadzone ręcznie przez posiadacza karty.
- 110 Aktualizacja kart do tachografów odbywa się w taki sposób, że gdy trzeba i biorąc pod uwagę rzeczywistą zdolność gromadzenia danych, najnowsze dane zastępują dane najstarsze.
- 111 W przypadku błędu zapisu urządzenie rejestrujące maksymalnie trzykrotnie powtarza to samo polecenie zapisu i w przypadku gdy zapis nadal nie jest możliwy, uznaje kartę za uszkodzoną i nieważną.
- 112 Przed oddaniem karty kierowcy i po zapisaniu na karcie wszystkich stosownych danych urządzenie rejestrujące zeruje dane sesji karty.

15. Wyświetlanie

- 113 Wyświetlacz umożliwia wyświetlanie przynajmniej 20 znaków.
- 114 Znaki mają przynajmniej 5 mm wysokości i 3,5 mm szerokości.
- 114a Wyświetlacz umożliwia wyświetlanie łacińskich i greckich znaków strony kodowej, według normy ISO 8859 części 1 i 7, określonych w dodatku 1 rozdział 4 »Zestawy znaków«. Wyświetlacz może wyświetlać uproszczone glyfy (np. znaki z akcentami można wyświetlać bez akcentu, a małe litery można wyświetlać jako duże).
- 115 Wyświetlacz ma nieoślepiające oświetlenie.
- 116 Wskazania są widoczne spoza urządzenia rejestrującego.
- 117 Urządzenie rejestrujące pokazuje:
- informacje standardowe,
 - informacje związane z ostrzeżeniami,
 - informacje związane z dostępem do menu,
 - inne informacje, których zażąda użytkownik.
- Urządzenie rejestrujące może wyświetlać również dodatkowe informacje, z tym jednak, że muszą być one łatwe do odróżnienia od wymienionych powyżej, wymaganych informacji.
- 118 Wyświetlacz urządzenia rejestrującego używa piktogramów lub kombinacji piktogramów pokazanych w dodatku 3. Dopuszcza się także dodatkowe piktogramy lub kombinacje piktogramów, jeżeli są one łatwe do odróżnienia od wymaganych piktogramów lub kombinacji piktogramów.
- 119 Gdy pojazd jest w ruchu wyświetlacz jest stale włączony.
- 120 Urządzenie rejestrujące może gasić wyświetlacz automatycznie lub umożliwiać gaszenie ręczne, gdy pojazd nie jest w ruchu.
- Format obrazowania określono w dodatku 5.
- ### 15.1. Informacje na wyświetlaczu w warunkach normalnych
- 121 Gdy nie trzeba wyświetlać innych informacji, urządzenie rejestrujące wyświetla domyślnie następujące informacje:
- miejscowy czas (czas UTC + przesunięcie wprowadzone przez kierowcę),
 - tryb pracy,
 - bieżącą czynność kierowcy i bieżącą czynność współkierowcy,

- informacje odnoszące się do kierowcy:
 - jeżeli jego bieżącą czynnością jest PROWADZENIE, jego bieżący nieprzerwany czas prowadzenia pojazdu i jego bieżący skumulowany czas przerwy,
 - jeżeli jego bieżącą czynnością nie jest PROWADZENIE, bieżący czas trwania tej czynności (od momentu wybrania) i jego bieżący skumulowany czas przerwy,
- informacje odnoszące się do współkierowcy:
 - bieżący czas trwania jego czynności (od momentu wybrania).

- 122 Prezentacja informacji odnoszących się do każdego kierowcy jest wyraźna, prosta i jednoznaczna. W przypadku gdy informacji odnoszących się do kierowcy i współkierowcy nie można wyświetlić w tym samym czasie, urządzenie rejestrujące pokazuje domyślnie informacje odnoszące się do kierowcy i pozwala użytkownikowi wyświetlić informacje odnoszące się do współkierowcy.
- 123 W przypadku gdy wyświetlacz nie pozwala na domyślne pokazywanie trybu pracy, to przy zmianie trybu pracy urządzenie rejestrujące przez krótki czas pokazuje nowy tryb pracy.
- 124 Przy wkładaniu karty urządzenie rejestrujące przez krótki czas pokazuje nazwisko jej posiadacza.
- 124a W przypadku rozpoczętego stanu »POZA ZAKRESEM«, na wyświetlaczu, w warunkach normalnych, muszą być informacje w postaci stosownego piktogramu wskazujące, że stan taki jest rozpoczęty (dopuszcza się, że w tym samym czasie nie jest pokazywana bieżąca czynność kierowcy).

15.2. Ostrzeżenia

- 125 Przy wyświetlaniu ostrzeżeń urządzenie rejestrujące korzysta przede wszystkim z piktogramów pokazanych w dodatku 3, gdy trzeba uzupełnić informacjami w postaci kodów liczbowych. Można też dodać wyszczególnienie słowne w preferowanym języku kierowcy.

15.3. Dostęp do menu

- 126 Urządzenie rejestrujące udostępnia niezbędne polecenia poprzez odpowiednie menu.

15.4. Inne informacje

- 127 Na żądanie jest możliwe selektywne wyświetlanie:
- daty i godziny UTC,
 - trybu pracy, (jeśli nie jest pokazywany domyślnie),
 - nieprzerwanego czasu prowadzenia pojazdu i skumulowanego czasu przerwy kierowcy,
 - nieprzerwanego czasu prowadzenia pojazdu i skumulowanego czasu przerwy współkierowcy,
 - skumulowanego czasu prowadzenia pojazdu kierowcy za poprzedni i bieżący tydzień,
 - skumulowanego czasu prowadzenia pojazdu współkierowcy za poprzedni i bieżący tydzień,
 - treści każdego z sześciu wydruków w takim samym formacie jak wydruki.
- 128 Treść wydruku jest wyświetlana sekwencyjnie wiersz po wierszu. Jeżeli w szerokości wyświetlacza mieści się mniej niż 24 znaki, użytkownik ma dostęp do pełnej informacji np. w kilku wierszach, przy pomocy przewijania, itp. Wiersze wydruku przeznaczone na ręczne adnotacje można pominąć na wyświetlaczu.

16. Drukowanie

- 129 Urządzenie rejestrujące umożliwia drukowanie sześciu określonych poniżej wydruków, na podstawie informacji zgromadzonych w pamięci urządzenia i/lub na kartach do tachografów:
- wydruk dzienny czynności kierowcy z karty,
 - wydruk dzienny czynności kierowcy z przyrządu rejestrującego,

- wydruk zdarzeń i usterek z karty,
- wydruk zdarzeń i usterek z przyrządu rejestrującego,
- wydruk danych technicznych,
- wydruk przekroczenia prędkości.

Szczegóły formatu i treści tych wydruków określono w dodatku 4.

Na zakończenie wydruków mogą być umieszczane informacje dodatkowe.

Urządzenie rejestrujące może wykonywać także dodatkowe wydruki, jeżeli są one łatwe do odróżnienia od sześciu, określonych powyżej wydruków.

- 130 »Wydruk dzienny czynności kierowcy z karty« i »wydruk zdarzeń i usterek z karty« dostępne są jedynie wtedy, gdy do urządzenia rejestrującego włożona jest karta kierowcy lub karta warsztatowa. Przed uruchomieniem drukowania urządzenie rejestrujące aktualizuje dane przechowywane na stosownej karcie.
- 131 W celu sporządzenia »wydruku dziennego czynności kierowcy z karty« lub »wydruku zdarzeń i usterek z karty« urządzenie rejestrujące:
- automatycznie wybiera kartę kierowcy lub kartę warsztatową, jeżeli tylko jedna z tych kart jest włożona do urządzenia rejestrującego,
 - albo umożliwia wybór karty źródłowej albo wybiera kartę znajdującą się w szczelinie karty kierowcy, jeżeli obie te karty włożone są do urządzenia rejestrującego.
- 132 Drukarka drukuje 24 znaki w wierszu.
- 133 Drukowane znaki mają wymiary przynajmniej 2,1 mm wysokości i 1,5 mm szerokości.
- 133a Drukarka umożliwia drukowanie łacińskich i greckich znaków strony kodowej według ISO 8859 części 1 i 7, określonych w dodatku 1 rozdział 4 »Zestawy znaków«.
- 134 Konstrukcja drukarki umożliwia sporządzanie wydruków z rozdzielczością eliminującą niejednoznaczność przy odczycie.
- 135 Wydruki zachowują wymiary i treść w warunkach normalnej wilgotności (10 do 90 %) i temperatury.
- 136 Papier używany w urządzeniu rejestrującym ma odpowiedni znak homologacji typu i oznakowanie typu(-ów) urządzenia rejestrującego, w którym może być używany. Wydruki są łatwe do odczytania i rozróżnienia, gdy są przechowywane w normalnych warunkach przechowywania — natężenie oświetlenia, wilgotność i temperatura, przez okres przynajmniej jednego roku.
- 137 Na wydruku można umieścić ręcznie adnotacje, takie jak podpis kierowcy.
- 138 Urządzenie rejestrujące obsługuje zdarzenia »brak papieru« w czasie drukowania, a po założeniu papieru, uruchamia drukowanie od początku wydruku lub kontynuuje drukowanie i umieszcza jednoznaczne odniesienie do części wcześniej wydrukowanej.

17. Ostrzeżenia

- 139 Urządzenie rejestrujące ostrzega kierowcę o wykryciu zdarzenia i/lub usterki.
- 140 Ostrzeżenie o przerwie zasilania może być opóźnione do czasu przywrócenia zasilania.
- 141 Urządzenie rejestrujące ostrzega kierowcę na 15 minut przed i w momencie przekroczenia 4 godz. 30 min. nieprzerwanego czasu prowadzenia pojazdu.
- 142 Ostrzeżenia są wizualne. Dopuszcza się ostrzeżenia akustyczne dodatkowo do ostrzeżeń wizualnych.

- 143 Ostrzeżenia wizualne są łatwo rozpoznawalne przez użytkownika, znajdują się w polu widzenia kierowcy i są łatwe do odczytania tak w dzień jak i w nocy.
- 144 Ostrzeżenia wizualne mogą być emitowane bezpośrednio przez urządzenie rejestrujące i/lub zdalnie od urządzenia rejestrującego.
- 145 W tym ostatnim przypadku są oznaczone symbolem »T« i są w kolorze bursztynowym lub pomarańczowym.
- 146 Ostrzeżenia trwają przez przynajmniej 30 sekund, chyba że są potwierdzone przez użytkownika poprzez wciśnięcie dowolnego przycisku w urządzeniu rejestrującym. To pierwsze potwierdzenie nie kasuje informacji o przyczynie ostrzeżenia omówionej w następnym punkcie.
- 147 Urządzenie rejestrujące wyświetla informację o przyczynie ostrzeżenia, aż do momentu potwierdzenia przez użytkownika przy pomocy specjalnego przycisku lub polecenia urządzenia rejestrującego.
- 148 Dopuszcza się dodatkowe ostrzeżenia, pod warunkiem że nie są mylące dla kierowców w odniesieniu do wcześniej zdefiniowanych ostrzeżeń.

18. Przesyłanie danych do nośnika zewnętrznego

- 149 Urządzenie rejestrujące umożliwia przesyłanie, na żądanie, danych ze swojej pamięci danych lub karty kierowcy do zewnętrznego nośnika poprzez gniazdo kalibracji/wczytywania danych. Przed przesłaniem danych urządzenie rejestrujące aktualizuje dane zgromadzone na stosownej karcie.
- 150 Dodatkowo i opcjonalnie, urządzenie rejestrujące może w trybie pracy i po dokonaniu uwierzytelnienia przysyłać dane poprzez inne gniazdo do firmy upoważnionej do korzystania z tego kanału. W takim przypadku do tak przesyłanych danych stosuje się prawa dostępu obowiązujące dla trybu firmowego.
- 151 Przesyłanie danych nie może zmieniać ani usuwać jakichkolwiek zgromadzonych danych.

Specyfikacje elektrycznego interfejsu dla gniazda kalibracji/wczytywania danych znajdują się w dodatku 6.

Protokoły przesyłania danych znajdują się w dodatku 7.

19. Wyjście danych dla dodatkowych urządzeń zewnętrznych

- 152 Jeżeli w urządzeniu rejestrującym nie ma funkcji wyświetlania prędkości i/lub licznika kilometrów, urządzenie rejestrujące dostarcza sygnał(-y) wyjściowy umożliwiający wyświetlenia prędkości pojazdu (prędkościomierz) i/lub całkowitej drogi przebytej przez pojazd (licznik kilometrów).
- 153 Przyrząd rejestrujący umożliwia też wyprowadzanie następujących danych poprzez odpowiednie, dedykowane łącze szeregowe niezależnie od opcjonalnego przyłączenia szyny CAN (norma ISO 11898 Pojazdy drogowe — Wymiana cyfrowych informacji — Szybka sieć obszaru kontroli CAN), umożliwiającą innym urządzeniom elektrycznym zainstalowanym w pojeździe przetwarzać następujących danych:

- aktualnej daty i godziny UTC,
- prędkości pojazdu,
- całkowitej drogi przebytej przez pojazd (licznik kilometrów),
- bieżąco wybranej czynności kierowcy i współkierowcy,
- informacji czy w szczelinach karty kierowcy i współkierowcy jest aktualnie włożona karta do tachografów i (gdy dotyczy) informacje identyfikacyjne odpowiednich kart (numer karty i Państwo Członkowskie wydające kartę).

Ten wykaz minimum można rozszerzyć o inne dane.

Przy wyłączonym zapłonie pojazdu dane te udostępniane są nieprzerwanie. Przy wyłączonym zapłonie pojazdu na odpowiednich wyjściach generowane są dane przynajmniej przy każdej zmianie czynności kierowcy lub współkierowcy i/lub włożeniu lub wyjęciu karty do tachografów. W przypadku gdy przy wyłączonym zapłonie wyprowadzanie danych jest zablokowane, dane te zostają udostępnione ponownie z chwilą włączenia zapłonu pojazdu.

20. Kalibracja

- 154 Funkcja kalibracji umożliwia:
- automatyczne sparowanie czujnika ruchu z VU,
 - cyfrowe dostosowanie stałej urządzenia rejestrującego (k) do współczynnika charakterystycznego pojazdu (w) (pojazdy mające dwa lub więcej przełożeń osi posiadają urządzenie przełączające, które automatycznie dopasowuje te różne przełożenia do przełożenia, dla którego urządzenie jest dostosowane w tym pojeździe),
 - regulację (bez ograniczenia) bieżącego czasu,
 - regulację bieżącego wskazania licznika kilometrów,
 - aktualizację danych identyfikacyjnych czujnika ruchu zapisanych w pamięci danych,
 - aktualizację lub potwierdzenie innych parametrów używanych przez urządzenie rejestrujące: identyfikacja pojazdu, w, l, rozmiar opon i ustawienie urządzenia ograniczenia prędkości, (gdy dotyczy).
- 155 Parowanie czujnika ruchu z VU obejmuje przynajmniej:
- aktualizację danych instalacyjnych czujnika ruchu zapisanych w pamięci czujnika ruchu, (gdy trzeba),
 - skopiowanie z czujnika ruchu do pamięci danych VU niezbędnych danych identyfikacyjnych czujnika ruchu.
- 156 Funkcja kalibracji umożliwia wprowadzanie niezbędnych danych poprzez gniazdo kalibracji/wczytywania danych zgodnie z protokołem kalibracji zdefiniowanym w dodatku 8. Funkcja kalibracji może także pozwalać na wprowadzanie niezbędnych danych poprzez inne gniazda.

21. Regulacja czasu

- 157 Funkcja regulacji czasu umożliwia regulację bieżącego czasu w granicach maksymalnie jednej minuty, w nie mniej niż siedmiodniowych odstępach czasu.
- 158 W trybie kalibracyjnym funkcja regulacji czasu umożliwia regulację bieżącego czasu bez ograniczenia.

22. Charakterystyki pracy

- 159 Przyrząd rejestrujący zachowuje pełną funkcjonalność w zakresie temperatur – 20 do 70 °C a czujnik ruchu w zakresie temperatur – 40 do 135 °C. Zawartość pamięci danych jest zachowana w temperaturach do – 40 °C.
- 160 Urządzenie rejestrujące zachowuje pełną funkcjonalność w zakresie wilgotności 10 do 90 %.
- 161 Urządzenie rejestrujące jest zabezpieczone przed przepięciami, odwróceniem biegunowości zasilania i zwarciami.
- 162 Urządzenie rejestrujące spełnia wymagania dyrektywy Komisji 95/54/WE z dnia 31 października 1995 r. ⁽¹⁾ dostosowującej do postępu technicznego dyrektywę Rady 72/245/EWG ⁽²⁾ odnoszącą się do kompatybilności elektromagnetycznej i jest zabezpieczone przed rozładowania elektrostatycznymi i stanami przejściowymi.

23. Materiały

- 163 Wszystkie części składowe urządzenia rejestrującego są wykonane z materiałów o wystarczającej stabilności i wytrzymałości mechanicznej oraz stabilnych właściwościach elektrycznych i magnetycznych.
- 164 Dla normalnych warunków eksploatacji wszystkie części wewnętrzne urządzeń są zabezpieczone przed wilgocią i pyłem.
- 165 Przyrząd rejestrujący spełnia wymagania klasy ochrony IP 40 a czujnik spełnia wymagania klasy ochrony IP 64 zgodnie z normą IEC 529.

⁽¹⁾ Dz.U. L 266 z 8.11.1995, str. 1.

⁽²⁾ Dz.U. L 152 z 6.7.1972, str. 15.

166 Urządzenie rejestrujące spełnia odpowiednie wymagania techniczne odnoszące się do ergonomii rozwiązania.

167 Urządzenie rejestrujące jest zabezpieczone przed przypadkowym uszkodzeniem.

24. Oznakowania

168 Jeżeli urządzenie rejestrujące pokazuje stan licznika kilometrów i prędkość, na jego wyświetlaczu widoczne są następujące informacje:

- przy liczbie pokazującej odległość, jednostka miary odległości wskazana skrótem »km«,
- przy liczbie pokazującej prędkość, wpis »km/h«.

Urządzenie rejestrujące może być przełączane na wskazywanie prędkości w milach na godzinę, w takim przypadku jednostka pomiaru prędkości jest wskazana skrótem »mph«.

169 Do każdego odrębnego elementu urządzenia rejestrującego jest przymocowana tabliczka zawierająca następujące informacje:

- nazwa (nazwisko) i adres producenta urządzenia,
- numer części producenta i rok produkcji urządzenia,
- numer fabryczny urządzenia,
- znak homologacji typu dla urządzenia.

170 Jeżeli dostępna powierzchnia nie wystarcza do pokazania wszystkich opisanych powyżej informacji, to na plakietce znajduje się przynajmniej: nazwa producenta lub jego logo i numer części.

IV. WYMAGANIA KONSTRUKCYJNE I FUNKCYJNALNE KART DO TACHOGRAFÓW

1. Dane widzialne

Na awersie znajdują się:

171 Wyrażenie »Karta kierowcy« lub »Karta kontrolna«, lub »Karta warsztatowa«, lub »Karta firmowa« drukowane dużą czcionką w języku urzędowym lub językach Państwa Członkowskiego wydającego kartę, zgodnie z typem karty;

172 To samo wyrażenie w innych, urzędowych językach Wspólnoty, drukowane, tak by tworzyć tło karty:

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

173 Nazwa Państwa Członkowskiego wydającego kartę (opcjonalnie);

- 174 Wyróżniający znak Państwa Członkowskiego wydającego kartę, drukowany w negatywie w niebieskim prostokącie i otoczony 12 żółtymi gwiazdkami. Wyróżniające znaki ustala się następująco:

B	Belgia
DK	Dania
D	Niemcy
GR	Grecja
E	Hiszpania
F	Francja
IRL	Irlandia
I	Włochy
L	Luksemburg
NL	Niderlandy
A	Austria
P	Portugalia
FIN	Finlandia
S	Szwecja
UK	Zjednoczone Królestwo;

- 175 Informacje szczególne dla wydanej karty, ponumerowane jak następuje:

	Karta kierowcy	Karta kontrolna	Karta firmowa lub warsztatowa
1.	Nazwisko kierowcy	Nazwa organu kontrolnego	Karta firmowa lub warsztatowa
2.	Imię(-ona) kierowcy	Nazwisko kontrolera, (gdy dotyczy)	Nazwisko posiadacza karty, (gdy dotyczy)
3.	Data urodzenia kierowcy	Imię(imiona) kontrolera, (gdy dotyczy)	Imię(imiona) posiadacza karty, (gdy dotyczy)
4.(a)	Data początku okresu ważności karty		
(b)	Data upływu ważności karty, (gdy dotyczy)		
(c)	Nazwa organu wydającego (może być umieszczona na odwrocie)		
(d)	Numer inny niż w pozycji 5, do celów administracyjnych (nieobowiązkowe)		
5.(a)	Numer prawa jazdy (dla daty wydania karty kierowcy)		
5.(b)	Numer karty		
6.	Zdjęcie kierowcy	Zdjęcie kontrolera (nieobowiązkowe)	—
7.	Podpis kierowcy	Podpis posiadacza karty (nieobowiązkowe)	
8.	Miejsce stałego zamieszkania lub adres pocztowy posiadacza karty (nieobowiązkowe)	Adres pocztowy organu kontrolnego	Adres pocztowy firmy lub warsztatu

- 176 Daty podaje się w formacie »dd/mm/rrrr« lub »dd.mm.rrrr« (dzień, miesiąc, rok);

na rewersie znajdują się:

- 177 Objaśnienia numerowanych pozycji znajdujących się na awersie karty;

- 178 Za szczególną, pisemną zgodą posiadacza karty, na karcie można dodatkowo umieścić informacje, które nie wiążą się z administrowaniem kartą, takie dodatkowe informacje w żaden sposób nie zmieniają sposobu używania danego modelu jako karty do tachografów.

WZORY WSPÓLNOTOWYCH KART DO TACHOGRAFÓW			
AWERS		REWERS	
A	 KARTA KIEROWCY 1. 2. 3. 4a. 4c. (4d.) 5a. 5b. 7. (8.)	Państwo TARJETA DEL CONDUCTOR FØRERKORT FAHRERKARTE 4b. KAPTA O ΔΗΤΟΥ DRIVER CARD CARTE DE CONDUCTEUR CÂRTA TROMÂNĂ CARTA DEL CONDUCENTE BESTUURDESKAART CARTÃO DE CONDUTOR KULJETTAJAKORTTILLA FÖRARKORT	B
	 KARTA KONTROLNA 1. (2.) (3.) 4a. (4d.) 5b. (6.) 7. 8.	Państwo TARJETA DE CONTROL KONTROLKORT KONTROLLKARTE 4b. KAPTA ΕΛΕΓΧΟΥ CONTROL CARD CARTE DE CONTROLEUR CÂRTA STIURTHA CARTA DI CONTROLLO CONTOLEKAART CARTÃO DE CONTROLO VALVONTAKORTTILLA KONTROLLKORT	
	 KARTA WARSZTATOWA 1. (2.) (3.) 4a. 4c. (4d.) 5b. (7.) 8.	Państwo TARJETA DEL CENTRO DE ENSAYO VÆRKSTEDSKORT WERKSTATTKARTE 4b. KAPTA KENTROU ΔΟΚΙΜΩΝ WORKSHOP CARD CARTE D'ATELIER CÂRTA CEARDLAINNE CARTA DELL'OFFICINA WERKPLAATSKAART CARTÃO DO CENTRO DE ENSAIO TESTAUSASEMAKORTTILLA VERKSTADSKORT	
	 KARTA FIRMOWA 1. (2.) (3.) 4a. 4c. (4d.) 5b. (7.) 8.	Państwo TARJETA DE LA EMPRESA VIRKSOMHEDSKORT UNTERNEHMENSKARTE 4b. KAPTA ETIKETTE COMPANY CARD CARTE D'ENTREPRISE CÂRTA COMLACHTA CARTA DELL'AZIENDA BEDRIJFSKAART CARTÃO DE EMPRESA YRITYSKORTTILLA FÖRETAGSKORT	
A	1. Nazwisko 2. Imię(a) 3. Data urodzenia 4a. Data początku okresu ważności karty 4b. Administracyjny termin ważności karty 4c. Organ wydający (4d). Nr dla krajowych celów administracyjnych 5a. Numer prawa jazdy 5b. Numer karty 6. Zdjęcie 7. Podpis (8.) Adres Proszę zwrócić do: NAZWA I ADRES ORGANU		B
	1. Organ kontrolny 2. Nazwisko 3. Imię(a) 4a. Data początku okresu ważności karty 4b. Administracyjny termin ważności karty 4c. Organ wydający (4d). Nr dla krajowych celów administracyjnych 5b. Numer karty (6.) Zdjęcie (7.) Podpis 8. Adres Proszę zwrócić do: NAZWA I ADRES ORGANU		
	1. Nazwa warsztatu 2. Nazwisko 3. Imię(a) 4a. Data początku okresu ważności karty 4b. Administracyjny termin ważności karty 4c. Organ wydający (4d). Nr dla krajowych celów administracyjnych 5b. Numer karty (7.) Podpis 8. Adres Proszę zwrócić do: NAZWA I ADRES ORGANU		
	1. Nazwa firmy 2. Nazwisko 3. Imię(a) 4a. Data początku okresu ważności karty 4b. Administracyjny termin ważności karty 4c. Organ wydający (4d). Nr dla krajowych celów administracyjnych 5b. Numer karty (7.) Podpis 8. Adres Proszę zwrócić do: NAZWA I ADRES ORGANU		

179 Karty do tachografów drukuje się w następujących dominujących kolorach tła:

- karta kierowcy: biały,
- karta kontrolna: niebieski,
- karta warsztatowa: czerwony,
- karta firmowa: żółty.

180 Karty do tachografów mają przynajmniej następujące zabezpieczenia przed fałszowaniem:

- zabezpieczający wzór tła z drukowanym drobnym giloszem i tęczą,
- w obszarze zdjęcia zabezpieczający wzór tła i zdjęcia zachodzą na siebie,
- przynajmniej dwubarwną linię wykonaną techniką mikrodruku.

- 181 Po konsultacji z Komisją, Państwa Członkowskie mogą dodać kolory lub oznakowania, takie jak symbole państwowe i zabezpieczenia, bez uszczerbku dla innych przepisów niniejszego Załącznika.

2. Zabezpieczenie

Celem systemu zabezpieczenia jest ochrona integralności i autentyczności danych wymienianych między kartami a urządzeniem rejestrującym, ochrona integralności i autentyczności danych wczytywanych z kart, umożliwienie niektórych czynności zapisu na kartach tylko urządzeniu rejestrującemu, uniemożliwienie fałszowania danych przechowywanych na kartach, uniemożliwienie fałszowania i wykrycie wszelkich prób fałszerstwa.

- 182 W celu osiągnięcia bezpieczeństwa systemu karty do tachografów spełniają zdefiniowane dla kart do tachografów ogólne cele zabezpieczenia (dodatek 10).
- 183 Karty do tachografów są odczytywane przy pomocy innych urządzeń, takich jak komputer osobisty.

3. Normy

- 184 Karty do tachografów spełniają wymagania następujących norm:

- ISO/IEC 7810 Identyfikacja kart — charakterystyki fizyczne,
- ISO/IEC 7816 Identyfikacja kart — obwody drukowane z zespołami stykowymi:
 - Część 1: Charakterystyki fizyczne,
 - Część 2: Wymiary i rozmieszczenie styków,
 - Część 3: Sygnały elektryczne i protokoły transmisji,
 - Część 4: Polecenia międzybranżowe dla wymiany danych,
 - Część 8: Polecenia międzybranżowe związane z bezpieczeństwem,
- ISO/IEC 10373 Identyfikacja kart — Metody badania.

4. Wymagania środowiskowe i elektryczne

- 185 Karty do tachografów prawidłowo pracują w warunkach klimatycznych normalnie występujących na terytorium Wspólnoty, przynajmniej w zakresie temperatur od -25 do $+70$ °C ze sporadycznymi temperaturami szczytowymi do $+85$ °C, przy czym »sporadyczny« oznacza nie dłużej niż 4 godziny jednorazowo i nie więcej niż 100 razy w okresie eksploatacji karty.
- 186 Karty do tachografów prawidłowo pracują w zakresie wilgotności od 10 do 90 %.
- 187 Karty do tachografów prawidłowo pracują przez okres pięciu lat, jeżeli są używane w warunkach określonych w warunkach środowiskowych i elektrycznych.
- 188 W czasie pracy karty do tachografów spełniają wymagania dyrektywy Komisji 95/54/WE z dnia 31 października 1995 r. ⁽¹⁾ odnoszącej się do kompatybilności elektromagnetycznej, i są zabezpieczone przed rozładowaniami elektrosztatycznymi.

5. Gromadzenie danych

Do celów niniejszego pkt:

- czas jest rejestrowany z dokładnością do jednej minuty, chyba że ustalono inaczej,
- stany licznika kilometrów rejestruje się z dokładnością do jednego kilometra,
- prędkości rejestruje się z dokładnością do 1 km/godz.

Funkcje kart do tachografów, polecenia i struktury logiczne, spełnianie wymagań dotyczących gromadzenia danych wyszczególniono w dodatku 2.

⁽¹⁾ Dz.U. L 266 z 8.11.1995, str. 1.

- 189 W niniejszym punkcie określono minimalne zdolności gromadzenia danych dla różnych zbiorów danych aplikacyjnych. Karty do tachografów przekazują do urządzenia rejestrującego bieżącą zdolność gromadzenia danych dla tych zbiorów danych.

Wszelkie dodatkowe dane, jakie mogą być zapisywane na kartach do tachografów, odnoszące się do innych aplikacji ewentualnie obsługiwanych przez kartę, są zapisywane zgodnie z dyrektywą 95/46/WE z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych ⁽¹⁾.

5.1. Identyfikacja kart i bezpieczeństwo danych

5.1.1. Identyfikacja aplikacji

- 190 Karty do tachografów umożliwiają przechowywanie następujących danych identyfikujących aplikacje:

- identyfikacja aplikacji tachograficznej,
- identyfikacja typu karty do tachografów.

5.1.2. Identyfikacja układu scalonego

- 191 Karty do tachografów umożliwiają przechowywanie następujących danych identyfikujących układ scalony (IC):

- numer fabryczny układu scalonego,
- oznaczenie fabryczne układu scalonego.

5.1.3. Identyfikacja kart mikroprocesorowych

- 192 Karty do tachografów umożliwiają przechowywanie następujących danych identyfikujących kartę inteligentną:

- numer fabryczny karty (włącznie z numerem karty producenta),
- numer homologacji typu dla karty,
- identyfikacja instytucji dokonującej personalizacji kart (ID),
- wbudowany identyfikator,
- identyfikator układu scalonego.

5.1.4. Zabezpieczenia

- 193 Karty do tachografów umożliwiają przechowywanie następujących danych dotyczących zabezpieczenia:

- europejski klucz publiczny,
- certyfikat Państwa Członkowskiego,
- certyfikat karty,
- klucz prywatny karty.

5.2. Karta kierowcy

5.2.1. Identyfikacja karty

- 194 Karta kierowcy umożliwia przechowywanie następujących danych identyfikujących kartę:

- numer karty,
- Państwo Członkowskie wydające, nazwa organu wydającego, data wydania,
- data rozpoczęcia okresu ważności karty, data upływu ważności karty.

⁽¹⁾ Dz.U. L 281 z 23.11.1995, str. 31.

5.2.2. Identyfikacja posiadacza karty

195 Karta kierowcy umożliwia przechowywanie następujących danych identyfikujących posiadacza karty:

- nazwisko posiadacza karty,
- imię (imiona) posiadacza karty,
- data urodzenia,
- preferowany język.

5.2.3. Dane dotyczące prawa jazdy

196 Karta kierowcy umożliwia przechowywanie następujących danych dotyczących prawa jazdy:

- Państwo Członkowskie wydające, nazwa organu wydającego,
- numer prawa jazdy (w dacie wydania karty).

5.2.4. Dane dotyczące używanego pojazdu

197 Karta kierowcy umożliwia przechowywanie, dla każdego dnia kalendarzowego, w którym karta jest użyta, i dla każdego okresu używania danego pojazdu w tym dniu (okres używania obejmuje cały okres włożenia wyjęcia karty w danym pojeździe z punktu widzenia karty), następujących danych:

- data i godzina pierwszego użycia pojazdu (tj. pierwsze włożenie karty w tym okresie używania pojazdu lub 00:00, jeżeli okres używania trwał w tym czasie),
- stan licznika kilometrów o tej godzinie,
- data i godzina ostatniego użycia pojazdu, (tj. ostatnie wyjęcie karty w tym okresie używania pojazdu lub 23:59, jeżeli okres używania trwał w tym czasie),
- stan licznika kilometrów o tej godzinie,
- numer VRN i Państwo Członkowskie rejestracji pojazdu.

198 Karta kierowcy umożliwia przechowywanie przynajmniej 84 takich zapisów.

5.2.5. Dane dotyczące czynności kierowcy

199 Karta kierowcy umożliwia przechowywanie, dla każdego dnia kalendarzowego, w którym karta jest użyta, lub dla każdego dnia, dla którego kierowca ręcznie wprowadza informacje dotyczące czynności, następujących danych:

- data,
- dzienny licznik obecności (zwiększony o jeden dla każdego z dni kalendarzowych),
- całkowita droga przebyta przez kierowcę w ciągu tego dnia,
- status kierowcy o godzinie 00:00,
- za każdym razem, kiedy kierowca zmienia czynność, i/lub zmienia stan prowadzenia pojazdu, i/lub wkłada lub wyjmuje swoją kartę:
 - stan prowadzenia pojazdu (ZAŁOGA, JEDEN KIEROWCA),
 - szczelina czytnika karty (KIEROWCA, WSPÓLKIEROWCA),
 - status karty (WŁOŻONA, NIEWŁOŻONA),
 - czynność (PROWADZENIE, DYSPOZYCYJNOŚĆ, PRACA, PRZERWA/ODPOCZYNEK),
 - godzina zmiany.

200 Pamięć karty kierowcy wystarcza do przechowywania danych dotyczących czynności kierowcy przez przynajmniej 28 dni (przeciętną aktywność kierowcy definiuje się jako 93 zmiany czynności dziennie).

- 201 Dane wyszczególnione w wymaganiach 197 i 199 przechowuje się w sposób umożliwiający wyszukiwanie ich w kolejności chronologicznej, nawet w przypadku nakładania się czasów.

5.2.6. *Miejsca rozpoczęcia i/lub zakończenia dziennego okresu pracy*

- 202 Karta kierowcy umożliwia przechowywanie następujących danych dotyczących miejsc rozpoczęcia i/lub zakończenia dziennego okresu pracy, wprowadzane przez kierowcę:

- data i godzina wprowadzenia danych (lub data/godzina odnosząca się do wpisu, jeżeli wpis wprowadza się w czasie procedury ręcznego wprowadzania danych),
- rodzaj wpisu (rozpoczęcie lub zakończenie, status wpisu),
- kraj i region,
- stan licznika kilometrów.

- 203 Pamięć karty kierowcy umożliwia przechowywanie przynajmniej 42 par takich zapisów.

5.2.7. *Dane dotyczące zdarzeń*

Do celów niniejszego pkt czas rejestruje się z dokładnością do jednej sekundy.

- 204 Karta kierowcy umożliwia przechowywanie następujących danych dotyczących zdarzeń wykrytych przez urządzenie rejestrujące przy włożonej karcie:

- nakładające się czasy (w przypadku gdy ta karta jest przedmiotem zdarzenia),
- włożenie karty podczas jazdy (w przypadku gdy ta karta jest przedmiotem zdarzenia),
- sesja ostatniej karty niezamknięta prawidłowo (w przypadku gdy ta karta jest przedmiotem zdarzenia),
- przerwa zasilania,
- błąd danych dotyczących ruchu,
- próba naruszenia zabezpieczeń.

- 205 Karta kierowcy umożliwia przechowywanie następujących danych dla tych zdarzeń:

- kod zdarzenia,
- data i godzina rozpoczęcia zdarzenia (lub włożenia karty, jeżeli zdarzenie trwało w tym czasie),
- data i godzina zakończenia zdarzenia (lub wyjęcia karty, jeżeli zdarzenie trwało w tym czasie),
- numer VRN i Państwo Członkowskie rejestracji pojazdu, w którym zdarzenie wystąpiło.

Uwaga: dla zdarzenia »nakładające się czasy«:

- data i godzina rozpoczęcia zdarzenia odpowiada dacie i godzinie wyjęcia karty z poprzedniego pojazdu,
- data i godzina zakończenia zdarzenia odpowiada dacie i godzinie włożenia karty w tym pojeździe,
- dane pojazdu odpowiadające bieżącemu pojazdowi powodującemu zdarzenie.

Uwaga: dla zdarzenia »sesja ostatniej karty niezamknięta prawidłowo«:

- data i godzina rozpoczęcia zdarzenia odpowiada dacie i godzinie włożenia karty dla sesji niezamkniętej prawidłowo,
- data i godzina zakończenia zdarzenia odpowiada dacie i godzinie włożenia karty dla sesji, w czasie której wykryto zdarzenie (bieżąca sesja),
- dane pojazdu odpowiadające pojazdowi, w którym sesja nie została zamknięta prawidłowo.

- 206 Karta kierowcy umożliwia przechowywanie następujących danych dotyczących sześciu ostatnich zdarzeń każdego typu (tj. 36 zdarzeń).

5.2.8. *Dane dotyczące usterek*

Do celów niniejszego pkt czas rejestruje się z dokładnością do jednej sekundy.

- 207 Karta kierowcy umożliwia przechowywanie następujących danych dotyczących usterek wykrytych przez urządzenie rejestrujące przy włożonej karcie:

- usterka karty (w przypadku gdy ta karta jest przedmiotem zdarzenia),
- usterka urządzenia rejestrującego.

- 208 Karta kierowcy umożliwia przechowywanie następujących danych dotyczących tych usterek:

- kod usterki,
- data i godzina rozpoczęcia usterki (lub włożenia karty, jeżeli usterka trwała w tym czasie),
- data i godzina zakończenia usterki (lub wyjęcia karty, jeżeli usterka trwała w tym czasie),
- numer VRN i Państwo Członkowskie rejestracji pojazdu, w którym usterka wystąpiła.

- 209 Karta kierowcy umożliwia przechowywanie następujących danych dotyczących dwunastu ostatnich usterek każdego rodzaju (tj. 24 usterki).

5.2.9. *Dane dotyczące czynności kontrolnej*

- 210 Karta kierowcy umożliwia przechowywanie następujących danych dotyczących czynności kontrolnych:

- data i godzina kontroli,
- numer karty kontrolnej i Państwo Członkowskie wydające kartę,
- rodzaj kontroli (wyświetlanie i/lub drukowanie i/lub wczytywanie danych z VU i/lub wczytywanie danych z karty — patrz uwaga),
- okres, dla którego wczytano dane, w przypadku wczytywania danych,
- numer VRN i Państwo Członkowskie rejestracji pojazdu, w którym kontrola miała miejsce.

Uwaga: zgodnie z wymaganiami bezpieczeństwa wczytywanie danych z karty jest rejestrowane wyłącznie wtedy, gdy jest wykonywane przez urządzenie rejestrujące.

- 211 Karta kierowcy umożliwia przechowywanie jednego takiego zapisu.

5.2.10. *Dane sesji karty*

- 212 Karta kierowcy umożliwia przechowywanie następujących danych dotyczących pojazdu, dla którego otwarto bieżącą sesję:

- data i godzina otwarcia sesji (tj. włożenia karty) z dokładnością do jednej sekundy,
- numer VRN i Państwo Członkowskie rejestracji.

5.2.11. *Dane dotyczące stanów szczególnych*

- 212a Karta kierowcy umożliwia przechowywanie następujących danych dotyczących stanów szczególnych wprowadzonych przy włożonej karcie (niezależnie od tego, do której szczeliny czytnika):

- data i godzina wprowadzenia danych,
- rodzaj stanu szczególnego.

- 212b Karta kierowcy umożliwia przechowywanie 56 takich zapisów.
- 5.3. **Karta warsztatowa**
- 5.3.1. *Zabezpieczenia*
- 213 Karta warsztatowa umożliwia przechowywanie osobistego numeru identyfikacyjnego (kodu PIN).
- 214 Karta warsztatowa umożliwia przechowywanie kluczy kryptograficznych potrzebnych przy parowaniu czujników ruchu z przyrządami rejestrującymi..
- 5.3.2. *Identyfikacja karty*
- 215 Karta warsztatowa umożliwia przechowywanie następujących danych identyfikujących kartę:
- numer karty,
 - wydające Państwo Członkowskie, nazwa organu wydającego, data wydania,
 - data rozpoczęcia okresu ważności karty, data ważności karty.
- 5.3.3. *Identyfikacja posiadacza karty*
- 216 Karta warsztatowa umożliwia przechowywanie następujących danych identyfikujących posiadacza karty:
- nazwa warsztatu,
 - adres warsztatu,
 - nazwisko posiadacza karty,
 - imię (imiona) posiadacza karty,
 - preferowany język.
- 5.3.4. *Dane dotyczące używanego pojazdu*
- 217 Karta warsztatowa umożliwia przechowywanie zapisów z danymi dotyczącymi używanego pojazdu, w taki sam sposób jak karta kierowcy.
- 218 Karta warsztatowa umożliwia przechowywanie przynajmniej 4 takich zapisów.
- 5.3.5. *Dane dotyczące czynności kierowcy*
- 219 Karta warsztatowa umożliwia przechowywanie danych dotyczących czynności kierowcy, w taki sam sposób jak karta kierowcy.
- 220 Karta warsztatowa umożliwia przechowywanie danych dotyczących czynności kierowcy przynajmniej za jeden dzień przeciętnej aktywności kierowcy.
- 5.3.6. *Dane dotyczące rozpoczęcia i/lub zakończenia dziennego okresu pracy*
- 221 Karta warsztatowa umożliwia przechowywanie zapisów z danymi dotyczącymi rozpoczęcia i/lub zakończenia dziennego okresu pracy, w taki sam sposób jak karta kierowcy.
- 222 Karta warsztatowa umożliwia przechowywanie przynajmniej trzech par takich zapisów.
- 5.3.7. *Dane dotyczące zdarzeń i usterek*
- 223 Karta warsztatowa umożliwia przechowywanie danych dotyczących zdarzeń i danych dotyczących zapisów usterek, w taki sam sposób jak karta kierowcy.
- 224 Karta warsztatowa umożliwia przechowywanie danych dotyczących trzech ostatnich zdarzeń każdego rodzaju (tj. 18 zdarzeń) i sześciu ostatnich usterek każdego rodzaju (tj. 12 usterek).
- 5.3.8. *Dane dotyczące czynności kontrolnej*
- 225 Karta warsztatowa umożliwia przechowywanie zapisu z danymi dotyczącymi czynności kontrolnej, w taki sam sposób jak karta kierowcy.

5.3.9. Dane dotyczące kalibracji i regulacji czasu

- 226 Karta warsztatowa umożliwia przechowywanie zapisów dotyczących kalibracji i/lub regulacji czasu wykonanych przy karcie włożonej do urządzenia rejestrującego.
- 227 Każdy zapis dotyczący kalibracji zawiera następujące dane:
- cel kalibracji (pierwsza instalacja, instalacja, przegląd okresowy),
 - identyfikacja pojazdu,
 - parametry uaktualnione lub potwierdzone (w, k, l, wielkość opon, ustawienie urządzenia ograniczenia prędkości, stan licznika kilometrów (nowe i stare wartości), data i godzina (nowe i stare wartości),
 - identyfikacja urządzenia rejestrującego (numer części VU, numer fabryczny VU, numer fabryczny czujnika ruchu).
- 228 Karta warsztatowa umożliwia przechowywanie przynajmniej 88 takich zapisów.
- 229 Karta warsztatowa jest wyposażona w licznik pokazujący łączną liczbę kalibracji wykonanych przy użyciu tej karty.
- 230 Karta warsztatowa jest wyposażona w licznik pokazujący liczbę kalibracji wykonanych od ostatniego wczytania danych.

5.3.10. Dane dotyczące stanów szczególnych

- 230a Karta warsztatowa umożliwia przechowywanie danych dotyczących odpowiednich stanów szczególnych, w taki sam sposób jak karta kierowcy. Karta warsztatowa umożliwia przechowywanie dwóch takich zapisów.

5.4. Karta kontrolna*5.4.1. Identyfikacja karty*

- 231 Karta kontrolna umożliwia przechowywanie następujących danych identyfikujących kartę:
- numer karty,
 - wydające Państwo Członkowskie, nazwa organu wydającego, data wydania,
 - data rozpoczęcia okresu ważności karty, data ważności karty, (gdy dotyczy).

5.4.2. Identyfikacja posiadacza karty

- 232 Karta kontrolna umożliwia przechowywanie następujących danych identyfikujących posiadacza karty:
- nazwa organu kontrolnego,
 - adres organu kontrolnego,
 - nazwisko posiadacza karty,
 - imię (imiona) posiadacza karty,
 - preferowany język.

5.4.3. Dane dotyczące czynności kontrolnej

- 233 Karta kontrolna umożliwia przechowywanie następujących danych dotyczących czynności kontrolnej:
- data i godzina kontroli,
 - typ kontroli (wyświetlanie i/lub drukowanie i/lub wczytywanie danych z VU i/lub wczytywanie danych z karty),

- okres, dla którego wczytano dane, (gdy dotyczy),
- numer VRN i organ Państwa Członkowskiego rejestracji kontrolowanego pojazdu,
- numer karty i Państwo Członkowskie wydające kartę kontrolowanego kierowcy.

234 Karta kontrolna umożliwia przechowywanie przynajmniej 230 takich zapisów.

5.5. **Karta firmowa**

5.5.1. *Identyfikacja karty*

235 Karta firmowa umożliwia przechowywanie następujących danych identyfikujących kartę:

- numer karty,
- wydające Państwo Członkowskie, nazwa organu wydającego, data wydania,
- data rozpoczęcia okresu ważności karty, data ważności karty, (gdy dotyczy).

5.5.2. *Identyfikacja posiadacza karty*

236 Karta firmowa umożliwia przechowywanie następujących danych identyfikujących posiadacza karty:

- nazwa firmy,
- adres firmy.

5.5.3. *Dane dotyczące czynności wykonywanych przez firmę*

237 Karta firmowa umożliwia przechowywanie następujących danych dotyczących czynności wykonywanych przez firmę:

- data i godzina czynności,
- typ czynności (blokowanie i/lub zdejmowanie blokady z VU, i/lub wczytywanie danych z VU i/lub wczytywanie danych z karty),
- okres, dla którego wczytano dane, (gdy dotyczy),
- numer VRN i Państwo Członkowskie organu rejestracji pojazdu,
- numer karty i Państwo Członkowskie wydające kartę (w przypadku wczytywania danych z karty).

238 Karta firmowa umożliwia przechowywanie przynajmniej 230 takich zapisów.

V. INSTALACJA URZĄDZENIA REJESTRUJĄCEGO

1. **Instalacja**

239 Nowe urządzenie rejestrujące dostarcza się instalatorom lub producentom pojazdów w stanie nieaktywowanym, z wszystkimi parametrami kalibracyjnymi, wyszczególnionymi w rozdziale III pkt 20, ustawionymi na odpowiednie i ważne wartości domyślne. W przypadku gdy nie ma konkretnej, odpowiedniej wartości, parametry literowe należy ustawić jako łańcuchy »?« a parametry liczbowe należy ustawić na »0«.

240 Przed aktywacją urządzenie rejestrujące umożliwia dostęp do funkcji kalibracji, nawet jeśli nie jest w trybie kalibracyjnym.

241 Przed aktywacją urządzenie rejestrujące nie może rejestrować ani przechowywać danych, o których mowa w rozdziale III w pkt 12.3.-12.9. i 12.12-12.14.

242 W czasie instalacji producenci pojazdów wstępnie ustawiają wszystkie znane parametry.

- 243 Producenci pojazdów lub instalatorzy aktywują zainstalowane urządzenie rejestrujące zanim pojazd opuści obiekt, w którym ma miejsce instalacja.
- 244 Aktywacja urządzenia rejestrującego uruchamiana jest automatycznie przez pierwsze włożenie karty warsztatowej do któregośkolwiek czytnika karty.
- 245 Szczególne czynności parujące, wymagane między czujnikiem ruchu a przyrządem rejestrującym, gdy konieczne, odbywają się automatycznie przed lub w czasie aktywacji.
- 246 Po aktywowaniu urządzenia rejestrującego wszystkie funkcje i prawa dostępu do danych są w pełni wdrożone.
- 247 Po aktywowaniu urządzenia rejestrującego wszystkie funkcje rejestrowania i przechowywania są w pełni funkcjonalne.
- 248 Następnym krokiem po instalacji jest kalibracja. W czasie pierwszej kalibracji między innymi wprowadza się numer VRN, a samą kalibrację wykonuje w terminie 2 tygodni od obecnej instalacji lub przypisania numeru VRN, w zależności od tego, która z tych czynności następuje później.
- 248a Urządzenie rejestrujące musi być umieszczone w pojeździe w taki sposób, aby kierowca miał ze swojego siedzenia dostęp do wszystkich, niezbędnych funkcji.

2. Tabliczka instalacyjna

- 249 Po zainstalowaniu i sprawdzeniu urządzenia rejestrującego mocuje się obok lub na urządzeniu rejestrującym tabliczkę pomiarową. Tabliczka jest łatwa do odczytania i łatwo dostępna. Po każdej inspekcji przeprowadzonej przez uprawnionego instalatora lub warsztat w miejsce starej mocuje się nową tabliczkę.
- 250 Tabliczka zawiera przynajmniej następujące dane:
- nazwa, adres lub firma uprawnionego instalatora lub warsztatu,
 - współczynnik charakterystyczny pojazdu, w postaci »w =...imp/km«,
 - stała urządzenia rejestrującego, w postaci »k =... imp/km«,
 - skuteczny obwód opon w postaci »l =... mm«,
 - rozmiar opon,
 - data ustalenia współczynnika charakterystycznego pojazdu i pomiaru skutecznego obwodu opon,
 - numer identyfikacyjny pojazdu.

3. Plombowanie

- 251 Następujące części są zaplombowane:
- wszelkie połączenia, których rozłączenie może powodować niewykrywalne zmiany danych lub niewykrywalne utraty danych,
 - tabliczka instalacyjna, dopóki nie jest przymocowana w taki sposób, że nie można jej usunąć bez uszkodzenia wykonanych na niej oznaczeń.
- 252 Plomby, o których mowa powyżej mogą być zdjęte:
- w przypadkach nagłej konieczności,
 - w celu zainstalowania, wyregulowania lub naprawy urządzenia ograniczenia prędkości lub innego urządzenia istotnego dla bezpieczeństwa drogowego, z zastrzeżeniem, że urządzenie rejestrujące nadal pracuje niezawodnie i prawidłowo i zostanie powtórnie zaplombowane przez uprawnionego instalatora lub warsztat (zgodnie z rozdziałem VI) niezwłocznie po zainstalowaniu urządzenia ograniczenia prędkości lub innego urządzenia istotnego dla bezpieczeństwa drogowego lub w terminie siedmiu dni w pozostałych przypadkach.

- 253 Każdy przypadek zniszczenia takiej plomby wymaga sporządzenia pisemnego oświadczenia podającego powody takiego działania, a oświadczenie to udostępniane jest właściwemu organowi.

VI. SPRAWDZENIA, INSPEKCJE I NAPRAWY

Wymagania odnośnie do okoliczności, w jakich można zdjąć plomby, określone w art. 12 ust. 5 rozporządzenia (EWG) nr 3821/85, ostatnio zmienionego rozporządzeniem (WE) nr 2135/98, definiuje rozdział V pkt 3 niniejszego załącznika.

1. Zatwierdzanie instalatorów lub warsztatów

Państwa Członkowskie zatwierdzają, regularnie kontrolują i certyfikują instytucje odpowiadające za:

- instalacje,
- sprawdzenia,
- inspekcje,
- naprawy.

Zgodnie z art. 12 ust. 1 niniejszego rozporządzenia karty warsztatowe wydaje się wyłącznie instalatorom i/lub warsztatom zatwierdzonym do aktywowania i/lub kalibrowania urządzenia rejestrującego zgodnie z niniejszym załącznikiem i, chyba że istnieją inne należyte uzasadnienia:

- którzy nie kwalifikują się do posiadania karty firmowej,
- i których inna działalność zawodowa nie stanowi potencjalnego zagrożenia dla ogólnego bezpieczeństwa systemu, zdefiniowanego w dodatku 10.

2. Kontrola techniczna przyrządów nowych i po naprawie

- 254 Każdy przyrząd, tak nowy jak i po naprawie, jest kontrolowany pod względem prawidłowego funkcjonowania oraz dokładności odczytów i rejestracji, w granicach ustanowionych w rozdziale III pkt 2.1. i 2.2, i otrzymuje plomby zgodnie z pkt 3 rozdział V oraz jest kalibrowany.

3. Kontrola techniczna po instalacji

- 255 Po zainstalowaniu w pojeździe cała instalacja (włącznie z urządzeniem rejestrującym) jest zgodna z przepisami dotyczącymi maksymalnych tolerancji ustanowionymi w rozdziale III pkt 2.1 i 2.2.

4. Przeglądy okresowe

- 256 Przeglądy okresowe urządzeń zainstalowanych w pojazdach przeprowadza się po każdej naprawie urządzenia, lub po jakiegokolwiek zmianie współczynnika charakterystycznego pojazdu lub skutecznego obwodu tocznego opon, lub gdy czas UTC urządzenia różni się od czasu UTC o więcej niż 20 minut, lub przy zmianie numeru VRN i przynajmniej raz w okresie dwóch lat (24 miesięcy) od ostatniej kontroli.

- 257 Przeglądy okresowe obejmują następujące kontrole:

- czy urządzenie rejestrujące działa prawidłowo, włącznie z funkcją gromadzenia danych na kartach do tachografów,
- czy jest zachowana zgodność z wymaganiami rozdziału III pkt 2.1 i 2.2 co do maksymalnych tolerancji przy instalacji,
- czy urządzenie rejestrujące opatrzone jest znakiem homologacji typu,
- czy zamocowana jest tabliczka instalacyjna,
- czy plomby na urządzeniu i na innych częściach instalacji są nienaruszone,
- sprawdzenie rozmiaru opon i wyznaczenie faktycznego obwodu tocznego kół.

258 W ramach przeglądu okresowego wykonuje się kalibrację.

5. Pomiar błędów

259 Pomiar błędów po zainstalowaniu i podczas użytkowania jest dokonywany w następujących warunkach, które stanowią normalne warunki badań:

- pojazd bez ładunku w normalnym stanie gotowym do jazdy,
- ciśnienie w ogumieniu zgodne z instrukcjami producenta,
- zużycie ogumienia w granicach dopuszczalnych przepisami,
- przemieszczanie pojazdu:
 - pojazd poruszać się napędzany własnym silnikiem, po linii prostej i po poziomej powierzchni, z prędkością 50 ± 5 km/h. Odległość pomiarowa wynosi przynajmniej 1 000 m,
- sprawdzenie może być również przeprowadzone inną metodą, np. na stanowisku warsztatowym, pod warunkiem, że zapewni ono porównywalną dokładność.

6. Naprawy

260 Warsztaty mogą wczytywać dane z urządzenia rejestrującego w celu przekazania tych danych odpowiedniej firmie przewozowej.

261 Uprawnione warsztaty wydają firmom przewozowym zaświadczenie o niemożliwości wczytania danych, w przypadku gdy uszkodzenie urządzenia rejestrującego uniemożliwia wczytanie zarejestrowanych danych nawet po naprawie w tym warsztacie. Warsztaty przechowują kopię każdego wydanego zaświadczenia przez okres przynajmniej jednego roku.

VII. WYDAWANIE KART

Procedury wydawania kart ustanowione przez Państwa Członkowskie spełniają następujące wymagania:

- 262 Pierwsza karta do tachografów wydana wnioskodawcy ma numer karty równy numerowi kolejnemu, (gdy dotyczy) a numer zastąpienia i numer odświeżenia ustawione na »0«.
- 263 Numery karty wszystkich nieosobistych kart do tachografów wydanych jednemu organowi kontrolnemu lub jednemu warsztatowi lub jednej firmie przewozowej mają te same pierwsze 13 cyfr i wszystkie mają różny numer kolejny.
- 264 Karta do tachografów wydana jako duplikat istniejącej karty do tachografów ma ten sam numer karty, co karta zastąpiona, z wyjątkiem numeru zastąpienia, który jest zwiększony o »1« (w kolejności 0,..., 9, A,..., Z).
- 265 Karta do tachografów wydana jako duplikat istniejącej karty do tachografów ma tę samą datę ważności karty co karta zastąpiona.
- 266 Karta do tachografów wydana jako odświeżenie istniejącej karty do tachografów ma ten sam numer karty, co karta odświeżona, z wyjątkiem numeru zastąpienia, który jest ustawiony na »0« i numeru odświeżenia, który jest zwiększony o »1« (w kolejności 0,..., 9, A,..., Z).
- 267 Przy wymianie istniejącej karty do tachografów, w celu zmiany danych administracyjnych, stosuje się te same zasady jak przy odświeżeniu, gdy jest wykonywana w tym samym Państwie Członkowskim lub zasady jak przy pierwszym wydaniu, gdy wykonywana jest przez inne Państwo Członkowskie.
- 268 W przypadku nieosobistych kart warsztatowych lub kontrolnych w rubryce »nazwisko posiadacza karty« wstawia się nazwę warsztatu lub organu kontrolnego.

VIII. HOMOLOGACJA TYPU DLA URZĄDZENIA REJESTRUJĄCEGO I KART DO TACHOGRAFÓW

1. Uwagi ogólne

Do celów niniejszego rozdziału wyrażenie »urządzenie rejestrujące« oznacza »urządzenie rejestrujące lub jego części składowe«. Homologacji typu nie wymaga się dla przewodu(-ów) łączącego czujnik ruchu z VU. Papier używany przez urządzenie rejestrujące uważa się za część składową urządzenia rejestrującego.

- 269 Urządzenie rejestrujące dostarcza się do homologacji w stanie kompletnym z wszystkimi zintegrowanymi urządzeniami dodatkowymi.
- 270 Homologacja typu urządzenia rejestrującego i kart do tachografów obejmuje badania związane z bezpieczeństwem, badania funkcjonalności i badania interoperacyjności. Pozytywne wyniki każdego z tych badań potwierdza się odpowiednim świadectwem.
- 271 Organy Państw Członkowskich właściwe dla homologacji typu nie wydają świadectwa homologacji typu zgodnie z art. 5 niniejszego rozporządzenia, dopóki nie mają:
- świadectwa bezpieczeństwa,
 - świadectwa funkcjonalności,
 - i świadectwa interoperacyjności
- dla urządzenia rejestrującego lub kart do tachografów, dla których złożono wnioski o homologację typu.
- 272 O wszelkich modyfikacjach oprogramowania lub sprzętu urządzenia lub charakteru materiałów użytych do wytworzenia urządzenia należy, przed zastosowaniem, zawiadomić organ, który wydał homologację typu dla urządzenia. Organ ten potwierdza producentowi rozszerzenie homologacji typu, lub też może zażądać uaktualnienia lub potwierdzenia stosownych świadectw funkcjonalności, bezpieczeństwa i/lub interoperacyjności.
- 273 Procedury aktualizacji oprogramowania w prawidłowo funkcjonującym urządzeniu rejestrującym zatwierdza organ, który wydał homologację typu dla tego urządzenia rejestrującego. Aktualizacja oprogramowania nie może zmienić ani usunąć żadnych danych dotyczących czynności kierowcy zgromadzonych w pamięci urządzenia rejestrującego. Oprogramowanie można aktualizować wyłącznie na odpowiedzialność producenta urządzenia.

2. Świadectwo bezpieczeństwa

- 274 Świadectwo bezpieczeństwa wydaje się zgodnie z przepisami dodatku 10 do niniejszego Załącznika.

3. Świadectwo funkcjonalności

- 275 Każdy ubiegający się o homologację typu dostarcza organowi Państwa Członkowskiego właściwemu dla homologacji typu wszelkie materiały i dokumentację, jakie organ ten uzna za niezbędne.
- 276 Świadectwo funkcjonalności wydaje się producentowi wyłącznie po pozytywnym przejściu przynajmniej przez wszystkie badania funkcjonalności wyszczególnione w dodatku 9.
- 277 Organ właściwy dla homologacji typu wydaje świadectwo funkcjonalności. W świadectwie tym podaje się, oprócz nazwy (nazwiska) otrzymującego świadectwo i identyfikacji modelu, szczegółowy wykaz wykonanych badań i uzyskanych wyników.

4. Świadectwo interoperacyjności

- 278 Badania interoperacyjności przeprowadza jedno laboratorium na mocy homologacji i na odpowiedzialność Komisji Europejskiej..
- 279 Laboratorium rejestruje wnioski o badania interoperacyjności złożone przez producentów w kolejności chronologicznej napływu tych wniosków.
- 280 Wnioski rejestruje się oficjalnie tylko wtedy, gdy w posiadaniu laboratorium znajdują się:
- komplet materiałów i dokumentów niezbędnych do takich badań interoperacyjności,
 - odpowiednie świadectwo bezpieczeństwa,
 - odpowiednie świadectwo funkcjonalności.
- Producenta zawiadamia się o dacie rejestracji wniosku.
- 281 Laboratorium nie przeprowadza żadnych badań interoperacyjności urządzenia rejestrującego ani karty do tachografów, które nie uzyskały świadectwa bezpieczeństwa i świadectwa funkcjonalności.
- 282 Producent wnioskujący o przeprowadzenie badań interoperacyjności zobowiązuje się do pozostawienia w laboratorium, które ma przeprowadzić te badania, kompletu materiałów i dokumentów, które dostarczył do przeprowadzenia tych badań.

Badania interoperacyjności przeprowadza się, zgodnie z przepisami pkt 5 dodatku 9 do niniejszego Załącznika, dla, odpowiednio, wszystkich typów urządzenia rejestrującego lub kart do tachografów:

- które mają jeszcze ważną homologację typu, lub
- których homologacja typu jest w toku załatwiania i które mają ważne świadectwo interoperacyjności.

284 Laboratorium wydaje producentowi świadectwo interoperacyjności tylko wtedy, gdy objęte nim urządzenia pomyślnie przejdą wszystkie wymagane badania interoperacyjności.

285 Jeżeli jedno lub więcej urządzenie rejestrujące lub karta do tachografów nie przejdzie pomyślnie badań interoperacyjności, zgodnie z wymaganiami 283, świadectwa interoperacyjności nie wydaje się dopóki wnioskujący producent nie wprowadzi niezbędnych poprawek i dopóki nie przejdą one pomyślnie przez badania interoperacyjności. Laboratorium, przy pomocy zainteresowanych producentów, rozpoznaje przyczynę problemu interoperacyjności i dokłada starań, by pomóc wnioskującemu producentowi w znalezieniu rozwiązania technicznego. W przypadku gdy producent modyfikuje swój produkt, to producent odpowiada za uzyskanie potwierdzenia właściwych organów, że świadectwo bezpieczeństwa i świadectwo funkcjonalności nadal zachowują ważność.

286 Świadectwo interoperacyjności ważne jest przez sześć miesięcy. Zostaje ono odwołane na koniec tego okresu, jeżeli producent nie uzyska odpowiadającego mu świadectwa homologacji typu. Producent przekazuje to świadectwo organowi właściwemu dla homologacji typu Państwa Członkowskiego, który wydał świadectwo funkcjonalności.

287 Żaden element, który może być źródłem usterki interoperacyjności, nie może być użyty do osiągnięcia korzyści z pozycji dominującej ani prowadzić do uzyskania takiej pozycji.

5. Świadectwo homologacji typu

288 Organ Państwa Członkowskiego, właściwy dla homologacji typu, może wydać świadectwo homologacji typu, gdy tylko posiada trzy wymagane świadectwa.

289 Organ właściwy dla homologacji typu przekazuje kopię świadectwa homologacji typu do laboratorium właściwego do przeprowadzenia badań interoperacyjności, w czasie dostarczania tego świadectwa producentowi.

290 Laboratorium właściwe do przeprowadzenia badań interoperacyjności prowadzi publiczną stronę internetową, na której znajduje się uaktualniony wykaz modeli urządzeń rejestrujących lub kart do tachografów:

- dla których zarejestrowano wnioski o badania interoperacyjności,
- które uzyskały świadectwo interoperacyjności (nawet czasowe),
- które uzyskały świadectwo homologacji typu.

6. Procedura szczegółna: pierwsze świadectwa interoperacyjności

291 Przez cztery miesiące od czasu, gdy pierwsza para urządzenie rejestrujące i karty do tachografów (karty kierowcy, warsztatowe, kontrolne i firmowe) uzyska świadectwa interoperacyjności, wszelkie wydane świadectwa interoperacyjności (włącznie z tym pierwszym), w związku z wnioskami zarejestrowanymi w tym okresie, uważa się za czasowe.

292 Jeżeli na koniec tego okresu wszystkie produkty, których to dotyczy, współdziałają, wszystkie odpowiednie świadectwa interoperacyjności zastępuje się świadectwem ostatecznym.

293 Jeżeli w tym okresie wykryje się usterki interoperacyjności, laboratorium właściwe do przeprowadzenia badań interoperacyjności rozpoznaje przyczyny problemów z pomocą wszystkich zainteresowanych producentów i zachęca ich do wprowadzenia niezbędnych poprawek.

294 Jeżeli na koniec tego okresu nadal występują problemy interoperacyjności, laboratorium właściwe do przeprowadzenia badań interoperacyjności, we współpracy z zainteresowanymi producentami i organami właściwymi do homologacji typu, która wydała odpowiednie świadectwo funkcjonalności, szuka przyczyn usterek interoperacyjności i ustala, jakie poprawki wprowadza każdy z zainteresowanych producentów. Poszukiwanie rozwiązań technicznych trwa maksymalnie dwa miesiące, po których, jeśli nie zostanie znalezione wspólne rozwiązanie, Komisja, po konsultacji z laboratorium właściwym do przeprowadzenia badań interoperacyjności decyduje, które urządzenie(-a) i karty otrzymują ostateczne świadectwa interoperacyjności wraz z uzasadnieniem swojej decyzji.

295 Wszelkie wnioski o przeprowadzenie badań interoperacyjności, zarejestrowane przez laboratorium w okresie między końcem czteromiesięcznego okresu po dostarczeniu pierwszego czasowego świadectwa interoperacyjności a datą decyzji Komisji, określonej w wymaganii 294, są odraczane, aż do rozwiązania początkowych problemów interoperacyjności. Następnie wnioski te załatwia się w kolejności chronologicznej rejestracji.

Dodatek 1

SŁOWNIK DANYCH

SPIS TREŚCI

1.	Wprowadzenie	332
1.1.	Podjęcie do definicji typów danych	332
1.2.	Odesłania	332
2.	Definicje typu danych	333
2.1.	ActivityChangeInfo	333
2.2.	Address	334
2.3.	BCDString	334
2.4.	CalibrationPurpose	334
2.5.	CardActivityDailyRecord	335
2.6.	CardActivityLengthRange	335
2.7.	CardApprovalNumber	335
2.8.	CardCertificate	335
2.9.	CardChipIdentification	335
2.10.	CardConsecutiveIndex	336
2.11.	CardControlActivityDataRecord	336
2.12.	CardCurrentUse	336
2.13.	CardDriverActivity	336
2.14.	CardDrivingLicenceInformation	337
2.15.	CardEventData	337
2.16.	CardEventRecord	337
2.17.	CardFaultData	338
2.18.	CardFaultRecord	338
2.19.	CardIccIdentification	338
2.20.	CardIdentification	339
2.21.	CardNumber	339
2.22.	CardPlaceDailyWorkPeriod	339
2.23.	CardPrivateKey	340
2.24.	CardPublicKey	340
2.25.	CardRenewalIndex	340
2.26.	CardReplacementIndex	340
2.27.	CardSlotNumber	340
2.28.	CardSlotsStatus	340
2.29.	CardStructureVersion	341

2.30.	CardVehicleRecord	341
2.31.	CardVehiclesUsed	341
2.32.	Certificate	342
2.33.	CertificateContent	342
2.34.	CertificateHolderAuthorisation	342
2.35.	CertificateRequestID	343
2.36.	CertificationAuthorityKID	343
2.37.	CompanyActivityData	343
2.38.	CompanyActivityType	344
2.39.	CompanyCardApplicationIdentification	344
2.40.	CompanyCardHolderIdentification	344
2.41.	ControlCardApplicationIdentification	345
2.42.	ControlCardControlActivityData	345
2.43.	ControlCardHolderIdentification	345
2.44.	ControlType	346
2.45.	CurrentDateTime	346
2.46.	DailyPresenceCounter	346
2.47.	Datef	347
2.48.	Distance	347
2.49.	DriverCardApplicationIdentification	347
2.50.	DriverCardHolderIdentification	347
2.51.	EntryTypeDailyWorkPeriod	348
2.52.	EquipmentType	348
2.53.	EuropeanPublicKey	348
2.54.	EventFaultType	348
2.55.	EventFaultRecordPurpose	349
2.56.	ExtendedSerialNumber	350
2.57.	FullCardNumber	350
2.58.	HighResOdometer	350
2.59.	HighResTripDistance	350
2.60.	HolderName	350
2.61.	K-ConstantOfRecordingEquipment	351
2.62.	KeyIdentifier	351
2.63.	L-TyreCircumference	351
2.64.	Language	351
2.65.	LastCardDownload	351
2.66.	ManualInputFlag	351
2.67.	ManufacturerCode	352

2.68.	MemberStateCertificate	352
2.69.	MemberStatePublicKey	353
2.70.	Name	353
2.71.	NationAlpha	353
2.72.	NationNumeric	354
2.73.	NoOfCalibrationRecords	355
2.74.	NoOfCalibrationSinceDownload	355
2.75.	NoOfCardPlaceRecords	355
2.76.	NoOfCardVehicleRecords	355
2.77.	NoOfCompanyActivityRecords	355
2.78.	NoOfControlActivityRecords	356
2.79.	NoOfEventsPerType	356
2.80.	NoOfFaultsPerType	356
2.81.	OdometerValueMidnight	356
2.82.	OdometerShort	356
2.83.	OverspeedNumber	356
2.84.	PlaceRecord	356
2.85.	PreviousVehicleInfo	357
2.86.	PublicKey	357
2.87.	RegionAlpha	357
2.88.	RegionNumeric	357
2.89.	RSAPublicModulus	358
2.90.	RSAPublicExponent	358
2.91.	RSAPrivateExponent	358
2.92.	SensorApprovalNumber	358
2.93.	SensorIdentification	358
2.94.	SensorInstallation	359
2.95.	SensorInstallationSecData	359
2.96.	SensorOSIdentifier	359
2.97.	SensorPaired	359
2.98.	SensorPairingDate	360
2.99.	SensorSerialNumber	360
2.100.	SensorSCIdentifier	360
2.101.	Signature	360
2.102.	SimilarEventsNumber	360
2.103.	SpecificConditionType	360
2.104.	SpecificConditionRecord	360
2.105.	Speed	361

2.106.	SpeedAuthorised	361
2.107.	SpeedAverage	361
2.108.	SpeedMax	361
2.109.	TdesSessionKey	361
2.110.	TimeReal	361
2.111.	TyreSize	361
2.112.	VehicleIdentificationNumber	362
2.113.	VehicleRegistrationIdentification	362
2.114.	VehicleRegistrationNumber	362
2.115.	VuActivityDailyData	362
2.116.	VuApprovalNumber	362
2.117.	VuCalibrationData	362
2.118.	VuCalibrationRecord	363
2.119.	VuCardIWDData	363
2.120.	VuCardIWRRecord	364
2.121.	VuCertificate	364
2.122.	VuCompanyLocksData	364
2.123.	VuCompanyLocksRecord	365
2.124.	VuControlActivityData	365
2.125.	VuControlActivityRecord	365
2.126.	VuDataBlockCounter	365
2.127.	VuDetailedSpeedBlock	365
2.128.	VuDetailedSpeedData	366
2.129.	VuDownloadablePeriod	366
2.130.	VuDownloadActivityData	366
2.131.	VuEventData	366
2.132.	VuEventRecord	367
2.133.	VuFaultData	367
2.134.	VuFaultRecord	367
2.135.	VuIdentification	368
2.136.	VuManufacturerAddress	368
2.137.	VuManufacturerName	368
2.138.	VuManufacturingDate	368
2.139.	VuOverSpeedingControlData	369
2.140.	VuOverSpeedingEventData	369
2.141.	VuOverSpeedingEventRecord	369
2.142.	VuPartNumber	369
2.143.	VuPlaceDailyWorkPeriodData	370

2.144.	VuPlaceDailyWorkPeriodRecord	370
2.145.	VuPrivateKey	370
2.146.	VuPublicKey	370
2.147.	VuSerialNumber	370
2.148.	VuSoftInstallationDate	370
2.149.	VuSoftwareIdentification	370
2.150.	VuSoftwareVersion	371
2.151.	VuSpecificConditionData	371
2.152.	VuTimeAdjustmentData	371
2.153.	VuTimeAdjustmentRecord	371
2.154.	W-VehicleCharacteristicConstant	371
2.155.	WorkshopCardApplicationIdentification	372
2.156.	WorkshopCardCalibrationData	372
2.157.	WorkshopCardCalibrationRecord	372
2.158.	WorkshopCardHolderIdentification	373
2.159.	WorkshopCardPIN	373
3.	Definicje wartości i zakresu wielkości	374
3.1.	Definicje dla karty kierowcy:	374
3.2.	Definicje dla karty warsztatowej:	374
3.3.	Definicje dla karty kontrolnej:	374
3.4.	Definicje dla karty firmowej:	374
4.	Zestawy znaków	374
5.	Kodowanie	374

1. WPROWADZENIE

Niniejszy dodatek określa formaty danych, elementy danych i struktury danych przeznaczone do wykorzystania w urządzeniach rejestrujących i kartach do tachografów.

1.1. Podejście do definicji typów danych

W niniejszym dodatku do definiowania typów danych użyto zapisu składni abstrakcyjnej 1 (ASN.1). Pozwala to na definiowanie prostych i strukturalnych danych bez narzucania żadnej swoistej składni przesyłania danych (reguł kodowania), która zależy od aplikacji i środowiska.

Konwencje nazewnictwa typu ASN.1 opracowano zgodnie z normą ISO/IEC 8824-1. Wymaga to, aby:

- tam gdzie możliwe wybrane nazwy opisywały znaczenie typu,
- tam gdzie typ danych zbudowany jest z innych typów danych nazwa typu danych ma postać pojedynczego ciągu znaków alfanumerycznych zaczynającego się od dużej litery, natomiast duże litery wewnątrz nazwy opisują odpowiednio znaczenia,
- ogólnie nazwy typów danych powiązane są z nazwami typów danych, z których są zbudowane, urządzeniem, w którym są zgromadzone i funkcją z nimi związaną.

Jeżeli typ ASN.1 jest już zdefiniowany jako część innej normy i jeżeli jest to stosowne do zastosowania w urządzeniu rejestrującym, to ten typ ASN.1 jest zdefiniowany w niniejszym dodatku.

Aby umożliwić stosowanie kilku reguł kodowania, niektóre typy ASN.1 w niniejszym dodatku są ograniczone identyfikatorami zakresu wartości. Identyfikatory zakresu wartości są zdefiniowane w pkt. 3.

1.2. Odesłania

Gdy użyte w niniejszym dodatku poniższe odesłania odnoszą się do opisanych przy nich dokumentów:

ISO 639	Kod reprezentacji nazw języków. Wydanie pierwsze: 1988 r.
EN 726-3	Identyfikacja systemów kart — telekomunikacyjne karty z układami scalonymi i terminale — część 3: Wymagania dla kart niezależnych od aplikacji. Grudzień 1994 r.
ISO 3779	Pojazdy drogowe — Numer identyfikacyjny pojazdu (VIN) — zawartość i struktura. Wydanie 3: 1983 r.
ISO/IEC 7816-5	Informatyka — Identyfikacja kart — karty z układami scalonymi ze stykami — część 5: Przydział numerów i kodów oraz procedura rejestracji dla identyfikatorów aplikacji. Wydanie pierwsze: 1994 r. + Nowelizacja 1: 1996 r.
ISO/IEC 8824-1	Informatyka — Zapis składni abstrakcyjnej 1 (ASN.1): Specyfikacja notacji podstawowej. Wydanie 2: 1998 r.
ISO/IEC 8825-2	Informatyka — Reguły kodowania ASN.1: Specyfikacja reguł upakowanego kodowania (PER). Wydanie 2: 1998 r.
ISO/IEC 8859-1	Informatyka — 8-bitowe jednobajtowe zestawy znaków graficznych — część 1: Zestaw łański 1. Wydanie pierwsze: 1998 r.
ISO/IEC 8859-7	Informatyka — 8-bitowe jednobajtowe zestawy znaków graficznych — część 7: alfabet łański/grecki. Wydanie pierwsze: 1987 r.
ISO 16844-3	Pojazdy drogowe — Systemy tachograficzne — interfejs czujnika ruchu. WD 3-20/05/99.

'aa'B Czynność (nieistotne, gdy »p« = 1 i »c« = 0 z wyjątkiem jak w uwadze poniżej):

'00'B: PRZERWA/ODPOCZYNEK,

'01'B: DYSPOZYCYJNOŚĆ,

'10'B: PRACA,

'11'B: PROWADZENIE,

'ttttttttttt'B Godzina zmiany: liczba minut od godziny 00:00 w danym dniu.

Uwaga dla przypadku »wyjęcie karty«:

Gdy karta jest wyjęta:

- »s« odnosi się i wskazuje szczylinę czytnika, z której wyjęta jest karta,
- »c« musi być ustawiony na 0,
- »p« musi być ustawiony na 1,
- »aa« musi kodować bieżącą czynność wybraną w tym czasie,

W wyniku ręcznego wprowadzenia danych bity »c« i »aa« wyrażenia (zapisanego na karcie) mogą być nadpisane później w celu odzwierciedlania zapisu.

2.2. Address

Adres.

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

codePage określa część strony kodowej ISO/IEC 8859 użytej do kodowania adresu,

address jest adresem zakodowanym zgodnie ze stroną kodową ISO/IEC 8859.

2.3. BCDString

BCDString jest stosowany do reprezentacji liczb w zapisie dziesiętnym kodowanym dwójkowo (BCD). Tego typu danych używa się do przedstawiania jednej cyfry dziesiętnej w półoktecie (4 bity). BCDString oparty jest na definicji z normy ISO/IEC 8824-1 »CharacterStringType«.

```
BCDString ::= CHARACTER STRING (ze składnikami {
    identification (ze składnikami {
        fixed PRESENT }) })
```

BCDString używa notacji »hstring«. Skrajna lewa cyfra heksadecymalna jest najbardziej znaczącym półoktetem pierwszego oktetu. Aby utworzyć wielokrotne oktety, wstawia się, gdy trzeba, zerowe półoktety o lewej skrajnej pozycji półoktetu w pierwszym okciecie.

Dozwolonymi cyframi są: 0, 1,... 9.

2.4. CalibrationPurpose

Kod wyjaśniający, dlaczego zarejestrowano zbiór parametrów kalibracyjnych. Ten typ danych związany jest z wymaganiami 097 i 098.

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

Przypisanie wartości:

'00'H wartość zastrzeżona,

'01'H aktywacja: zapis parametrów kalibracyjnych znanych w momencie aktywacji VU,

'02'H pierwsza instalacja: pierwsza kalibracja VU po aktywacji,

'03'H instalacja: pierwsza kalibracja VU w bieżącym pojeździe,

'04'H przegląd okresowy.

2.5. CardActivityDailyRecord

Informacje, zapisane na karcie, dotyczące czynności kierowcy w danym dniu kalendarzowym. Ten typ danych związany jest z wymaganiami 199 i 219.

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

ActivityPreviousRecordLength jest całkowitą długością w bajtach poprzedniego zapisu dziennego. Maksymalną wartość określa długość OCTET STRING zawierającego te zapisy (patrz pkt 3 CardActivityLengthRange). Gdy zapis ten jest najstarszym zapisem dziennym, wartość activityPreviousRecordLength musi być ustawiona na 0.

ActivityRecordLength jest całkowitą długością tego zapisu w bajtach. Maksymalną wartość określa długość OCTET STRING zawierającego te zapisy.

ActivityRecordDate jest datą zapisu.

ActivityDailyPresenceCounter jest licznikiem obecności dla karty w tym dniu.

ActivityDayDistance jest całkowitą drogą przebytą w tym dniu.

ActivityChangeInfo jest zbiorem danych ActivityChangeInfo dla kierowcy w tym dniu. Może zawierać maksymalnie 1 440 wartości (jedna zmiana czynności na minutę). W tym zbiorze danych zawsze znajduje się activityChangeInfo określający status kierowcy o godzinie 00:00.

2.6. CardActivityLengthRange

Liczba bajtów na karcie kierowcy lub warsztatowej, dostępnych do przechowywania zapisów z czynnościami kierowcy.

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

Przypisanie wartości: patrz ust. 3.

2.7. CardApprovalNumber

Numer homologacji typu karty.

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

Przypisanie wartości: nieokreślona.

2.8. CardCertificate

Certyfikat klucza publicznego karty.

```
CardCertificate ::= Certificate.
```

2.9. CardChipIdentification

Informacje, zapisane na karcie, dotyczące identyfikacji układu scalonego karty (IC) (wymóg 191).

```
CardChipIdentification ::= SEQUENCE {
    IcSerialNumber                OCTET STRING (SIZE(4)),
    IcManufacturingReferences      OCTET STRING (SIZE(4))
}
```


ActivityPointerOldestDayRecord jest wskaźnikiem początku miejsca gromadzenia danych (liczba bajtów od początku łańcucha znaków) najstarszego, pełnego zapisu dziennego w łańcuchu activityDailyRecords. Maksymalna wartość jest określona długością łańcucha.

ActivityPointerNewestRecord jest wskaźnikiem początku miejsca gromadzenia danych (liczba bajtów od początku łańcucha znaków) najświeższego zapisu dziennego w łańcuchu activityDailyRecords. Maksymalna wartość jest określona długością łańcucha.

ActivityDailyRecords jest przestrzenią dostępną do przechowywania danych dotyczących czynności kierowcy (struktura danych: CardActivityDailyRecord) dla każdego dnia kalendarzowego, w którym karta jest użyta.

Przypisanie wartości: ten OCTET STRING jest cyklicznie wypełniany zapisami CardActivityDailyRecord. Przy pierwszym użyciu gromadzenie rozpoczyna się od pierwszego bajtu łańcucha. Wszystkie nowe zapisy dołącza się do końca poprzedniego rekordu. Gdy łańcuch zostaje zapełniony wypełnianie rozpoczyna się od pierwszego bajtu łańcucha niezależnie od przerwy w elemencie danych. Przed wstawieniem do łańcucha danych o nowej czynności (zwiększenie bieżącego rekordu activityDailyRecord lub wstawienie nowego rekordu activityDailyRecord), który zamienia stare dane o starej czynności, wskaźnik activityPointerOldestDayRecord musi być uaktualniony w celu odzwierciedlenia nowego położenia najstarszego, pełnego zapisu dziennego a długość activityPreviousRecordLength tego (nowego) najstarszego, pełnego zapisu dziennego musi być wyzerowana.

2.14. CardDrivingLicenceInformation

Informacje przechowywane na karcie kierowcy dotyczące posiadacza karty prawa jazdy kierowcy (wymaganie 196).

```
CardDrivingLicenceInformation ::= SEQUENCE {
    DrivingLicenceIssuingAuthority      Nazwisko,
    DrivingLicenceIssuingNation         NationNumeric,
    DrivingLicenceNumber                IA5String(SIZE(16))
}
```

Driving Licence Issuing Authority jest organem, który wydał prawo jazdy.

Driving Licence Issuing Nation jest przynależnością państwową organu, który wydał prawo jazdy.

DrivingLicenceNumber jest numerem prawa jazdy.

2.15. CardEventData

Informacje przechowywane na karcie kierowcy lub warsztatowej dotyczące zdarzeń związanych z posiadaczem karty (wymaganie 204 i 223).

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

CardEventData jest sekwencją uporządkowaną w kolejności rosnącej typu EventFaultType, w zapisach cardEventRecords (z wyjątkiem zapisów związanych z próbami naruszenia zabezpieczeń, które gromadzone są w ostatnim zbiorze sekwencji).

CardEventRecords jest zbiorem zapisów ze zdarzeniami dla danego typu zdarzenia (lub kategorii prób naruszeń zabezpieczenia).

2.16. CardEventRecord

Informacje przechowywane na karcie kierowcy lub warsztatowej dotyczące zdarzenia związanego z posiadaczem karty (wymaganie 205 i 223).

```
CardEventRecord ::= SEQUENCE {
    EventType                EventFaultType,
    EventBeginTime           TimeReal,
    EventEndTime             TimeReal,
    EventVehicleRegistration VehicleRegistrationIdentification
}
```

EventType jest typem zdarzenia.

EventBeginTime jest datą i godziną rozpoczęcia zdarzenia.

EventEndTime jest datą i godziną zakończenia zdarzenia.

EventVehicleRegistration jest numerem VRN i Państwa Członkowskiego rejestracji pojazdu, w którym zdarzenie miało miejsce.

2.17. CardFaultData

Informacje przechowywane na karcie kierowcy lub warsztatowej dotyczące usterek związanych z posiadaczem karty (wymagania 207 i 223).

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

CardFaultData jest sekwencją zbioru zapisów dotyczących usterek urządzenia rejestrującego poprzedzającego zbiór zapisów dotyczących usterek kart.

CardFaultRecords jest zbiorem zapisów dotyczących usterek danej kategorii usterek (urządzenia rejestrującego lub karty).

2.18. CardFaultRecord

Informacje przechowywane na karcie kierowcy lub warsztatowej dotyczące usterki związanej z posiadaczem karty (wymagania 208 i 223).

```
CardFaultRecord ::= SEQUENCE {
    FaultType                               EventFaultType,
    FaultBeginTime                           TimeReal,
    FaultEndTime                             TimeReal,
    FaultVehicleRegistration                 VehicleRegistrationIdentification
}
```

FaultType jest typem usterki.

faultBeginTime jest datą i godziną rozpoczęcia usterki.

faultEndTime jest datą i godziną zakończenia usterki.

FaultVehicleRegistration jest numerem VRN i Państwa Członkowskiego rejestracji pojazdu, w którym usterka zdarzyła się.

2.19. CardIccIdentification

Informacje zapisane na karcie dotyczące identyfikacji karty z układem scalonym (IC) (wymaganie 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 jest trybem Clockstop zdefiniowanym w normie EN 726-3.

CardExtendedSerialNumber jest numerem fabrycznym karty z układem scalonym i oznaczeniem producenta karty z układem scalonym, zdefiniowanym w normie EN 726-3 i dalej określonym typem danych w ExtendedSerialNumber.

CardApprovalNumber jest numerem homologacji typu karty.

CardPersonaliserID jest identyfikatorem personalizującego karty zdefiniowanym w normie EN 726-3.

EmbedderIdAssemblerId jest identyfikatorem wbudowującego/montującego układ scalony zdefiniowanym w normie EN 726-3.

IdIdentifier jest identyfikatorem układu scalonego na karcie i producenta układu scalonego zdefiniowanym w normie EN 726-3.

2.20. CardIdentification

Informacje zapisane na karcie dotyczące identyfikacji karty (wymagania 194, 215, 231 i 235).

CardIdentification ::= SEQUENCE

CardIssuingMemberState	NationNumeric,
CardNumber	CardNumber,
CardIssuingAuthorityName	Name,
CardIssueDate	TimeReal,
CardValidityBegin	TimeReal,
CardExpiryDate	TimeReal

}

CardIssuingMemberState jest kodem Państwa Członkowskiego wydającego kartę.

CardNumber jest numerem karty.

CardIssuingAuthorityName jest nazwą organu wydającego kartę.

CardIssueDate jest datą wydania karty aktualnemu posiadaczowi.

CardValidityBegin jest pierwszą datą ważności karty.

CardExpiryDate jest datą ważności karty.

2.21. CardNumber

Numer karty zgodny z definicją g).

CardNumber ::= CHOICE {

SEQUENCE {	
DriverIdentification	IA5String(SIZE(14)),
CardReplacementIndex	CardReplacementIndex,
CardRenewalIndex	CardRenewalIndex
}	
SEQUENCE {	
OwnerIdentification	IA5String(SIZE(13)),
CardConsecutiveIndex	CardConsecutiveIndex,
CardReplacementIndex	CardReplacementIndex,
CardRenewalIndex	CardRenewalIndex
}	

}

DriverIdentification jest jednoznaczoną identyfikacją kierowcy w Państwie Członkowskim.

OwnerIdentification jest jednoznaczoną identyfikacją firmy lub warsztatu lub organu kontrolnego w Państwie Członkowskim.

CardConsecutiveIndex jest numerem kolejnym karty.

CardReplacementIndex jest numerem wymiany karty.

CardRenewalIndex jest numerem odświeżenia karty.

Pierwsza wybierana sekwencja odnosi się do kodu numeru karty kierowcy a druga wybierana sekwencja odnosi się do kodu numeru karty warsztatowej, kontrolnej i firmowej.

2.22. CardPlaceDailyWorkPeriod

Informacje przechowywane na karcie kierowcy lub warsztatowej dotyczące miejsc rozpoczęcia i/lub zakończenia dziennych okresów pracy (wymagania 202 i 221).

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

PlacePointerNewestRecord jest indeksem ostatniego, uaktualnionego zapisu miejsca.

Przypisanie wartości: liczba odpowiadająca stanowi licznika zapisów miejsca, zaczynająca się od »0« dla pierwszego wystąpienia zapisów miejsca w strukturze.

PlaceRecords jest zbiorem zapisów dotyczących wprowadzonych miejsc.

2.23. CardPrivateKey

Klucz prywatny karty.

CardPrivateKey ::= RSAKeyPrivateExponena temat.

2.24. CardPublicKey

Klucz publiczny karty.

CardPublicKey ::= PublicKey.

2.25. CardRenewalIndex

Numer odświeżenia karty (definicja i)).

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

Przypisanie wartości: (patrz rozdział VII niniejszego załącznika).

'0' Wydanie pierwsze.

Kolejność zwiększania: '0, ..., 9, A, ..., Z'.

2.26. CardReplacementIndex

Numer wymiany karty (definicja j)).

CardReplacementIndex ::= IA5String(SIZE(1))

Przypisanie wartości: (patrz rozdział VII niniejszego załącznika).

'0' Oryginał karty.

Kolejność zwiększania: '0, ..., 9, A, ..., Z'.

2.27. CardSlotNumber

Kod rozróżnienia między dwiema szczelinami kart w przyrządzie rejestrującym.

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

Przypisanie wartości: bez dalszego określenia.

2.28. CardSlotsStatus

Kod wskazujący typ kart włożonych do dwóch szczelin czytników karty przyrządu rejestrującego.

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

Przypisanie wartości — Octet Aligned: 'ccccdddd'B:

'cccc'B	identyfikacja typu karty włożonej do szczeliny karty współkierowcy,
---------	---

'ddd'd'B identyfikacja typu karty włożonej do szczeliny karty kierowcy,

z następującymi kodami identyfikującymi:

'0000'B	brak karty,
---------	-------------

'0001'B włożona jest karta kierowcy,

'0010'B włożona jest karta warsztatowa,

'0011'B włożona jest karta kontrolna,

'0100'B włożona jest karta firmowa.

2.29. CardStructureVersion

Kod wskazujący wersję struktury na karcie do tachografów.

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

Przypisanie wartości: 'aabb'H:

'aa'H indeks zmian struktury,

⁷bb'H indeks zmian dotyczących użycia elementów danych zdefiniowanych dla struktury określony wyższym bajtem.

2.30. CardVehicleRecord

Informacje przechowywane na karcie kierowcy lub warsztatowej dotyczące okresu używania pojazdu w czasie dnia kalendarzowego (wymagania 197 i 217).

```
CardVehicleRecord := SEQUENCE {
    vehicleOdometerBegin          OdometerShort,
    vehicleOdometerEnd            OdometerShort,
    vehicleFirstUse               TimeReal,
    vehicleLastUse                TimeReal,
    vehicleRegistration            VehicleRegistrationIdentification,
    vuDataBlockCounter            VuDataBlockCounter
}
```

VehicleOdometerBegin jest stanem licznika kilometrów na początku okresu używania pojazdu.

VehicleOdometerEnd jest stanem licznika kilometrów na końcu okresu używania pojazdu.

VehicleFirstUse jest datą i godziną rozpoczęcia okresu używania pojazdu.

VehicleLastUse jest datą i godziną zakończenia okresu używania pojazdu.

VehicleRegistration jest numerem VRN i Państwa Członkowskiego rejestracji pojazdu.

VuDataBlockCounter jest wartością licznika VuDataBlockCounter ostatniego wyciągu okresu użycia pojazdu.

2.31. CardVehiclesUsed

Informacje przechowywane na karcie kierowcy lub warsztatowej dotyczące pojazdów używanych przez posiadacza karty (wymagania 197 i 217).

```
CardVehiclesUsed := SEQUENCE {
    VehiclePointerNewestRecord      INTEGER(0..NoOfCardVehicleRecords-1),
    CardVehicleRecords              SET SIZE (NoOfCardVehicleRecords) OF
                                   CardVehicleRecord
}
```

VehiclePointerNewestRecord jest indeksem ostatniego, uaktualnionego zapisu dotyczącego pojazdu.

Przypisanie wartości: liczba odpowiadająca stanowi licznika zapisów dotyczących pojazdów, rozpoczynając od '0' dla pierwszego wystąpienia w strukturze zapisów dotyczących pojazdów.

CardVehicleRecords jest zbiorem zapisów zawierających informacje o używanych pojazdach.

2.32. Certificate

Certyfikat klucza publicznego wydany przez jednostkę certyfikującą.

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

Przypisanie wartości: podpis cyfrowy z częściowym odzyskiwaniem zawartości CertificateContent, zgodnie z dodatkiem 11 »Wspólne mechanizmy bezpieczeństwa«: podpis (128 bajtów) || reszta klucza publicznego (58 bajtów) || odesłanie do jednostki certyfikującej (8 bajtów).

2.33. CertificateContent

Treść certyfikatu klucza publicznego zgodnie z dodatkiem 11 Wspólne mechanizmy bezpieczeństwa.

```
CertificateContent ::= SEQUENCE {
    CertificateProfileIdentifier          INTEGER(0..255),
    CertificationAuthorityReference      KeyIdentifier,
    CertificateHolderAuthorisation       CertificateHolderAuthorisation,
    CertificateEndOfValidity             TimeReal,
    CertificateHolderReference           KeyIdentifier,
    PublicKey                           PublicKey
}
```

CertificateProfileIdentifier jest wersją odpowiedniego certyfikatu.

Przypisanie wartości: '01h' dla tej wersji.

CertificationAuthorityReference identyfikuje jednostkę certyfikującą wydającą certyfikat. Jest tu także odesłanie do klucza publicznego tej jednostki certyfikującej.

certificateHolderAuthorisation identyfikuje prawa posiadacza certyfikatu.

certificateEndOfValidity data administracyjnego wygaśnięcia certyfikatu.

certificateHolderReference identyfikuje posiadacza certyfikatu. Jest tu także odesłanie do jego klucza publicznego.

PublicKey jest kluczem publicznym, który jest poświadczony tym certyfikatem.

2.34. CertificateHolderAuthorisation

Identyfikacja praw posiadacza certyfikatu.

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

TachographApplicationID jest identyfikatorem aplikacji dla aplikacji tachograficznej.

Przypisanie wartości: 'FFh' '54h' '41h' '43h' '48h' '4Fh'. Ten AID jest zastrzeżonym, nierejestrowanym identyfikatorem aplikacji zgodnie z ISO/IEC 7816-5.

EquipmentType jest identyfikacją typu urządzenia, dla którego przeznaczony jest certyfikat.

Przypisanie wartości: zgodnie z typem danych, EquipmentType. 0 gdy jest to certyfikat jednego z Państw Członkowskich.

2.35. CertificateRequestID

Jednoznaczna identyfikacja wniosku o certyfikat. Może być także używana jako identyfikator klucza publicznego przyrzędu rejestrującego, jeżeli numer fabryczny przyrzędu rejestrującego, do którego ten klucz jest przeznaczony, nie jest znany w czasie sporządzania certyfikatu.

```
CertificateRequestID ::= SEQUENCE {
    RequestSerialNumber      INTEGER(0..232-1)
    RequestMonthYear         BCDString(SIZE(2))
    CrIdentifier              OCTET STRING(SIZE(1))
    ManufacturerCode         ManufacturerCode
}
```

RequestSerialNumber jest numerem fabrycznym wniosku o certyfikat, unikatowym dla producenta i miesiąca określonego poniżej.

RequestMonthYear jest identyfikacją miesiąca i roku wniosku o certyfikat.

Przypisanie wartości: podane w kodzie BCD miesiąc (dwie cyfry) i rok (ostatnie dwie cyfry).

CrIdentifier: jest identyfikatorem umożliwiającym rozróżnienie wniosku o certyfikat od rozszerzonego numeru fabrycznego.

Przypisanie wartości: 'FFh'.

ManufacturerCode: jest kodem numerycznym producenta wnioskującego o certyfikat.

2.36. CertificationAuthorityKID

Identyfikator klucza publicznego organu certyfikującego (organu certyfikującego Państwa Członkowskiego lub europejskiego).

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

NationNumeric jest numerycznym kodem krajowym organu certyfikującego.

NationAlpha jest alfanumerycznym kodem krajowym organu certyfikującego.

KeySerialNumber jest numerem fabrycznym umożliwiającym rozróżnienie różnych kluczy organu certyfikującego w przypadku zmiany kluczy.

AdditionalInfo jest dwubajtowym polem przeznaczonym na dodatkowy kod (swoisty dla organu certyfikującego).

CaIdentifier jest identyfikatorem umożliwiającym rozróżnienie identyfikatora klucza organu certyfikującego od innych identyfikatorów kluczy.

Przypisanie wartości: '01h'.

2.37. CompanyActivityData

Informacje przechowywane na karcie firmowej dotyczące czynności wykonanych przy użyciu karty (wymaganie 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 jest indeksem ostatniego, uaktualnionego rekordu **companyActivityRecord**.

Przypisanie wartości: liczba odpowiadająca stanowi licznika zapisów czynności firmy, rozpoczynając od '0' dla pierwszego wystąpienia zapisu czynności firmy w strukturze.

CompanyActivityRecords jest zbiorem wszystkich zapisów czynności firmy.

CompanyActivityRecord jest sekwencją informacji dotyczących jednej czynności firmy.

CompanyActivityType jest typem czynności firmy.

CompanyActivityTime jest datą i godziną czynności firmy.

CardNumberInformation jest numerem karty i Państwa Członkowskiego wydającego kartę, z której wczytano dane, gdy dotyczy.

VehicleRegistrationInformation jest numerem VRN i Państwem Członkowskim rejestracji pojazdu, dla którego wczytano dane lub zablokowano lub zdjęto blokadę.

DownloadPeriodBegin i **downloadPeriodEnd** jest okresem, dla którego wczytano dane, z VU, gdy dotyczy.

2.38. CompanyActivityType

Kod wskazujący czynność wykonaną przez firmę z wykorzystaniem jej karty firmowej.

```

CompanyActivityType ::= INTEGER {
    wczytywanie danych z karty                1,
    wczytywanie danych z VU                   2,
    blokowanie VU                             3,
    zdejmowanie blokady w VU                  4.
}

```

2.39. CompanyCardApplicationIdentification

Informacje przechowywane na karcie firmowej dotyczące identyfikacji aplikacji na karcie (wymaganie 190).

```

CompanyCardApplicationIdentification ::= SEQUENCE {
    TypeOfTachographCardId                    EquipmentType,
    CardStructureVersion                      CardStructureVersion,
    NoOfCompanyActivityRecords                 NoOfCompanyActivityRecords
}

```

TypeOfTachographCardId określa wdrożony typ karty.

CardStructureVersion określa wersję struktury zastosowanej na karcie.

NoOfCompanyActivityRecords jest liczbą zapisów z czynnościami firmy, które można przechowywać na karcie.

2.40. CompanyCardHolderIdentification

Informacje przechowywane na karcie firmowej dotyczące identyfikacji posiadacza karty (wymaganie 236).

```

CompanyCardHolderIdentification ::= SEQUENCE {
    CompanyName                               Name,
    CompanyAddress                           Address,
    CardHolderPreferredLanguage              Language
}

```

CompanyName jest nazwą (nazwiskiem) właściciela firmy.

CompanyAddress jest adresem właściciela firmy.

CardHolderPreferredLanguage jest preferowanym językiem właściciela firmy.

2.41. **ControlCardApplicationIdentification**

Informacje przechowywane na karcie kontrolnej dotyczące identyfikacji aplikacji na karcie (wymaganie 190).

```
ControlCardApplicationIdentification ::= SEQUENCE {
    TypeOfTachographCardId          EquipmentType,
    CardStructureVersion             CardStructureVersion,
    NoOfControlActivityRecords       NoOfControlActivityRecords
}
```

TypeOfTachographCardId określa wdrożony typ karty.

CardStructureVersion określa wersję struktury, która jest wdrożona na karcie.

NoOfControlActivityRecords jest liczbą zapisów czynności kontrolnych, które mogą być zapisane na karcie.

2.42. **ControlCardControlActivityData**

Informacje przechowywane na karcie kontrolnej dotyczące czynności kontrolnych wykonanych w odniesieniu do karty (wymaganie 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 jest indeksem ostatniego, uaktualnionego zapisu czynności kontrolnych.

Przypisanie wartości: liczba odpowiadająca stanowi licznika zapisów czynności kontrolnych, rozpoczynając od »0« dla pierwszego wystąpienia w strukturze zapisu czynności kontroli.

ControlActivityRecords jest zbiorem wszystkich zapisów czynności kontrolnych.

ControlActivityRecord jest ciągiem informacji dotyczących jednej kontroli.

ControlType jest typem kontroli.

ControlTime jest datą i godziną kontroli.

ControlledCardNumber jest numerem karty i Państwa Członkowskiego wydającego kartę, która jest kontrolowana.

ControlledVehicleRegistration jest numerem VRN i Państwa Członkowskiego rejestracji pojazdu, w którym kontrola miała miejsce.

ControlDownloadPeriodBegin i **controlDownloadPeriodEnd** wyznaczają ewentualnie wczytany okres.

2.43. **ControlCardHolderIdentification**

Informacje przechowywane na karcie kontrolnej dotyczące identyfikacji posiadacza karty (wymaganie 232).

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

ControlBodyName jest nazwą organu kontrolnego posiadacza karty.

ControlBodyAddress jest adresem organu kontrolnego posiadacza karty.

CardHolderName jest nazwą i imieniem (imionami) posiadacza karty kontrolnej.

CardHolderPreferredLanguage jest preferowanym językiem posiadacza karty.

2.44. ControlType

Kod wskazujący czynności wykonane podczas kontroli. Ten typ danych związany jest z wymaganiami 102, 210 i 225.

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

Przypisanie wartości — oktet o budowie: 'c'p'd'v'x'B (8 bitów)

'c'B wczytywanie danych z karty:
 '0'B: nie wczytano z karty w czasie tej kontroli,
 '1'B: wczytano z karty w czasie tej kontroli

'v'B VU wczytywanie danych:
 '0'B: nie wczytano z VU w czasie tej kontroli,
 '1'B: wczytano z VU w czasie tej kontroli

'p'B drukowanie:
 '0'B: nie wykonano wydruków w czasie tej kontroli,
 '1'B: wykonano wydruki w czasie tej kontroli

'd'B wyświetlacz:
 '0'B: nie użyto wyświetlacza w czasie tej kontroli,
 '1'B: użyto wyświetlacza w czasie tej kontroli

'xxx'B Nieużywany.

2.45. CurrentDateTime

Bieżąca data i godzina urzędowania rejestrującego.

```
CurrentDateTime ::= TimeReal
```

Przypisanie wartości: nie określa się.

2.46. DailyPresenceCounter

Licznik znajdujący się na karcie kierowcy lub warsztatowej zwiększany o jeden dla każdego dnia kalendarzowego, w którym karta jest włożona do VU. Ten typ danych związany jest z wymaganiami 199 i 219.

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

Przypisanie wartości: Kolejna liczba do maksymalnej wartości = 9 999, i następnie ponownie zaczyna od 0. Przy pierwszym wydaniu karty licznik jest ustawiany na 0.

2.47. Datef

Data wyrażona w czytelnym, przeznaczonym do druku formacie numerycznym.

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

Przypisanie wartości:

```
yyyy      rok
mm        miesiąc
dd        dzień
```

'00000000'H oznacza jednoznacznie brak daty.

2.48. Distance

Przebyta odległość (wynik obliczenia różnicy między dwoma odczytami licznika kilometrów pojazdu wyrażona w kilometrach).

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

Przypisanie wartości: Liczba binarna bez znaku. Wartość w km w zakresie operacyjnym 0 do 9 999 km.

2.49. DriverCardApplicationIdentification

Informacje przechowywane na karcie kierowcy dotyczące identyfikacji aplikacji na karcie (wymaganie 190).

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

TypeOfTachographCardId określa wdrożony typ karty.

CardStructureVersion określa wersję struktury wdrożoną na karcie.

NoOfEventsPerType jest liczbą zdarzeń według typów możliwą do zarejestrowania na karcie.

NoOfFaultsPerType jest liczbą usterek według typów możliwą do zarejestrowania na karcie.

ActivityStructureLength podaje liczbę bajtów dostępnych do rejestrowania rekordów czynności.

NoOfCardVehicleRecords jest liczbą zapisów pojazdu możliwą do zarejestrowania na karcie.

NoOfCardPlaceRecords jest liczbą miejsc możliwą do zarejestrowania na karcie.

2.50. DriverCardHolderIdentification

Informacje przechowywane na karcie kierowcy dotyczące identyfikacji posiadacza karty (wymaganie 195).

```
DriverCardHolderIdentification ::= SEQUENCE {
    CardHolderName      HolderName,
    CardHolderBirthDate Datef,
    CardHolderPreferredLanguage Language
}
```

CardHolderName jest nazwą i imieniem (imionami) posiadacza karty kierowcy.

CardHolderBirthDate jest datą urodzenia posiadacza karty kierowcy.

CardHolderPreferredLanguage jest preferowanym językiem posiadacza karty.

2.51. EntryTypeDailyWorkPeriod

Kod umożliwiający rozróżnienie między początkiem a końcem wpisu dotyczącego dziennego okresu pracy oraz miejsca i sposobu wprowadzenia wpisu.

```
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)
}
```

Przypisanie wartości: zgodnie z normą ISO/IEC8824-1.

2.52. EquipmentType

Kod umożliwiający rozróżnienie typów urządzeń dla aplikacji tachograficznej.

```
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)
```

Przypisanie wartości: zgodnie z ISO/IEC 8824-1.

Wartość 0 jest zastrzeżona do celów oznaczenia Państwa Członkowskiego lub Europy w rubryce CHA certyfikatów.

2.53. EuropeanPublicKey

Europejski klucz publiczny.

EuropeanPublicKey ::= **PublicKey**.

2.54. EventFaultType

Kod kwalifikujący zdarzenie lub usterkę.

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

Przypisanie wartości:

'0x'H	zdarzenia,
'00'H	brak dalszych szczegółów,
'01'H	włożenie nieważnej karty,
'02'H	konflikt kart,
'03'H	nakładające się czasy,
'04'H	przewodzenie bez prawidłowej karty,
'05'H	włożenie karty podczas jazdy,
'06'H	sesja ostatniej karty niezamknięta prawidłowo,
'07'H	przekroczenie prędkości,

'08'H	przerwa zasilania,
'09'H	błąd danych o ruchu,
'0A'H to '0F'H	RFU,
'1x'H	zdarzenia związane z próbami naruszenia zabezpieczenia przyrządu rejestrującego,
'10'H	brak dalszych szczegółów,
'11'H	błąd uwierzytelnienia czujnika ruchu,
'12'H	błąd uwierzytelnienia kart do tachografów,
'13'H	nieupoważniona zmiana w czujniku ruchu,
'14'H	błąd integralności wprowadzania danych na kartę
'15'H	błąd integralności przechowywanych danych użytkownika,
'16'H	błąd wewnętrznego przesyłania danych,
'17'H	nieupoważnione otwarcie obudowy,
'18'H	uszkodzenie sprzętu,
'19'H to '1F'H	RFU,
'2x'H	zdarzenia związane z próbami naruszenia zabezpieczenia czujnika,
'20'H	brak dalszych szczegółów,
'21'H	błąd uwierzytelnienia,
'22'H	błąd integralności przechowywanych danych,
'23'H	błąd wewnętrznego przesyłania danych,
'24'H	nieupoważnione otwarcie obudowy,
'25'H	uszkodzenie sprzętu,
'26'H to '2F'H	RFU,
'3x'H	usterka urządzenia rejestrującego,
'30'H	brak dalszych szczegółów,
'31'H	wewnętrzna usterka VU,
'32'H	usterka drukarki,
'33'H	usterka wyświetlacza,
'34'H	usterka wczytywania danych,
'35'H	usterka czujnika,
'36'H to '3F'H	RFU
'4x'H	usterki karty,
'40'H	brak dalszych szczegółów,
'41'H to '4F'H	RFU
'50'H to '7F'H	RFU,
'80'H to 'FF'H	swoisty dla producenta.

2.55. EventFaultRecordPurpose

Kod wyjaśniający, dlaczego zarejestrowano zdarzenie lub usterkę.

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

Przypisanie wartości:

'00'H	jedno z 10 ostatnich (lub ostatnie) zdarzeń lub usterek
'01'H	najdłuższe zdarzenie w jednym z ostatnich 10 dni ich występowania
'02'H	jedno z 5 najdłuższych zdarzeń w ciągu ostatnich 365 dni
'03'H	ostatnie zdarzenie w jednym z ostatnich 10 dni ich występowania
'04'H	najpoważniejsze zdarzenie w jednym z ostatnich 10 dni ich występowania
'05'H	jedno z 5 najpoważniejszych zdarzeń w ciągu ostatnich 365 dni
'06'H	pierwsze zdarzenie lub usterka zaistniałe po ostatniej kalibracji
'07'H	aktywne/trwające zdarzenie lub usterka
'08'H to '7F'H	RFU
'80'H to 'FF'H	swoisty dla producenta.

2.56. ExtendedSerialNumber

Unikalna identyfikacja urządzenia. Może być używana także jako identyfikator klucza publicznego urządzenia.

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

SerialNumber jest numerem fabrycznym urządzenia, unikalnym dla producenta, typu urządzenia i miesiąca, jak wyjaśniono poniżej.

MonthYear jest identyfikacją miesiąca i roku produkcji (lub przypisanym numerem fabrycznym).

Przypisanie wartości: miesiąc (dwie cyfry) i rok (dwie ostatnie cyfry) w kodzie BCD.

Type jest identyfikatorem typu urządzenia.

Przypisanie wartości: swoisty dla producenta, z wartością zastrzeżoną FFh'.

ManufacturerCode: jest kodem numerycznym producenta urządzenia.

2.57. FullCardNumber

Kod całkowicie identyfikujący kartę do tachografów.

```
FullCardNumber ::= SEQUENCE {
    CardType              EquipmentType,
    CardIssuingMemberState NationNumeric,
    CardNumber            CardNumber
}
```

CardType jest typem karty do tachografów.

CardIssuingMemberState jest kodem Państwa Członkowskiego, które wydało kartę.

CardNumber jest numerem karty.

2.58. HighResOdometer

Stan licznika kilometrów pojazdu: skumulowana odległość przebyta przez pojazd w czasie jego eksploatacji.

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

Przypisanie wartości: liczba binarna bez znaku. Wyrażona w 1/200 km w zakresie operacyjnym 0 do 21 055 406 km.

2.59. HighResTripDistance

Odległość przebyta w czasie całej lub części podróży.

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

Przypisanie wartości: liczba binarna bez znaku. Wyrażona w 1/200 km w zakresie operacyjnym 0 do 21 055 406 km.

2.60. HolderName

Nazwisko i imię (imiona) posiadacza karty.

```
HolderName ::= SEQUENCE {
    HolderSurname          Name,
    HolderFirstNames       Name
}
```

HolderSurname jest nazwiskiem posiadacza. Tu nazwisko nie zawiera tytułów.

Przypisanie wartości: w przypadku kart nieosobowych, holderSurname zawiera te same informacje, co companyName lub workshopName lub controlBodyName.

HolderFirstNames jest imieniem (imionami) i inicjałami posiadacza.

2.61. **K-ConstantOfRecordingEquipment**

Stała urządzenia rejestrującego (definicja m)).

$K-ConstantOfRecordingEquipment ::= INTEGER(0..2^{16}-1)$

Przypisanie wartości: liczba impulsów na kilometr w zakresie operacyjnym 0 do 64 255 impulsów/km.

2.62. **KeyIdentifier**

Unikalny identyfikator klucza publicznego używany przy odwoływaniu się do klucza i do wybierania klucza. Identyfikuje także posiadacza klucza.

```
KeyIdentifier ::= CHOICE {
    ExtendedSerialNumber          ExtendedSerialNumber,
    CertificateRequestID           CertificateRequestID,
    CertificationAuthorityKID       CertificationAuthorityKID
}
```

Pierwsza pozycja jest odpowiednia przy odesłaniu do klucza publicznego przyrządu rejestrującego lub karty do tachografów.

Druga pozycja jest odpowiednia przy odesłaniu do klucza publicznego przyrządu rejestrującego (w przypadku, gdy numer fabryczny przyrządu rejestrującego może nie być znany w czasie sporządzenia certyfikatu).

Trzecia pozycja jest odpowiednia przy odesłaniu do klucza publicznego Państwa Członkowskiego.

2.63. **L-TyreCircumference**

Skuteczny obwód opon (definicja u)).

$L-TyreCircumference ::= INTEGER(0..2^{16}-1)$

Przypisanie wartości: liczba binarna bez znaku, wyrażona w 1/8 mm w zakresie operacyjnym 0 do 8 031 mm.

2.64. **Language**

Kod identyfikujący język.

$Language ::= IA5String(SIZE(2))$

Przypisanie wartości: kod składający się z dwóch małych liter zgodny z normą ISO 639.

2.65. **LastCardDownload**

Data i godzina, zapisane na karcie kierowcy, ostatniego wczytywania danych z karty (do innych celów niż kontrola). Datę tę aktualizuje VU lub dowolny czytnik kart.

$LastCardDownload ::= TimeReal$

Przypisanie wartości: nie określa się.

2.66. **ManualInputFlag**

Kod identyfikujący czy CardHolder wprowadza ręcznie czynności kierowcy przy wkładaniu karty (wymaganie 081).

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

Przypisanie wartości: nie określa się.

2.67. ManufacturerCode

Kod identyfikujący producenta.

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

Przypisanie wartości:

'00'H	brak informacji
'01'H	wartość zastrzeżona
'02'H .. '0F'H	zastrzeżony do wykorzystania w przyszłości
'10'H	ACTIA
'11'H .. '17'H	zastrzeżony dla producentów, których nazwa (nazwisko) rozpoczyna się literą 'A'
'18'H .. '1F'H	zastrzeżony dla producentów, których nazwa (nazwisko) rozpoczyna się literą 'B'
'20'H .. '27'H	zastrzeżony dla producentów, których nazwa (nazwisko) rozpoczyna się literą 'C'
'28'H .. '2F'H	zastrzeżony dla producentów, których nazwa (nazwisko) rozpoczyna się literą 'D'
'30'H .. '37'H	zastrzeżony dla producentów, których nazwa (nazwisko) rozpoczyna się literą 'E'
'38'H .. '3F'H	zastrzeżony dla producentów, których nazwa (nazwisko) rozpoczyna się literą 'F'
'40'H	Giesecke & Devrient GmbH
'41'H	GEM plus
'42'H .. '47'H	zastrzeżony dla producentów, których nazwa (nazwisko) rozpoczyna się literą 'G'
'48'H .. '4F'H	zastrzeżony dla producentów, których nazwa (nazwisko) rozpoczyna się literą 'H'
'50'H .. '57'H	zastrzeżony dla producentów, których nazwa (nazwisko) rozpoczyna się literą 'I'
'58'H .. '5F'H	zastrzeżony dla producentów, których nazwa (nazwisko) rozpoczyna się literą 'J'
'60'H .. '67'H	zastrzeżony dla producentów, których nazwa (nazwisko) rozpoczyna się literą 'K'
'68'H .. '6F'H	zastrzeżony dla producentów, których nazwa (nazwisko) rozpoczyna się literą 'L'
'70'H .. '77'H	zastrzeżony dla producentów, których nazwa (nazwisko) rozpoczyna się literą 'M'
'78'H .. '7F'H	zastrzeżony dla producentów, których nazwa (nazwisko) rozpoczyna się literą 'N'
'80'H	OSCARD
'81'H .. '87'H	zastrzeżony dla producentów, których nazwa (nazwisko) rozpoczyna się literą 'O'
'88'H .. '8F'H	zastrzeżony dla producentów, których nazwa (nazwisko) rozpoczyna się literą 'P'
'90'H .. '97'H	zastrzeżony dla producentów, których nazwa (nazwisko) rozpoczyna się literą 'Q'
'98'H .. '9F'H	zastrzeżony dla producentów, których nazwa (nazwisko) rozpoczyna się literą 'R'
'A0'H	SETEC
'A1'H	SIEMENS VDO
'A2'H	STONERIDGE
'A3'H .. 'A7'H	zastrzeżony dla producentów, których nazwa (nazwisko) rozpoczyna się literą 'S'
'AA'H	TACHOCONTROL
'AB'H .. 'AF'H	zastrzeżony dla producentów, których nazwa (nazwisko) rozpoczyna się literą 'T'
'B0'H .. 'B7'H	zastrzeżony dla producentów, których nazwa (nazwisko) rozpoczyna się literą 'U'
'B8'H .. 'BF'H	zastrzeżony dla producentów, których nazwa (nazwisko) rozpoczyna się literą 'V'
'C0'H .. 'C7'H	zastrzeżony dla producentów, których nazwa (nazwisko) rozpoczyna się literą 'W'
'C8'H .. 'CF'H	zastrzeżony dla producentów, których nazwa (nazwisko) rozpoczyna się literą 'X'
'D0'H .. 'D7'H	zastrzeżony dla producentów, których nazwa (nazwisko) rozpoczyna się literą 'Y'
'D8'H .. 'DF'H	zastrzeżony dla producentów, których nazwa (nazwisko) rozpoczyna się literą 'Z'

2.68. MemberStateCertificate

Certyfikat klucza publicznego Państwa Członkowskiego wydany przez europejski organ certyfikujący.

```
MemberStateCertificate ::= Certificate
```

2.69. MemberStatePublicKey

Klucz publiczny Państwa Członkowskiego.

`MemberStatePublicKey := PublicKey.`

2.70. Name

Nazwa (nazwisko).

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

CodePage określa część strony kodowej normy ISO/IEC 8859 użytą do zakodowania nazwy (nazwiska),

Name jest nazwą (nazwiskiem) zakodowanym zgodnie ze stroną kodową normy ISO/IEC 8859.

2.71. NationAlpha

Alfabetyczne określenie państwa, zgodnie z konwencjonalnym oznakowaniem państw na nalepkach umieszczanych na zderzakach pojazdów, i/lub jak używane w międzynarodowych, zharmonizowanych dokumentach ubezpieczeniowych pojazdów (zielona karta).

`NationAlpha := IA5String (SIZE (3))`

Przypisanie wartości:

' '	brak informacji
'A'	Austria
'AL'	Albania
'AND'	Andora
'ARM'	Armenia
'AZ'	Azerbejdżan
'B'	Belgia
'BG'	Bułgaria
'BIH'	Bośnia i Hercegowina
'BY'	Białoruś
'CH'	Szwajcaria
'CY'	Cypr
'CZ'	Republika Czeska
'D'	Niemcy
'DK'	Dania
'E'	Hiszpania
'EST'	Estonia
'F'	Francja
'FIN'	Finlandia
'FL'	Liechtenstein
'FR'	Wyspy Owcze
'UK'	Zjednoczone Królestwo, Alderney, Guernsey, Jersey, Wyspa Man, Gibraltar
'GE'	Gruzja
'GR'	Grecja
'H'	Węgry
'HR'	Chorwacja
'I'	Włochy
'IRL'	Irlandia
'IS'	Islandia
'KZ'	Kazachstan
'L'	Luksemburg
'LT'	Litwa
'LV'	Łotwa
'M'	Malta
'MC'	Monako

'MD'	Republika Mołdowa
'MK'	Macedonia
'N'	Norwegia
'NL'	Niderlandy
'P'	Portugalia
'PL'	Polska
'RO'	Rumunia
'RSM'	San Marino
'RUS'	Federacja Rosyjska
'S'	Szwecja
'SK'	Słowacja
'SLO'	Słowenia
'TM'	Turkmenia
'TR'	Turcja
'UA'	Ukraina
'V'	Państwo Watykańskie
'YU'	Jugosławia
'UNK'	Nieznane
'EC'	Wspólnota Europejska
'EUR'	reszta Europy
'WLD'	reszta świata.

2.72. NationNumeric

Numeryczne odniesienie do państwa.

NationNumeric ::= INTEGER(0..255)

Przypisanie wartości:

-- brak informacji	(00)H,
-- Austria	(01)H,
-- Albania	(02)H,
-- Andora	(03)H,
-- Armenia	(04)H,
-- Azerbejdżan	(05)H,
-- Belgia	(06)H,
-- Bułgaria	(07)H,
-- Bośnia i Hercegowina	(08)H,
-- Białoruś	(09)H,
-- Szwajcaria	(0A)H,
-- Cypr	(0B)H,
-- Republika Czeska	(0C)H,
-- Niemcy	(0D)H,
-- Dania	(0E)H,
-- Hiszpania	(0F)H,
-- Estonia	(10)H,
-- Francja	(11)H,
-- Finlandia	(12)H,
-- Liechtenstein	(13)H,
-- Wyspy Owcze	(14)H,
-- Zjednoczone Królestwo	(15)H,
-- Gruzja	(16)H,
-- Grecja	(17)H,
-- Węgry	(18)H,
-- Chorwacja	(19)H,
-- Włochy	(1A)H,
-- Irlandia	(1B)H,
-- Islandia	(1C)H,

-- Kazachstan	(1D) H,
-- Luksemburg	(1E) H,
-- Litwa	(1F) H,
-- Łotwa	(20) H,
-- Malta	(21) H,
-- Monako	(22) H,
-- Republika Mołdowa	(23) H,
-- Macedonia	(24) H,
-- Norwegia	(25) H,
-- Niderlandy	(26) H,
-- Portugalia	(27) H,
-- Polska	(28) H,
-- Rumunia	(29) H,
-- San Marino	(2A) H,
-- Federacja Rosyjska	(2B) H,
-- Szwecja	(2C) H,
-- Słowacja	(2D) H,
-- Słowenia	(2E) H,
-- Turkmenia	(2F) H,
-- Turcja	(30) H,
-- Ukraina	(31) H,
-- Państwo Watykańskie	(32) H,
-- Jugosławia	(33) H,
-- RFU	(34 . . FC) H,
-- Wspólnota Europejska	(FD) H,
-- reszta Europy	(FE) H,
-- reszta świata	(FF) H

2.73. NoOfCalibrationRecords

Liczba zapisów kalibracyjnych, możliwych do przechowywania na karcie.

NoOfCalibrationRecords := INTEGER(0..255)

Przypisanie wartości: patrz pkt 3.

2.74. NoOfCalibrationsSinceDownload

Licznik pokazujący liczbę kalibracji wykonanych przy użyciu karty warsztatowej od ostatniego wczytania danych z tej karty (wymaganie 230).

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

Przypisanie wartości: nie określa się.

2.75. NoOfCardPlaceRecords

Liczba zapisów dotyczących miejsca, możliwych do przechowywania na karcie kierowcy lub warsztatowej.

NoOfCardPlaceRecords := INTEGER(0..255)

Przypisanie wartości: patrz pkt 3.

2.76. NoOfCardVehicleRecords

Liczba zapisów dotyczących użytych pojazdów, możliwych do przechowywania na karcie kierowcy lub warsztatowej.

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

Przypisanie wartości: patrz pkt 3.

2.77. NoOfCompanyActivityRecords

Liczba zapisów dotyczących czynności firmy, możliwych do przechowywania na karcie firmowej.

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

Przypisanie wartości: patrz pkt 3.

2.78. NoOfControlActivityRecords

Liczba zapisów dotyczących czynności kontrolnych, możliwych do przechowywania na karcie kontrolnej.

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

Przypisanie wartości: patrz pkt 3.

2.79. NoOfEventsPerType

Liczba zdarzeń według typu, możliwych do przechowywania na karcie.

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

Przypisanie wartości: patrz pkt 3.

2.80. NoOfFaultsPerType

Liczba usterek według typu, możliwych do przechowywania na karcie.

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

Przypisanie wartości: patrz pkt 3.

2.81. OdometerValueMidnight

Stan licznika kilometrów o północy w danym dniu (wymaganie 090).

`OdometerValueMidnight := OdometerShort`

Przypisanie wartości: nie określa się.

2.82. OdometerShort

Stan licznika kilometrów pojazdu w skróconej postaci.

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

Przypisanie wartości: liczba binarna bez znaku. Wyrażona w km w zakresie operacyjnym 0-9 999 999 km.

2.83. OverspeedNumber

Liczba zdarzeń przekroczenia prędkości od ostatniej kontroli przekroczenia prędkości.

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

Przypisanie wartości: 0 oznacza, że nie było zdarzenia przekroczenia prędkości od ostatniej kontroli przekroczenia prędkości, 1 oznacza, że było jedno zdarzenie przekroczenia prędkości od ostatniej kontroli przekroczenia prędkości... 255 oznacza, że było 255 lub więcej zdarzeń przekroczenia prędkości od ostatniej kontroli przekroczenia prędkości.

2.84. PlaceRecord

Informacje dotyczące miejsca rozpoczęcia lub zakończenia dziennego okresu pracy (wymagania 087, 202, 221).

```
PlaceRecord := SEQUENCE {
    EntryTime                               TimeReal,
    EntryTypeDailyWorkPeriod               EntryTypeDailyWorkPeriod,
    DailyWorkPeriodCountry                  NationNumeric,
    DailyWorkPeriodRegion                   RegionNumeric,
    VehicleOdometerValue                    OdometerShort
}
```

EntryTime jest datą i godziną wpisu.

EntryTypeDailyWorkPeriod jest typem wpisu.

DailyWorkPeriodCountry jest wprowadzonym krajem.

DailyWorkPeriodRegion jest wprowadzonym regionem.

VehicleOdometerValue jest stanem licznika kilometrów w czasie wprowadzania miejsca.

2.85. PreviousVehicleInfo

Informacje dotyczące pojazdu poprzednio używanego przez kierowcę w chwili wkładania jego karty do przyrządu rejestrującego (wymaganie 081).

```
PreviousVehicleInfo ::= SEQUENCE {
    VehicleRegistrationIdentification      VehicleRegistrationIdentification,
    CardWithdrawalTime                    TimeReal
}
```

VehicleRegistrationIdentification jest numerem VRN i Państwa Członkowskiego rejestracji pojazdu.

CardWithdrawalTime jest datą i godziną wyjęcia karty.

2.86. PublicKey

Klucz publiczny RSA.

```
PublicKey ::= SEQUENCE {
    RsaKeyModulus                      RSAKeyModulus,
    RsaKeyPublicExponent               RSAKeyPublicExponent
}
```

RsaKeyModulus jest modulem pary kluczy.

RsaKeyPublicExponent jest wykładnikiem publicznym pary kluczy.

2.87. RegionAlpha

Alfabetyczne odniesienie do regionu w określonym kraju.

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

Przypisanie wartości:

' ' brak informacji

Hiszpania:

'AN'	Andaluzja
'AR'	Aragonia
'AST'	Asturia
'C'	Cantabria
'CAT'	Katalonia
'CL'	Kastylija-León
'CM'	Kastylija-La Mancha
'CV'	Walencja
'EXT'	Extremadura
'G'	Galicja
'IB'	Baleary
'IC'	Wyspy Kanaryjskie
'LR'	La Rioja
'M'	Madryt
'MU'	Murcia
'NA'	Navarra
'PV'	Kraj Basków.

2.88. RegionNumeric

Numeryczne odniesienie do regionu w określonym kraju.

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

Przypisanie wartości:

'00'H brak informacji

Hiszpania:

'01'H Andaluzja
 '02'H Aragonia
 '03'H Asturia
 '04'H Cantabria
 '05'H Katalonia
 '06'H Kastylia-León
 '07'H Kastylia-La Mancha
 '08'H Walencja
 '09'H Extremadura
 '0A'H Galicja
 '0B'H Baleary
 '0C'H Wyspy Kanaryjskie
 '0D'H La Rioja
 '0E'H Madryt
 '0F'H Murcia
 '10'H Navarra
 '11'H Kraj Basków.

2.89. RSAKeyModulus

Moduł pary kluczy RSA.

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

Przypisanie wartości: nieokreślona.

2.90. RSAKeyPrivateExponent

Wykładnik prywatny pary kluczy RSA.

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

Przypisanie wartości: nieokreślona.

2.91. RSAKeyPublicExponent

Wykładnik publiczny pary kluczy RSA.

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

Przypisanie wartości: nieokreślona.

2.92. SensorApprovalNumber

Numer homologacji typu czujnika.

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

Przypisanie wartości: nieokreślona.

2.93. SensorIdentification

Informacje przechowywane w czujniku ruchu dotyczące jego identyfikacji (wymaganie 077).

```
SensorIdentification ::= SEQUENCE {
    SensorSerialNumber          SensorSerialNumber,
    SensorApprovalNumber       SensorApprovalNumber,
    SensorSCIdentifier          SensorSCIdentifier,
    SensorOSIdentifier          SensorOSIdentifier
}
```

SensorSerialNumber jest rozszerzonym numerem fabrycznym czujnika ruchu (zawiera numer części i kod producenta).

SensorApprovalNumber jest numerem homologacji czujnika ruchu.

SensorSCIdentifier jest identyfikatorem elementu zabezpieczenia czujnika ruchu.

SensorOSIdentifier jest identyfikatorem systemu operacyjnego czujnika ruchu.

2.94. SensorInstallation

Informacje przechowywane w czujniku ruchu dotyczące jego instalacji (wymaganie 099).

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

SensorPairingDateFirst jest datą pierwszego sparowania czujnika ruchu z przyrządem rejestrującym.

FirstVuApprovalNumber jest numerem homologacji pierwszego przyrządu rejestrującego sparowanego z czujnikiem ruchu.

FirstVuSerialNumber jest numerem fabrycznym pierwszego przyrządu rejestrującego sparowanego z czujnikiem ruchu.

SensorPairingDateCurrent jest datą obecnego sparowania czujnika ruchu z przyrządem rejestrującym.

CurrentVuApprovalNumber jest numerem homologacji przyrządu rejestrującego obecnie sparowanego z czujnikiem ruchu.

CurrentVUSerialNumber jest numerem fabrycznym przyrządu rejestrującego obecnie sparowanego z czujnikiem ruchu.

2.95. SensorInstallationSecData

Informacje przechowywane na karcie warsztatowej dotyczące zabezpieczenia potrzebne do sparowania czujników ruchu z przyrządami rejestrującymi (wymaganie 214).

```
SensorInstallationSecData ::= TDesSessionKey
```

Przypisanie wartości: zgodnie z ISO 16844-3.

2.96. SensorOSIdentifier

Identyfikator systemu operacyjnego czujnika ruchu.

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

Przypisanie wartości: swoisty dla producenta.

2.97. SensorPaired

Informacje przechowywane w przyrządzie rejestrującym dotyczące identyfikacji czujnika ruchu sparowanego z przyrządem rejestrującym (wymaganie 079).

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

SensorSerialNumber jest numerem fabrycznym czujnika ruchu obecnie sparowanego z przyrządem rejestrującym.

SensorApprovalNumber jest numerem homologacji czujnika ruchu obecnie sparowanego z przyrządem rejestrującym.

SensorPairingDateFirst jest datą pierwszego sparowania z przyrządem rejestrującym czujnika ruchu obecnie sparowanego z przyrządem rejestrującym.

2.98. **SensorPairingDate**

Data sparowania czujnika ruchu z przyrządem rejestrującym.

`SensorPairingDate := TimeReal`

Przypisanie wartości: nieokreślona.

2.99. **SensorSerialNumber**

Numer fabryczny czujnika ruchu.

`SensorSerialNumber := ExtendedSerialNumber:`

2.100. **SensorSCIdentifier**

Identyfikator elementu zabezpieczenia czujnika ruchu.

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

Przypisanie wartości: element swoisty dla producenta.

2.101. **Signature**

Podpis cyfrowy.

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

Przypisanie wartości: zgodnie z dodatkiem 11, »Wspólne mechanizmy zabezpieczenia«.

2.102. **SimilarEventsNumber**

Liczba podobnych zdarzeń w jednym, określonym dniu (wymaganie 094).

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

Przypisanie wartości: 0 nie używany, 1 oznacza, że tylko jedno zdarzenie tego typu wystąpiło i jest zapamiętane dla tego dnia, 2 oznacza, że 2 zdarzenia wystąpiły w tym dniu (zapamiętane jest tylko jedno),... 255 oznacza, że 255 lub więcej zdarzeń wystąpiło w tym dniu.

2.103. **SpecificConditionType**

Kod identyfikujący stan szczególny (wymaganie 050b, 105a, 212a and 230a).

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

Przypisanie wartości:

'00'H	RFU
'01'H	poza zakresem — początek
'02'H	poza zakresem — zakończenie
'03'H	PRZEPRAWA PROMOWA/PRZEJAZD KOLEJOWY
'04'H .. 'FF'H	RFU.

2.104. **SpecificConditionRecord**

Informacje przechowywane na karcie kierowcy, karcie warsztatowej lub w przyrządzie rejestrującym dotyczące stanu szczególnego (wymaganie 105a, 212a and 230a).

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

EntryTime jest datą i godziną wprowadzenia danych.

SpecificConditionType jest kodem identyfikującym stan szczególny.

2.105. **Speed**

Prędkości pojazdu (km/godz).

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

Przypisanie wartości: kilometry na godzinę w zakresie operacyjnym 0 do 220 km/godz.

2.106. **SpeedAuthorised**

Maksymalne dozwolone prędkości pojazdu (definicja bb)).

```
SpeedAuthorised ::= Speed.
```

2.107. **SpeedAverage**

Prędkość średnia w uprzednio zdefiniowanym przedziale czasu (km/godz).

```
SpeedAverage ::= Speed.
```

2.108. **SpeedMax**

Prędkość maksymalna zmierzona w uprzednio zdefiniowanym przedziale czasu.

```
SpeedMax ::= Speed.
```

2.109. **TDesSessionKey**

Klucz sesyjny T-DES.

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

Przypisanie wartości: nie określa się.

2.110. **TimeReal**

Kod w polu zawierającym łącznie datę i godzinę, gdzie data i godzina są wyrażone w sekundach liczonych od godziny 00h.00m.00s. w dniu 1 stycznia 1970 r. GMT.

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

Przypisanie wartości – zapisane oktetami: liczba sekund od północy 1 stycznia 1970 r. GMT.

Maksymalna możliwa data/godzina wypada w 2106 r.

2.111. **TyreSize**

Oznaczenie wymiarów opon.

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

Przypisanie wartości: zgodnie z dyrektywą 92/23 (EWG) 31.3.1992, Dz.U. L 129, str. 95..

2.112. VehicleIdentificationNumber

Number identyfikacyjny pojazdu (VIN) odnoszący się do pojazdu jako całości, normalnie numer fabryczny nadwozia lub ramy.

VehicleIdentificationNumber ::= IA5String(SIZE(17))

Przypisanie wartości: zdefiniowany w ISO 3779.

2.113. VehicleRegistrationIdentification

Identyfikacja pojazdu, unikalna dla Europy (VRN i Państwo Członkowskie).

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

VehicleRegistrationNation jest państwem, w którym pojazd jest zarejestrowany.

VehicleRegistrationNumber jest numerem rejestracyjnym pojazdu (VRN).

2.114. VehicleRegistrationNumber

Numer rejestracyjny pojazdu (VRN). Numer rejestracyjny przydziela do pojazdu organ rejestracyjny.

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

CodePage określa stronę kodową według normy ISO/IEC 8859, używaną do zakodowania vehicleRegNumber,

VehicleRegNumber jest numerem VRN zakodowanym zgodnie z ISO/IEC 8859-codePage.

Przypisanie wartości: swoisty dla państwa.

2.115. VuActivityDailyData

Informacje przechowywane w VU dotyczące zmian czynności i/lub zmian stanu prowadzenia pojazdu i/lub zmian stanu karty dla określonego dnia kalendarzowego (wymaganie 084) i stanu szczelin o godzinie 00:00 tego dnia.

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

NoOfActivityChanges jest liczbą słów ActivityChangeInfo w zbiorze activityChangeInfos.

ActivityChangeInfos jest zbiorem słów ActivityChangeInfo przechowywanych w VU dla tego dnia. Zawsze zawiera dwa wyrazy ActivityChangeInfo opisujące stan dwóch szczelin o godzinie 00:00 tego dnia.

2.116. VuApprovalNumber

Numer homologacji typu przyrządu rejestrującego.

VuApprovalNumber ::= IA5String(SIZE(8))

Przypisanie wartości: nieokreślona.

2.117. VuCalibrationData

Informacje przechowywane w przyrządzie rejestrującym dotyczące kalibracji urządzenia rejestrującego (wymaganie 098).

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

NoOfVuCalibrationRecords jest liczbą zapisów w zbiorze vuCalibrationRecords.

vuCalibrationRecords jest zbiorem zapisów kalibracyjnych.

2.118. VuCalibrationRecord

Informacje przechowywane w przyrządzie rejestrującym dotyczące kalibracji urządzenia rejestrującego (wymaganie 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 jest celem kalibracji.

WorkshopName, **workshopAddress** są nazwą (nazwiskiem) i adresem warsztatu.

WorkshopCardNumber identyfikuje kartę warsztatową używaną przy kalibracji.

WorkshopCardExpiryDate jest datą ważności karty.

VehicleIdentificationNumber jest numerem VIN.

VehicleRegistrationIdentification zawiera numer VRN i Państwa Członkowskiego rejestracji.

WVehicleCharacteristicConstant jest współczynnikiem charakterystycznym pojazdu.

KConstantOfRecordingEquipment jest stałą urządzenia rejestrującego.

lTyreCircumference jest skutecznym obwodem tocznym kół.

TyreSize jest oznaczeniem rozmiaru opon zamontowanych w pojeździe.

AuthorisedSpeed jest dozwoloną prędkością pojazdu.

OldOdometerValue, **newOdometerValue** są starym i nowym stanem licznika kilometrów.

OldTimeValue, **newTimeValue** są starą i nową wartością daty i godziny.

NextCalibrationDate jest datą następnej kalibracji typu określonego w CalibrationPurpose, którą powinien przeprowadzić upoważniony organ kontrolny.

2.119. VuCardIWData

Informacje przechowywane w przyrządzie rejestrującym dotyczące cykli wkładania i wyjmowania kart dla kart kierowcy lub kart warsztatowych w przyrządzie rejestrującym (wymaganie 081).

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

noOfIWRecords jest liczbą zapisów w zbiorze vuCardIWRecords.

vuCardIWRecords jest zbiorem zapisów dotyczących cykli wkładania i wyjmowania kart.

2.120. VuCardIWRecord

Informacje przechowywane w przyrządzie rejestrującym dotyczące cykli wkładania i wyjmowania kart dla kart kierowcy lub kart warsztatowych w przyrządzie rejestrującym (wymaganie 081).

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

CardHolderName jest nazwiskiem i imionami posiadacza karty kierowcy lub warsztatowej zapisanymi na karcie.

FullCardNumber jest typem karty, Państwem Członkowskim wydającym kartę i numerem karty zapisanymi na karcie.

CardExpiryDate jest datą ważności karty zapisaną na karcie.

CardInsertionTime jest datą i godziną włożenia karty.

VehicleOdometerValueAtInsertion jest stanem licznika kilometrów przy wkładaniu karty.

CardSlotNumber jest szczeliną czytnika, do której karta jest włożona.

CardWithdrawalTime jest datą i godziną wyjęcia karty.

VehicleOdometerValueAtWithdrawal jest stanem licznika kilometrów przy wyjęciu karty.

PreviousVehicleInfo zawiera informacje o pojeździe poprzednio używanym przez kierowcę, zapisane na karcie.

ManualInputFlag jest flagą pokazującą, czy CardHolder przy wkładaniu karty wprowadził ręcznie czynności kierowcy.

2.121. VuCertificate

Certyfikat klucza publicznego przyrządu rejestrującego.

```
VuCertificate ::= Certificate
```

2.122. VuCompanyLocksData

Informacje przechowywane w przyrządzie rejestrującym dotyczące blokad firmowych (wymaganie 104).

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

NoOfLocks jest liczba blokad wyszczególnionych w vuCompanyLocksRecords.

VuCompanyLocksRecords jest zbiorem zapisów blokad firmowych.

2.123. VuCompanyLocksRecord

Informacje przechowywane w przyrządzie rejestrującym, dotyczące pojedynczej blokady firmowej (wymaganie 104).

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

LockInTime, **lockOutTime** są datą i godziną założenia i zdjęcia blokady.

CompanyName, **companyAddress** są nazwą (nazwiskiem) i adresem firmy związanej z założeniem blokady.

CompanyCardNumber identyfikuje kartę użytą przy założeniu blokady.

2.124. VuControlActivityData

Informacje przechowywane w przyrządzie rejestrującym, dotyczące kontroli przeprowadzonych przy użyciu tego VU (wymaganie 102).

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

NoOfControls jest liczbą kontroli wyszczególnionych w **vuControlActivityRecords**.

VuControlActivityRecords jest zbiorem zapisów czynności kontrolnych.

2.125. VuControlActivityRecord

Informacje przechowywane w przyrządzie rejestrującym, dotyczące kontroli przeprowadzonej przy użyciu tego VU (wymaganie 102).

```
VuControlActivityRecord ::= SEQUENCE {
    ControlType               ControlType,
    ControlTime               TimeReal,
    ControlCardNumber         FullCardNumber,
    DownloadPeriodBeginTime   TimeReal,
    DownloadPeriodEndTime     TimeReal
}
```

ControlType jest typem kontroli.

ControlTime jest datą i godziną kontroli.

ControlCardNumber identyfikuje kartę kontrolną użytą przy kontroli.

DownloadPeriodBeginTime jest czasem rozpoczęcia okresu, dla którego wczytano dane, w przypadku wczytywania danych.

DownloadPeriodEndTime jest czasem zakończenia okresu, dla którego wczytano dane, w przypadku wczytywania danych.

2.126. VuDataBlockCounter

Licznik zapisany na karcie pokazujący kolejno cykle wkładania/wyjmowania karty dla przyrządów rejestrujących.

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

Przypisanie wartości: kolejna liczba, po osiągnięciu wartości maksymalnej 9 999 liczenie rozpoczyna się ponownie od 0.

2.127. VuDetailedSpeedBlock

Informacje przechowywane w przyrządzie rejestrującym dotyczące szczegółowej prędkości pojazdu dla minuty, przez którą pojazd był w ruchu (wymaganie 093).

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

SpeedBlockBeginDate jest datą i godziną pierwszego odczytu prędkości w bloku.

SpeedsPerSecond jest chronologicznym ciągiem prędkości pomierzonych co sekunda w ciągu minuty rozpoczynającej się od godziny określonej w speedBlockBeginDate (włącznie).

2.128. VuDetailedSpeedData

Informacje przechowywane w przyrządzie rejestrującym dotyczące szczegółowej prędkości pojazdu.

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

NoOfSpeedBlocks jest liczbą bloków zarejestrowanych prędkości w zbiorze vuDetailedSpeedBlocks.

VuDetailedSpeedBlocks jest zbiorem bloków szczegółowej prędkości.

2.129. VuDownloadablePeriod

Najstarsza i najświeższa data i godzina, wyznaczające okres, dla którego przyrząd rejestrujący przechowuje dane dotyczące czynności kierowców (wymagania 081, 084 lub 087).

```
VuDownloadablePeriod ::= SEQUENCE {
    MinDownloadableTime         TimeReal
    MaxDownloadableTime         TimeReal
}
```

MinDownloadableTime jest przechowywaną w VU datą i godziną najstarszego włożenia karty lub zmiany czynności lub miejsca wprowadzania danych.

MaxDownloadableTime jest przechowywaną w VU datą i godziną ostatniego włożenia karty lub zmiany czynności lub miejsca wprowadzania danych.

2.130. VuDownloadActivityData

Informacje przechowywane w przyrządzie rejestrującym dotyczące ostatniego wczytywania danych (wymaganie 105).

```
VuDownloadActivityData ::= SEQUENCE {
    DownloadingTime              TimeReal,
    FullCardNumber               FullCardNumber,
    CompanyOrWorkshopName        Name
}
```

DownloadingTime jest datą i godziną wczytywania danych.

FullCardNumber identyfikuje kartę użytą do autoryzowania wczytywania danych.

CompanyOrWorkshopName jest nazwą (nazwiskiem) firmy lub warsztatu.

2.131. VuEventData

Informacje przechowywane w przyrządzie rejestrującym, dotyczące zdarzeń (wymaganie 094 z wyłączeniem przekroczenia prędkości).

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

NoOfVuEvents jest liczbą zdarzeń wyszczególnionych w zbiorze vuEventRecords.

VuEventRecords jest zbiorem zapisów dotyczących zdarzeń.

2.132. **VuEventRecord**

Informacje przechowywane w przyrządzie rejestrującym dotyczące zdarzenia (wymaganie 094 z wyłączeniem przekroczenia prędkości).

```
VuEventRecord ::= SEQUENCE {
    EventType                      EventFaultType,
    EventRecordPurpose            EventFaultRecordPurpose,
    EventBeginTime                TimeReal,
    EventEndTime                  TimeReal,
    CardNumberDriverSlotBegin     FullCardNumber,
    CardNumberCodriverSlotBegin   FullCardNumber,
    CardNumberDriverSlotEnd       FullCardNumber,
    CardNumberCodriverSlotEnd     FullCardNumber,
    SimilarEventsNumber           SimilarEventsNumber
}
```

EventType jest typem zdarzenia.

EventRecordPurpose jest celem, dla którego to zdarzenie jest zarejestrowane.

EventBeginTime jest datą i godziną rozpoczęcia zdarzenia.

EventEndTime jest datą i godziną zakończenia zdarzenia.

CardNumberDriverSlotBegin identyfikuje kartę włożoną do szczeliny karty kierowcy na początku zdarzenia.

CardNumberCodriverSlotBegin identyfikuje kartę włożoną do szczeliny karty współkierowcy na początku zdarzenia.

CardNumberDriverSlotEnd identyfikuje kartę włożoną do szczeliny karty kierowcy na końcu zdarzenia.

CardNumberCodriverSlotEnd identyfikuje kartę włożoną do szczeliny karty współkierowcy na końcu zdarzenia.

SimilarEventsNumber jest liczbą podobnych zdarzeń w tym dniu.

Sekwencji tej można używać dla wszystkich zdarzeń innych niż przekroczenie prędkości.

2.133. **VuFaultData**

Informacje przechowywane w przyrządzie rejestrującym dotyczące usterek (wymaganie 096).

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

NoOfVuFaults jest liczbą usterek wyszczególnionych w zbiorze vuFaultRecords.

VuFaultRecords jest zbiorem zapisów dotyczących usterek.

2.134. **VuFaultRecord**

Informacje przechowywane w przyrządzie rejestrującym dotyczące usterki (wymaganie 096).

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

FaultType jest typem usterki urządzenia rejestrującego.

FaultRecordPurpose jest celem, dla którego ta usterka jest zarejestrowana.

FaultBeginTime jest datą i godziną rozpoczęcia usterki.

FaultEndTime jest datą i godziną zakończenia usterki.

CardNumberDriverSlotBegin identyfikuje kartę włożoną do szczeliny karty kierowcy na początku usterki.

CardNumberCodriverSlotBegin identyfikuje kartę włożoną do szczeliny karty współkierowcy na początku usterki.

CardNumberDriverSlotEnd identyfikuje kartę włożoną do szczeliny karty kierowcy na końcu usterki.

CardNumberCodriverSlotEnd identyfikuje kartę włożoną do szczeliny karty współkierowcy na końcu usterki.

2.135. VuIdentification

Informacje przechowywane w przyrządzie rejestrującym dotyczące identyfikacji przyrządu rejestrującego (wymaganie 075).

```
VuIdentification ::= SEQUENCE {
    VuManufacturerName          VuManufacturerName,
    VuManufacturerAddress       VuManufacturerAddress,
    VuPartNumber                VuPartNumber,
    VuSerialNumber              VuSerialNumber,
    VuSoftwareIdentification     VuSoftwareIdentification,
    VuManufacturingDate         VuManufacturingDate,
    VuApprovalNumber            VuApprovalNumber
}
```

VuManufacturerName jest nazwą producenta przyrządu rejestrującego.

VuManufacturerAddress jest adresem producenta przyrządu rejestrującego.

VuPartNumber jest numerem części przyrządu rejestrującego.

VuSerialNumber jest numerem fabrycznym przyrządu rejestrującego.

VuSoftwareIdentification identyfikuje oprogramowanie zainstalowane w przyrządzie rejestrującym.

VuManufacturingDate jest datą produkcji przyrządu rejestrującego.

VuApprovalNumber jest numerem homologacji typu przyrządu rejestrującego.

2.136. VuManufacturerAddress

Adres producenta przyrządu rejestrującego.

```
VuManufacturerAddress ::= Address
```

Przypisanie wartości: nieokreślona.

2.137. VuManufacturerName

Nazwa producenta przyrządu rejestrującego.

```
VuManufacturerName ::= Name
```

Przypisanie wartości: nieokreślona.

2.138. VuManufacturingDate

Data produkcji przyrządu rejestrującego.

```
VuManufacturingDate ::= TimeReal
```

Przypisanie wartości: nieokreślona.

2.139. VuOverSpeedingControlData

Informacje przechowywane w przyrządzie rejestrującym dotyczące przekroczeń prędkości od ostatniej kontroli przekroczenia prędkości (wymaganie 095).

```
VuOverSpeedingControlData ::= SEQUENCE {
    LastOverspeedControlTime      TimeReal,
    FirstOverspeedSince           TimeReal,
    NumberOfOverspeedSince        OverspeedNumber
}
```

LastOverspeedControlTime jest datą i godziną ostatniej kontroli przekroczenia prędkości.

FirstOverspeedSince jest datą i godziną pierwszego przekroczenia prędkości po tej ostatniej kontroli przekroczenia prędkości.

NumberOfOverspeedSince jest liczbą zdarzeń przekroczenia prędkości od ostatniej kontroli przekroczenia prędkości.

2.140. VuOverSpeedingEventData

Informacje przechowywane w przyrządzie rejestrującym dotyczące zdarzeń przekroczenia prędkości (wymaganie 094).

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

NoOfVuOverSpeedingEvents jest liczbą zdarzeń wyszczególnionych w zbiorze vuOverSpeedingEventRecords.

VuOverSpeedingEventRecords jest zbiorem zapisów zdarzeń przekroczenia prędkości.

2.141. VuOverSpeedingEventRecord

Informacje przechowywane w przyrządzie rejestrującym dotyczące zdarzeń przekroczenia prędkości (wymaganie 094).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
    EventType                     EventFaultType,
    EventRecordPurpose            EventFaultRecordPurpose,
    EventBeginTime                TimeReal,
    EventEndTime                  TimeReal,
    MaxSpeedValue                 SpeedMax,
    AverageSpeedValue             SpeedAverage,
    CardNumberDriverSlotBegin     FullCardNumber,
    SimilarEventsNumber           SimilarEventsNumber
}
```

EventType jest typem zdarzenia.

EventRecordPurpose jest celem, dla którego zarejestrowano to zdarzenie.

EventBeginTime jest datą i godziną rozpoczęcia zdarzenia.

EventEndTime jest datą i godziną zakończenia zdarzenia.

MaxSpeedValue jest maksymalną prędkością pomierzoną w czasie zdarzenia.

AverageSpeedValue jest średnią arytmetyczną prędkości pomierzonych w czasie zdarzenia.

CardNumberDriverSlotBegin identyfikuje kartę włożoną do szczeliny karty kierowcy na początku zdarzenia.

SimilarEventsNumber jest liczbą podobnych zdarzeń w tym dniu.

2.142. VuPartNumber

Numer części przyrządu rejestrującego.

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

Przypisanie wartości: swoisty dla producenta VU.

2.143. VuPlaceDailyWorkPeriodData

Informacje przechowywane w przyrządzie rejestrującym dotyczące miejsc rozpoczęcia lub zakończenia dziennych okresów pracy kierowców (wymaganie 087).

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

NoOfPlaceRecords jest liczbą zapisów wyszczególnionych w zbiorze vuPlaceDailyWorkPeriodRecords.

VuPlaceDailyWorkPeriodRecords jest zbiorem zapisów dotyczących miejsca.

2.144. VuPlaceDailyWorkPeriodRecord

Informacje przechowywane w przyrządzie rejestrującym dotyczące miejsc rozpoczęcia lub zakończenia dziennego okresu pracy kierowcy (wymaganie 087).

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

FullCardNumber zawiera typ karty kierowcy, Państwo Członkowskie wydające kartę i numer karty.

PlaceRecord zawiera informacje dotyczące wprowadzonego miejsca.

2.145. VuPrivateKey

Klucz prywatny przyrządu rejestrującego.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.146. VuPublicKey

Klucz publiczny przyrządu rejestrującego.

```
VuPublicKey ::= PublicKey
```

2.147. VuSerialNumber

Numer fabryczny przyrządu rejestrującego (wymaganie 075).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.148. VuSoftInstallationDate

Data instalacji wersji oprogramowania przyrządu rejestrującego.

```
VuSoftInstallationDate ::= TimeReal
```

Przypisanie wartości: nieokreślona.

2.149. VuSoftwareIdentification

Informacje przechowywane w przyrządzie rejestrującym dotyczące zainstalowanego oprogramowania.

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

VuSoftwareVersion jest numerem wersji oprogramowania przyrządu rejestrującego.

VuSoftInstallationDate jest datą zainstalowania wersji oprogramowania.

2.150. VuSoftwareVersion

Numer wersji oprogramowania przyrządu rejestrującego.

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

Przypisanie wartości: nieokreślona.

2.151. VuSpecificConditionData

Informacje przechowywane w przyrządzie rejestrującym dotyczące stanów szczególnych.

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

NoOfSpecificConditionRecords jest liczbą zapisów wyszczególnionych w zbiorze **specificConditionRecords**.

SpecificConditionRecords jest zbiorem zapisów dotyczących stanów szczególnych.

2.152. VuTimeAdjustmentData

Informacje przechowywane w przyrządzie rejestrującym dotyczące regulacji czasu wykonanych poza regularną kalibracją (wymaganie 101).

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

NoOfVuTimeAdjRecords jest liczbą zapisów w zbiorze **vuTimeAdjustmentRecords**.

VuTimeAdjustmentRecords jest zbiorem zapisów dotyczących regulacji czasu.

2.153. VuTimeAdjustmentRecord

Informacje przechowywane w przyrządzie rejestrującym dotyczące regulacji czasu wykonanej poza regularną kalibracją (wymaganie 101).

```
VuTimeAdjustmentRecord ::= SEQUENCE {
    OldTimeValue                        TimeReal,
    OldTimeValue                        TimeReal,
    NewTimeValue                        TimeReal,
    WorkshopName                        Name,
    WorkshopAddress                     Address,
    WorkshopCardNumber                  FullCardNumber
}
```

OldTimeValue, **newTimeValue** są starymi i nowymi wartościami daty i godziny.

WorkshopName, **workshopAddress** są nazwą (nazwiskiem) i adresem warsztatu.

WorkshopCardNumber identyfikuje kartę warsztatową użytą do wykonania regulacji czasu.

2.154. W-VehicleCharacteristicConstant

Współczynnik charakterystyczny pojazdu (definicja k).

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

Przypisanie wartości: liczba impulsów na kilometr w zakresie operacyjnym 0 do 64 255 impulsów/km.

2.155. WorkshopCardApplicationIdentification

Informacje przechowywane na karcie warsztatowej dotyczące identyfikacji aplikacji na karcie (wymaganie 190).

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
    TypeOfTachographCardId          EquipmentType,
    CardStructureVersion             CardStructureVersion,
    NoOfEventsPerType               NoOfEventsPerType,
    NoOfFaultsPerType               NoOfFaultsPerType,
    ActivityStructureLength          CardActivityLengthRange,
    NoOfCardVehicleRecords          NoOfCardVehicleRecords,
    NoOfCardPlaceRecords            NoOfCardPlaceRecords,
    NoOfCalibrationRecords          NoOfCalibrationRecords
}
```

TypeOfTachographCardId określa wdrożony typ karty.

CardStructureVersion określa wersję struktury wdrożonej na karcie.

NoOfEventsPerType jest liczbą zdarzeń według typu zdarzenia możliwych do zarejestrowania na karcie.

NoOfFaultsPerType jest liczbą usterek według typu usterki możliwych do zarejestrowania na karcie.

ActivityStructureLength podaje liczbę bajtów dostępnych do zapisania zapisów czynności.

NoOfCardVehicleRecords jest liczbą zapisów dotyczących pojazdów możliwych do zarejestrowania na karcie.

NoOfCardPlaceRecords jest liczbą miejsc możliwych do zarejestrowania na karcie.

NoOfCalibrationRecords jest liczbą zapisów kalibracyjnych możliwych do zarejestrowania na karcie.

2.156. WorkshopCardCalibrationData

Informacje przechowywane na karcie warsztatowej dotyczące czynności warsztatowych wykonanych przy użyciu karty (wymagania 227 and 229).

```
WorkshopCardCalibrationData ::= SEQUENCE {
    CalibrationTotalNumber          INTEGER(0..216-1),
    CalibrationPointerNewestRecord  INTEGER(0..NoOfCalibrationRecords-1),
    CalibrationRecords              SET SIZE (NoOfCalibrationRecords)
                                   WorkshopCardCalibrationRecord
}
```

CalibrationTotalNumber jest całkowitą liczbą kalibracji wykonanych przy użyciu karty.

CalibrationPointerNewestRecord jest indeksem ostatniego, uaktualnionego zapisu kalibracyjnego.

Przypisanie wartości: Liczba odpowiadająca licznikowi zapisów kalibracyjnych, rozpoczynając od '0' dla pierwszego wystąpienia zapisu kalibracyjnego w strukturze.

CalibrationRecords jest zbiorem zapisów zawierających informacje o kalibracji i/lub regulacji czasu.

2.157. WorkshopCardCalibrationRecord

Informacje przechowywane na karcie warsztatowej dotyczące kalibracji wykonanej przy użyciu karty (wymaganie 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 jest celem kalibracji.

VehicleIdentificationNumber jest numerem VIN.

VehicleRegistration zawiera numer VRN i Państwa Członkowskiego rejestracji.

WVehicleCharacteristicConstant jest współczynnikiem charakterystycznym pojazdu.

KConstantOfRecordingEquipment jest stałą urządzenia rejestrującego.

LTyreCircumference jest skutecznym obwodem tocznym kół.

TyreSize jest oznaczeniem wymiarów opon zamontowanych w pojeździe.

AuthorisedSpeed jest maksymalną, dozwoloną prędkością pojazdu.

OldOdometerValue, newOdometerValue są starym i nowym stanem licznika kilometrów.

OldTimeValue, newTimeValue są starą i nową wartością daty i godziny.

NextCalibrationDate jest datą następnej kalibracji typu określonego w **CalibrationPurpose**, którą powinien przeprowadzić autoryzowany organ kontrolny.

VuPartNumber, vuSerialNumber i **sensorSerialNumber** są elementami danych do identyfikacji urządzenia rejestrującego.

2.158. WorkshopCardHolderIdentification

Informacje przechowywane na karcie warsztatowej dotyczące identyfikacji posiadacza karty (wymaganie 216).

```

WorkshopCardHolderIdentification ::= SEQUENCE {
    WorkshopName                Name,
    WorkshopAddress              Address,
    CardHolderName               HolderName,
    CardHolderPreferredLanguage  Language
}

```

WorkshopName jest nazwą (nazwiskiem) posiadacza karty warsztatowej.

WorkshopAddress jest adresem posiadacza karty warsztatowej.

CardHolderName jest nazwą (nazwiskiem) i imieniem (imionami) posiadacza karty (np. nazwiskiem mechanika).

CardHolderPreferredLanguage jest preferowanym językiem posiadacza karty.

2.159. WorkshopCardPIN

Osobisty numer identyfikacyjny (PIN) karty warsztatowej (wymaganie 213).

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

Przypisanie wartości: PIN znany CardHolder, z prawej strony wypełniony bajtami o wartości »FF« aż do 8 bajtów.

3. DEFINICJE WARTOŚCI I ZAKRESU WIELKOŚCI

Definicja wartości zmiennych używana w definicjach w ust. 2.

TimeRealRange := $2^{32}-1$

3.1. Definicje dla karty kierowcy:

Nazwa wartości zmiennej	Minimalnie	Maksymalnie
CardActivityLengthRange	5 544 bajty (28 dni 93 zmiany czynności na dzień)	13 776 bajtów (28 dni 240 zmian czynności na dzień)
NoOfCardPlaceRecords	84	112
NoOfCardVehicleRecords	84	200
NoOfEventsPerType	6	12
NoOfFaultsPerType	12	24

3.2. Definicje dla karty warsztatowej:

Nazwa wartości zmiennej	Minimalnie	Maksymalnie
CardActivityLengthRange	198 bajtów (1 dzień 93 zmiany czynności)	492 bajty (1 dzień 240 zmian czynności)
NoOfCardPlaceRecords	6	8
NoOfCardVehicleRecords	4	8
NoOfEventsPerType	3	3
NoOfFaultsPerType	6	6
NoOfCalibrationRecords	88	255

3.3. Definicje dla karty kontrolnej:

Nazwa wartości zmiennej	Minimalnie	Maksymalnie
NoOfControlActivityRecords	230	520

3.4. Definicje dla karty firmowej:

Nazwa wartości zmiennej	Minimalnie	Maksymalnie
NoOfCompanyActivityRecords	230	520

4. ZESTAWY ZNAKÓW

W łańcuchach IA5Strings używa się znaków ASCII zdefiniowanych w normie ISO/IEC 8824-1. Dla potrzeb czytelności i łatwego odwoływania się poniżej podano przypisanie wartości. W przypadku rozbieżności między tą uwagą a normą obowiązują przepisy normy ISO/IEC 8824-1.

```
! " # % & ' ( ) * + , - . / 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 { | } ~
```

W innych łańcuchach znaków (Address, Name, VehicleRegistrationNumber) używa się dodatkowo znaków zdefiniowanych kodami 192 do 255 normy ISO/IEC 8859-1 (zbiór znaków łacińskich 1) lub normy ISO/IEC 8859-7 (zbiór znaków greckich).

5. KODOWANIE

Przy kodowaniu zgodnie z zasadami ASN.1, wszystkie zdefiniowane typy danych koduje się zgodnie z wariantem unormowanym w ISO/IEC 8825-2.

Dodatek 2

SPECYFIKACJA KART DO TACHOGRAFÓW

Spis treści

1.	Wprowadzenie	377
1.1.	Skróty.	377
1.2.	Odniesienia	378
2.	Charakterystyki elektryczne i fizyczne	378
2.1.	Napięcie zasilające i pobór prądu	378
2.2.	Napięcie programowania V_{pp}	379
2.3.	Generowanie i częstotliwość zegara	379
2.4.	Styk We/Wy	379
2.5.	Stany karty	379
3.	Sprzęt i komunikacja	379
3.1.	Wprowadzenie	379
3.2.	Protokół komunikacyjny	379
3.2.1.	Protokoły	379
3.2.2.	ATR	380
3.2.3.	PTS	381
3.3.	Warunki dostępu (AC)	381
3.4.	Szyfrowanie danych	382
3.5.	Przegląd poleceń i kodów błędów	382
3.6.	Opis poleceń	383
3.6.1.	Wybór pliku (Select_file)	383
3.6.1.1.	Wybór przez nazwę (AID)	383
3.6.1.2.	Wybór pliku elementarnego przy pomocy identyfikatora pliku	384
3.6.2.	Odczyt binarny (Read_binary)	384
3.6.2.1.	Polecenie bez bezpiecznej wymiany komunikatów	385
3.6.2.2.	Polecenie z bezpieczną wymianą komunikatów	385
3.6.3.	Uaktualnianie binarne (Update_binary)	387
3.6.3.1.	Polecenie bez bezpiecznej wymiany komunikatów	387
3.6.3.2.	Polecenie z bezpieczną wymianą komunikatów	388
3.6.4.	Wydanie wezwania (Get_challenge)	389
3.6.5.	Weryfikacja (Verify)	389
3.6.6.	Przyjęcie odpowiedzi (Get response)	390
3.6.7.	PSO: Weryfikacja certyfikatu Verify_certificate	390
3.6.8.	Uwierzytelnianie wewnętrzne (Internal_authenticate)	391

3.6.9.	Uwierzytelnianie zewnętrzne (External_authenticate)	392
3.6.10.	Zarządzanie środowiskiem bezpieczeństwa (Manage security environment)	393
3.6.11.	PSO: HASH (haszowanie-mieszanie)	394
3.6.12.	Oblicz skrót pliku	394
3.6.13.	PSO: oblicz podpis cyfrowy	395
3.6.14.	PSO: skontroluj podpis cyfrowy	396
4.	Struktura kart do tachografów	396
4.1.	Struktura karty kierowcy	397
4.2.	Struktura karty warsztatowej	399
4.3.	Struktura karty kontrolnej	401
4.4.	Struktura karty firmowej	403

1. WPROWADZENIE

1.1. Skróty

Do celów niniejszego dodatku stosuje się następujące skróty:

AC	warunki dostępu
AID	identyfikator aplikacji
ALW	zawsze
APDU	jednostka danych protokołu aplikacji (struktura polecenia)
ATR	reakcja na sprowadzenie do stanu wyjściowego
AUT	uwierzytniony
C6, C7	styki 6 i 7 karty opisane w normie ISO/IEC 7816-2
Cc	cykle zegarowe
CHV	informacje weryfikacyjne posiadacza karty
CLA	bajt klasy polecenia APDU
DF	plik dedykowany. DF może zawierać inne pliki (EF lub DF)
EF	plik elementarny
ENC	zaszyfrowany: dostęp możliwy tylko poprzez kodowane dane
Etu	elementarna jednostka czasu
IC	układ scalony
ICC	karta z układem scalonym
ID	identyfikator
IFD	urządzenie interfejsu
IFS	wielkość pola informacyjnego
IFSC	wielkość pola informacyjnego dla karty
IFSD	wielkość pola informacyjnego dla urządzenia (dla terminala)
INS	bajt instrukcji w poleceniu APDU
Lc	długość danych wejściowych dla polecenia APDU
Le	długość danych oczekiwanych (dane wyjściowe dla polecenia)
MF	plik główny (root DF)
P1-P2	bajty parametryczne
NAD	adres węzła używany w protokole T=1
NEV	nigdy
PIN	osobisty numer identyfikacyjny
PRO SM	chroniony z bezpieczną wymianą komunikatów
PTS	wybór protokołu transmisyjnego
RFU	zastrzeżony do wykorzystania w przyszłości

RST	sprowadzenie do stanu wyjściowego (karty)
SM	bezpieczna wymiana komunikatów
SW1-SW2	bajty stanu
TS	początkowy znak ATR
VPP	napięcie programowania
XXh	wartość XX w zapisie heksadecymalnym
	symbol konkatencji 03 04=0304.

1.2. Odniesienia

W niniejszym dodatku używa się następujących odniesień:

EN 726-3	Systemy identyfikacji kart — Telekomunikacyjne karty i terminale z układami scalonymi — część 3: Wymagania dla kart niezależne od aplikacji. Grudzień 1994 r.
ISO/IEC 7816-2	Informatyka — Identyfikacja kart — Karty z układami scalonymi ze stykami — część 2: Wymiary i rozmieszczenie styków. Wydanie pierwsze: 1999 r.
ISO/IEC 7816-3	Informatyka — Identyfikacja kart — Karty z układami scalonymi ze stykami — część 3: Sygnały elektryczne i protokół komunikacyjny. Wydanie 2: 1997 r.
ISO/IEC 7816-4	Informatyka — Identyfikacja kart — Karty z układami scalonymi ze stykami — część 4: Międzybranżowe polecenia wymiany informacji. Wydanie pierwsze: 1995 + Nowelizacja 1: 1997 r.
ISO/IEC 7816-6	Informatyka — Identyfikacja kart — Karty z układami scalonymi ze stykami — część 6: Międzybranżowe elementy danych. Wydanie pierwsze: 1996 + Popr. 1: 1998 r.
ISO/IEC 7816-8	Informatyka — Identyfikacja kart — Karty z układami scalonymi ze stykami — część 8: Polecenia międzybranżowe związane z bezpieczeństwem. Wydanie pierwsze: 1999 r.
ISO/IEC 9797	Informatyka — Techniki bezpieczeństwa — Mechanizm integralności danych wykorzystujący funkcję kontroli kryptograficznej używającą algorytmu szyfru blokowego. Wydanie 2: 1994 r.

2. CHARAKTERYSTYKI ELEKTRYCZNE I FIZYCZNE

TCS_200 Wszystkie sygnały elektryczne są zgodne z normą ISO/IEC 7816-3, chyba że określono inaczej.

TCS_201 Rozmieszczenie i wymiary styków kart są zgodne z normą ISO/IEC 7816-2.

2.1. Napięcie zasilające i pobór prądu

TCS_202 Karta pracuje zgodnie ze specyfikacją przy poborze w granicach określonych w normie ISO/IEC 7816-3.

TCS_203 Karta pracuje z $V_{cc} = 3 \text{ V}$ (+/- 0,3 V) lub $V_{cc} = 5 \text{ V}$ (+/- 0,5 V).

Wybór napięcia odbywa się zgodnie z normą ISO/IEC 7816-3.

2.2. Napięcie programowania V_{pp}

- TCS_204 Karta nie wymaga napięcia programowania na styku C6. Oczekuje się, że styk C6 nie jest przyłączony w IFD. Styk C6 może być przyłączony do V_{cc} na karcie, ale nie może być przyłączony do masy. W żadnym przypadku napięcie to nie może być interpretowane.

2.3. Generowanie i częstotliwość zegara

- TCS_205 Karta pracuje w zakresie częstotliwości 1 do 5 MHz. W czasie jednej sesji karty częstotliwość zegara może zmieniać się w granicach $\pm 2\%$. Częstotliwość zegara generuje przyrząd rejestrujący a nie karta. Cykl pracy może zmieniać się w granicach 40 do 60 %.
- TCS_206 W warunkach określonych na karcie w pliku EF_{ICC}, zewnętrzny zegar może zostać zatrzymany. Pierwszy bajt treści pliku EF_{ICC} koduje warunki trybu pracy Clockstop (szczegóły znajdują się w EN 726-3):

Niski	Wysoki		
Bit 3	Bit 2	Bit 1	
0	0	1	Clockstop dozwolony, brak preferowanego poziomu
0	1	1	Clockstop dozwolony, preferowany poziom wysoki
1	0	1	Clockstop dozwolony, preferowany poziom niski
0	0	0	Clockstop niedozwolony
0	1	0	Clockstop dozwolony tylko przy wysokim poziomie
1	0	0	Clockstop dozwolony tylko przy niskim poziomie

Bitów 4 do 8 nie używa się.

2.4. Styk We/Wy

- TCS_207 Styk We/Wy C7 służy do odbierania i wysyłania danych do IFD. W czasie pracy tylko karta albo tylko IFD jest w trybie nadawania. Gdyby jednak obie jednostki jednocześnie znalazły się w trybie nadawania, nie może to spowodować uszkodzenia karty. Karta wchodzi do trybu odbioru, chyba że nadaje dane.

2.5. Stany karty

- TCS_208 Gdy podawane jest napięcie zasilające, karta pracuje w stanach:

- stan operacyjny, gdy karta wykonuje polecenia lub jest połączona z jednostką cyfrową,
- stan jałowy we wszystkich pozostałych sytuacjach; w tym stanie karta zachowuje wszystkie dane.

3. SPRZĘT I KOMUNIKACJA

3.1. Wprowadzenie

W punkcie tym opisano minimalną funkcjonalność wymaganą od kart do tachografów i VU w celu zagwarantowania prawidłowego funkcjonowania i interoperacyjności.

Karty do tachografów są zgodne, na ile tylko możliwe, z obowiązującymi normami ISO/IEC (w szczególności z normą ISO/IEC 7816). Niemniej jednak szczegółowo opisano polecenia i protokoły w celu określenia pewnych ograniczonych zastosowań lub różnic, o ile występują. Opisane polecenia są w pełni zgodne z przywołanymi normami, jeżeli nie wskazano inaczej.

3.2. Protokół komunikacyjny

- TCS_300 Protokół komunikacyjny jest zgodny z normą ISO/IEC 7816-3. W szczególności VU rozpoznaje wysyłane przez kartę przedłużenia czasu oczekiwania.

3.2.1. Protokoły

- TCS_301 Karta obsługuje oba protokoły T=0 i T=1.

TCS_302 T=0 jest protokołem domyślnym, dlatego też polecenie PTS jest niezbędne do zmiany protokołu na T=1.

TCS_303 Urządzenia stosują konwencję bezpośrednią w obu protokołach: tak więc konwencja bezpośrednia jest obowiązkowa dla karty.

TCS_304 Bajt informacji o wielkości pola karty znajduje się w ATR w znaku TA3. Wartość ta jest nie mniejsza niż 'F0h' (= 240 bajtów).

Do protokołów stosuje się następujące ograniczenia:

TCS_305 T=0

- Urządzenie interfejsu wspiera odpowiedź na We/Wy po wzroście krawędzi narastającego sygnału na RST z 400 cc.
- Urządzenie interfejsu potrafi odczytać znaki rozdzielone 12 etu.
- Urządzenie interfejsu odczytuje błędny znak i jego powtórzenie, jeżeli rozdzielone 13 etu. W przypadku wykrycia błędnego znaku, na We/Wy znajduje się sygnał błędu między 1 etu a 2 etu. Urządzenie obsługuje opóźnienie 1 etu.
- Urządzenie interfejsu akceptuje 33-bajtowe ATR (TS+32)
- Jeżeli TC1 znajduje się w ATR, to dla znaków wysyłanych przez urządzenie interfejsu jest dodatkowy czas ochronny (Extra Guard Time), chociaż znaki wysyłane przez kartę mogą być jeszcze przedzielone odstępami 12 etu. Odnosi się to także do znaku ACK wysyłanego przez kartę po wysłaniu znaku P3 przez urządzenie interfejsu.
- Urządzenie interfejsu bierze pod uwagę znak NUL wysyłany przez kartę.
- Urządzenie interfejsu akceptuje tryb uzupełniający dla ACK.
- Polecenia odbierz-odpowiedź (get-response) nie można używać w trybie łańcuchowym do otrzymywania danych, których długość może być większa niż 255 bajtów.

TCS_306 T=1

- Bajt NAD: nieużywany (NAD ustawia się na '00').
- S-block ABORT: nieużywany.
- Błąd stanu S-block VPP: nieużywany.
- Całkowita długość łańcucha dla pola danych nie może przekraczać 255 bajtów (IFD musi to zapewniać).
- IFD bezpośrednio po ATR podaje wielkość pola informacyjnego dla urządzenia (IFSD): IFD wysyła żądanie S-Block IFS po ATR a karta odpowiada S-Block IFS. Zalecaną wartością dla IFSD są 254 bajty.
- Karta nie pyta o skorygowane IFS.

3.2.2. ATR

TCS_307 Urządzenie sprawdza bajty ATR, zgodnie z normą ISO/IEC 7816-3. Nie wykonuje się weryfikacji znaków historycznych ATR.

Przykład podstawowego Biprotocol ATR zgodnego z normą ISO/IEC 7816-3

Znak	Wartość	Uwagi
TS	'3Bh'	wskazuje konwencję bezpośrednią
T0	'85h'	TD1 obecny; jest 5 bajtów historycznych
TD1	'80h'	TD2 obecny; będzie użyty T=0
TD2	'11h'	TA3 obecny; będzie użyty T=1
TA3	'XXh' (mind. 'F0h')	wielkość pola informacyjnego dla karty (IFSC)
TH1 bis TH5	'XXh'	znaki historyczne
TCK	'XXh'	znak kontrolny (exclusive OR)

TCS_308 Po ATR wybierany jest domyślnie plik główny (MF) i staje się katalogiem bieżącym.

3.2.3. PTS

TCS_309 Domyślnym protokołem jest T=0. Aby wybrać protokół T=1, urządzenie musi wysłać do karty PTS (znane też jako PPS).

TCS_310 Jako że oba protokoły T=0 i T=1 są wymagane dla karty, podstawowy PTS do przełączania między protokołami wymagany jest dla karty.

PTS można używać, jak wskazano w normie ISO/IEC 7816-3, do przełączania na szybkości transmisji większe niż standardowa, proponowane przez kartę w ATR, gdy dotyczy (bajt TA(1)).

Większe szybkości transmisji są opcjonalne dla karty.

TCS_311 Jeżeli karta nie obsługuje innej szybkości transmisji niż standardowa (lub jeżeli nie obsługuje wybranej szybkości transmisji), karta odpowiada na PTS prawidłowo, zgodnie z normą ISO/IEC 7816-3, opuszczając bajt PPS1.

Poniżej pokazano przykłady podstawowego PTS do wyboru protokołu:

Znak	Wartość	Uwagi
PPSS	'FFh'	znak inicjujący
PPS0	'00h' lub '01h'	nie ma PPS1 do PPS3; '00h', aby wybrać T0, '01h', aby wybrać T1
PK	'XXh'	znak kontrolny: 'XXh' = 'FFh', jeżeli PPS0 = '00h'; 'XXh' = 'FEh', jeżeli PPS0 = '01h'

3.3. Warunki dostępu (AC)

Warunki dostępu, (AC) dla poleceń, UPDATE_BINARY i READ_BINARY definiuje się dla każdego pliku elementarnego.

TCS_312 AC bieżącego pliku muszą być spełnione przed dostępem do pliku za pośrednictwem tych poleceń.

Definicje dostępnych warunków dostępu są następujące:

- ALW: operacja jest zawsze możliwa i może być wykonywana bez ograniczeń.
- NEV: operacja nie jest nigdy możliwa.
- AUT: prawo odpowiadające pomyślnemu, zewnętrznemu uwierzytelnianiu musi być otwarte (zrobiono poleceniem EXTERNAL_AUTHENTICATE).
- PRO SM: polecenie musi być przesłane z kryptograficzną sumą kontrolną, wykorzystując bezpieczną wymianę komunikatów (patrz dodatek 11).
- AUT i PRO SM (połączone)

Przy poleceniach przetwarzania (UPDATE_BINARY i READ_BINARY), w karcie mogą być ustawione następujące warunki dostępu:

	UPDATE_BINARY	READ_BINARY
ALW	tak	tak
NEV	tak	tak
AUT	tak	tak
PRO SM	tak	nie
AUT i PRO SM	tak	nie

warunek dostępu PRO SM nie jest dostępny dla polecenia READ_BINARY. Oznacza to, że dla polecenia READ nigdy nie jest obowiązkowa obecność kryptograficznej sumy kontrolnej. Jednakże, używając wartości 'OC' dla klasy, można używać polecenia READ_BINARY w bezpiecznej wymianie komunikatów, jak opisano w punkcie 3.6.2.

3.4. Szyfrowanie danych

W przypadku gdy trzeba chronić poufność danych, które mają być odczytane z pliku, plik jest oznakowany »Encrypted«. Szyfrowanie wykonuje się poprzez stosowanie bezpiecznej wymiany komunikatów (patrz dodatek 11).

3.5. Przegląd poleceń i kodów błędów

Polecenia i organizacja pliku wynikają z normy ISO/IEC 7816-4 i spełniają jej wymagania.

TCS_313 W części tej opisano następujące pary polecenie-odpowiedź dla APDU:

Polecenie	INS
SELECT FILE	A4
READ BINARY	B0
UPDATE BINARY	D6
GET CHALLENGE	84
VERIFY	20
GET RESPONSE	C0
WYKONAJ OPERACJĘ BEZPIECZEŃSTWA: VERIFY CERTIFICATE COMPUTE DIGITAL SIGNATURE VERIFY DIGITAL SIGNATURE HASH	2A
INTERNAL AUTHENTICATE	88
EXTERNAL AUTHENTICATE	82
ZARZĄDZANIE ŚRODOWISKIEM BEZPIECZEŃSTWA: SETTING A KEY	22
WYKONAJ HASZOWANIE (MIESZANIE) PLIKÓW	2A

TCS_314 Wyrazy stanu SW1 SW2 są zwracane w komunikacie odpowiedzi i oznaczają stan przetwarzania polecenia.

SW1	SW2	Znaczenie
90	00	Normalne przetwarzanie
61	XX	Normalne przetwarzanie. XX = liczba dostępnych bajtów odpowiedzi
62	81	Przetwarzanie ostrzeżenia. Część zwracanych danych może być uszkodzona
63	CX	Nieprawidłowe CHV (PIN). 'X' oznacza licznik pozostałych prób
64	00	Błąd wykonania — Stan pamięci nieulotnej bez zmian. Błąd integralności
65	00	Błąd wykonania — Stan pamięci nieulotnej zmieniony
65	81	Błąd wykonania — Stan pamięci nieulotnej zmieniony — Uszkodzona pamięć
66	88	Błąd zabezpieczenia: nieprawidłowa kryptograficzna suma kontrolna (w czasie bezpiecznej wymiany komunikatów) lub nieprawidłowy certyfikat (w czasie weryfikacji certyfikatu), lub nieprawidłowy kryptogram (w czasie zewnętrznego uwierzytelniania) lub nieprawidłowy podpis (w czasie weryfikacji podpisu)
67	00	Nieprawidłowa długość (nieprawidłowe Lc lub Le)
69	00	Niedozwolone polecenie (brak dostępnej odpowiedzi w T=0)
69	82	Niespełniony stan zabezpieczenia
69	83	Metoda uwierzytelnienia zablokowana
69	85	Warunki użycia niespełnione
69	86	Polecenie niedozwolone (brak bieżącego EF)
69	87	Brak oczekiwanych obiektów danych w bezpiecznej wymianie komunikatów
69	88	Nieprawidłowe obiekty danych w bezpiecznej wymianie komunikatów
6A	82	Nie znaleziono pliku
6A	86	Nieprawidłowe parametry P1-P2
6A	88	Nie znaleziono powołanych danych
6B	00	Nieprawidłowe parametry (przesunięcie poza EF)

SW1	SW2	Znaczenie
6C	XX	Nieprawidłowa długość, SW2 wskazuje dokładną długość. Pole danych nie jest zwracane
6D	00	Kod instrukcji nieobsługiwany lub nieważny
6E	00	Klasa nieobsługiwana
6F	00	Inne błędy kontroli

3.6. Opis poleceń

W tym rozdziale opisano polecenia dla kart do tachografów, które są obowiązkowe.

Dodatkowe, szczegółowe informacje dotyczące stosowanych czynności kryptograficznych zamieszczono w dodatku 11 Wspólne mechanizmy zabezpieczenia.

Wszystkie polecenia opisane są niezależnie od używanego protokołu (T=0 lub T=1). Bajty CLA, INS, P1, P2, Lc i Le w APDU są zawsze wskazywane. Jeżeli Lc lub Le nie jest potrzebny dla opisywanego polecenia, związane z nimi długość, wartość i opis są puste.

TCS_315 Jeżeli żądane są oba bajty długości (Lc i Le), opisywane polecenie musi być podzielone na dwie części, jeśli IFD używa protokołu T=0: IFD wysyła to polecenie z P3=Lc + dane i następnie wysyła polecenie GET_RESPONSE (patrz pkt 3.6.6) z P3=Le.

TCS_316 Jeżeli żądane są oba bajty długości i Le=0 (bezpieczna wymiana komunikatów):

- gdy używany jest protokół T=1, karta odpowiada na Le=0 wysyłając wszystkie, dostępne dane wyjściowe,
- gdy używany jest protokół T=0, IFD wysyła pierwsze polecenie z P3=Lc + dane, karta odpowiada (na to niejawne Le=0) bajtami stanu '61La', gdzie La jest liczbą dostępnych bajtów odpowiedzi. Następnie IFD generuje polecenie GET_RESPONSE z P3=La w celu odczytania danych.

3.6.1. Select file (Wybierz plik)

Polecenie to jest zgodne z normą ISO/IEC 7816-4, ale jego zastosowanie jest ograniczone w porównaniu z poleceniem zdefiniowanym w tej normie.

Polecenia SELECT FILE używa się:

- do wybierania aplikacji DF (musi być wybór przez nazwę)
- do wybierania pliku elementarnego odpowiadającego przekazanemu IP pliku.

3.6.1.1. Wybór przez nazwę (AID)

Polecenie to pozwala wybrać aplikację DF na karcie.

TCS_317 Polecenie to można wykonywać z dowolnego miejsca w strukturze pliku (po ATR lub w dowolnym czasie).

TCS_318 Wybór aplikacji powoduje przywrócenie bieżącego stanu środowiska bezpieczeństwa do stanu wyjściowego. Po wybraniu aplikacji, żaden bieżący klucz publiczny nie jest wybrany, a klucz poprzedniej sesji nie jest dostępny dla bezpiecznej wymiany komunikatów. Także warunek dostępu AUT jest utracony.

TCS_319 Komunikat polecenia

Bajt	Długość	Wartość	Opis
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'04h'	wybór przez nazwę (AID)
P2	1	'0Ch'	brak oczekiwanej odpowiedzi
Lc	1	'NNh'	liczba bajtów wysłanych do karty (długość AID): '06h' dla aplikacji tachograficznej
#6-#(5+NN)	NN	'XX..XXh'	AID: 'FF 54 41 43 48 4F' dla aplikacji tachograficznej

Dla polecenia SELECT FILE nie jest potrzebna żadna odpowiedź (brak Le w T=1, lub nie ma żądania odpowiedzi w T=0).

TCS_320 Komunikat odpowiedzi (brak żądania odpowiedzi)

Bajt	Długość	Wartość	Wyszczególnienie
SW	2	'XXXXh'	Wyrazy stanu (SW1, SW2)

- jeżeli wykonanie zakończyło się pomyślnie, karta zwraca '9000',
- jeżeli nie znaleziono aplikacji wyszczególnionej przez AID, zwróconym stanem przetwarzania jest '6A82',
- w T=1, jeżeli jest bajt Le, zwróconym stanem jest '6700',
- w T=0, jeżeli po poleceniu SELECT FILE wymaga się odpowiedzi, zwróconym stanem jest '6900',
- jeżeli wybrana aplikacja uznana jest za uszkodzoną (znaleziony błąd integralności w atrybutach pliku), zwróconym stanem przetwarzania jest '6400' lub '6581'.

3.6.1.2. Wybór pliku elementarnego przy pomocy identyfikatora pliku

TCS_321 Komunikat polecenia

Bajt	Długość	Wartość	Wyszczególnienie
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'02h'	wybór EF pod bieżącym DF
P2	1	'0Ch'	brak oczekiwanej odpowiedzi
Lc	1	'02h'	liczba bajtów wysłanych do karty
#6-#7	2	'XXXXh'	identyfikator pliku

Dla polecenia SELECT FILE nie jest potrzebna żadna odpowiedź (brak Le w T=1, lub nie ma żądania odpowiedzi w T=0).

TCS_322 Komunikat odpowiedzi (brak żądania odpowiedzi)

Bajt	Długość	Wartość	Wyszczególnienie
SW	2	'XXXXh'	Wyrazy stanu (SW1, SW2)

- Jeżeli wykonanie zakończyło się pomyślnie, karta zwraca '9000',
- jeżeli nie znaleziono pliku odpowiadającego identyfikatorowi pliku, zwróconym stanem przetwarzania jest '6A82',
- w T=1, jeżeli jest bajt Le, zwróconym stanem jest '6700',
- w T=0, jeżeli po poleceniu SELECT FILE wymaga się odpowiedzi, zwróconym stanem jest '6900',
- jeżeli wybrany plik uznany jest za uszkodzony, (znaleziony błąd integralności w atrybutach pliku), zwróconym stanem przetwarzania jest '6400' lub '6581'.

3.6.2. **Read Binary (Odczyt binarny)**

Polecenie to jest zgodne z normą ISO/IEC 7816-4, ale jego zastosowanie jest ograniczone w porównaniu z poleceniem zdefiniowanym w tej normie.

Polecenie READ BINARY służy do odczytu danych z przezroczystego pliku.

Odpowiedź karty obejmuje zwrot odczytanych danych, opcjonalnie obudowane w strukturę bezpiecznej wymiany komunikatów.

TCS_323 Polecenie może być wykonane tylko wtedy gdy stan zabezpieczenia spełnia atrybuty zabezpieczenia zdefiniowane dla EF dla funkcji READ.

3.6.2.1. Polecenie bez bezpiecznej wymiany komunikatów

Polecenie to umożliwia IFD odczyt danych z bieżąco wybranego EF bez bezpiecznej wymiany komunikatów.

TCS_324 Odczyt danych z pliku oznakowanego »Encrypted« przy pomocy tego polecenia nie jest możliwy.

TCS_325 Komunikat polecenia

Bajt	Długość	Wartość	Wyszczególnienie
CLA	1	'00h'	bez bezpiecznej wymiany komunikatów
INS	1	'B0h'	
P1	1	'XXh'	przesunięcie w bajtach od początku pliku: bajt najbardziej znaczący
P2	1	'XXh'	przesunięcie w bajtach od początku pliku: bajt najmniej znaczący
Le	1	'XXh'	oczekiwana długość danych. Liczba bajtów do odczytu

Uwaga: bit 8 w P1 musi być ustawiony na 0.

TCS_326 Komunikat odpowiedzi

Bajt	Długość	Wartość	Wyszczególnienie
#1-#X	X	'XX..XXh'	odczyt danych
SW	2	'XXXXh'	Wyrazy stanu (SW1, SW2)

- Jeżeli wykonanie zakończyło się pomyślnie, karta zwraca '9000',
- jeżeli nie wybrano EF, zwróconym stanem przetwarzania jest '6986',
- jeżeli wymagania kontroli dostępu wybranego pliku nie są spełnione, polecenie zostaje przerwane z '6982',
- jeżeli przesunięcie nie jest zgodne z wielkością EF (przesunięcie > wielkość EF), zwróconym stanem przetwarzania jest '6B00',
- jeżeli wielkość danych nie jest zgodna z wielkością EF (przesunięcie + Le > wielkość EF), zwróconym stanem przetwarzania jest '6700' lub '6Cxx', gdzie 'xx' wskazuje dokładną długość,
- jeżeli błąd integralności zostaje wykryty w atrybutach pliku, karta uznaje, że plik jest uszkodzony i nienaprawialny, a zwróconym stanem przetwarzania jest '6400' lub '6581',
- jeżeli błąd integralności zostaje wykryty w zgromadzonych danych, karta zwraca żądane dane, a zwróconym stanem przetwarzania jest '6281'.

3.6.2.2. Polecenie z bezpieczną wymianą komunikatów

Polecenie to umożliwia IDF odczyt danych z bieżąco wybranego EF z bezpieczną wymianą komunikatów, w celu weryfikowania integralności odebranych danych ochrony poufności danych, w przypadku gdy EF jest oznakowany »Encrypted«.

TCS_327 Komunikat polecenia

Bajt	Długość	Wartość	Opis
CLA	1	'0Ch'	żądana bezpieczna wymiana komunikatów
INS	1	'B0h'	INS
P1	1	'XXh'	P1 (przesunięcie w bajtach od początku pliku): bajt najbardziej znaczący
P2	1	'XXh'	P2 (przesunięcie w bajtach od początku pliku): bajt najmniej znaczący
Lc	1	'09h'	długość danych wejściowych dla bezpiecznej wymiany komunikatów
#6	1	'97h'	T _{LE} : znacznik specyfikacji oczekiwanej długości
#7	1	'01h'	L _{LE} : długość oczekiwanej długości
#8	1	'NNh'	specyfikacja oczekiwanej długości (początkowy Le): liczba bajtów do odczytu

Bajt	Długość	Wartość	Opis
#9	1	'8Eh'	T _{CC} : znacznik kryptograficznej sumy kontrolnej
#10	1	'04h'	L _{CC} : długość znajdującej się dalej kryptograficznej sumy kontrolnej
#11-#14	4	'XX..XXh'	kryptograficzna suma kontrolna (4 bajty najbardziej znaczące)
Le	1	'00h'	wg specyfikacji w normie ISO/EWG 7816-4

TCS_328 Komunikat odpowiedzi, jeżeli EF nie ma oznakowania »Encrypted« i jeżeli format wejściowy bezpiecznej wymiany komunikatów jest prawidłowy:

Bajt	Długość	Wartość	Opis
#1	1	'81h'	T _{PV} : znacznik wartości danych odkrytych
#2	L	'NNh' lub '81 NNh'	L _{PV} : długość zwracanych danych (= początkowemu Le) L 2 ma 2 bajty, jeżeli L _{PV} > 127 bajtów
#(2+L)-#(1+L+NN)	NN	'XX..XXh'	wartość danych odkrytych
#(2+L+NN)	1	'8Eh'	T _{CC} : znacznik kryptograficznej sumy kontrolnej
#(3+L+NN)	1	'04h'	L _{CC} : długość znajdującej się dalej kryptograficznej sumy kontrolnej
#(4+L+NN)-#(7+L+NN)	4	'XX..XXh'	kryptograficzna suma kontrolna (4 bajty najbardziej znaczące)
SW	2	'XXXXh'	Wyrazy stanu (SW1, SW2)

TCS_329 Komunikat odpowiedzi, jeżeli EF ma oznakowanie »Encrypted« i jeżeli format wejściowy bezpiecznej wymiany komunikatów jest prawidłowy:

Bajt	Długość	Wartość	Opis
#1	1	'87h'	T _{PI CG} : znacznik zaszyfrowanych danych (kryptogram)
#2	L	'MMh' lub '81 MMh'	L _{PI CG} : długość zwracanych zaszyfrowanych danych (różna od początkowego Le z polecenia, ze względu na wypełnienie) L ma 2 bajty, jeżeli L _{PV} > 127 bajtów
#(2+L)-#(1+L+MM)	MM	'01XX..XXh'	dane szyfrowane: wskaźnik wypełnienia i kryptogram
#(2+L+MM)	1	'8Eh'	T _{CC} : znacznik kryptograficznej sumy kontrolnej
#(3+L+MM)	1	'04h'	L _{CC} : długość znajdującej się dalej kryptograficznej sumy kontrolnej
#(4+L+MM)-#(7+L+MM)	4	'XX..XXh'	kryptograficzna suma kontrolna (4 bajty najbardziej znaczące)
SW	2	'XXXXh'	Wyrazy stanu (SW1, SW2)

Pierwszy bajt zwracanych danych wskazuje na zastosowany tryb wypełnienia. W przypadku aplikacji tachograficznej, wskaźnik wypełnienia zawsze przyjmuje wartość '01h', wskazując że zastosowany tryb wypełnienia jest jednym z określonych w normie ISO/IEC 7816-4 (jeden bajt o wartości '80h' i następnie pewna ilość bajtów zerowych: ISO/IEC 9797 metoda 2).

Stany »regularnego« przetwarzania, opisane dla polecenia READ BINARY, bez bezpiecznej wymiany komunikatów (patrz pkt 3.6.2.1), mogą być zwracane przy użyciu struktur komunikatu odpowiedzi opisanego powyżej, za znacznikiem '99h' Tag (jak opisano w TCS 335).

Ponadto mogą wystąpić niektóre błędy, swoiście dotyczące bezpiecznej wymiany komunikatów. W takim przypadku zwracany jest po prostu stan przetwarzania bez struktury bezpiecznej wymiany komunikatów:

TCS_330 Komunikat odpowiedzi przy nieprawidłowym formacie wejściowym bezpiecznej wymiany komunikatów

Bajt	Długość	Wartość	Wyszczególnienie
SW	2	'XXXXh'	Wyrazy stanu (SW1, SW2)

- Jeżeli klucz bieżącej sesji nie jest dostępny, zwracany jest stan przetwarzania '6A88'. Zdarza się to albo wtedy gdy klucz sesyjny nie jest już generowany, albo gdy już wygaśnie ważność kluczy sesyjnych (w tym przypadku IFD musi powtórnie uruchomić proces wzajemnego uwierzytelnienia w celu utworzenia nowego klucza sesyjnego).
- Jeżeli w formacie bezpiecznej wymiany komunikatów brakuje pewnych, oczekiwanych obiektów (określonych powyżej), zwracany jest stan przetwarzania '6987': ten błąd ma miejsce, jeżeli brakuje oczekiwanego znacznika lub jeżeli treść polecenia nie jest prawidłowo skonstruowana.

- Jeżeli pewne obiekty danych nie są prawidłowe, zwróconym stanem przetwarzania jest '6988': ten błąd ma miejsce, jeżeli są wszystkie wymagane znaczniki, ale niektóre długości różnią się od oczekiwanych.
- Jeżeli weryfikacja kryptograficznej sumy kontrolnej wykaże niezgodność, zwróconym stanem przetwarzania jest '6688'.

3.6.3. Update Binary (Uaktualnianie binarne)

Polecenie to jest zgodne z normą ISO/IEC 7816-4, ale jego zastosowanie jest ograniczone w porównaniu z poleceniem zdefiniowanym w tej normie.

Komunikat polecenia UPDATE BINARY inicjuje aktualizację (kasowanie + zapis) bitów już znajdujących się w binarnym EF zastępując je bitami podanymi w poleceniu APDU.

TCS_331 Polecenie może być wykonane tylko wtedy gdy stan zabezpieczenia spełnia atrybuty zabezpieczenia zdefiniowane dla EF dla funkcji UPDATE (jeżeli kontrola dostępu funkcji UPDATE obejmuje PRO SM, w poleceniu musi być dodana bezpieczna wymiana komunikatów).

3.6.3.1. Polecenie bez bezpiecznej wymiany komunikatów

Polecenie to umożliwia IFD zapis danych do bieżąco wybranego EF, bez sprawdzenia przez kartę integralności otrzymanych danych. Ten tryb odkryty dozwolony jest tylko wtedy, gdy wybrany plik nie ma oznakowania »Encrypted«.

TCS_332 Komunikat polecenia

Bajt	Długość	Wartość	Wyszczególnienie
CLA	1	'00h'	bez bezpiecznej wymiany komunikatów
INS	1	'D6h'	przesunięcie w bajtach od początku pliku: bajt najbardziej znaczący
P1	1	'XXh'	
P2	1	'XXh'	
Lc	1	'NNh'	Lc długość aktualizowanych danych. Liczba zapisywanych bajtów
#6-#(5+NN)	NN	'XX..XXh'	zapisywane dane

Uwaga: bit 8 w P1 musi być ustawiony na 0.

TCS_333 Komunikat odpowiedzi

Bajt	Długość	Wartość	Wyszczególnienie
SW	2	'XXXXh'	Wyraży stanu (SW1, SW2)

- Jeżeli wykonanie zakończyło się pomyślnie, karta zwraca '9000',
- jeżeli nie jest wybrany EF, zwróconym stanem przetwarzania jest '6986',
- jeżeli kontrola dostępu wybranego pliku nie jest spełniona, polecenie zostaje przerwane z '6982',
- jeżeli przesunięcie nie jest zgodne z wielkością EF (przesunięcie > wielkość EF), zwróconym stanem przetwarzania jest '6B00',
- jeżeli wielkość danych, które mają być zapisane, nie jest zgodna z wielkością EF (przesunięcie + Le > wielkość EF), zwróconym stanem przetwarzania jest '6700',
- jeżeli w atrybutach pliku wykryty jest błąd integralności, karta uznaje, że plik jest uszkodzony i nienaprawialny, zwróconym stanem przetwarzania jest '6400' lub '6500',
- jeżeli zapis nie jest wykonany pomyślnie, zwróconym stanem przetwarzania jest '6581'.

3.6.3.2. Polecenie z bezpieczną wymianą komunikatów

Polecenie to umożliwia IFD zapis danych do bieżąco wybranego EF, ze sprawdzeniem przez kartę integralności otrzymanych danych. Gdy nie jest wymagana poufność, dane nie są szyfrowane. Ten tryb odkryty dozwolony jest tylko wtedy, gdy wybrany plik nie ma oznakowania »Encrypted«

TCS_334 Komunikat polecenia

Bajt	Długość	Wartość	Opis
CLA	1	'0Ch'	żądana bezpieczna wymiana komunikatów
INS	1	'D6h'	INS
P1	1	'XXh'	przesunięcie w bajtach od początku pliku: bajt najbardziej znaczący
P2	1	'XXh'	przesunięcie w bajtach od początku pliku: bajt najmniej znaczący
Lc	1	'XXh'	długość chronionego pola danych
#6	1	'81h'	T _{PV} : znacznik odkrytych wartości danych
#7	L	'NNh' lub '81NNh'	L _{PV} : długość transmitowanych danych L jest 2 bajty, jeżeli L _{PV} > 127 bajtów
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	wartość odkrytych danych (dane, które mają być zapisane)
#(7+L+NN)	1	'8Eh'	T _{CC} : znacznik kryptograficznej sumy kontrolnej
#(8+L+NN)	1	'04h'	L _{CC} : długość następnej kryptograficznej sumy kontrolnej
#(9+L+NN)-#(12+L+NN)	4	'XX..XXh'	kryptograficzna suma kontrolna (4 bajty najbardziej znaczące)
Le	1	'00h'	wg specyfikacji w normie ISO/IEC 7816-4

TCS_335 Komunikat odpowiedzi, gdy format wejścia bezpiecznej wymiany komunikatów jest prawidłowy

Bajt	Długość	Wartość	Opis
#1	1	'99h'	T _{SW} : znacznik wyrazu stanu (chroniony przez CC)
#2	1	'02h'	L _{SW} : długość zwracanego wyrazu stanu
#3-#4	2	'XXXXh'	wyraz stanu (SW1, SW2)
#5	1	'8Eh'	T _{CC} : znacznik kryptograficznej sumy kontrolnej
#6	1	'04h'	L _{CC} : długość następnej kryptograficznej sumy kontrolnej
#7-#10	4	'XX..XXh'	kryptograficzna suma kontrolna (4 bajty najbardziej znaczące)
SW	2	'XXXXh'	wyraz stanu (SW1, SW2)

Stany »regularnego« przetwarzania, opisane dla polecenia READ BINARY z bezpieczną wymianą komunikatów (patrz ppkt 3.6.3.1), mogą być zwracane przy użyciu struktur komunikatu odpowiedzi opisanego powyżej.

Ponadto mogą wystąpić niektóre błędy, swoiście dotyczące bezpiecznej wymiany komunikatów. W takim przypadku zwracany jest po prostu stan przetwarzania bez struktury bezpiecznej wymiany komunikatów:

TCS_336 Komunikat odpowiedzi w przypadku błędu w bezpiecznej wymianie komunikatów

Bajt	Długość	Wartość	Opis
SW	2	'XXXXh'	Wyraz stanu (SW1, SW2)

- Jeżeli klucz bieżącej sesji nie jest dostępny, zwracany jest stan przetwarzania '6A88',
- jeżeli w formacie bezpiecznej wymiany komunikatów brakuje pewnych, oczekiwanych obiektów (określonych powyżej), zwracany jest stan przetwarzania '6987': ten błąd ma miejsce, jeżeli brakuje oczekiwanego znacznika lub jeżeli treść polecenia nie jest prawidłowo skonstruowana,
- jeżeli pewne obiekty danych nie są prawidłowe, zwróconym stanem przetwarzania jest '6988': ten błąd ma miejsce, jeżeli są wszystkie wymagane znaczniki, ale niektóre długości różnią się od oczekiwanych,
- jeżeli weryfikacja kryptograficznej sumy kontrolnej wykaże niezgodność, zwróconym stanem przetwarzania jest '6688'.

3.6.4. *Get challenge (Wydanie wyzwania)*

Polecenie to jest zgodne z normą ISO/IEC 7816-4, ale jego zastosowanie jest ograniczone w porównaniu z poleceniem zdefiniowanym w tej normie.

Polecenie GET CHALLENGE żąda od karty wydania wyzwania, w celu użycia go w procedurze związanej z zabezpieczeniem, w której do karty wysyłany jest kryptogram lub pewne, szyfrowane dane.

TCS_337 Wyzwanie wydane przez kartę ważne jest tylko dla następnego polecenia, które używa wyzwania, wysłanego do karty.

TCS_338 Komunikat polecenia

Bajt	Długość	Wartość	Wyszczególnienie
CLA	1	'00h'	CLA
INS	1	'84h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Le	1	'08h'	Le (długość oczekiwanego wyzwania)

TCS_339 Komunikat odpowiedzi

Bajt	Długość	Wartość	Wyszczególnienie
#1-#8	8	'XX..XXh'	wyzwanie
SW	2	'XXXXh'	wyraz stanu (SW1, SW2)

- Jeżeli wykonanie zakończyło się pomyślnie, karta zwraca '9000',
- jeżeli Le nie jest '08h', zwracany jest stan przetwarzania '6700',
- jeżeli parametry P1-P2 są nieprawidłowe, zwracany jest stan przetwarzania '6A86'.

3.6.5. *Verify (Weryfikacja)*

Polecenie to jest zgodne z normą ISO/IEC 7816-4, ale jego zastosowanie jest ograniczone w porównaniu z poleceniem zdefiniowanym w tej normie.

Polecenie VERIFY inicjuje porównanie w karcie danych CHV (PIN) wysłanych w poleceniu z referencyjnymi CHV przechowywanymi na karcie.

Uwaga: PIN wprowadzony przez użytkownika musi być prawidłowo wypełniony przez IFD bajtami »FFh« do długości 8 bajtów.

TCS_340 Jeżeli wykonanie zakończyło się pomyślnie, prawa odpowiadające przedstawionemu CHV są udostępniane, a licznik dozwolonych prób CHV przywrócony do stanu wyjściowego.

TCS_341 Jeżeli porównanie wykaze niezgodność, jest ono rejestrowane na karcie w celu ograniczenia liczby dalszych prób użyciu referencyjnego CHV.

TCS_342 Komunikat polecenia

Bajt	Długość	Wartość	Wyszczególnienie
CLA	1	'00h'	CLA
INS	1	'20h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (zweryfikowane CHV jest domniemanie znane)
Lc	1	'08h'	długość przesyłanego kodu CHV
#6-#13	8	'XX..XXh'	CHV

TCS_343 Komunikat odpowiedzi

Bajt	Długość	Wartość	Wyszczególnienie
SW	2	'XXXXh'	wyraz stanu (SW1, SW2)

- Jeżeli wykonanie zakończyło się pomyślnie, karta zwraca '9000',
- jeżeli nie znaleziono referencyjnego CHV, zwróconym stanem przetwarzania jest '6A88',
- jeżeli CHV jest zablokowane, (licznik dozwolonych prób CHV jest wyzerowany), zwróconym stanem przetwarzania jest '6983'. Po znalezieniu się w tym stanie CHV nie może już nigdy być pomyślnie przekazane,
- jeżeli porównanie wykaże niezgodność, licznik dozwolonych prób CHV jest zmniejszany i zwracany stan '63CX' (X > 0, gdzie X pokazuje stan licznika dozwolonych prób CHV. X = 'F', oznacza że liczba dozwolonych prób CHV jest większa niż 'F'),
- jeżeli referencyjne CHV uznane jest za uszkodzone, zwróconym stanem przetwarzania jest '6400' lub '6581'.

3.6.6. **Get response (Przyjęcie odpowiedzi)**

Polecenie to jest zgodne z normą ISO/IEC 7816-4.

Polecenia tego (niezbędnego i dostępnego tylko dla protokołu T=0) używa się do przesyłania przygotowanych danych z karty do urządzenia interfejsu (przypadek, gdy polecenie zawiera oba parametry Lc i Le).

Polecenie GET RESPONSE musi być wydane bezpośrednio po poleceniu przygotowującym dane, w przeciwnym przypadku dane są tracone. Po wykonaniu polecenia GET RESPONSE (wyjawszy, gdy wystąpi błąd '61xx' lub '6Cxx', patrz poniżej), wcześniej przygotowane dane nie są już dostępne.

TCS_344 Komunikat polecenia

Bajt	Długość	Wartość	Opis
CLA	1	'00h'	
INS	1	'C0h'	
P1	1	'00h'	
P2	1	'00h'	
Le	1	'XXh'	oczekiwana liczba bajtów

TCS_345 Komunikat odpowiedzi

Bajt	Długość	Wartość	Opis
#1-#X	X	'XX..XXh'	dane
SW	2	'XXXXh'	wyraz stanu (SW1, SW2)

- Jeżeli wykonanie zakończyło się pomyślnie, karta zwraca '9000'.
- Jeżeli karta nie przygotowuje żadnych danych, zwróconym stanem przetwarzania jest '6900' lub '6F00'.
- Jeżeli Le przekracza liczbę dostępnych bajtów lub Le jest zero, zwróconym stanem przetwarzania jest '6Cxx', gdzie 'xx' oznacza dokładną liczbę dostępnych bajtów. W takim przypadku przygotowane dane pozostają dostępne dla następnego polecenia GET RESPONSE.
- Jeżeli Le jest różne od zera i jest mniejsze od liczby dostępnych bajtów, normalnie karta wysyła żądane dane i zwróconym stanem przetwarzania jest '61xx', gdzie 'xx' oznacza liczbę dodatkowych bajtów jeszcze dostępnych dla następnego polecenia GET RESPONSE.
- Jeżeli polecenie nie jest obsługiwane (protokół T=1), karta zwraca '6D00'.

3.6.7. **PSO: verify certificate (weryfikacja certyfikatu)**

Polecenie to jest zgodne z normą ISO/IEC 7816-8, ale jego zastosowanie jest ograniczone w porównaniu z poleceniem zdefiniowanym w tej normie.

Karta używa polecenia VERIFY_CERTIFICATE do otrzymania klucza publicznego z zewnątrz i do sprawdzenia ważności tego klucza.

TCS_346 W przypadku pomyślnego weryfikacji poleceniem VERIFY_CERTIFICATE klucz publiczny jest zapamiętany do przyszłego wykorzystania w środowisku bezpieczeństwa. Klucz ten jest jawnie przydzielony do używania w poleceniach związanych z zabezpieczeniem (INTERNAL_AUTHENTICATE, EXTERNAL_AUTHENTICATE lub VERIFY_CERTIFICATE) przez polecenie MSE (patrz pkt 3.6.10) używając swojego identyfikatora klucza.

TCS_347 W każdym przypadku polecenie VERIFY_CERTIFICATE używa klucza publicznego uprzednio wybranego przez polecenie MSE do otwarcia certyfikatu. Ten klucz publiczny musi być kluczem jednego z Państw Członkowskich lub Europy.

TCS_348 Komunikat polecenia

Bajt	Długość	Wartość	Wyszczególnienie
CLA	1	'00h'	CLA
INS	1	'2Ah'	wykonaj operację bezpieczeństwa
P1	1	'00h'	P1
P2	1	'AEh'	P2: dane niekodowane w BER-TLV (konkatenacja elementów danych)
Lc	1	'CEh'	Lc: długość certyfikatu, 194 bajty
#6-#199	194	'XX..XXh'	certyfikat: konkatenacja elementów danych (opisana w dodatku 11)

TCS_349 Komunikat odpowiedzi

Bajt	Długość	Wartość	Wyszczególnienie
SW	2	'XXXXh'	wyrazy stanu (SW1, SW2)

- Jeżeli wykonanie zakończyło się pomyślnie, karta zwraca '9000',
- jeżeli weryfikacja certyfikatu nie uda się, zwróconym stanem przetwarzania jest '6688'. Proces weryfikacji i otwierania certyfikatu opisano w dodatku 11,
- jeżeli klucza publicznego nie ma w środowisku bezpieczeństwa, zwróconym stanem przetwarzania jest '6A88',
- jeżeli wybrany klucz publiczny (użyty do otwierania certyfikatu) uznany jest za uszkodzony, zwróconym stanem przetwarzania jest '6400' lub '6581',
- jeżeli CHA.LSB (CertificateHolderAuthorisation.equipmentType) wybranego klucza publicznego (użytego do otwierania certyfikatu) różni się od '00' (tj. nie jest kluczem Państwa Członkowskiego lub Europy), zwróconym stanem przetwarzania jest '6985'.

3.6.8. Internal authenticate (Uwierzytelnianie wewnętrzne)

Polecenie to jest zgodne z normą ISO/IEC 7816-4.

Poleceniem INTERNAL_AUTHENTICATE IFD można uwierzytelnić kartę.

Proces uwierzytelnienia opisano w dodatku 11. W procesie tym używa się następujących instrukcji:

TCS_350 Polecenie INTERNAL_AUTHENTICATE używa klucza prywatnego karty (wybranego niejawnie) do podpisania danych uwierzytelniających obejmujących K1 (pierwszy element do uzgodnienia kluczy sesyjnych) i RND1, oraz używa bieżąco wybranego klucza publicznego (w ostatnim poleceniu MSE) do zaszyfrowania podpisu i utworzenia znacznika uwierzytelnienia (token) (dokładniej opisano w dodatku 11).

TCS_351 Komunikat polecenia

Bajt	Długość	Wartość	Wyszczególnienie
CLA	1	'00h'	CLA
INS	1	'88h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Lc	1	'10h'	długość danych wysłanych do karty
#6-#13	8	'XX..XXh'	wyzwanie użyte do uwierzytelnienia karty
#14-#21	8	'XX..XXh'	VU.CHR (patrz dodatek 11)
Le	1	'80h'	długość danych oczekiwanych z karty

TCS_352 Komunikat odpowiedzi

Bajt	Długość	Wartość	Wyszczególnienie
#1-#128	128	'XX..XXh'	znacznik (token) uwierzytelnienia karty (patrz dodatek 11)
SW	2	'XXXXh'	wyraz stanu (SW1, SW2)

- Jeżeli wykonanie zakończyło się pomyślnie, karta zwraca '9000',
- jeżeli klucza publicznego nie ma w środowisku bezpieczeństwa, zwróconym stanem przetwarzania jest '6A88',
- jeżeli klucza prywatnego nie ma w środowisku bezpieczeństwa, zwróconym stanem przetwarzania jest '6A88',
- jeżeli VU.CHR nie zgadza się z bieżącym identyfikatorem klucza publicznego, zwróconym stanem przetwarzania jest '6A88',
- jeżeli wybrany klucz prywatny uznany jest za uszkodzony, zwróconym stanem przetwarzania jest '6400' lub '6581'.

TCS_353 Jeżeli uwierzytelnienie poleceniem INTERNAL AUTHENTICATE jest pomyślne, klucz bieżącej sesji, o ile istnieje, zostaje skasowany i nie jest dalej dostępny. W celu uzyskania nowego klucza sesji, konieczne jest uwierzytelnienie poleceniem EXTERNAL AUTHENTICATE.

3.6.9. External authenticate (Uwierzytelnianie zewnętrzne)

Polecenie to jest zgodne z normą ISO/IEC 7816-4.

Poleceniem EXTERNAL AUTHENTICATE karta może uwierzytelić IFD.

Proces uwierzytelnienia opisano w dodatku 11. W procesie tym używa się następujących instrukcji:

TCS_354 Polecenie GET CHALLENGE musi bezpośrednio poprzedzać polecenie EXTERNAL AUTHENTICATE. Karta wydaje wyzwanie na zewnątrz (RND3).

TCS_355 Do weryfikacji kryptogramu używa się RND3 (wyzwania wydanego przez kartę), klucza prywatnego karty (wybranego niejawnie) i klucza publicznego wcześniej wybranego poleceniem MSE.

TCS_356 Karta weryfikuje kryptogram i, gdy wynik weryfikacji jest prawidłowy, otwiera warunek dostępu AUT.

TCS_357 Kryptogram wejściowy przynosi drugi element uzgodnienia kluczy sesyjnych — K2.

TCS_358 Komunikat polecenia

Bajt	Długość	Wartość	Wyszczególnienie
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (klucz publiczny, który ma być używany, znany niejawnie i wcześniej ustawiony poleceniem MSE)
Lc	1	'80h'	Lc (długość danych wysłanych do karty)
#6-#133	128	'XX..XXh'	Kryptogram (patrz dodatek 11)

TCS_359 Komunikat odpowiedzi

Bajt	Długość	Wartość	Wyszczególnienie
SW	2	'XXXXh'	wyraz stanu (wyraz stanu (SW1, SW2))

- Jeżeli wykonanie zakończyło się pomyślnie, karta zwraca '9000',
- jeżeli klucza publicznego nie ma w środowisku bezpieczeństwa, karta zwraca '6A88',
- jeżeli CHA bieżącego ustawionego klucza publicznego nie jest konkatencją AID aplikacji tachograficznej i typu urządzenia VU, zwróconym stanem przetwarzania jest '6F00' (patrz dodatek 11),
- jeżeli klucza prywatnego nie ma w środowisku bezpieczeństwa, zwróconym stanem przetwarzania jest '6A88',
- jeżeli weryfikacja kryptogramu daje zły wynik, zwróconym stanem przetwarzania jest '6688',
- jeżeli bezpośrednio przed poleceniem nie znajduje się polecenie GET CHALLENGE, zwróconym stanem przetwarzania jest '6985',
- jeżeli wybrany klucz prywatny uznany jest za uszkodzony, zwróconym stanem przetwarzania jest '6400' lub '6581'.

TCS_360 Jeżeli uwierzytelnienie poleceniem EXTERNAL AUTHENTICATE jest pomyślne i jeżeli pierwsza część klucza sesji jest dostępna w wyniku wcześniej wykonanego polecenia INTERNAL AUTHENTICATE, klucz sesji zostaje ustawiony dla przyszłych poleceń używających bezpiecznej wymiany komunikatów.

TCS_361 Jeżeli pierwsza część klucza sesji nie jest dostępna w wyniku wcześniej wykonanego polecenia INTERNAL AUTHENTICATE, karta nie zapisuje drugiej części klucza sesyjnego, wysłanej przez IFD. Taki mechanizm zapewnia, że proces wzajemnego uwierzytelnienia przebiega w sposób określony w dodatku 11.

3.6.10. *Manage security environment (Zarządzanie środowiskiem bezpieczeństwa)*

Poleceniem tym ustawia się klucz publiczny dla potrzeb uwierzytelnienia.

Polecenie to jest zgodne z normą ISO/IEC 7816-8, ale jego zastosowanie jest ograniczone w porównaniu z poleceniem zdefiniowanym w tej normie.

TCS_362 Klucz powołany w polu danych MSE jest ważny dla każdego tachograficznego pliku DF.

TCS_363 Klucz powołany w polu danych MSE pozostaje bieżącym kluczem publicznym aż do następnego, prawidłowego polecenia MSE.

TCS_364 Jeżeli powołany klucza nie ma (już) na karcie, środowisko bezpieczeństwa pozostaje niezmienione.

TCS_365 Komunikat polecenia

Bajt	Długość	Wartość	Wyszczególnienie
CLA	1	'00h'	CLA
INS	1	'22h'	INS
P1	1	'C1h'	P1: powołany klucz ważny dla wszystkich czynności kryptograficznych
P2	1	'B6h'	P2 (powołane dane dotyczące podpisu cyfrowego)
Lc	1	'0Ah'	Lc: długość następnego pola danych
#6	1	'83h'	znacznik do powołanego klucza publicznego w przypadkach asymetrycznych
#7	1	'08h'	długość referencji klucza (identyfikator klucza)
#8-#15	08h	'XX..XXh'	identyfikator klucza określony w dodatku 11

TCS_366 Komunikat odpowiedzi

Bajt	Długość	Wartość	Wyszczególnienie
SW	2	'XXXXh'	wyraz stanu (SW1, SW2)

- Jeżeli wykonanie zakończyło się pomyślnie, karta zwraca '9000',
- jeżeli powołany klucz nie znajduje się na karcie, zwróconym stanem przetwarzania jest '6A88',
- jeżeli niektórych oczekiwanych obiektów danych brakuje w formacie bezpiecznej wymiany komunikatów, zwracany jest stan przetwarzania '6987'. To może zdarzyć się, gdy brakuje znacznika '83h',
- jeżeli niektóre obiekty danych są nieprawidłowe, zwróconym stanem przetwarzania jest '6988'. To może zdarzyć się, gdy długość identyfikatora klucza różna jest od '08h',
- jeżeli wybrany klucz uznany jest za uszkodzony, zwróconym stanem przetwarzania jest '6400' lub '6581'.

3.6.11. **PSO: HASH (haszowanie-mieszanie)**

Polecenia tego używa się do przesłania na kartę wyniku obliczeń funkcji skrótu dla niektórych danych. Polecenia tego używa się do weryfikowania podpisów cyfrowych. Wartość skrótu zapamiętywana jest w pamięci EEPROM dla późniejszego polecenia weryfikacji podpisu cyfrowego.

Polecenie to jest zgodne z normą ISO/IEC 7816-8, ale jego zastosowanie jest ograniczone w porównaniu z poleceniem zdefiniowanym w tej normie.

TCS_367 Komunikat polecenia

Bajt	Długość	Wartość	Wyszczególnienie
CLA	1	'00h'	CLA
INS	1	'2Ah'	wykonaj operację bezpieczeństwa
P1	1	'90h'	zwróć skrót
P2	1	'A0h'	znacznik: pole danych zawiera DO stosowne do obliczania skrótu
Lc	1	'16h'	długość Lc następnego pola danych
#6	1	'90h'	znacznik dla kodu skrótu
#7	1	'14h'	długość kodu skrótu
#8-#27	20	'XX..XXh'	kod skrótu

TCS_368 Komunikat odpowiedzi

Bajt	Długość	Wartość	Wyszczególnienie
SW	2	'XXXXh'	wyrazy stanu (SW1, SW2)

- Jeżeli wykonanie zakończyło się pomyślnie, karta zwraca '9000',
- jeżeli brakuje niektórych oczekiwanych obiektów danych (jak określone powyżej), zwracany jest stan przetwarzania '6987'. Ten błąd może zdarzyć się, jeżeli brakuje jednego ze znaczników '90h',
- jeżeli niektóre obiekty danych są nieprawidłowe, zwróconym stanem przetwarzania jest '6988'. Ten błąd zdarza się, gdy żądany znacznik jest, ale ma długość różną niż '14h'.

3.6.12. **Oblicz skrót pliku**

Polecenie to nie jest zgodne z normą ISO/IEC 7816-8. Tym samym bajt CLA w tym poleceniu wskazuje na zastrzeżone użycie polecenia PERFORM SECURITY OPERATION/HASH.

TCS_369 Polecenia PERFORM HASH of FILE używa się do obliczenia skrótu obszaru danych bieżącego, przezroczystego pliku EF.

TCS_370 Wynik operacji obliczania skrótu zapamiętywany jest na karcie. Następnie może być używany do otrzymania podpisu cyfrowego pliku przy pomocy polecenia PSO-COMPUTE_DIGITAL_SIGNATURE. Wynik ten pozostaje dostępny dla polecenia COMPUTE_DIGITAL_SIGNATURE aż do następnego, wykonanego pomyślnie polecenia PERFORM HASH of FILE.

TCS_371 Komunikat polecenia

Bajt	Długość	Wartość	Wyszczególnienie
CLA	1	'80h'	CLA
INS	1	'2Ah'	wykonaj operację bezpieczeństwa
P1	1	'90h'	Tag: hasz
P2	1	'00h'	P2: oblicz skrót danych dla bieżącego, wybranego, przezroczystego pliku

TCS_372 Komunikat odpowiedzi

Bajt	Długość	Wartość	Wyszczególnienie
SW	2	'XXXXh'	wyrazy stanu (SW1, SW2)

- Jeżeli wykonanie zakończyło się pomyślnie, karta zwraca '9000',
- jeżeli nie wybrano żadnej aplikacji, zwracany jest stan przetwarzania '6985',
- jeżeli wybrany plik EF uznany jest za uszkodzony (błąd atrybutów pliku lub błąd integralności przechowywanych danych), zwracany jest stan przetwarzania '6400' lub '6581'.
- jeżeli wybrany plik nie jest plikiem przezroczystym, zwracany jest stan przetwarzania '6986'.

3.6.13. PSO: oblicz podpis cyfrowy

Polecenia tego używa się do obliczania podpisu cyfrowego z obliczonego wcześniej kodu skrótu (patrz polecenie PERFORM HASH of FILE, pkt 3.6.12).

Polecenie to jest zgodne z normą ISO/IEC 7816-8, ale jego zastosowanie jest ograniczone w porównaniu z poleceniem zdefiniowanym w tej normie.

TCS_373 Klucza prywatnego karty, który jest niejawnie znany karcie, używa się do obliczania podpisu cyfrowego.

TCS_374 Karta wykonuje podpis cyfrowy metodą wypełniania zgodną z PKCS1 (dokładniejszy opis w dodatku 11).

TCS_375 Komunikat polecenia

Bajt	Długość	Wartość	Wyszczególnienie
CLA	1	'00h'	CLA
INS	1	'2Ah'	wykonaj operację bezpieczeństwa
P1	1	'9Eh'	zwracany podpis cyfrowy
P2	1	'9Ah'	znacznik: pole danych zawiera dane do podpisania. Gdy nie zawarto pola danych, przyjmuje się, że dane te są już na karcie (skrót pliku)
Le	1	'80h'	długość oczekiwanego podpisu

TCS_376 Komunikat odpowiedzi

Bajt	Długość	Wartość	Wyszczególnienie
#1-#128	128	'XX..XXh'	podpis uprzednio obliczonego skrótu
SW	2	'XXXXh'	wyrazy stanu (SW1, SW2)

- Jeżeli wykonanie zakończyło się pomyślnie, karta zwraca '9000',
- jeżeli niejawnie wybrany klucz prywatny uznany jest za uszkodzony, zwróconym stanem przetwarzania jest '6400' lub '6581'.

3.6.14. PSO: skontroluj podpis cyfrowy

Polecenia tego używa się do weryfikowania podpisu cyfrowego, dostarczanego jako dane wejściowe, zgodnie z PKCS1, komunikatu, którego skrót jest znany karcie. Algorytm podpisu jest niejawnie znany karcie.

Polecenie to jest zgodne z normą ISO/IEC 7816-8, ale jego zastosowanie jest ograniczone w porównaniu z poleceniem zdefiniowanym w tej normie.

TCS_377 Polecenie Verify Digital Signature zawsze używa klucza publicznego wybranego poprzednim poleceniem manage security environment i poprzednim kodem skrótu wprowadzonym poleceniem PSO: hash.

TCS_378 Komunikat polecenia

Bajt	Długość	Wartość	Opis
CLA	1	'00h'	CLA
INS	1	'2Ah'	wykonaj operację bezpieczeństwa
P1	1	'00h'	znacznik: pole danych zawiera obiekty DO stosowne do weryfikacji
P2	1	'A8h'	
Lc	1	'83h'	Lc — długość następnego pola danych
#28	1	'9Eh'	znacznik dla podpisu cyfrowego
#29-#30	2	'8180h'	długość podpisu cyfrowego (128 bajtów, kodowane zgodnie z ISO/IEC 7816-6)
#31-#158	128	'XX..XXh'	treść podpisu cyfrowego

TCS_379 Komunikat odpowiedzi

Bajt	Długość	Wartość	Opis
SW	2	'XXXXh'	wyraz stanu (SW1, SW2)

- Jeżeli wykonanie zakończyło się pomyślnie, karta zwraca '9000',
- jeżeli podpis jest zweryfikowany negatywnie, zwróconym stanem przetwarzania jest '6688'. Proces weryfikacji opisano w dodatku 11,
- jeżeli nie wybrano klucza publicznego, zwróconym stanem przetwarzania jest '6A88',
- jeżeli brakuje niektórych oczekiwanych obiektów danych (jak określone powyżej), zwracany jest stan przetwarzania '6987'. Taka sytuacja może zdarzyć się, gdy brakuje jednego ze znaczników,
- jeżeli kod skrótu nie jest dostępny dla przetwarzania polecenia (w wyniku poprzedniego polecenia PSO: hash), zwróconym stanem przetwarzania jest '6985',
- jeżeli niektóre obiekty danych są nieprawidłowe, zwróconym stanem przetwarzania jest '6988'. Taka sytuacja może zdarzyć się, gdy długość jednego z wymaganych obiektów danych jest nieprawidłowa,
- jeżeli wybrany klucz publiczny uznany jest za uszkodzony, zwróconym stanem przetwarzania jest '6400' lub '6581'.

4. STRUKTURA KART DO TACHOGRAFÓW

W tym rozdziale opisano struktury plików na kartach do tachografów przeznaczonych do gromadzenia dostępnych danych.

Nie stanowi to opisu wewnętrznych struktur właściwych dla producenta, takich jak nagłówki plików, ani sposobu gromadzenia i manipulowania elementami danych do użytku wewnętrznego, tylko takich jak `EuropeanPublicKey`, `CardPrivateKey`, `TDesSessionKey` lub `WorkshopCardPin`.

Pojemność użytkowa pamięci kart do tachografów wynosi przynajmniej 11 kbajtów. Większe pojemności są dopuszczalne. W takich przypadkach struktura karty pozostaje niezmienną, ale zwiększa się liczbę zapisów niektórych elementów struktury. W niniejszym rozdziale podano też minimalne i maksymalne liczby tych zapisów.

4.1. Struktura karty kierowcy

TCS_400 Po personalizacji karta kierowcy ma następującą, trwałą strukturę plików i warunki dostępu do plików:

Plik	ID pliku	Warunki dostępu		
		Odczyt	Aktualizacja	Szyfrowany
MF	3F00			
EF ICC	0002	ALW	NEV	No
EF IC	0005	ALW	NEV	No
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	No
EF Card_Certificate	C100	ALW	NEV	No
EF CA_Certificate	C108	ALW	NEV	No
EF Identification	0520	ALW	NEV	No
EF Card_Download	050E	ALW	ALW	No
EF Driving_Licence_Info	0521	ALW	NEV	No
EF Events_Data	0502	ALW	PRO SM / AUT	No
EF Faults_Data	0503	ALW	PRO SM / AUT	No
EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	No
EF Vehicles_Used	0505	ALW	PRO SM / AUT	No
EF Places	0506	ALW	PRO SM / AUT	No
EF Current_Usage	0507	ALW	PRO SM / AUT	No
EF Control_Activity_Data	0508	ALW	PRO SM / AUT	No
EF Specific_Conditions	0522	ALW	PRO SM / AUT	No

TCS_401 Wszystkie struktury plików EF są przezroczyste.

TCS_402 Odczyt wszystkich plików w DF Tachograph możliwy jest w bezpiecznej wymianie komunikatów.

TCS_403 Karta kierowcy ma następującą strukturę danych:

Plik/Element danych	Liczba zapisów	Wielk. (w bajtach)		Wartość domyślna
		Min.	Maks.	
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 W tabeli poniżej podano wartości odnoszące się do tabeli powyżej, wyznaczające minimalne i maksymalne liczby zapisów, które musi stosować struktura danych karty kierowcy:

		Min.	Maks.
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 bajty (28 dni * 93 zmiany czynności)	13 776 bajtów (28 dni * 240 zmian czynności)

4.2. Struktura karty warsztatowej

TCS_405 Po personalizacji karta warsztatowa ma następującą, trwałą strukturę plików i warunki dostępu do plików:

Plik	ID pliku	Warunki dostępu		
		Oczyt	Aktualizacja	Szyfrowany
MF	3F00			
EF ICC	0002	ALW	NEV	No
EF IC	0005	ALW	NEV	No
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	No
EF Card_Certificate	C100	ALW	NEV	No
EF CA_Certificate	C108	ALW	NEV	No
EF Identification	0520	ALW	NEV	No
EF Card_Download	0509	ALW	ALW	No
EF Calibration	050A	ALW	PRO SM / AUT	No
EF Sensor_Installation_Data	050B	ALW	NEV	Yes
EF Events_Data	0502	ALW	PRO SM / AUT	No
EF Faults_Data	0503	ALW	PRO SM / AUT	No
EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	No
EF Vehicles_Used	0505	ALW	PRO SM / AUT	No
EF Places	0506	ALW	PRO SM / AUT	No
EF Current_Usage	0507	ALW	PRO SM / AUT	No
EF Control_Activity_Data	0508	ALW	PRO SM / AUT	No
EF Specific_Conditions	0522	ALW	PRO SM / AUT	No

TCS_406 Wszystkie struktury plików EF są przezroczyste.

TCS_407 Odczyt wszystkich plików w DF Tachograph możliwy jest w bezpiecznej wymianie komunikatów.

TCS_408 Karta warsztatowa ma następującą strukturę danych:

Plik/Element danych	Liczba zapisów	Wielk. (w bajtach)		Wartość domyślna
		Min.	Maks.	
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
EF Vehicles_Used	126	250	
CardVehiclesUsed	126	250	
vehiclePointerNewestRecord	2	2	{00 00}
cardVehicleRecords	124	248	
CardVehicleRecord	n ₃	31	31
vehicleOdometerBegin	3	3	{00..00}

vehicleOdometerEnd	3	3	{00..00}
vehicleFirstUse	4	4	{00..00}
vehicleLastUse	4	4	{00..00}
vehicleRegistration			
vehicleRegistrationNation	1	1	{00}
vehicleRegistrationNumber	14	14	{00, 20..20}
vuDataBlockCounter	2	2	{00 00}
EF Places	61	81	
CardPlaceDailyWorkPeriod	61	81	
placePointerNewestRecord	1	1	{00}
placeRecords	60	80	
PlaceRecord	n ₄	10	10
entryTime	4	4	{00..00}
entryTypeDailyWorkPeriod	1	1	{00}
dailyWorkPeriodCountry	1	1	{00}
dailyWorkPeriodRegion	1	1	{00}
vehicleOdometerValue	3	3	{00..00}
EF Current_Usage	19	19	
CardCurrentUse	19	19	
sessionOpenTime	4	4	{00..00}
sessionOpenVehicle			
vehicleRegistrationNation	1	1	{00}
vehicleRegistrationNumber	14	14	{00, 20..20}
EF Control_Activity_Data	46	46	
CardControlActivityDataRecord	46	46	
controlType	1	1	{00}
controlTime	4	4	{00..00}
controlCardNumber			
cardType	1	1	{00}
cardIssuingMemberState	1	1	{00}
cardNumber	16	16	{20..20}
controlVehicleRegistration			
vehicleRegistrationNation	1	1	{00}
vehicleRegistrationNumber	14	14	{00, 20..20}
controlDownloadPeriodBegin	4	4	{00..00}
controlDownloadPeriodEnd	4	4	{00..00}
EF Specific_Conditions	10	10	
SpecificConditionRecord	2	5	5
entryTime	4	4	{00..00}
SpecificConditionType	1	1	{00}

TCS_409 W tabeli poniżej podano wartości odnoszące się do tabeli powyżej wyznaczające minimalne i maksymalne liczby zapisów, które musi zawierać struktura danych karty warsztatowej:

		Min.	Maks.
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 bajtów (1 dzień * 93 zmiany czynności)	492 bajty (1 dzień * 240 zmian czynności)

4.3. Struktura karty kontrolnej

TCS_410 Po personalizacji karta kontrolna ma następującą, trwałą strukturę plików i warunki dostępu do plików:

Plik	ID pliku	Warunki dostępu		
		Oczyt	Aktualizacja	Szyfrowany
MF	3F00			
EF ICC	0002	ALW	NEV	No
EF IC	0005	ALW	NEV	No
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	No
EF Card_Certificate	C100	ALW	NEV	No
EF CA_Certificate	C108	ALW	NEV	No
EF Identification	0520	AUT	NEV	No
EF Controller_Activity_Data	050C	ALW	PRO SM / AUT	No

TCS_411 Wszystkie struktury plików EF są przezroczyste.

TCS_412 Odczyt wszystkich plików w DF Tachograph możliwy jest w bezpiecznej wymianie komunikatów.

TCS_413 Karta kontrolna ma następującą strukturę danych:

Plik/element danych	Liczba rekordów	Wielk. (w bajtach)		Wartość domyślna
		Min.	Maks.	
MF	11219	25	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 W tabeli poniżej podano wartości odnoszące się do tabeli powyżej wyznaczające minimalne i maksymalne liczby zapisów, które musi zawierać struktura danych karty kontrolnej:

		Min.	Maks.
n ₇	NoOfControlActivityRecords	230	520

4.4. Struktura karty firmowej

TCS_415 Po personalizacji karta firmowa ma następującą, trwałą strukturę plików i warunki dostępu do plików:

Plik	ID pliku	Warunki dostępu		
		Odczyt	Aktualizacja	Szyfrowany
MF	3F00			
EF ICC	0002	ALW	NEV	No
EF IC	0005	ALW	NEV	No
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	No
EF Card_Certificate	C100	ALW	NEV	No
EF CA_Certificate	C108	ALW	NEV	No
EF Identification	0520	AUT	NEV	No
EF Company_Activity_Data	050D	ALW	PRO SM / AUT	No

TCS_416 Wszystkie struktury plików EF są przezroczyste.

TCS_417 Odczyt wszystkich plików w DF Tachograph możliwy jest w bezpiecznej wymianie komunikatów.

TCS_418 Karta firmowa ma następującą strukturę danych:

Plik/element danych	Liczba rekordów	Wielk. (w bajtach)		Wartość domyślna
		Min.	Maks.	
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 W tabeli poniżej podano wartości odnoszące się do powyższej tabeli wyznaczające minimalne i maksymalne liczby zapisów, których musi używać struktura danych karty firmowej:

		Min.	Maks.
n8	NoOfCompanyActivityRecords	230	520

Dodatek 3

PIKTOGRAMY

PIC_001 Urządzenie rejestrujące może używać następujących piktogramów i kombinacji piktogramów:

1. PODSTAWOWE PIKTOGRAMY

	Ludzie	Operacje	Tryby działania
	firma		tryb firmowy
	kontroler	kontrola	tryb kontrolny
	kierowca	eksploatacja	tryb eksploatacyjny
	warsztat/stanowisko badań	badanie/kalibracja	tryb kalibracyjny
	producent		
	Czynności	Czas trwania	
	dyspozycyjność	bieżący okres dyspozycyjności	
	prowadzenie pojazdu	nieprzerwany czas prowadzenia pojazdu	
	odpoczynek	bieżący okres odpoczynku	
	praca	bieżący okres pracy	
	przerwa	skumulowany czas przerwy	
	nieznane		
	Urządzenie	Funkcje	
	szczelina karty kierowcy		
	szczelina karty współkierowcy		
	karta		
	zegar		
	wyświetlacz	wyświetlanie	
	zewnętrzne gromadzenie danych	wczytywanie danych	
	zasilanie		
	drukarka/wydruk	drukowanie	
	czujnik		
	rozmiar opon		
	pojazd/przyrząd rejestrujący		
	Warunki szczególne		
	poza zakresem		
	PRZEPRAWA PROMOWA/PRZEJAZD KOLEJOWY		
	Różne		
	zdarzenia		usterki
	początek dziennego okresu pracy		koniec dziennego okresu pracy
	umiejscowienie		ręczne wprowadzenie czynności kierowcy
	zabezpieczenie		prędkość
	godzina		razem/podsumowanie
	Kwalifikatory		
	dobowo		
	tygodniowo		
	dwa tygodnie		
	od lub do		

2. KOMBINACJE PIKTOGRAMÓW

Różne							
		miejsce kontroli					
		umiejscowienie początek dziennego okresu pracy			umiejscowienie koniec dziennego okresu pracy		
		od godziny				do godziny	
		z pojazdu					
		początek poza zakresem				koniec poza zakresem	

Karty

	karta kierowcy
	karta firmowa
	karta kontrolna
	karta warsztatowa
	brak karty

Prowadzenie

	załoga
	czas prowadzenia w ciągu jednego tygodnia
	czas prowadzenia w ciągu dwóch tygodni

Wydruki

24h	wydruk dzienny czynności kierowcy z karty
24h	wydruk dzienny czynności kierowcy z VU
	wydruk zdarzeń i usterek z karty
	wydruk zdarzeń i usterek z VU
	wydruk danych technicznych
	wydruk przekroczenia prędkości

Zdarzenia

	włożenie nieważnej karty
	konflikt kart
	nakładające się czasy
	prowadzenie bez prawidłowej karty
	włożenie karty podczas jazdy
	sesja ostatniej karty niezamknięta prawidłowo
	przekroczenie prędkości
	przerwa zasilania
	błąd danych dotyczących ruchu
	naruszenie zabezpieczenia
	regulacja czasu (w warsztacie)
	kontrola przekroczenia prędkości

Usterki

	usterka karty (szczelina karty kierowcy)
	usterka karty (szczelina karty współkierowcy)
	usterka wyświetlacza
	usterka wczytywania danych
	usterka drukarki
	usterka czujnika
	usterka wewnętrzna VU

Procedura ręcznego wprowadzania danych

	czy nadal ten sam dzienny okres pracy?
	czy koniec poprzedniego okresu pracy?
	potwierdź lub wprowadź miejsce zakończenia okresu pracy
	wprowadź godzinę rozpoczęcia
	wprowadź umiejscowienie rozpoczęcia okresu pracy.

Uwaga: Dodatkowe kombinacje piktogramów używane do tworzenia bloków wydruków lub identyfikatorów zapisów zdefiniowano w dodatku 4.

Dodatek 4

WYDRUKI

SPIS TREŚCI

1.	Uwagi ogólne	409
2.	Specyfikacja bloków danych	409
3.	Specyfikacje wydruku	415
3.1.	Wydruk dzienny czynności kierowcy z karty	416
3.2.	Wydruk dzienny czynności kierowcy z VU	416
3.3.	Wydruk zdarzeń i usterek z karty	417
3.4.	Wydruk zdarzeń i usterek z VU	417
3.5.	Wydruk danych technicznych	418
3.6.	Wydruk przekroczenia prędkości	418

2. **Typ wydruku**

Identyfikator bloku
Kombinacja drukowanych piktogramów (patrz dodatek 3),
ustawienie urządzenia ograniczenia prędkości (tylko dla
wydruku przekroczenia prędkości).

-----P-----
Picto xxx km/h

3. **Identyfikacja posiadacza karty**

Identyfikator bloku. P = piktogram ludzi
Nazwisko posiadacza karty
Imię (imiona) posiadacza karty (gdy jest)
Identyfikacja karty
Data ważności karty, (gdy jest)
W przypadku gdy karta nie jest kartą osobistą i nie ma na
niej nazwiska posiadacza karty, w miejscu nazwiska drukuje
się nazwę firmy, warsztatu lub organu kontrolnego.

-----P-----
P Last_Name _____
First_Name _____
Card_Identification _____
dd/mm/yyyy

4. **Identyfikacja pojazdu**

Identyfikator bloku
(VIN)
Państwo Członkowskie rejestracji i numer VRN

-----A-----
A VIN _____
Nat/VRN _____

5. **Identyfikacja VU**

Identyfikator bloku
Nazwa producenta VU
Numer części VU.

-----B-----
B VU_Manufacturer _____
VU_Part_Number _____

6. **Ostatnia kalibracja urządzenia rejestrującego**

Identyfikator bloku
Nazwa warsztatu
Identyfikacja karty warsztatowej
Data kalibracji.

-----T-----
T Last_Name _____
Card_Identification _____
T dd/mm/yyyy

7. **Ostatnia kontrola (przeprowadzona przez urzędnika kontroli)**

Identyfikator bloku
Identyfikacja karty kontrolnej
Data, godzina i typ kontroli
Typ kontroli: maks. cztery piktogramy. Są następujące typy
kontroli (i ich kombinacje):
■: wczytywanie danych z karty, T: wczytywanie danych z
VU, P: drukowanie, □: wyświetlanie.

-----□-----
Card_Identification _____
□ dd/mm/yyyy hh:mm pppp

8. **Czynności kierowcy zapisane na karcie w kolejności występowania**

Identyfikator bloku
Data zapytania o datę (dzień kalendarzowy drukowanych
czynności) + dzienny licznik obecności karty.

-----□-----
dd/mm/yyyy xxx

8.1. *Okres, w którym karta nie była wkładana*

8.1a. Identyfikator zapisu (początek okresu)

8.1b. *Okres czynności nieznanych. Godzina rozpoczęcia i zakończenia, czas trwania*8.1c. *Czynność wprowadzona ręcznie*

Piktogram czynności, godzina rozpoczęcia i zakończenia
(włącznie), czas trwania, okresy odpoczynku trwające przy-
najmniej godzinę są oznakowane gwiazdką.

-----□-----
? hh:mm hh:mm hh:mm
A hh:mm hh:mm hh:mm *

- 8.2. **Wkładanie karty do szczeliny czytnika S**
 Identyfikator rekordu; S = piktogram szczeliny karty
 Państwo Członkowskie rejestracji i numer VRN pojazdu
 Stan licznika kilometrów przy wkładaniu karty.
- 8.3. **Czynność (przy włożonej karcie)**
 Piktogram czynności, godzina rozpoczęcia i zakończenia (włącznie), czas trwania, stan załogi (piktogram załogi, jeżeli pojazd obsługuje ZAŁOGA, a spacje, jeżeli JEDEN KIEROWCA), okresy odpoczynku trwające przynajmniej godzinę są oznakowane gwiazdką.
- 8.3a. **Warunki szczególne.** Godzina, piktogram warunku szczególnego (lub kombinacja piktogramów).
- 8.4. **Wyjęcie karty**
 Stan licznika kilometrów i odległość przebyta od ostatniego włożenia karty, dla którego znany jest stan licznika kilometrów.
9. **Czynności kierowcy zapamiętane w VU według szczeliny czytnika w kolejności chronologicznej**
 Identyfikator bloku
 Data zapytania (dzień kalendarzowy drukowanych czynności)
 Stan licznika kilometrów o 00:00 i 24:00.
10. **Czynności wykonane przy karcie w szczeliny czytnika S**
 Identyfikator bloku.
- 10.1. **Okres, kiedy karta nie jest włożona do szczeliny czytnika S**
 Identyfikator rekordu
 Brak karty
 Stan licznika kilometrów na początku okresu.
- 10.2. **Wkładanie karty**
 Identyfikator rekordu wkładania karty
 Nazwisko kierowcy
 Imię kierowcy
 Identyfikacja karty kierowcy
 Data ważności karty kierowcy
 Rejestrujący MS i numer VRN poprzednio używanego pojazdu
 Data i godzina wyjęcia karty z poprzednio używanego pojazdu
 Pusty wiersz
 Stan licznika kilometrów przy wkładaniu karty, flaga ręcznego wprowadzania czynności kierowcy (M, gdy tak, spacja, gdy nie).
- 10.3. **Czynność**
 Piktogram czynności, godzina rozpoczęcia i zakończenia (włącznie), czas trwania, stan załogi (piktogram stanu załogi, jeżeli ZAŁOGA, spacje, jeżeli JEDEN KIEROWCA), przerwy na odpoczynek trwające przynajmniej godzinę są oznakowane gwiazdką.

-----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

-----☐-----
 dd/mm/yyyy
 x xxx xxx - x xxx xxx km

----- S -----

 ☐☐ ---
 x xxx xxx km

 ☐ Last_Name _____
 First_Name _____
 Card_Identification _____
 dd/mm/yyyy
 A + Nat/VRN _____
 dd/mm/yyyy hh:mm
 x xxx xxx km M

A hh:mm hh:mm hh:mm ☐☐ *

10.3a.	Warunki szczególne. Godzina, piktogram warunku szczególnego (lub kombinacja piktogramów).	hh:mm ----- pppp -----
10.4.	Wyjęcie karty lub zakończenie okresu »brak karty« Stan licznika kilometrów przy wyjęciu karty lub zakończeniu okresu »brak karty« i odległość przebyta od włożenia karty lub rozpoczęcia okresu »brak karty«.	x xxx xxx km; x xxx km
11.	Zestawienie dzienne Identyfikator bloku.	----- Σ -----
11.1.	Zestawienie okresów bez karty w szczelinie karty kierowcy dla VU Identyfikator bloku.	1 0 - - -
11.2.	Zestawienie okresów bez karty w szczelinie karty współkierowcy dla VU Identyfikator bloku.	2 0 - - -
11.3.	VU zestawienie dzienne dla kierowcy Identyfikator rekordu Nazwisko kierowcy Imię (imiona) kierowcy Identyfikacja karty kierowcy.	----- ⊙ Last_Name _____ First_Name _____ Card_Identification _____
11.4.	Wprowadzenie miejsca rozpoczęcia i/lub zakończenia dziennego okresu pracy pi = piktogram miejsca rozpoczęcia/zakończenia, godzina, kraj, region, stan licznika kilometrów.	pihh:mm Cou Reg x xxx xxx km
11.5.	Podsumowania dla czynności (z karty) Całkowity czas prowadzenia pojazdu, odległość przebyta Całkowity czas pracy i dyspozycyjności Całkowity czas odpoczynku i nieznanymi czynności Całkowity czas czynności załogi.	⊙ hhhmm x xxx km ✱ hhhmm ⊠ hhhmm ┌ hhhmm ? hhhmm ⊙⊙ hhhmm
11.6.	Podsumowania dla czynności (okresy bez karty w szczelinie karty kierowcy) Całkowity czas prowadzenia pojazdu, odległość przebyta Całkowity czas pracy i dyspozycyjności Całkowity czas odpoczynku.	⊙ hhhmm x xxx km ✱ hhhmm ⊠ hhhmm ┌ hhhmm
11.7.	Podsumowania dla czynności (okresy bez karty w szczelinie karty współkierowcy) Całkowity czas pracy i dyspozycyjności Całkowity czas odpoczynku.	✱ hhhmm ⊠ hhhmm ┌ hhhmm

11.8. Podsumowania dla czynności (według kierowcy dla obu szczelin kart)

Całkowity czas prowadzenia pojazdu, odległość przebyta

Całkowity czas prowadzenia pojazdu, odległość przebyta

Całkowity czas odpoczynku

Całkowity czas czynności załogi

Gdy dzienny wydruk zbiorczy potrzebny jest dla bieżącego dnia, zestawienie dzienne oblicza się na podstawie danych dostępnych w czasie sporządzania wydruku.

⊗ hh:mm x xxxx km

⌘ hh:mm ⊠ hh:mm

⌒ hh:mm

⊗⊗ hh:mm

12. Zdarzenia i/lub usterki zarejestrowane na karcie

12.1. Identyfikator bloku ostatnich 5 »Zdarzeń i usterek« na karcie

----- ! x ⊠ -----

12.2. Identyfikator bloku wszystkie zarejestrowane »Zdarzenia« na karcie

----- ! ⊠ -----

12.3. Identyfikator bloku wszystkie zarejestrowane »Usterki« na karcie

----- x ⊠ -----

12.4. Zapis zdarzenie i/lub usterka

Identyfikator zapisu

Piktogram zdarzenia/usterki, cel zarejestrowania, data i godzina rozpoczęcia,

Kod dodatkowego zdarzenia/usterki (gdy jest), czas trwania

Państwo Członkowskie rejestracji i numer VRN pojazdu, w którym zdarzenie lub usterka miało miejsce.

Pic dd/mm/yyyy hh:mm
! xxx hh:mm
⌘ Nat/VRN _____

13. Zdarzenia i/lub usterki zarejestrowane lub trwające w VU

13.1. Identyfikator bloku ostatnich 5 »Zdarzeń i usterek« z VU

----- ! x ⌘ -----

13.2. Identyfikator bloku zarejestrowanych lub trwających »Zdarzeń« w VU

----- ! ⌘ -----

13.3. Identyfikator bloku zarejestrowanych lub trwających »Usterek« w VU

----- x ⌘ -----

13.4. Zapis zdarzenie i/lub usterka

Identyfikator zapisu

Piktogram zdarzenia/usterki, cel zarejestrowania, data i godzina rozpoczęcia,

Kod dodatkowego zdarzenia/usterki, (gdy jest), liczba podobnych zdarzeń w tym dniu, czas trwania

Identyfikacja kart włożonych na początku lub po zakończeniu zdarzenia lub usterki (maksymalnie 4 wiersze bez powtórzenia tych samych numerów kart)

Przypadek braku karty

Cel zarejestrowania (p) jest to kod liczbowy wyjaśniający, dlaczego zdarzenie lub usterka zostało zarejestrowane, zaktualizowany zgodnie z elementem danych EventFaultRecordPurpose.

Pic (p) dd/mm/yyyy hh:mm
! xxx (xxx) hh:mm

Card_Identification _____
Card_Identification _____
Card_Identification _____
Card_Identification _____
⊠ ---

14. **Identyfikacja VU**

Identyfikator bloku
 Nazwa producenta VU
 Adres producenta VU
 Numer części VU
 Numer homologacji VU
 Numer fabryczny VU
 Rok produkcji VU
 Wersja oprogramowania i data instalacji VU.

-----B-----
 B Name _____
 Address _____
 PartNumber _____
 Apprv _____
 S/N _____
 yyyy
 V xx.xx.xx dd/mm/yyyy

15. **Identyfikacja czujnika**

Identyfikator bloku
 Numer fabryczny czujnika
 Numer homologacji czujnika
 Data pierwszej instalacji czujnika.

-----L-----
 L S/N _____
 Apprv _____
 dd/mm/yyyy

16. **Dane dotyczące kalibracji**

Identyfikator bloku

-----T-----

16.1. *Zapis kalibracji*

Identyfikator zapisu
 Warsztat, który przeprowadził kalibrację
 Adres warsztatu
 Identyfikacja karty warsztatowej
 Data ważności karty warsztatowej
 Pusty wiersz
 Data kalibracji + cel kalibracji
 Numer VIN
 Państwo Członkowskie rejestracji i numer VRN
 Współczynnik charakterystyczny pojazdu
 Stała urządzenia rejestrującego
 Skuteczny obwód opon
 Rozmiar zamontowanych opon
 Ustawienie urządzenia ograniczenia prędkości
 Stary i nowy stan licznika kilometrów
 Cel kalibracji(p) jest to kod liczbowy wyjaśniający, dlaczego te parametry kalibracyjne zostały zarejestrowane, zakodowane zgodnie z elementem danych *CalibrationPurpose*.

 T Workshop_name _____
 Workshop_address _____
 Card-Identification _____
 dd/mm/yyyy
 T dd/mm/yyyy (p)
 A VIN _____
 Nat/VRN _____
 w xx xxx Imp/km
 k xx xxx Imp/km
 l xx xxx mm
 e TyreSize _____
 > xxx km/h
 x xxx xxx - x xxx xxx km

17. **Regulacja czasu**

Identyfikator bloku

-----C-----

17.1. *Zapis regulacji czasu*

Identyfikator zapisu
 Stara data i godzina
 Nowa data i godzina
 Warsztat, który przeprowadził regulację czasu
 Adres warsztatu
 Identyfikacja karty warsztatowej
 Data ważności karty warsztatowej.

 ! C dd/mm/yyyy hh:mm
 C dd/mm/yyyy hh:mm
 T Workshop_name _____
 Workshop_address _____
 Card_Identification _____
 dd/mm/yyyy

18. Ostatnie zdarzenie i usterka zarejestrowane w VU

Identyfikator bloku

Data i godzina ostatniego zdarzenia

Data i godzina ostatniej usterki.

```

----- ! x A -----
!  jj/mm/aaaa  hh:mm
x  jj/mm/aaaa  hh:mm

```

19. Informacje dla kontroli przekroczenia prędkości

Identyfikator bloku

Data i godzina ostatniej KONTROLI PRZEKROCZENIA PRĘDKOŚCI

Data/godzina pierwszego przekroczenia prędkości i liczba przekroczeń prędkości od tego czasu.

```

----- >> -----
>  dd/mm/yyyy  hh:mm
>> dd/mm/yyyy  hh:mm (nnn)

```

20. Zapis przekroczenia prędkości

20.1. Identyfikator bloku »Pierwsze przekroczenie prędkości po ostatniej kalibracji«

```

----- >>T -----

```

20.2. Identyfikator bloku »5 najpoważniejszych w ciągu ostatnich 365 dni«.

```

----- >> (365) -----

```

20.3. Identyfikator bloku »Najpoważniejsze dla każdego z ostatnich 10 dni występowania przekroczeń prędkości«

```

----- >> (10) -----

```

20.4. Identyfikator zapisu

Data, godzina i czas trwania

Prędkości maks. i przeciętne,

liczba podobnych zdarzeń w tym dniu Nazwisko kierowcy

Imię (imiona) kierowcy

Identyfikacja karty kierowcy

```

-----
>> dd/mm/yyyy hh:mm hh:mm
xxx km/h xxx km/h (xxx)
[ ] Last_Name _____
    First_Name _____
Card_Identification _____

```

20.5. Gdy w bloku nie ma żadnego zapisu przekroczenia prędkości.

```

>> - - -

```

21. Informacje wpisywane ręcznie

Identyfikator bloku

21.1. Miejsce kontroli

21.2. Podpis kontrolera

21.3. Od godziny

21.4. Do godziny

21.5. Podpis kierowcy

```

-----
[ ] .....
[ ] .....
[ ] .....
[ ] .....
[ ] .....

```

»Informacje wpisywane ręcznie« Ponad wpisywaną ręcznie pozycją należy wstawić wystarczająco dużo pustych wierszy, by zapewnić miejsce na wpisanie tych informacji i złożenie podpisu.

3. SPECYFIKACJE WYDRUKU

W tym rozdziale przyjęto następujące konwencje zapisu:

N
N
X/Y

Wydruk bloku lub zapisu o numerze N

Wydruk bloku lub zapisu o numerze N powtarzany tylkokrotnie ile trzeba
Wydruk bloków lub zapisów X i/lub Y w zależności od potrzeby i powtórzenie tylkokrotnie ile trzeba

3.1. Wydruk dzienny czynności kierowcy z karty

PRT_007 Wydruk dzienny czynności kierowcy z karty jest zgodny z poniższym formatem:

1	Data i godzina drukowania dokumentu
2	Typ wydruku
3	Identyfikacja kontrolera (jeżeli w czytniku VU znajduje się karta kontrolna)
3	Identyfikacja kierowcy (z karty, dla której sporządzany jest wydruk)
4	Identyfikacja pojazdu (tego, dla którego sporządzany jest wydruk)
5	Identyfikacja VU (tego, dla którego sporządzany jest wydruk)
6	Ostatnia kalibracja tego VU
7	Ostatnia kontrola sprawdzanego kierowcy
8	Ogranicznik czynności kierowcy
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Czynności kierowcy w kolejności występowania
11	Ogranicznik zestawienia dziennego
11.4	Miejsca wprowadzone w kolejności chronologicznej
11.5	Podsumowania dla czynności
12.1	Zdarzenia lub usterki z ogranicznika karty
12.4	Zapisy zdarzeń/usterek (5 ostatnich zdarzeń lub usterek zapisanych na karcie)
13.1	Zdarzenia lub usterki z ogranicznika VU
13.4	Zapisy zdarzeń/usterek (5 ostatnich zdarzeń lub usterek zapisanych lub trwających w VU)
21.1	Miejsce kontroli
21.2	Podpis kontrolera
21.5	Podpis kierowcy

3.2. Wydruk dzienny czynności kierowcy z VU

PRT_008 Wydruk dzienny czynności kierowcy z VU jest zgodny z poniższym formatem:

1	Data i godzina drukowania dokumentu
2	Typ wydruku
3	Identyfikacja posiadacza karty (dla wszystkich kart włożonych do VU)
4	Identyfikacja pojazdu (tego, dla którego sporządzany jest wydruk)
5	Identyfikacja VU (tego, dla którego sporządzany jest wydruk)
6	Ostatnia kalibracja tego VU
7	Ostatnia kontrola tego urządzenia rejestrującego
9	Ogranicznik czynności kierowcy
10	Ogranicznik dla szczeliny karty kierowcy (szczelina karty 1)
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Czynności w kolejności chronologicznej (szczelina karty kierowcy)
10	Ogranicznik dla szczeliny karty współkierowcy (szczelina karty 2)
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Czynności w kolejności chronologicznej (szczelina karty współkierowcy)
11	Ogranicznik zestawienia dziennego
11.1	Zestawienie okresów bez karty w szczelinie karty kierowcy
11.4	Miejsca wprowadzone w kolejności chronologicznej
11.6	Podsumowania dla czynności

11.2	Zestawienie okresów bez karty w szczelinie karty współkierowcy
11.4	Miejsca wprowadzone w kolejności chronologicznej
11.7	Podsumowania dla czynności
11.3	Zestawienie czynności dla kierowcy dla obu szczelin kart łącznie
11.4	Miejsca wprowadzone przez tego kierowcę w kolejności chronologicznej
11.7	Podsumowania dla czynności dla tego kierowcy
13.1	Ogranicznik zdarzeń/usterek
13.4	Zapisy zdarzeń/usterek (5 ostatnich zdarzeń lub usterek zapisanych lub trwających w VU)
21.1	Miejsce kontroli
21.2	Podpis kontrolera
21.3	Od godziny (miejsce przeznaczone dla kierowcy bez karty w celu wskazania okresów odnoszących się do niego)
21.4	Do godziny
21.5	Podpis kierowcy

3.3. Wydruk zdarzeń i usterek z karty

PRT_009 Wydruk zdarzeń i usterek z karty jest zgodny z poniższym formatem:

1	Data i godzina drukowania dokumentu
2	Typ wydruku
3	Identyfikacja kontrolera, (jeżeli w czytniku VU znajduje się karta kontrolna)
3	Identyfikacja kierowcy (z karty, dla której sporządzany jest wydruk)
4	Identyfikacja pojazdu (tego, dla którego sporządzany jest wydruk)
12.2	Ogranicznik zdarzeń
12.4	Zapisy zdarzeń (wszystkie zdarzenia zarejestrowane na karcie)
12.3	Ogranicznik usterek
12.4	Zapisy usterek (wszystkie usterki zarejestrowane na karcie)
21.1	Miejsce kontroli
21.2	Podpis kontrolera
21.5	Podpis kierowcy

3.4. Wydruk zdarzeń i usterek z VU

PRT_010 Wydruk zdarzeń i usterek z VU jest zgodny z poniższym formatem:

1	Data i godzina drukowania dokumentu
2	Typ wydruku
3	Identyfikacja posiadacza karty (dla wszystkich kart włożonych do VU)
4	Identyfikacja pojazdu (tego, dla którego sporządzany jest wydruk)
13.2	Ogranicznik zdarzeń
13.4	Zapisy zdarzeń (wszystkie zdarzenia zarejestrowane lub trwające w VU)
13.3	Ogranicznik usterek
13.4	Zapisy usterek (wszystkie usterki zarejestrowane lub trwające w VU)
21.1	Miejsce kontroli
21.2	Podpis kontrolera
21.5	Podpis kierowcy

3.5. Wydruk danych technicznych

PRT_011 Wydruk danych technicznych jest zgodny z poniższym formatem:

1	Data i godzina drukowania dokumentu
2	Typ wydruku
3	Identyfikacja posiadacza karty (dla wszystkich kart włożonych do VU)
4	Identyfikacja pojazdu (tego, dla którego sporządzany jest wydruk)
14	Identyfikacja VU
15	Identyfikacja czujnika
16	Ogranicznik danych kalibracyjnych
16.1	Zapisy kalibracji (wszystkie dostępne rekordy w kolejności chronologicznej)
17	Ogranicznik regulacji czasu
17.1	Zapisy regulacji czasu (wszystkie dostępne zapisy z zapisów regulacji czasu i zapisów kalibracji)
18	Ostatnie zdarzenie i usterka zarejestrowane w VU

3.6. Wydruk przekroczenia prędkości

PRT_012 Wydruk przekroczenia prędkości jest zgodny z poniższym formatem:

1	Data i godzina drukowania dokumentu
2	Typ wydruku
3	Identyfikacja posiadacza karty (dla wszystkich kart włożonych do VU)
4	Identyfikacja pojazdu (tego, dla którego sporządzany jest wydruk)
19	Informacje kontrolne dotyczące przekroczenia prędkości
20.1	Identyfikator danych dotyczących przekroczenia prędkości
20.4 / 20.5	Pierwsze przekroczenie prędkości po ostatniej kalibracji
20.2	Identyfikator danych dotyczących przekroczenia prędkości
20.4 / 20.5	5 najpoważniejszych przekroczeń prędkości w ciągu ostatnich 365 dni
20.3	Identyfikator danych dotyczących przekroczenia prędkości
20.4 / 20.5	Najpoważniejsze przekroczenie prędkości dla każdego z ostatnich 10 dni ich występowania
21.1	Miejsce kontroli
21.2	Podpis kontrolera
21.5	Podpis kierowcy.

Dodatek 5

WYŚWIETLACZ

W tym rozdziale przyjęto następujące konwencje zapisu formatu:

- znaki wytłuszczonym drukiem oznaczają odkryty tekst widoczny na wyświetlaczu (są wyświetlane jako normalne znaki),
- znaki normalne oznaczają zmienne (piktogramy lub dane), które na wyświetlaczu zastępowane są przez odpowiadające im wartości:
 - dd mm yyyy: dzień, miesiąc, rok,
 - hh: godziny,
 - mm: minuty,
 - D: piktogram czasu trwania,
 - EF: kombinacja piktogramów zdarzeń lub usterek,
 - O: piktogram trybu pracy.

DIS_001 Urządzenie rejestrujące wyświetla dane zgodnie z poniższymi formatami:

Dane	Format
Wyświetlanie ustawień domyślnych	
Czas miejscowy	hh:mm
Tryb pracy	O
Informacje dotyczące kierowcy	1 Dhhmm hhmm
Informacje dotyczące współkierowcy	2 Dhhmm
Otwarty warunek poza zakresem	OUT
Ostrzeżenia	
Nadmierny nieprzerwany czas prowadzenia pojazdu	1 0hhmm hhmm
Zdarzenie lub usterka	EF
Inne komunikaty	
Data UTC	UTC 0 dd/mm/yyyy or UTC 0 dd.mm.yyyy
godzina	hh:mm
Nieprzerwany czas prowadzenia pojazdu przez kierowcę i skumulowany czas przerwy	1 0hhmm hhmm
Nieprzerwany czas prowadzenia pojazdu przez współkierowcę i skumulowany czas przerwy	2 0hhmm hhmm
Skumulowany czas prowadzenia pojazdu przez kierowcę za ubiegły i obecny tydzień	1 0 hhhhmm
Skumulowany czas prowadzenia pojazdu przez współkierowcę za ubiegły i obecny tydzień	2 0 hhhhmm

*Dodatek 6***INTERFEJSY ZEWNĘTRZNE**

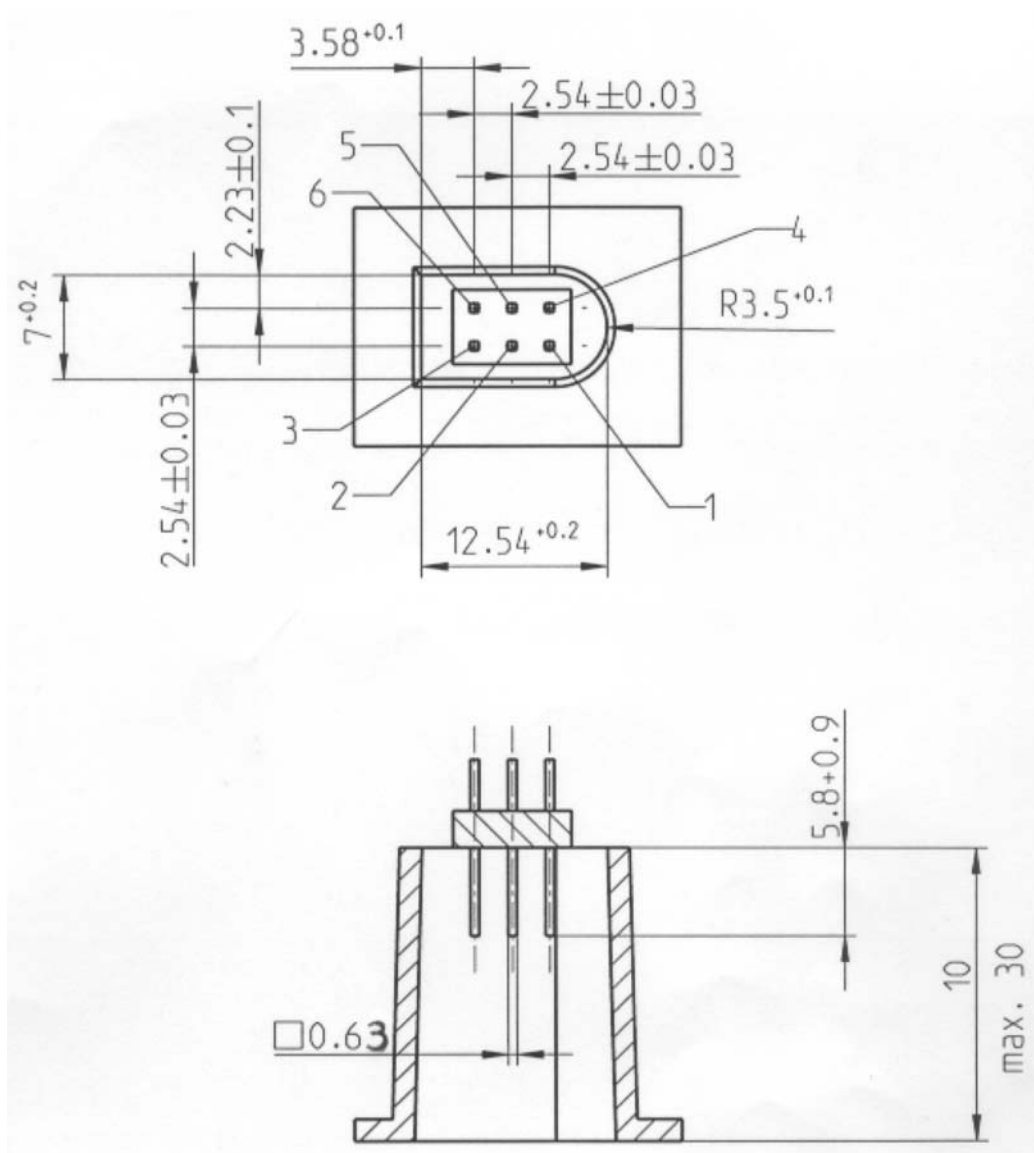
SPIS TREŚCI

1.	Sprzęt	422
1.1.	Złącze	422
1.2.	Rozmieszczenie styków	424
1.3.	Schemat blokowy	424
2.	Interfejs wczytywania danych	425
3.	Interfejs kalibracyjny	425

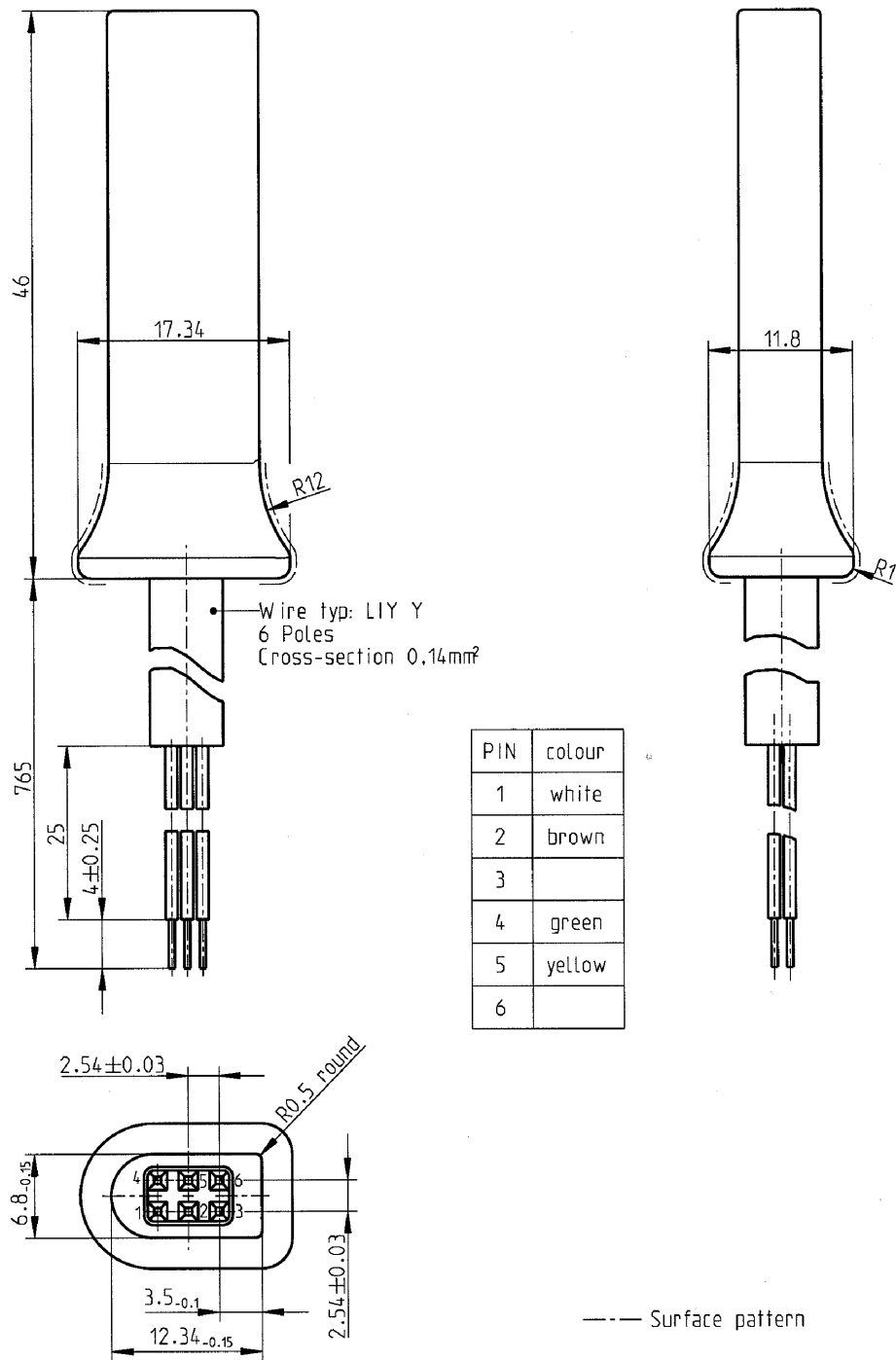
1. SPRZĘT

1.1. Złącze

INT_001 Złącze wczytywania danych/kalibracji jest złączem sześciostykowym, dostępnym od strony panelu czołowego bez potrzeby odłączania jakiegokolwiek części urządzenia rejestrującego. Złącze musi mieć wymiary zgodne z pokazanymi na rysunku poniżej (wszystkie wymiary w milimetrach):



Na rysunku poniżej pokazano typową sześciostykową bolcową wtyczkę złączną:



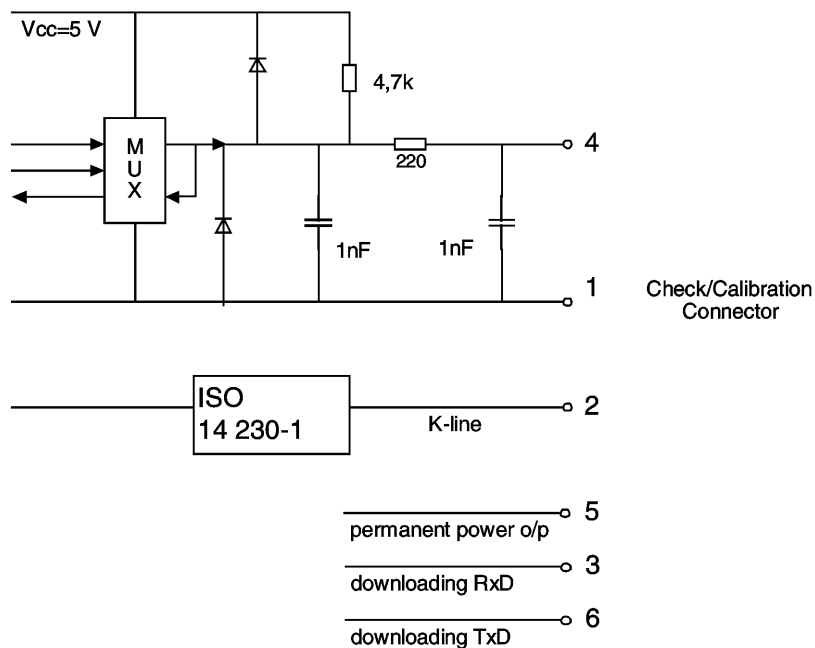
1.2. Rozmieszczenie styków

INT_002 Funkcje styków opisuje poniższa tabela:

Styk	Opis	Uwagi
1	minus akumulatora	Przyłączony do minusa akumulatora pojazdu
2	przesyłanie danych	K-line (ISO 14 230-1)
3	RxD — wczytywanie danych	Wejście danych do urządzenia rejestrującego
4	Sygnał we/wy	Kalibracja
5	Wyjście zasilania	Zakres napięcia musi być taki jak dla zasilania pojazdu minus 3V w celu umożliwienia spadku napięcia na obwodzie ochronnym Wyjście 40 mA
6	TxD — wczytywanie danych	Wyjście danych z urządzenia rejestrującego

1.3. Schemat blokowy

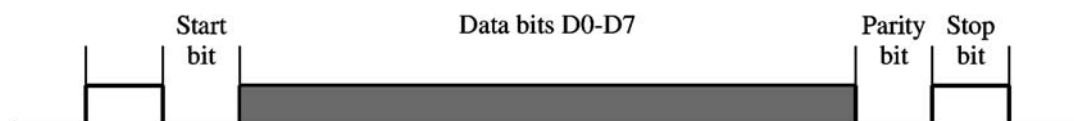
INT_003 Schemat blokowy jest następujący:



2. INTERFEJS WCZYTYWANIA DANYCH

INT_004 Interfejs wczytywania danych jest zgodny z wymaganiami RS232.

INT_005 Interfejs wczytywania danych jest skonfigurowany w następujący sposób: jeden bit startowy, 8 bitów danych najmniej znaczących na początku, jeden bit parzystości i jeden bit stopu.



Organizacja bajtu danych

bit startowy: jeden bit na poziomie logicznym 0

bity danych: przesłane z najmniej znaczącym na początku

bit parzystości: kontrola parzystości

bit stopu: jeden bit na poziomie logicznym 1

W przypadku przesyłania danych liczbowych złożonych z więcej niż jednego bajtu bajt najbardziej znaczący jest przesyłany pierwszy a bajt najmniej znaczący ostatni.

INT_006 Bitowa szybkość transmisji danych regulowana jest w zakresie od 9 600 bit/s do 115 200 bit/s. Transmisja odbywa się z najwyższą możliwą szybkością, przy czym szybkość początkowa przy inicjowaniu sesji ustawiona jest na 9 600 bit/s.

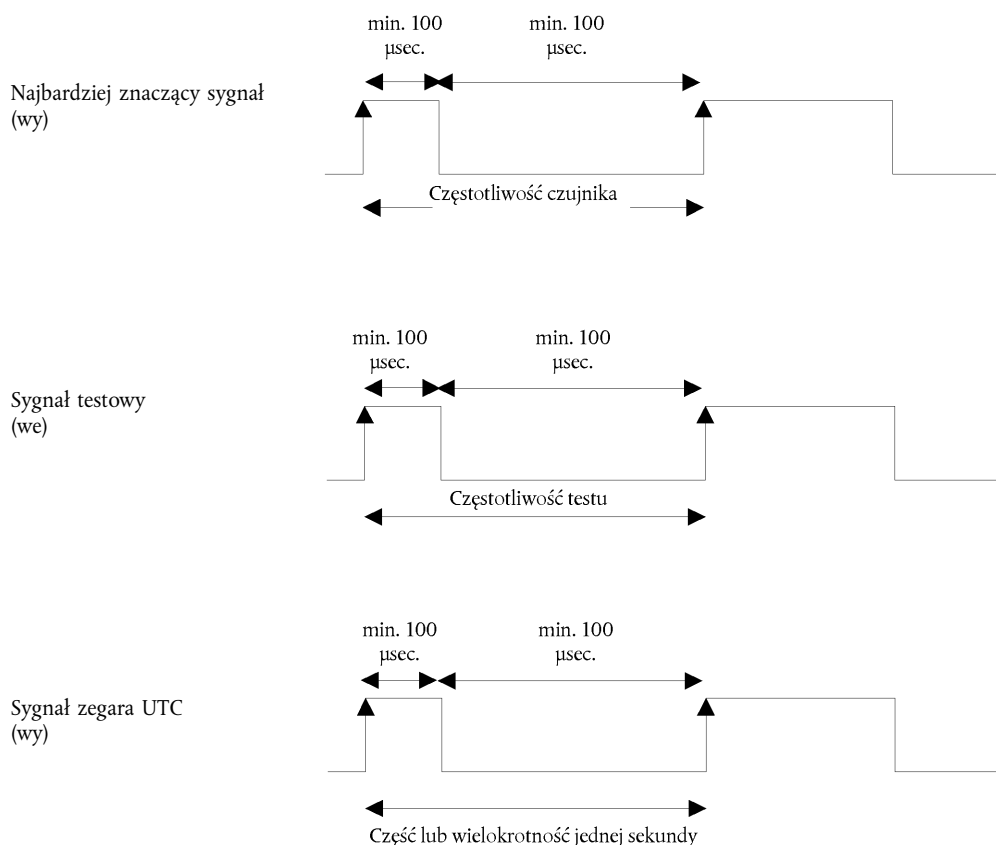
3. INTERFEJS KALIBRACYJNY

INT_007 Przesyłanie danych jest zgodne z normą ISO 14 230-1 Pojazdy drogowe — Systemy diagnostyczne — Protokół słów kluczowych 2000 — część 1: Warstwa fizyczna, Wydanie pierwsze: 1999 r.

INT_008 Sygnał we/wy jest zgodny z następującymi wymaganiami elektrycznymi:

Parametr	Min.	Typowy	Maks.	Uwagi
U_{low} (in)			1,0 V	$I = 750 \mu\text{A}$
U_{high} (in)	4 V			$I = 200 \mu\text{A}$
Częstotliwość			4 kHz	
U_{low} (in)			1,0 V	$I = 1 \text{ mA}$
U_{high} (out)	4 V			$I = 1 \text{ mA}$

INT_009 Sygnał we/wy jest zgodny z następującymi przebiegami czasowymi:



Dodatek 7

PROTOKOŁY WCZYTYWANIA DANYCH

SPIS TREŚCI

1.	Wprowadzenie	428
1.1.	Zakres	428
1.2.	Akronimy i skróty	428
2.	Wczytywanie danych z VU	429
2.1.	Procedura wczytywania danych	429
2.2.	Protokół wczytywania danych	429
2.2.1.	Struktura komunikatu	429
2.2.2.	Typy komunikatów	430
2.2.2.1.	Żądanie rozpoczęcia transmisji (SID 81)	432
2.2.2.2.	Pozytywna odpowiedź na żądanie rozpoczęcia transmisji (SID C1)	432
2.2.2.3.	Żądanie rozpoczęcia sesji diagnostycznej (SID 10)	432
2.2.2.4.	Pozytywna odpowiedź na żądanie rozpoczęcia sesji diagnostycznej (SID 50)	432
2.2.2.5.	Obsługa sterowania łączem (SID 87)	432
2.2.2.6.	Pozytywna odpowiedź na żądanie sterowania łączem (SID C7)	432
2.2.2.7.	Żądanie wczytywania (SID 35)	432
2.2.2.8.	Pozytywna odpowiedź na żądanie wczytywania (SID 75)	432
2.2.2.9.	Żądanie przesłania danych (SID 36)	432
2.2.2.10.	Pozytywna odpowiedź na żądanie przesłania danych (SID 76)	433
2.2.2.11.	Żądanie wyjścia z przesyłania danych (SID 37)	433
2.2.2.12.	Pozytywna odpowiedź na żądanie wyjścia z przesyłania danych (SID 77)	433
2.2.2.13.	Żądanie zatrzymania transmisji (SID 82)	433
2.2.2.14.	Pozytywna odpowiedź na żądanie zatrzymania transmisji (SID C2)	433
2.2.2.15.	Potwierdzenie podkomunikatu (SID 83)	433
2.2.2.16.	Odpowiedź negatywna (SID 7F)	433
2.2.3.	Przepływ komunikatów	434
2.2.4.	Przebiegi czasowe	435
2.2.5.	Obsługa błędów	435
2.2.5.1.	Faza rozpoczęcia komunikacji	435
2.2.5.2.	Faza komunikacji	435
2.2.6.	Treść komunikatu odpowiedzi	438
2.2.6.1.	Pozytywna odpowiedź na żądanie przesłania informacji ogólnych	438
2.2.6.2.	Pozytywna odpowiedź na żądanie przesłania danych dotyczących czynności	439
2.2.6.3.	Pozytywna odpowiedź na żądanie przesłania danych dotyczących zdarzeń i usterek	440

2.2.6.4.	Pozytywna odpowiedź na żądanie przesłania danych szczegółowych dotyczących prędkości	441
2.2.6.5.	Pozytywna odpowiedź na żądanie przesłania danych technicznych	441
2.3.	Plik ESM	442
3.	Protokół wczytywania danych z kart do tachografów	442
3.1.	Zakres	442
3.2.	Definicje	442
3.3.	Wczytywanie danych z karty	442
3.3.1.	Sekwencja inicjalizująca	443
3.3.2.	Sekwencja dla niepodpisanych plików danych	443
3.3.3.	Sekwencja dla podpisanych plików danych	443
3.3.4.	Sekwencja zerowania licznika kalibracji	444
3.4.	Format gromadzenia danych	444
3.4.1.	Wprowadzenie	444
3.4.2.	Format pliku	444
4.	Wczytywanie danych z karty do tachografów za pośrednictwem przyrządu rejestrującego	445

1. WPROWADZENIE

Niniejszy dodatek zawiera procedury stosowane przy wczytywaniu danych różnych typów na media zewnętrzne, wraz z protokołami, które muszą być wdrożone w celu zagwarantowania prawidłowego przesyłania danych i pełnej zgodności formatu wczytanych danych, tak by umożliwić każdemu kontrolerowi sprawdzenie tych danych oraz sprawdzenie autentyczności i integralności przed przystąpieniem do analizy danych.

1.1. Zakres

Dane mogą być wczytywane do ESM:

- z przyrządu rejestrującego za pośrednictwem inteligentnego, wydzielonego urządzenia (IDE) przyłączonego do VU,
- z karty do tachografów za pośrednictwem IDE spasowanego z urządzeniem interfejsu (IFD) karty,
- z karty do tachografów za pośrednictwem przyrządu rejestrującego poprzez IDE przyłączone do VU.

Aby umożliwić weryfikację autentyczności i integralności wczytanych danych zgromadzonych w ESM, dane są wczytywane razem z dołączonym podpisem, zgodnie z dodatkiem 11 Wspólne mechanizmy zabezpieczenia. Razem z danymi wczytywane są również identyfikacja urządzenia źródłowego (VU lub karta) i jego świadectwo bezpieczeństwa (Państwo Członkowskie i urządzenie). Niezależnie od tego weryfikator danych musi mieć zaufany europejski klucz publiczny.

DDP_001 Dane wczytane podczas jednej sesji wczytywania muszą być przechowywane w ESM w jednym pliku.

1.2. Akronimy i skróty

W niniejszym dodatku używa się następujących skrótów:

AID	identyfikator aplikacji
ATR	odpowiedź na ponowne inicjowanie
CS	bajt sumy kontrolnej
DF	plik dedykowany
DS_	sesja diagnostyczna
EF	plik elementarny
ESM	zewnętrzne medium gromadzenia danych
FID	identyfikator pliku (ID pliku)
FMT	bajt formatu (pierwszy bajt nagłówka komunikatu)
ICC	karta z układem scalonym
IDE	inteligentne urządzenie dedykowane: urządzenie służące do wczytywania danych do ESM (np. komputer osobisty)
IFD	urządzenie interfejsu
KWP	protokół słowa kluczowego 2000
LEN	bajt długości (ostatni bajt nagłówka komunikatu)
PPS	wybór parametru protokołu
PSO	wykonaj operację bezpieczeństwa
SID	identyfikator usługi
SRC	bajt źródłowy
TGT	bajt docelowy
TLV	wartość długości znacznika
TREP	parametr odpowiedzi na przesłanie danych
TRTP	parametr żądania przesłania danych
VU	przyrząd rejestrujący.

2. WCZYTYWANIE DANYCH Z VU

2.1. Procedura wczytywania danych

W celu wczytania danych z VU operator musi wykonać następujące czynności:

- włożyć swoją kartę do tachografów do czytnika karty w VU ⁽¹⁾,
- podłączyć IDE do gniazda wczytywania w VU,
- nawiązać połączenie między IDE i VU,
- wybrać w IDE dane do wczytania i wysłać żądanie do VU,
- zamknąć sesję wczytywania danych.

2.2. Protokół wczytywania danych

Protokół skonstruowany jest zgodnie z zasadą nadrzędny-podległy, gdzie IDE jest urządzeniem nadrzędnym a VU podległym.

Struktura komunikatu, typy komunikatów i przepływ są zasadniczo oparte na Protokole słowa kluczowego 2000 (KWP) (według normy ISO 14230-2 Pojazdy drogowe — Systemy diagnostyczne — Protokół słowa kluczowego 2000 — część 2: Warstwa łączy danych).

Warstwa aplikacji zbudowana jest zasadniczo w oparciu o bieżący projekt normy ISO 14229-1 (Pojazdy drogowe — Systemy diagnostyczne — część 1: Usługi diagnostyczne, wersja 6 z dnia 22 lutego 2001 r.)

2.2.1. Struktura komunikatu

DDP_002 Wszystkie komunikaty wymieniane między IDE i VU mają strukturę złożoną z następujących trzech części:

- nagłówek zawierający bajt formatu (FMT), bajt docelowy (TGT), bajt źródłowy (SRC) i ewentualnie bajt długości (LEN),
- pole danych zawierające bajt identyfikator usługi (SID) i zmienną liczbę bajtów z danymi, w których może być bajt opcjonalnej sesji diagnostycznej (DS_) lub bajt opcjonalnego parametru przesyłania (TRTP lub TREP).
- suma kontrolna zawierająca bajt sumy kontrolnej (CS).

Nagłówek				Pole danych					Suma kontrolna
FMT	TGT	SRC	LEN	SID	ADAT	...	...	...	CS
4 bajty				Maks. 225 bajtów					1 bajt

Bajty TGT i SRC reprezentują fizyczny adres adresata i źródła komunikatu. Przyjmują one wartości F0 Hex dla IDE i EE Hex dla VU.

Bajt LEN jest długością pola danych.

Bajt sumy kontrolnej jest ośmiobitową sumą serii modulo 256 wszystkich bajtów komunikatu, z wyłączeniem bajtu CS.

Bajty FMT, SID, DS_, TRTP i TREP są zdefiniowane w dalszej części niniejszego dokumentu.

⁽¹⁾ Włożenie karty otwiera właściwe prawo dostępu do uaktywnienia funkcji oraz do danych.

DDP_003 W przypadku gdy dane przesyłane komunikatem są dłuższe niż dysponowane pole danych, komunikat wysyła się w kilku podkomunikatach. Każdy podkomunikat ma nagłówek, te same bajty SID i TREP oraz dwubajtowy licznik podkomunikatu pokazujący liczbę podkomunikatów w całym komunikacie. Aby umożliwić kontrolę błędów i przerwanie przesyłania, IDE potwierdza każdy komunikat. IDE może przyjmować podkomunikat, żądać powtórzenia transmisji, żądać od VU powtórzenia transmisji od początku lub przerywania transmisji.

DDP_004 Jeżeli ostatni podkomunikat ma dokładnie 255 bajtów w polu danych, musi być dołączony końcowy podkomunikat z pustym polem danych (z wyjątkiem SID TREP i licznika podkomunikatów) w celu pokazania końca komunikatu.

Przykład:

Nagłówek	SID	TREP	Komunikat	CS
4 bajty	dłuższy niż 255 bajtów			

zostanie przesłany w następujący sposób:

Nagłówek	SID	TREP	00	01	Podkomunikat 1	CS
4 bajty	255 bajtów					

Nagłówek	SID	TREP	00	01	Podkomunikat 2	CS
4 bajty	255 bajtów					

...

Nagłówek	SID	TREP	xx	yy	Podkomunikat n	CS
4 bajty	Mniej niż 255 bajtów					

lub:

Nagłówek	SID	TREP	00	01	Podkomunikat 1	CS
4 bajty	255 bajtów					

Nagłówek	SID	TREP	00	02	Podkomunikat 2	CS
4 bajty	255 bajtów					

...

Nagłówek	SID	TREP	xx	yy	Podkomunikat n	CS
4 bajty	255 bajtów					

Nagłówek	SID	TREP	xx	yy+1	CS
4 bajty	4 bajty				

2.2.2. Typy komunikatów

Protokół komunikacyjny wczytywania danych między VU i IDE wymaga wymiany komunikatów ośmiu różnych typów.

W tabeli poniżej opisano te komunikaty.

Struktura komunikatu	Nagłówek maks. 4 bajty				Dane maks. 255 bajtów			Suma Kontrolna 1 bajt
IDE ->	FMT	TGT	SRC	LEN	SID	DS/TRTP	DATA	CS
<- VU								
Żądanie rozpoczęcia transmisji	81	EE	F0		81			E0
Pozytywna odpowiedź na żądanie rozpoczęcia transmisji	80	F0	EE	03	C1		8F,EA	9B
Żądanie rozpoczęcia sesji diagnostycznej	80	EE	F0	02	10	81		F1
Pozytywna odpowiedź na żądanie rozpoczęcia sesji diagnostycznej	80	F0	EE	02	50	81		31
Obsługa sterowania łączem								
weryfikacja szybkości transmisji (etap 1)								
9 600 bit/s	80	EE	F0	04	87		01,01,01	EC
19 200 bit/s	80	EE	F0	04	87		01,01,02	ED
38 400 bit/s	80	EE	F0	04	87		01,01,03	ED
57 600 bit/s	80	EE	F0	04	87		01,01,04	EF
115 200 bit/s	80	EE	F0	04	87		01,01,05	F0
Pozytywna odpowiedź na weryfikację szybkości transmisji	80	F0	EE	02	C7		01	28
Zmiana szybkości transmisji (etap 2)	80	EE	F0	03	87		02,03	ED
Żądanie wczytywania	80	EE	F0	0A	35		00,00,00, 00,00,FF,FF, FF,FF	99
Pozytywna odpowiedź na żądanie wczytywania	80	F0	EE	03	75		00,FF	D5
Żądanie przesłania danych								
Informacje ogólne	80	EE	F0	02	36	01		97
Czynności	80	EE	F0	06	36	02	Data	CS
Zdarzenia i usterki	80	EE	F0	02	36	03		99
Szczegółowe dane dotyczące prędkości	80	EE	F0	02	36	04		9A
Dane techniczne	80	EE	F0	02	36	05		9B
Wczytywanie karty	80	EE	F0	02	36	06		9C
Pozytywna odpowiedź na żądanie przesłania danych	80	F0	EE	Len	76	TREP	Data	CS
Żądanie wyjścia z przesyłania danych	80	EE	F0	01	37			96
Pozytywna odpowiedź na żądanie wyjścia z przesyłania danych	80	F0	EE	01	77			D6
Żądanie zatrzymania transmisji	80	EE	F0	01	82			E1
Pozytywna odpowiedź na żądanie zatrzymania transmisji	80	F0	EE	01	C2			21
Potwierdzenie podkomunikatu	80	EE	F0	Len	83		Data	CS
Odpowiedzi negatywne								
Generalne odrzucenie	80	F0	EE	03	7F	Sid Req	10	CS
Usługa nieobsługiwana	80	F0	EE	03	7F	Sid Req	11	CS
Podfunkcja nieobsługiwana	80	F0	EE	03	7F	Sid Req	12	CS
Nieprawidłowa długość komunikatu	80	F0	EE	03	7F	Sid Req	13	CS
Nieprawidłowe warunki lub błąd kolejności żądań	80	F0	EE	03	7F	Sid Req	22	CS
Żądanie poza zakresem	80	F0	EE	03	7F	Sid Req	31	CS
Ładowanie nie przyjęte	80	F0	EE	03	7F	Sid Req	50	CS
Odpowiedź zawieszona	80	F0	EE	03	7F	Sid Req	78	CS
Brak dostępnych danych	80	F0	EE	03	7F	Sid Req	FA	CS

Uwagi:

— Sid Req = Sid odpowiadającego żądania.

— TREP = TRTP odpowiadającego żądania.

— Ciemne rubryki oznaczają, że nic nie jest przesyłane.

— Pojęcia ładowanie (widziane z IDE) używa się zgodnie z normą ISO 14229. Oznacza to samo co wczytywanie (gdy widziane z VU).

— W tabeli nie pokazano potencjalnych, dwubajtowych liczników podkomunikatów.

2.2.2.1. Żądanie rozpoczęcia transmisji (SID 81)

DDP_005 Komunikat ten wysyła IDE w celu zestawienia łącza komunikacyjnego z VU. Początkowe komunikaty są zawsze wysyłane z szybkością 9 600 bit/s (aż do ewentualnej zmiany szybkości transmisji przy wykorzystaniu odpowiedniej obsługi sterowania łączem).

2.2.2.2. Pozytywna odpowiedź na żądanie rozpoczęcia transmisji (SID C1)

DDP_006 Komunikat ten wysyła VU w celu przesłania pozytywnej odpowiedzi na żądanie rozpoczęcia transmisji. Komunikat zawiera 2 kluczowe bajty 2 »8F«EA» wskazujące, że urządzenie obsługuje protokół z nagłówkiem zawierającym informacje o adresie, źródle i długości.

2.2.2.3. Żądanie rozpoczęcia sesji diagnostycznej (SID 10)

DDP_007 Komunikat żądania rozpoczęcia sesji diagnostycznej wysyła IDE w celu zażądania nowej sesji diagnostycznej z VU. Podfunkcja »default session« (81 Hex) wskazuje, że IDE żąda otwarcia standardowej sesji diagnostycznej.

2.2.2.4. Pozytywna odpowiedź na żądanie rozpoczęcia sesji diagnostycznej (SID 50)

DDP_008 Komunikat pozytywnej odpowiedzi na żądanie rozpoczęcia sesji diagnostycznej wysyła VU w celu przesłania pozytywnej odpowiedzi na żądanie sesji diagnostycznej.

2.2.2.5. Obsługa sterowania łączem (SID 87)

DDP_052 IDE używa obsługi sterowania łączem do zainicjowania zmiany szybkości transmisji (bit/s). Odbywa się to dwustopniowo. Najpierw IDE proponuje zmianę szybkości transmisji podając nową szybkość (pierwszy krok). Po otrzymaniu pozytywnej odpowiedzi od VU IDE wysyła do VU potwierdzenie zmiany szybkości (drugi krok). Następnie IDE przechodzi na nową szybkość transmisji. Po otrzymaniu potwierdzenia VU przechodzi na nową szybkość transmisji.

2.2.2.6. Pozytywna odpowiedź na żądanie sterowania łączem (SID C7)

DDP_053 VU wysyła pozytywną odpowiedź na żądanie sterowania łączem w celu przesłania pozytywnej odpowiedzi na żądanie obsługi sterowania łączem (pierwszy krok). Zwracamy uwagę, że na żądanie potwierdzenia (drugi krok) nie ma odpowiedzi.

2.2.2.7. Żądanie wczytywania (SID 35)

DDP_009 IDE wysyła komunikat żądania wczytywania w celu przekazania VU, że żądana jest operacja wczytywania. Aby spełnić wymagania normy ISO14229 przesyłane są szczegółowe informacje dotyczące adresu, wielkości i szczegółów żądanych danych. Ponieważ informacje te nie są znane IDE przed wczytywaniem, adres pamięci ustawiony jest na 0, format jest nieszyfrowany i bez kompresji a wielkość pamięci ustawiona na maksimum.

2.2.2.8. Pozytywna odpowiedź na żądanie wczytywania (SID 75)

DDP_010 VU wysyła pozytywną odpowiedź na żądanie wczytywania, aby wskazać IDE, że VU jest gotowe do wczytywania danych. Aby spełnić wymagania normy ISO 14229 ten komunikat pozytywnej odpowiedzi zawiera dane wskazujące IDE, że dalsze komunikaty pozytywnej odpowiedzi na żądanie przesłania danych będą zawierały maksymalnie 00FF hex bajtów.

2.2.2.9. Żądanie przesłania danych (SID 36)

DDP_011 IDE wysyła żądanie przesłania danych w celu wskazania VU typu danych, które mają być wczytywane. Jednobajtowy parametr żądania przesłania danych (TRTP) wskazuje typ przesyłania.

Rozróżnia się sześć typów przesyłania danych:

- informacje ogólne (TRTP 01),
- czynności o określonej dacie (TRTP 02),
- zdarzenia i usterki (TRTP 03),
- szczegółowe dane dotyczące prędkości (TRTP 04),
- dane techniczne (TRTP 05),
- wczytywanie karty (TRTP 06).

DDP_054 IDE musi obowiązkowo zażądać przesłania informacji ogólnych (TRTP 01) w czasie sesji wczytywania, ponieważ tylko to zagwarantuje, że certyfikaty VU są zarejestrowane we wczytywanym pliku (i umożliwi weryfikację podpisu cyfrowego).

W drugim przypadku (TRTP 02) w komunikacie żądanie przesłania danych znajduje się informacja o dniu kalendarzowym (TimeReal format), dla którego dane mają być wczytane.

2.2.2.10. Pozytywna odpowiedź na żądanie przesłania danych (SID 76)

DDP_012 VU wysyła pozytywną odpowiedź na żądanie przesłania w odpowiedzi na żądanie przesłania danych. Komunikat zawiera żądane dane z parametrem odpowiedzi na przesłanie danych (TREP) odpowiadającym TRTP żądania.

DDP_055 W pierwszym przypadku (TREP 01), VU wyśle dane pomagające operatorowi IDE w wyborze danych, które chce dalej wczytać. Komunikat ten zawiera następujące informacje:

- świadectwa bezpieczeństwa,
- identyfikacja pojazdu,
- bieżąca data i godzina VU,
- minimalna i maksymalna data, dla której można dokonać wczytania (VU dane),
- sygnalizacja obecności kart w VU,
- poprzednie wczytanie dla firmy,
- blokady firmowe,
- poprzednie kontrole.

2.2.2.11. Żądanie wyjścia z przesyłania danych (SID 37)

DDP_013 IDE wysyła komunikat żądania wyjścia z przesyłania danych w celu zawiadomienia VU, że sesja wczytywania jest zakończona.

2.2.2.12. Pozytywna odpowiedź na żądanie wyjścia z przesyłania danych (SID 77)

DDP_014 VU wysyła komunikat pozytywnej odpowiedzi na żądanie wyjścia z przesyłania danych w celu potwierdzenia otrzymania żądania wyjścia z przesyłania danych.

2.2.2.13. Żądanie zatrzymania transmisji (SID 82)

DDP_015 IDE wysyła komunikat żądania zatrzymania transmisji w celu rozłączenia łącza komunikacyjnego z VU.

2.2.2.14. Pozytywna odpowiedź na żądanie zatrzymania transmisji (SID C2)

DDP_016 VU wysyła komunikat pozytywnej odpowiedzi na żądanie zatrzymania transmisji w celu potwierdzenia otrzymania żądania zatrzymania transmisji.

2.2.2.15. Potwierdzenie podkomunikatu (SID 83)

DDP_017 IDE wysyła potwierdzenie podkomunikatu w celu potwierdzenia otrzymania każdej części komunikatu przesyłanego w kilku podkomunikatach. W polu danych znajduje się SID otrzymany z VU i dwubajtowy kod opisany poniżej:

- MsgC +1 potwierdza prawidłowy odbiór podkomunikatu o numerze MsgC.

Żądanie od IDE dla VU wysłania następnego podkomunikatu,

- MsgC wskazuje na problem z odbiorem podkomunikatu o numerze MsgC.

Żądanie od IDE dla VU powtórnego wysłania podkomunikatu,

- FFFF żąda zakończenia komunikatu.

IDE może użyć tego do zakończenia transmisji komunikatu z VU z dowolnej przyczyny.

Ostatni podkomunikat komunikatu (bajt LEN < 255) może być potwierdzony przy pomocy dowolnego z tych kodów lub być niepotwierdzony.

Odpowiedziami VU, które składają się z kilku podkomunikatów są:

- pozytywna odpowiedź na żądanie przesłania danych (SID 76)

2.2.2.16. Odpowiedź negatywna (SID 7F)

DDP_018 VU wysyła komunikat negatywnej odpowiedzi w odpowiedzi na powyższe komunikaty żądań, gdy VU nie może obsłużyć żądania. Pole danych komunikatu zawiera SID odpowiedzi (7F), SID żądania i kod podający przyczynę negatywnej odpowiedzi. Dozwolone są następujące kody:

- 10 generalne odrzucenie
Czynności nie można wykonać z przyczyny innej niż określone poniżej
- 11 usługa nieobsługiwana
SID żądania nie jest zrozumiany
- 12 podfunkcja nieobsługiwana
DS_ lub TRTP żądania nie jest zrozumiany lub nie ma dalszych komunikatów do wysłania
- 13 nieprawidłowa długość komunikatu
Długość odebranego komunikatu jest nieprawidłowa
- 22 nieprawidłowe warunki lub błąd kolejności żądań
Żądana usługa nie jest aktywna lub sekwencja komunikatów żądań nie jest prawidłowa
- 31 żądanie poza zakresem
Żądany zapis parametru (pole danych) nie jest ważny
- 50 ładowanie nieprzyjęte
Żądania nie można obsłużyć (VU w nieodpowiednim trybie pracy lub wewnętrzna usterka VU)
- 78 odpowiedź zawieszona
Czynności nie można zakończyć na czas i VU nie jest gotowe do przyjęcia innego żądania
- FA brak dostępnych danych
Obiekt danych żądania przesłania danych nie jest dostępny w VU (np. karta nie jest włożona,...)

2.2.3. Przepływ komunikatów

Typowy przepływ komunikatów podczas normalnej procedury wczytywania danych wygląda następująco:

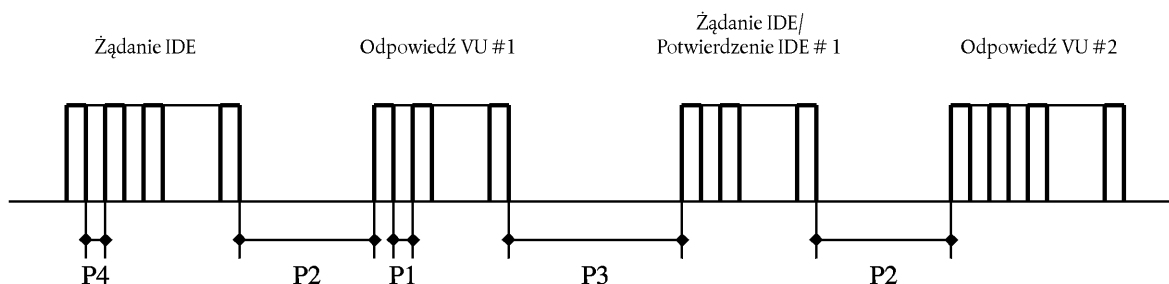
IDE		FE
Żądanie rozpoczęcia transmisji	⇒ ⇐	Pozytywna odpowiedź
Żądanie rozpoczęcia usługi diagnostycznej	⇒ ⇐	Pozytywna odpowiedź
Żądanie wczytywania	⇒ ⇐	Pozytywna odpowiedź
Żądanie przesłania danych informacje ogólne	⇒ ⇐	Pozytywna odpowiedź na żądanie przesłania danych
Żądanie danych #2	⇒ ⇐	Pozytywna odpowiedź #1
Potwierdzenie podkomunikatu #1	⇒ ⇐	Pozytywna odpowiedź #2
Potwierdzenie podkomunikatu #2	⇒ ⇐	Pozytywna odpowiedź #m
Potwierdzenie podkomunikatu #m	⇒ ⇐	Pozytywna odpowiedź na żądanie (pole danych < 255 bajtów)
Potwierdzenie podkomunikatu (nieobowiązkowe)	⇒	
...		
Żądanie przesłania danych #n	⇒ ⇐	Pozytywna odpowiedź
Żądanie wyjścia z przesyłania danych	⇒ ⇐	Pozytywna odpowiedź
Żądanie zatrzymania transmisji	⇒ ⇐	Pozytywna odpowiedź

2.2.4. Przebiegi czasowe

DDP_019 Podczas normalnej pracy przebiegi czasowe wyglądają jak następuje:

Rysunek 1

Przepływ komunikatów, przebiegi czasowe



Gdzie:

P1 = czas między bajtami dla odpowiedzi VU.

P2 = czas między końcem żądania IDE a początkiem odpowiedzi VU, lub między końcem potwierdzenia IDE a początkiem następnej odpowiedzi VU.

P3 = między końcem odpowiedzi VU a początkiem nowego żądania IDE, lub między końcem odpowiedzi VU a początkiem potwierdzenia IDE, lub między końcem żądania IDE a początkiem nowego żądania IDE, jeżeli VU nie odpowiada.

P4 = czas między bajtami dla żądania IDE.

P5 = przedłużona wartość P3 dla wczytywania danych z karty.

Dozwolone wartości przebiegów czasowych pokazano w tabeli poniżej (KWP rozszerzony zestaw parametrów przebiegów czasowych używany w przypadku adresowania fizycznego w celu uzyskania szybszej komunikacji).

Parametr czasowy	Dolna wartość graniczna Pmin (ms)	Górna wartość graniczna Pmax (ms)
P1	0	20
P2	20	1 000 (*)
P3	10	5 000
P4	5	20
P5	10	20 minut

(*) Jeżeli VU daje negatywną odpowiedź zawierającą kod o znaczeniu »żądane odebrane prawidłowo, odpowiedź zawieszona«, wartość ta zostaje przedłużona do górnej wartości granicznej P3.

2.2.5. Obsługa błędów

W przypadku wystąpienia błędu w czasie wymiany komunikatów, schemat przepływu komunikatów zostaje zmodyfikowany zależnie od tego, które urządzenie wykryło błąd i od komunikatu generującego błąd.

Na rysunkach 2 i 3 pokazano odpowiednio procedury obsługi błędów dla VU i IDE.

2.2.5.1. Faza rozpoczęcia komunikacji

DDP_020 Jeżeli w czasie fazy rozpoczęcia komunikacji IDE wykryje błąd zarówno synchronizacji jak i strumienia bitowego, to odczeka okres P3 min przed powtórным wysłaniem żądania.

DDP_021 Jeżeli VU wykryje błąd w sekwencji przychodzącej z IDE, to nie wysyła żadnej odpowiedzi i czeka na następny komunikat żądania rozpoczęcia transmisji przez okres P3 max.

2.2.5.2. Faza komunikacji

W tym przypadku można zdefiniować dwa różne obszary obsługi błędów:

1. VU wykrywa błąd transmisji IDE.

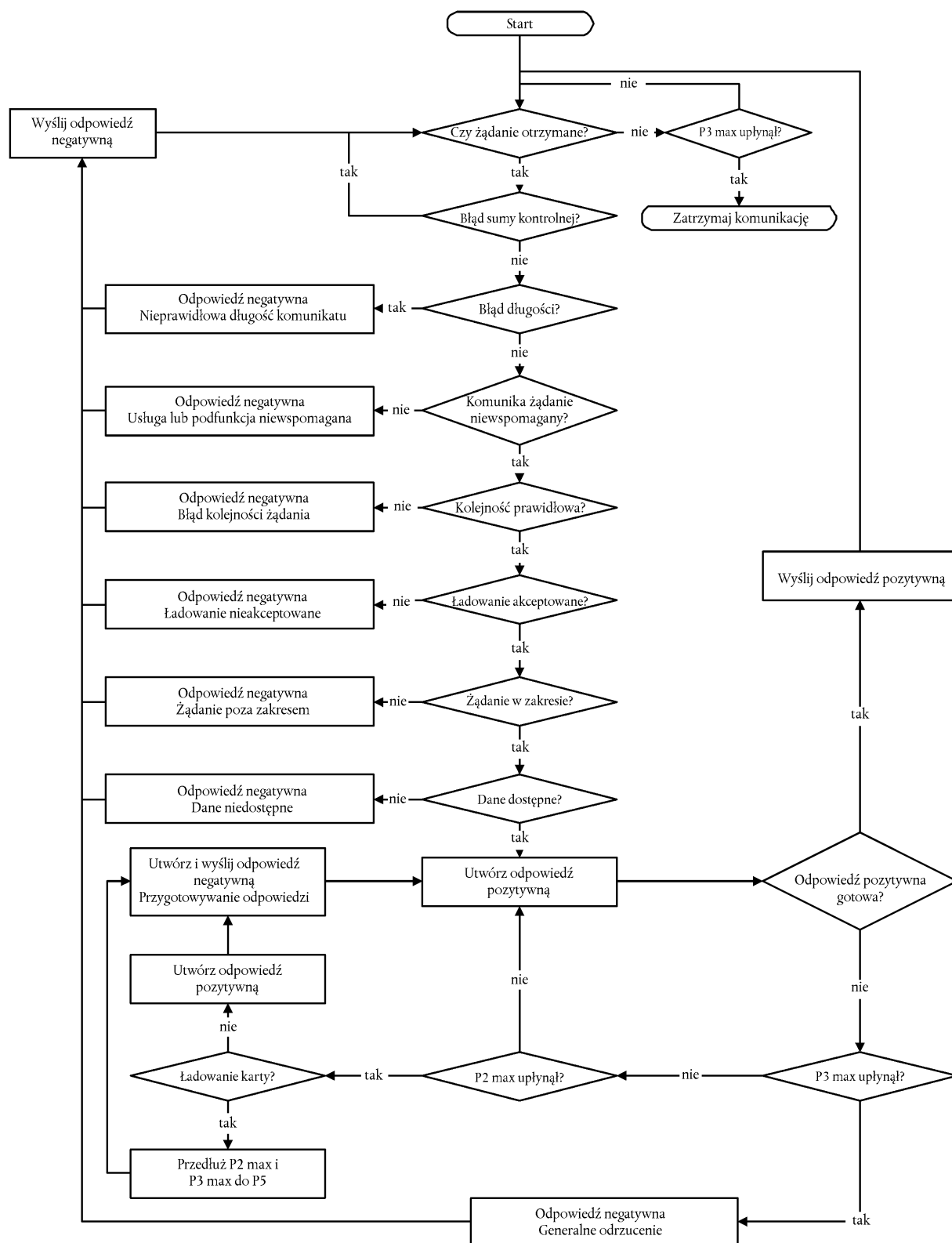
DDP_022 Dla każdego odebranego komunikatu VU wykrywa błędy synchronizacji, błędy formatu bajtowego (np. błędy bitów startu i stopu) i błędy ramki (zła liczba odebranych bajtów, zły bajt sumy kontrolnej).

DDP_023 Jeżeli VU wykryje jeden z powyższych błędów, to nie wysyła odpowiedzi i ignoruje odebrany komunikat.

DDP_024 VU może wykrywać inne błędy formatu lub treści otrzymanego komunikatu (np. komunikat nieobsługiwany) nawet jeżeli długości i sumy kontrolne są prawidłowe; w takim przypadku VU wysyła do IDE komunikat negatywnej odpowiedzi określający charakter błędu.

Rysunek 2

Obsługa błędów w VU

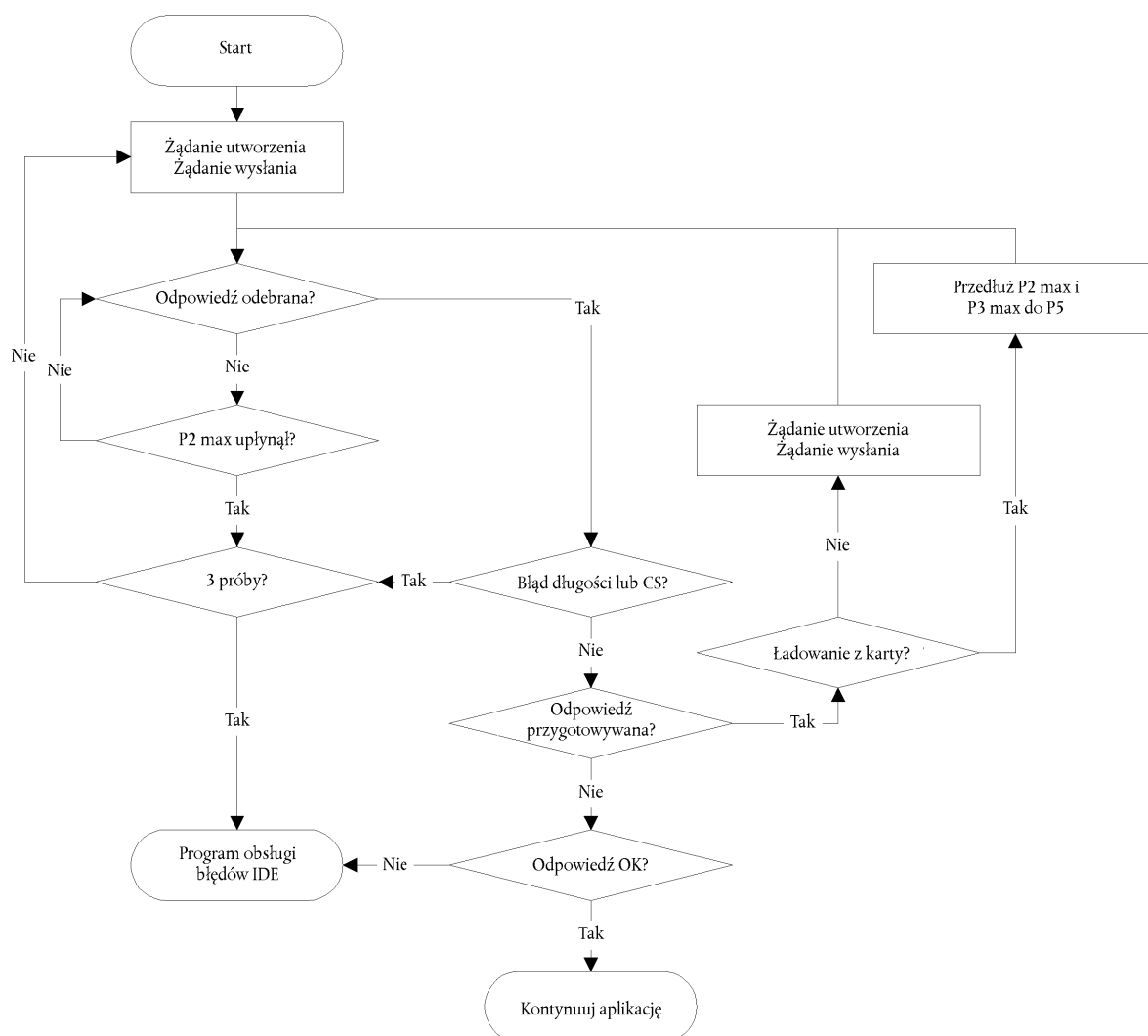


2. IDE wykrywa błąd transmisji VU

- DDP_025 Dla każdego odebranego komunikatu IDE wykrywa błędy synchronizacji, błędy formatu bajtowego (np. błędy bitów startu i stopu) i błędy ramki (zła liczba odebranych bajtów, nieprawidłowy bajt sumy kontrolnej).
- DDP_026 IDE wykrywa błędy kolejności, np. nieprawidłowe zwiększenie stanu licznika podkomunikatów w kolejnych komunikatach.
- DDP_027 Jeżeli IDE wykrywa błąd lub nie ma odpowiedzi z VU w okresie P2 max, wysyła ponownie komunikat żądania, z tym że maksymalnie mogą być trzy transmisje. Dla potrzeb tego wykrywania błędów VU traktuje potwierdzenie podkomunikatu jako żądanie.
- DDP_028 Przed rozpoczęciem każdej transmisji IDE oczekuje przez okres P3 min; okres oczekiwania odmierza się od ostatniego bitu stopu po wykryciu błędu.

Rysunek 3

Obsługa błędów w IDE



2.2.6. Treść komunikatu odpowiedzi

W tym punkcie określono treść pól danych w różnych komunikatach pozytywnej odpowiedzi.

Elementy danych zdefiniowano w dodatku 1 Słownik danych.

2.2.6.1. Pozytywna odpowiedź na żądanie przesłania informacji ogólnych

DDP_029 Pole danych w komunikacie »Pozytywna odpowiedź na żądanie przesłania informacji ogólnych« zawiera następujące dane w określonej tu kolejności pod SID 76 Hex, TREP 01 Hex z odpowiednim podziałem na podkomunikaty i licznikami:

Element danych	Długość (bajtów)	Uwagi
MemberStateCertificate	194	świadczenia bezpieczeństwa VU
VUCertificate	194	
VehicleIdentificationNumber	17	identyfikacja pojazdu
VehicleRegistrationIdentification	1	
vehicleRegistrationNation	14	
vehicleRegistrationNumber	14	
CurrentDateTime	4	bieżąca data i godzina VU
VuDownloadablePeriod	4	okres wczytywany
minDownloadableTime	4	
maxDownloadableTime	4	
CardSlotsStatus	1	typy kart włożonych do VU
VuDownloadActivityData	4	poprzednie wczytywanie z VU
downloadingTime	18	
fullCardNumber	36	
companyOrWorkshopName	36	
VuCompanyLocksData	1	wszystkie zapisane blokady firmowe; jeżeli ta część jest pusta, zwracany jest tylko status noOfLocks = 0.
noOfLocks	(98)	
...		
Vu Company Locks Record	4	
lockInTime	4	
lockOutTime	36	
companyName	36	
companyAddress	36	
companyCardNumber	18	
...		
VuControlActivityData	1	wszystkie zapisy dotyczące kontroli zgromadzone w VU; jeżeli ta część jest pusta, zwracany jest tylko status noOf-Controls = 0.
noOfControls	(31)	
...		
Vu Control Activity Record	1	
controlType	4	
controlTime	18	
controlCardNumber	4	
downloadPeriodBeginTime	4	
downloadPeriodEndTime	4	
...		
Signature	128	Podpis RSA wszystkich danych (z wyłączeniem świadectw) poczynając od VehicleIdentificationNumber do ostatniego bajtu ostatniego VuControlActivityRecord.

2.2.6.2. Pozytywna odpowiedź na żądanie przesłania danych dotyczących czynności

DDP_030 Pole danych w komunikacie »Pozytywna odpowiedź na żądanie przesłania danych czynności« zawiera następujące dane w określonej tu kolejności pod SID 76 Hex, TREP 02 Hex z odpowiednim podziałem na podkomunikaty i z licznikami:

Element danych	Długość (bajty)	Opis
TimeReal	4	Data dnia wczytywanego
OdometerValueMidnight	3	Stan licznika na koniec wczytywanego dnia
VuCardIWData noOfVuCardIWRecords	2	Dane dotyczące cykli wkładania – wyjmowania kart.
...	(129)	– Jeżeli w części tej nie ma dostępnych danych, zwracany jest tylko status noOfVuCardIWRecords = 0.
VuCardIWRecord	36	– Jeżeli zapis VuCardIWRecord obejmuje godzinę 00:00 (wkładanie karty poprzedniego dnia) lub 24:00 (wyjęcie karty następnego dnia), to w całości pojawi się w obu tych dniach.
cardHolderName	36	
holderSurname	36	
holderFirstNames	18	
fullCardNumber	4	
cardExpiryDate	4	
cardInsertionTime	3	
vehicleOdometerValueAtInsertion	1	
cardSlotNumber	4	
cardWithdrawalTime	3	
vehicleOdometerValueAtWithdrawal	1	
previousVehicleInfo	14	
vehicleRegistrationIdentification	4	
vehicleRegistrationNation	4	
vehicleRegistrationNumber	1	
cardWithdrawalTime	1	
manualInputFlag	1	
...		
VuActivityDailyData noOfActivityChanges	2	Status szczelin czytnika o godzinie 00:00 zmiany zarejestrowane dla wczytywanego dnia.
...		
ActivityChangeInfo	2	
...		
VuPlaceDailyWorkPeriodData noOfPlaceRecords	1	Dane dotyczące miejsc zarejestrowane dla wczytywanego dnia; jeżeli ta część jest pusta, zwracany jest tylko status noOfPlaceRecords = 0.
...	(28)	
VuPlaceDailyWorkPeriodRecord	18	
fullCardNumber	4	
placeRecord	1	
entryTime	1	
entryTypeDailyWorkPeriod	1	
dailyWorkPeriodCountry	1	
dailyWorkPeriodRegion	1	
vehicleOdometerValue	3	
...		
VuSpecificConditionData noOfSpecificConditionRecords	2	Dane dotyczące warunków szczególnych zarejestrowane dla wczytywanego dnia; jeżeli ta część jest pusta, zwracany jest tylko status noOfSpecificCondition- Records = 0
...	(5)	
SpecificConditionRecord	4	
EntryTime	1	
specificConditionType	1	
...		
Signature	128	Podpis RSA wszystkich danych poczynając od TimeReal do ostatniego bajtu rekordu warunku szczególnego.

2.2.6.3. Pozytywna odpowiedź na żądanie przesłania danych dotyczących zdarzeń i usterek

DDP_031 Pole danych w komunikacie »Pozytywna odpowiedź na żądanie przesłania danych dotyczących zdarzeń i usterek« zawiera następujące dane w określonej tu kolejności pod SID 76 Hex, TREP 03 Hex, z odpowiednim podziałem na podkomunikaty i z licznikami:

Element danych		Długość (bajty)	Opis
VuFaultData			
NoOfVuFaults		1	Wszystkie usterki zarejestrowane lub trwające w VU; jeżeli ta część jest pusta, zwracany jest tylko status noOfVu-Faults = 0.
...		(82)	
VuFaultRecord	FaultType	1	
	FaultRecordPurpose	1	
	FaultBeginTime	4	
	FaultEndTime	4	
	CardNumberDriverSlotBegin	18	
	cardNumberCodriverSlotBegin	18	
	CardNumberDriverSlotEnd	18	
	CardNumberCodriverSlotEnd	18	
...			
VuEventData			
NoOfVuEvents		1	Wszystkie zdarzenia (z wyłączeniem przekroczenia prędkości) zarejestrowane lub trwające w VU; jeżeli ta część jest pusta, zwracany jest tylko status noOfVuEvents = 0.
...		(83)	
VuEventRecord	EventType	1	
	EventRecordPurpose	1	
	EventBeginTime	4	
	EventEndTime	4	
	CardNumberDriverSlotBegin	18	
	cardNumberCodriverSlotBegin	18	
	CardNumberDriverSlotEnd	18	
	CardNumberCodriverSlotEnd	18	
SimilarEventsNumber		1	
...			
VuOverSpeedingControlData			
LastOverspeedControlTime		4	Dane dotyczące ostatniej kontroli przekroczenia prędkości (przy braku danych wartość standardowa).
FirstOverspeedSince		4	
NumberOfOverspeedSince		1	
VuOverSpeedingEventData			
NoOfVuOverSpeedingEvents		1	Wszystkie zdarzenia przekroczenia prędkości zarejestrowane w VU; jeżeli ta część jest pusta, zwracany jest tylko status noOf-VuOverSpeedingEvents = 0.
...		(31)	
VuOverSpeedingEventRecord	EventType	1	
	EventRecordPurpose	1	
	EventBeginTime	4	
	EventEndTime	4	
	MaxSpeedValue	1	
	AverageSpeedValue	1	
	CardNumberDriverSlotBegin	18	
	SimilarEventsNumber	1	
...			
VuTimeAdjustmentData			
NoOfVuTimeAdjRecords		1	Wszystkie zdarzenia regulacji czasu zarejestrowane w VU (poza ramami pełnej kalibracji); jeżeli ta część jest pusta, zwracany jest tylko status noOfVuTimeAdjRecords = 0.
...		(98)	
VuTimeAdjustmentRecord	OldTimeValue	4	
	NewTimeValue	4	
	WorkshopName	36	
	WorkshopAddress	36	
	WorkshopCardNumber	18	
...			
Signature		128	Podpis RSA wszystkich danych poczynając od noOfVuFaults do ostatniego bajtu w ostatnim zapisie regulacji czasu.

2.2.6.4. Pozytywna odpowiedź na żądanie przesłania danych szczegółowe dane dotyczące prędkości

DDP_032 Pole danych w komunikacie »Pozytywna odpowiedź na żądanie przesłania danych szczegółowe dane dotyczące prędkości« zawiera następujące dane w określonej tu kolejności pod SID 76 Hex, TREP 04 Hex z odpowiednim podziałem na podkomunikaty i z licznikami:

Element danych	Długość (bajtów)	Uwagi
VuDetailedSpeedData		
NoOfSpeedBlocks	2	Wszystkie zdarzenia regulacji czasu zgromadzone w VU (wykonane poza ramami pełnej kalibracji); jeżeli ta część jest pusta, zwracany jest tylko status noOfVuTimeAdjRecords = 0.
...		
VuDetailedSpeedBlock	4	
SpeedBlockBeginDate speedsPerSecond	60	
...		
Signature	128	Podpis RSA wszystkich danych poczynając od noOfVuFaults do ostatniego bajtu w ostatnim zapisie regulacji czasu.

2.2.6.5. Pozytywna odpowiedź na żądanie przesłania danych technicznych

DDP_033 Pole danych w komunikacie »Pozytywna odpowiedź na żądanie przesłania danych technicznych« zawiera następujące dane w określonej tu kolejności pod SID 76 Hex, TREP 05 Hex, z odpowiednim podziałem na podkomunikaty i z licznikami:

Element danych	Długość (bajtów)	Uwagi
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	Wszystkie zapisy kalibracji zgromadzone w VU.
...	(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	Podpis RSA wszystkich danych poczynając od vuManufacturerName do ostatniego bajtu w ostatnim zapisie VuCalibrationRecord.

2.3. Plik ESM

DDP_034 Jeżeli sesja wczytywania obejmuje przesłanie danych z VU, IDE w jednym fizycznym pliku gromadzi wszystkie dane odebrane z VU w czasie tej sesji przesłane z komunikatami pozytywnej odpowiedzi na żądanie przesłania danych. Dane gromadzi się bez nagłówków komunikatów, liczników podkomunikatów, pustych podkomunikatów i sum kontrolnych, ale wraz z SID i TREP (tylko pierwszego podkomunikatu w przypadku kilku podkomunikatów).

3. PROTOKÓŁ WCZYTYWANIA DANYCH Z KART DO TACHOGRAFÓW

3.1. Zakres

W tym punkcie opisano bezpośrednie wczytywanie danych z karty do tachografów do IDE. IDE nie jest częścią bezpiecznego środowiska; dlatego też nie wykonuje się uwierzytelnienia między kartą a IDE.

3.2. Definicje

Sesja wczytywania: Sesja wczytywania ma miejsca za każdym razem, gdy wczytuje się dane z karty ICC. Sesja obejmuje całą procedurę od zainicjowania karty ICC przez IFD do dezaktywowania karty ICC (wyjęcie karty lub następne zainicjowanie).

Podpisany plik danych: plik z karty ICC. Plik przesyła się do IFD w formie odkrytego tekstu. Na karcie ICC obliczany jest skrót pliku i podpisywany a następnie przesyłany do IFD.

3.3. Wczytywanie danych z karty

DDP_035 Wczytywanie danych z karty do tachografów składa się z następujących kroków:

- wczytanie plików EF zawierających wspólne informacje dotyczące karty ICC i układu scalonego. Dane te są nieobowiązkowe i nie są chronione podpisem cyfrowym,
- Wczytanie plików EF Card_Certificate i CA_Certificate. Dane te nie są chronione podpisem cyfrowym,

Wczytanie tych plików jest obowiązkowe dla każdej sesji wczytywania.

- wczytanie plików EF zawierających inne dane aplikacyjne (w DF Tachograph) z wyłączeniem EF Card_Download. Dane te są chronione podpisem cyfrowym,
- wczytanie przynajmniej plików Application_Identification i ID jest obowiązkowe dla każdej sesji wczytywania,
- przy wczytywaniu danych z karty kierowcy obowiązkowe jest wczytanie także następujących plików EF:
 - Events_Data,
 - Faults_Data,
 - Driver_Activity_Data,
 - Vehicles_Used,
 - Places,
 - Control_Activity_Data,
 - Specific_Conditions.
- przy wczytywaniu danych z karty kierowcy, aktualizowana jest data LastCardDownload w pliku Card_Download,
- przy wczytywaniu danych z karty warsztatowej, zerowany jest licznik kalibracji w pliku Card_Download.

3.3.1. Sekwencja inicjalizująca

DDP_036 IDE inicjuje następującą sekwencję:

Karta	Kierunek	IDE/IFD	Znaczenie/Uwagi
	⇐	restart sprzętowy	
ATR	⇒		

Opcjonalnie można używać protokołu PPS do przełączania na większą szybkość transmisji, o ile ICC obsługuje tę funkcję.

3.3.2. Sekwencja dla odpisanych plików danych

DDP_037 Sekwencja wczytania ICC, IC, Card_Certificate i CA_Certificate jest następująca:

Karta	Kierunek	IDE/IFD	Znaczenie/Uwagi
	⇐	wybierz plik	wybierz plik poprzez identyfikator pliku
OK	⇒		
	⇐	odczyt binarny	jeżeli wielkość danych w pliku jest większa od pojemności bufora czytnika lub karty, polecenie musi być powtarzane aż do odczytania całego pliku.
Plik danych OK	⇒	zapisz dane na ESM	zgodnie z punktem 3.4, (Format gromadzenia danych).

Uwaga: przed wybraniem pliku Card_Certificate musi być wybrana aplikacja tachograficzna (wybór poprzez AID).

3.3.3. Sekwencja dla podpisanych plików danych

DDP_038 Dla każdego pliku, który wczytany jest z podpisem, stosuje się następującą sekwencję operacji:

Karta	Kierunek	IDE/IFD	Znaczenie/Uwagi
	⇐	wybierz plik	
OK	⇒		
	⇐	oblicz skrót pliku	oblicza skrót dla danych wybranego pliku przy pomocy wymaganego algorytmu skrótu zgodnie z dodatkiem 11. Polecenie to nie jest poleceniem ISO.
Oblicza skrót pliku i czasowo zachowuje wartość skrótu			
OK	⇒		
	⇐	odczyt binarny	jeżeli wielkość danych w pliku jest większa od pojemności bufora czytnika lub karty, polecenie musi być powtarzane aż do odczytania całego pliku.
Dane pliku	⇒	zapisz odebrane dane na ESM	zgodnie z punktem 3.4, (Format gromadzenia danych).
OK			
	⇐	PSO: oblicz podpis cyfrowy	
Wykonaj operację bezpieczeństwa »compute digital signature« używając czasowo zachowaną wartość skrótu			
Podpis	⇒	dołącz dane do poprzednio zapisanych danych na ESM	zgodnie z punktem 3.4, (Format gromadzenia danych).
OK			

3.3.4. Sekwencja zerowania licznika kalibracji

DDP_039 Sekwencja zerowania licznika kalibracji NoOfCalibrationsSinceDownload w pliku Card_Download na karcie warsztatowej jest następująca:

Karta	Kierunek	IDE/IFD	Znaczenie/Uwagi
OK	⇐	Wybierz plik Card_Download	Wybierz poprzez identyfikator pliku
	⇒		
	⇐	Aktualizacja binarna licznika NoOfCalibrationsSinceDownload = '00 00'	
Zeruje liczbę wczytań karty			
OK	⇒		

3.4. Format gromadzenia danych

3.4.1. Wprowadzenie

DDP_040 Wczytane dane należy przechowywać w sposób zgodny z następującymi wymaganiami:

- dane przechowuje się transparentnie. Oznacza to, że przy gromadzeniu należy zachować kolejność bajtów jak i kolejność bitów w bajcie taką jak przy przesyłaniu z karty,
- wszystkie pliki wczytane z karty w ramach sesji wczytywania przechowuje się w jednym pliku na ESM.

3.4.2. Format pliku

DDP_041 Format pliku jest konkatencją kilku obiektów TLV.

DDP_042 Znacznikiem pliku EF jest jego identyfikator FID z dodatkiem »00«.

DDP_043 Znacznikiem podpisu pliku jest identyfikator pliku FID z dodatkiem »01«.

DDP_044 Długość podana jest w postaci dwubajtowej wartości. Wartość określa liczbę bajtów w polu wartości. Wartość »FF FF« w polu długości jest zastrzeżona do wykorzystania w przyszłości.

DDP_045 Gdy plik nie jest wczytany, nie zachowuje się żadnych danych dotyczących tego pliku (nie ma znacznika i nie ma zerowej długości).

DDP_046 Podpis zachowuje się w obiekcie TLV znajdującym się bezpośrednio za obiektem TLV zawierającym dane pliku.

Definicja	Znaczenie	Długość
FID (2 bajty) »00«	Znacznik pliku (FID)	3 bajty
FID (2 bajty) »01«	Znacznik podpisu pliku (FID)	3 bajty
xx xx	pole wartości długości	2 bajty

Przykładowe dane w pliku wczytania na ESM:

Znacznik	Długość	Wartość
00 02 00	00 11	Dane pliku ICC
C1 00 00	00 C2	Dane pliku Card_Certificate
		...
05 05 00	0A 2E	Dane pliku Vehicles_Used
05 05 01	00 80	Podpis pliku Vehicles_Used

4. WCZYTYWANIE DANYCH Z KARTY DO TACHOGRAFÓW ZA POŚREDNICTWEM PRZYRZĄDU REJESTRUJĄCEGO

- DDP_047 VU musi umożliwiać wczytywanie danych z włożonej karty kierowcy do przyłączonego IDE.
- DDP_048 IDE wysyła do VU komunikat »żądanie przesłania danych wczytywanie karty« w celu zainicjowania tego trybu (patrz pkt 2.2.2.9).
- DDP_049 Następnie VU wczytuje całą kartę, plik po pliku, zgodnie z protokołem wczytywania danych z karty zdefiniowanym w punkcie 3 oraz przekazuje wszystkie dane odebrane z karty do IDE w odpowiednim formacie pliku TLV (patrz ppkt 3.4.2) i zapakowane w komunikacie »pozytywna odpowiedź na żądanie przesłania danych«.
- DDP_050 IDE odzyskuje dane z karty z komunikatu »pozytywna odpowiedź na żądanie przesłania danych«(usuając wszystkie nagłówki, SID, TREP, liczniki podkomunikatów i sumy kontrolne) i zachowuje te dane w jednym fizycznym pliku jak opisano w pkt 2.3.
- DDP_051 Następnie VU, gdy właściwe, aktualizuje plik `Control_Activity_Data` lub `Card_Download` na karcie kierowcy.
-

Dodatek 8

PROTOKÓŁ KALIBRACJI

SPIS TREŚCI

1.	Wprowadzenie	448
2.	Pojęcia, definicje i odniesienia	448
3.	Informacje ogólne o usługach	448
3.1.	Dostępne usługi	448
3.2.	Kody odpowiedzi	449
4.	Usługi komunikacyjne	449
4.1.	Usługa StartCommunication	449
4.2.	Usługa StopCommunication	451
4.2.1.	Opis komunikatu	451
4.2.2.	Format komunikatu	452
4.2.3.	Definicje parametrów	453
4.3.	Usługa TesterPresent	453
4.3.1.	Opis komunikatu	453
4.3.2.	Format komunikatu	453
5.	Usługi zarządzania	454
5.1.	Usługa StartDiagnosticSession	454
5.1.1.	Opis komunikatu	454
5.1.2.	Format komunikatu	455
5.1.3.	Definicja parametru	456
5.2.	Usługa Security Access	456
5.2.1.	Opis komunikatu	456
5.2.2.	Format komunikatu — SecurityAccess — requestSeed	457
5.2.3.	Format komunikatu — SecurityAccess — sendKey	458
6.	Usługi przesyłania danych	459
6.1.	Usługa ReadDataByIdentifier	459
6.1.1.	Opis komunikatu	459
6.1.2.	Format komunikatu	459
6.1.3.	Definicja parametru	460
6.2.	Usługa WriteDataByIdentifier	461
6.2.1.	Opis komunikatu	461
6.2.2.	Format komunikatu	461
6.2.3.	Definicja parametru	462
7.	Sterowanie impulsami testującymi — jednostka funkcjonalna sterowania we/wy	462
7.1.	Sterowanie we/wy / usługa ByIdentifier	462

7.1.1.	Opis komunikatu	462
7.1.2.	Format komunikatu	463
7.1.3.	Definicja parametru	464
8.	Format zapisów danych	465
8.1.	Zakresy przesyłanych parametrów	465
8.2.	Format dataRecords	466

1. WPROWADZENIE

Niniejszy dodatek opisuje wymianę danych między przyrządem rejestrującym a testerem poprzez łącze K-line, które stanowi część interfejsu kalibracyjnego opisanego w dodatku 6. Opisano tu także sterowanie linią sygnałową we/wy w związku kalibracji.

Komunikaty zestawiające łącze K-line opisano w sekcji 4 „Usługi komunikacyjne”.

W niniejszym dodatku wykorzystano koncepcję „sesji diagnostycznych do ustalania zakresu kontroli K-line dla różnych warunków. Sesją domyślną jest »StandardDiagnosticSession«, w której wszystkie dane można odczytać z przyrządu rejestrującego, ale żadnych danych nie można zapisać w przyrządzie rejestrującym.”

Wybór sesji diagnostycznej opisano w sekcji 5 „Usługi zarządzania”.

CPR_001 Sesja „ECUProgrammingSession” umożliwia wprowadzanie danych do przyrządu rejestrującego. W przypadku wprowadzania danych kalibracyjnych (wymagania 097 i 098) przyrząd rejestrujący musi pracować w trybie kalibracyjnym.

Przesyłanie danych poprzez K-line opisano w sekcji 6 „usługi przesyłania danych”. Formaty przesyłanych danych opisano szczegółowo w sekcji 8 „Format zapisów danych”.

CPR_002 Sesja „ECUAdjustmentSession” umożliwia wybranie trybu we/wy dla kalibracji linii sygnału we/wy poprzez interfejs K-line. Sterowanie kalibracją linii sygnałowej we/wy opisano w sekcji 7 „Sterowanie impulsami testującymi — jednostka funkcjonalna sterowania we/wy”.

CPR_003 W niniejszym dokumencie adres testera określony jest jako 'tt'. Chociaż mogą być zalecane adresy dla testerów, VU odpowiada prawidłowo na dowolny adres testera. Fizycznym adresem VU jest 0xEE.

2. POJĘCIA, DEFINICJE I ODNIESIENIA

Protokoły, komunikaty i kody błędów oparte są zasadniczo na aktualnym projekcie normy ISO 14229-1 (Pojazdy drogowe — Systemy diagnostyczne — część 1: Usługi diagnostyczne, wersja 6 z dnia 22 lutego 2001 r.).

Kodowania bajtowego i wartości heksadecymalnych używa się w identyfikatorach usług, żądaniach obsługi i odpowiedziach oraz parametrach standardowych.

Pojęcie „tester” oznacza urządzenie służące do wprowadzania do VU danych programistycznych/kalibracyjnych.

Pojęcia „klient” i „serwer” oznaczają odpowiednio tester i VU.

Pojęcie ECU oznacza „sterownik elektroniczny” i odnosi się do VU.

Odniesienia:

ISO 14230-2: Pojazdy drogowe — systemy diagnostyczne — Protokół słowa kluczowego 2000 — część 2: Warstwa łącza danych. Wydanie pierwsze: 1999 r. Pojazdy — systemy diagnostyczne.

3. INFORMACJE OGÓLNE O USŁUGACH

3.1. Dostępne usługi

Tabela poniżej zawiera informacje ogólne o usługach, które są dostępne w urządzeniu rejestrującym i są zdefiniowane w niniejszym dokumencie.

CPR_004 Tabela wskazuje usługi dostępne przy włączonej sesji diagnostycznej.

— Pierwsza kolumna zawiera wykaz dostępnych usług,

— druga kolumna zawiera numer sekcji w niniejszym dodatku, gdzie usługa jest dokładniej zdefiniowana,

- trzecia kolumna przypisuje wartości identyfikatora usługi „values” dla komunikatów żądań,
- czwarta kolumna określa usługi „StandardDiagnosticSession” (SD), których wdrożenie jest wymagane w każdym VU,
- piąta kolumna określa usługi „ECUAdjustmentSession” (ECUAS), które muszą być wdrożone w celu umożliwienia sterowania linią sygnałową we/wy w złączu kalibracji w panelu czołowym VU,
- szósta kolumna określa usługi „ECUProgrammingSession” (ECUPS), które muszą być wdrożone w celu umożliwienia programowania parametrów w VU.

Tabela 1

Zestawienie wartości identyfikatorów usług

Nazwa usługi diagnostycznej	nr sekcji	Wartość SId Req.	Sesje diagnostyczne		
			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		■	

■ Symbol ten oznacza, że usługa jest obowiązkowa w tej sesji diagnostycznej.
 Brak symbolu oznacza, że usługa nie jest dozwolona w tej sesji diagnostycznej.

3.2. Kody odpowiedzi

Kody odpowiedzi są zdefiniowane dla każdej usługi.

4. USŁUGI KOMUNIKACYJNE

Niektóre usługi są niezbędne do ustanowienia i utrzymania komunikacji. Nie występują one w warstwie aplikacji. Dostępne usługi wyszczególniono w tabeli poniżej:

Tabela 2

Usługi komunikacyjne

Nazwa usługi	Opis
StartCommunication	Klient żąda rozpoczęcia sesji komunikacyjnej z serwerem(ami)
StopCommunication	Klient żąda zaprzestania bieżącej sesji komunikacyjnej
TesterPresent	Klient wskazuje serwerowi, że jest jeszcze obecny

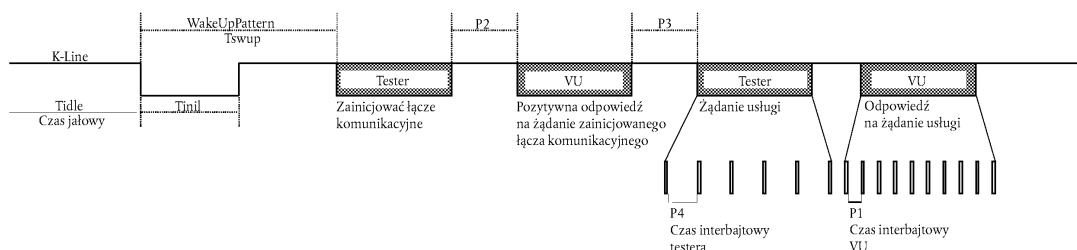
CPR_005 Usługa StartCommunication służy do rozpoczęcia komunikacji. W celu wykonania usługi konieczne jest zainicjowanie komunikacji i ustawienie parametrów odpowiednio dla pożądanego trybu.

4.1. Usługa StartCommunication

CPR_006 Po odebraniu prymitywu wskazania StartCommunication VU sprawdza czy w obecnych warunkach można zainicjować żądane łącze komunikacyjne. Warunki zezwalające na zainicjowanie łącza komunikacyjnego opisano w normie ISO 14230-2.

CPR_007 Następnie VU wykonuje wszystkie działania niezbędne do zainicjowania łącza komunikacyjnego i wysyła prymityw odpowiedzi StartCommunication z wybranymi parametrami odpowiedzi pozytywnej.

- CPR_008 Jeżeli VU, które jest już zainicjowane (ma otwartą dowolną sesję diagnostyczną) otrzymuje nowe żądanie StartCommunication (np. wskutek usuwania błędu w testerze), żądanie zostanie przyjęte a VU ponownie zainicjowane.
- CPR_009 Jeżeli z jakiegokolwiek przyczyny nie można zainicjować łącza komunikacyjnego, VU pracuje tak jak pracowało bezpośrednio przed próbą zainicjowania łącza komunikacyjnego.
- CPR_010 Komunikat żądania StartCommunicationRequest musi mieć fizyczny adres.
- CPR_011 Inicjowanie usług w VU odbywa się metodą „szybkiej inicjalizacji”,
- przed każdą czynnością występuje czas jałowy magistrali,
 - następnie tester wysyła kod inicjujący,
 - wszystkie informacje niezbędne do nawiązania komunikacji zawarte są w odpowiedzi VU.
- CPR_012 Po zakończeniu inicjalizacji,
- wszystkie parametry komunikacyjne zostają ustawione na wartości zdefiniowane w tabeli 4 zgodnie z bajtami kluczowymi,
 - VU czeka na pierwsze żądanie testera,
 - VU znajduje się w domyślnym trybie diagnostycznym, tj. StandardDiagnosticSession,
 - linia sygnałowa we/wy kalibracji jest w stanie domyślnym, tj. w stanie oczekiwania.
- CPR_014 Szybkość transmisji K-line jest ustawiona na 10 400 bit/s.
- CPR_016 Szybka inicjalizację uruchamia tester wysyłając kod wywołania (Wup) przez K-line. Kod rozpoczyna się po czasie jałowym na K-line niskim stanem w czasie T_{inil} . Tester wysyła pierwszy bit usługi StartCommunication po czasie T_{wup} następującym po pierwszej krawędzi opadającej.



- CPR_017 Wartości czasów dla szybkiej inicjalizacji i ogólnie komunikatów podano w tabeli poniżej. Dla czasu jałowego są inne możliwości:
- pierwsza transmisja po włączeniu zasilania, $T_{idle} = 300$ ms.
 - po zakończeniu usługi StopCommunication, $T_{idle} = P3$ min.
 - po zatrzymaniu komunikacji wskutek upływu czasu oczekiwania $P3$ max, $T_{idle} = 0$.

Tabela 3

Wartości czasów dla szybkiej inicjalizacji

Parametr	Wart. minimalna	Wart. maksymalna
T_{inil}	25 ± 1 ms	26 ms
T_{wup}	50 ± 1 ms	51 ms

Tabela 4

Wartości czasów dla komunikacji

Parametr	Opis parametru	Dolna granica (ms)	Górna granica (ms)
		minimum	maksimum
P1	Czas między bajtami dla odpowiedzi VU	0	20
P2	Czas między żądaniem testera a odpowiedzią VU lub dwiema odpowiedziami VU	25	250
P3	Czas między końcem odpowiedzi VU a początkiem nowego żądania testera	55	5 000
P4	Czas między bajtami dla żądania testera	5	20

CPR_018 Format komunikatu dla szybkiej inicjalizacji opisano szczegółowo w poniższych tabelach:

Tabela 5

Komunikat żądania StartCommunication

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu — adresowanie fizyczne	81	FMT
#2	Bajt adresu docelowego	EE	TGT
#3	Bajt adresu źródłowego	tt	SRC
#4	Żądanie usługi StartCommunication	81	SCR
#5	Suma kontrolna	00-FF	CS

Tabela 6

StartCommunication komunikat pozytywnej odpowiedzi

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu — adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT
#3	Bajt adresu źródłowego	EE	SRC
#4	Dodatkowy bajt długości	03	LEN
#5	Pozytywna odpowiedź na żądanie usługi StartCommunication	C1	SCRPR
#6	Bajt kluczowy 1	EA	KB1
#7	Bajt kluczowy 2	8F	KB2
#8	Suma kontrolna	00-FF	CS

CPR_019 Nie ma negatywnej odpowiedzi na komunikat żądania StartCommunication, gdy nie zostanie wysłana pozytywna odpowiedź, VU nie zostaje zainicjowany, nic nie jest przesyłane i VU pozostaje w stanie normalnej pracy.

4.2. Usługa StopCommunication

4.2.1. Opis komunikatu

Celem tej usługi warstwy komunikacji jest zakończenie sesji komunikacyjnej.

CPR_020 Po odebraniu prymitywu wskazania StopCommunication, VU sprawdza czy bieżące warunki pozwalają na zakończenie tej komunikacji. W tym przypadku VU wykonuje wszystkie działania niezbędne do zakończenia sesji komunikacyjnej.

- CPR_021 Jeżeli zakończenie sesji komunikacyjnej jest możliwe, VU, przed zakończeniem komunikacji, wysyła prymityw odpowiedzi StopCommunication z wybranymi parametrami pozytywnej odpowiedzi.
- CPR_022 Jeżeli zakończenie sesji komunikacyjnej nie jest możliwe z jakiejkolwiek przyczyny, VU wysyła prymityw odpowiedzi StopCommunication z wybranym parametrem negatywnej odpowiedzi.
- CPR_023 Jeżeli VU wykryje przekroczenia czasu P3 max, komunikacja zostaje zakończona bez wysyłania żadnego prymitywu odpowiedzi.

4.2.2. Format komunikatu

- CPR_024 Format komunikatów dla prymitywów StopCommunication opisano szczegółowo w poniższych tabelach:

Tabela 7

Komunikat żądania StopCommunication

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu — adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	EE	TGT
#3	Bajt adresu źródłowego	tt	SRC
#4	Dodatkowy bajt długości	01	LEN
#5	ID usługi żądania StopCommunication	82	SPR
#6	Suma kontrolna	00-FF	CS

Tabela 8

Komunikat pozytywnej odpowiedzi StopCommunication

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu — adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT
#3	Bajt adresu źródłowego	EE	SRC
#4	Dodatkowy bajt długości	01	LEN
#5	Pozytywna odpowiedź na żądanie usługi StopCommunication	C2	SPRPR
#6	Suma kontrolna	00-FF	CS

Tabela 9

Komunikat negatywnej odpowiedzi StopCommunication

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu — adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT
#3	Bajt adresu źródłowego	EE	SRC
#4	Dodatkowy bajt długości	03	LEN
#5	ID negatywnej odpowiedzi	7F	NR
#6	ID usługi żądania StopCommunication	82	SPR
#7	Kod odpowiedzi = generalReject	10	RC_GR
#8	Suma kontrolna	00-FF	CS

4.2.3. Definicje parametrów

Usługa ta nie wymaga żadnych definicji parametrów.

4.3. Usługa TesterPresent

4.3.1. Opis komunikatu

Tester używa usługi TesterPresent do wskazania serwerowi, że jeszcze jest obecny, w celu zapobieżenia automatycznego powrotu serwera do normalnego trybu pracy i zerwania komunikacji. Usługa ta, wysyłana okresowo, utrzymuje sesję diagnostyczną/komunikacyjną w stanie aktywnym zerując timer P3 za każdym razem po odebraniu żądania tej usługi.

4.3.2. Format komunikatu

CPR_079 Formaty komunikatu dla prymitywów TesterPresent opisano szczegółowo w poniższych tabelach.

Tabela 10

Komunikat żądania TesterPresent

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu — adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	EE	TGT
#3	Bajt adresu źródłowego	tt	SRC
#4	Dodatkowy bajt długości	02	LEN
#5	ID usługi żądania TesterPresent	3E	TP
#6	Sub Function = responseRequired = [tak nie]	01 02	RESPREQ_Y RESPREQ_NR
#7	Suma kontrolna	00-FF	CS

CPR_080 Jeżeli parametr responseRequired jest ustawiony na „tak”, to serwer odpowie następującym komunikatem pozytywnej odpowiedzi. Jeżeli jest ustawiony na „nie”, serwer nie wysyła żadnej odpowiedzi.

Tabela 11

Komunikat pozytywnej odpowiedzi TesterPresent

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu — adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT
#3	Bajt adresu źródłowego	EE	SRC
#4	Dodatkowy bajt długości	01	LEN
#5	ID usługi pozytywnej odpowiedzi TesterPresent	7E	TPPR
#6	Suma kontrolna	00-FF	CS

CPR_081 Usługa używa następujących kodów negatywnej odpowiedzi:

Tabela 12

Komunikat negatywnej odpowiedzi TesterPresent

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu — adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT
#3	Bajt adresu źródłowego	EE	SRC
#4	Dodatkowy bajt długości	03	LEN
#5	ID negatywnej odpowiedzi	7F	NR
#6	ID usługi TesterPresent	3E	TP
#7	Kod odpowiedzi = [SubFunctionNotSupported-InvalidFormat incorrectMessageLength]	12	RC_SFNS_IF
		13	RC_IML
#8	Suma kontrolna	00-FF	CS

5. USŁUGI ZARZĄDZANIA

Dostępne usługi opisano szczegółowo w poniższej tabeli:

Tabela 13

Usługi zarządzania

Nazwa usługi	Opis
StartDiagnosticSession	Klient żąda rozpoczęcia sesji diagnostycznej z VU
SecurityAccess	Klient żąda dostępu do funkcji zastrzeżonych dla uprawnionych użytkowników

5.1. Usługa StartDiagnosticSession

5.1.1. Opis komunikatu

CPR_025 Usługa StartDiagnosticSession służy do włączania różnych sesji diagnostycznych w serwerze. Sesja diagnostyczna udostępnia swoisty zestaw usług zgodnie z opisem w tabeli 17. Sesja może udostępnić producentowi pojazdu usługi swoiste nieobjęte tym dokumentem. Zasady wdrożenia spełniają następujące wymagania:

- w VU aktywna jest zawsze dokładnie jedna sesja diagnostyczna,
- po włączeniu zasilania VU zawsze uruchamia StandardDiagnosticSession. Jeżeli żadna inna sesja diagnostyczna nie zostanie uruchomiona, wówczas StandardDiagnosticSession pozostaje uruchomiona tak długo jak włączone jest zasilanie VU,
- jeżeli jest już uruchomiona sesja diagnostyczna zażądana przez tester, VU wysyła komunikat pozytywnej odpowiedzi,
- za każdym razem kiedy tester żąda nowej sesji diagnostycznej, VU najpierw wysyła komunikat pozytywnej odpowiedzi StartDiagnosticSession zanim nowa sesja stanie się aktywna w VU. Jeżeli VU nie może uruchomić żądanej nowej sesji diagnostycznej, to odpowiada komunikatem negatywnej odpowiedzi StartDiagnosticSession i bieżąca sesja jest kontynuowana.

CPR_026 Sesja diagnostyczna może zostać uruchomiona tylko wtedy, gdy nawiązana jest komunikacja między klientem a VU.

CPR_027 Parametry czasowe zdefiniowane w tabeli 4 są aktywne po pomyślnym uruchomieniu sesji StartDiagnosticSession z parametrem diagnosticSession ustawionym na „StandardDiagnosticSession” w komunikacie żądania, jeżeli poprzednio aktywna była inna sesja diagnostyczna.

5.1.2. **Format komunikatu**

CPR_028 Formaty komunikatu dla prymitywów StartDiagnosticSession opisano szczegółowo w poniższych tabelach:

Tabela 14

Komunikar żądania StartDiagnosticSession

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu — adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	EE	TGT
#3	Bajt adresu źródłowego	tt	SRC
#4	Dodatkowy bajt długości	02	LEN
#5	StartDiagnosticSession ID usługi żądania	10	STDS
#6	diagnosticSession = (jedna wartość z tabeli 17)	xx	DS_...
#7	Suma kontrolna	00-FF	CS

Tabela 15

Komunikat pozytywnej odpowiedzi StartDiagnosticSession

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu — adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT
#3	Bajt adresu źródłowego	EE	SRC
#4	Dodatkowy bajt długości	02	LEN
#5	StartDiagnosticSession Pozytywna odpowiedź na żądanie Service Id	50	STDSPR
#6	DiagnosticSession = (ta sama wartość co w bajcie #6 w tabeli 14)	xx	DS_...
#7	Suma kontrolna	00-FF	CS

Tabela 16

Komunikat negatywnej odpowiedzi StartDiagnosticSession

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu — adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT
#3	Bajt adresu źródłowego	EE	SRC
#4	Dodatkowy bajt długości	03	LEN
#5	ID negatywnej odpowiedzi	7F	NR
#6	StartDiagnosticSession ID usługi żądania	10	STDS
#7	Kod odpowiedzi = (subFunctionNotSupported ^(a))	12	RC_SFNS
	incorrectMessageLength ^(b)	13	RC_IML
	conditionsNotCorrect ^(c)	22	RC_CNC
#8	Suma kontrolna	00-FF	CS

^(a) Wartość wstawiona w bajcie #6 komunikatu żądania nie jest obsługiwana, tj. nie ma jej w tabeli 17.

^(b) Zła długość komunikatu.

^(c) Kryteria żądania StartDiagnosticSession nie są spełnione.

5.1.3. Definicja parametru

CPR_029 Parametr *diagnosticSession* (*DS_*) używany jest w usłudze *StartDiagnosticSession* do wybierania szczególnego zachowania serwera(ów). W dokumencie tym określone są następujące sesje diagnostyczne:

Tabela 17

Definicja wartości *diagnosticSession*

Hex	Opis	Mnemonik
81	StandardDiagnosticSession Ta sesja diagnostyczna udostępnia wszystkie usługi wyszczególnione w tabeli 1 w kolumnie 4 „SD”. Usługi te umożliwiają odczyt danych z serwera (VU). Ta sesja diagnostyczna jest aktywna po pomyślnym zakończeniu inicjacji między klientem (tester) a serwerem (VU). Tę sesję diagnostyczną można zastąpić każdą inną sesją diagnostyczną wyszczególnioną w tej sekcji.	SD
85	ECUProgrammingSession Ta sesja diagnostyczna udostępnia wszystkie usługi wyszczególnione w tabeli 1 w kolumnie 6 „ECUPS”. Usługi te wspomagają programowanie pamięci serwera (VU). Tę sesję diagnostyczną można zastąpić każdą inną sesją diagnostyczną wyszczególnioną w tej sekcji.	ECUPS
87	ECUAdjustmentSession Ta sesja diagnostyczna udostępnia wszystkie usługi wyszczególnione w tabeli 1 w kolumnie 5 „ECUAS”. Usługi te wspomagają sterowania we/wy serwera (VU). Tę sesję diagnostyczną można zastąpić każdą inną sesją diagnostyczną wyszczególnioną w tej sekcji.	ECUAS

5.2. Usługa *SecurityAccess*

Zapis danych kalibracyjnych lub dostęp do linii we/wy kalibracji nie jest możliwy, chyba że VU jest w trybie kalibracyjnym. Dodatkowo, oprócz włożenia do VU ważnej karty warsztatowej, niezbędne jest wprowadzenie numeru PIN do VU przed uzyskaniem dostępu do trybu kalibracyjnego.

Usługa *SecurityAccess* umożliwia wprowadzenie numeru PIN i przekazanie testerowi czy VU jest w trybie kalibracyjnym.

Dopuszcza się wprowadzanie numeru PIN alternatywnymi metodami.

5.2.1. Opis komunikatu

Usługa *SecurityAccess* zawiera komunikat *SecurityAccess „requestSeed”*, po którym może nastąpić komunikat *SecurityAccess „sendKey”*. Usługa *SecurityAccess* musi być przeprowadzona po usłudze *StartDiagnosticSession*.

CPR_033 Tester używa komunikatu *SecurityAccess „requestSeed”* do sprawdzenia czy przyrząd rejestrujący jest gotowy do przyjęcia numeru PIN.

CPR_034 Jeżeli przyrząd rejestrujący jest już w trybie kalibracyjnym, odpowiada na żądanie wysyłając „seed” równy 0x0000 przy pomocy usługi pozytywnej odpowiedzi *SecurityAccess*.

CPR_035 Jeżeli przyrząd rejestrujący jest gotowy do przyjęcia numeru PIN w celu zweryfikowania go przez kartę warsztatową, odpowiada na żądanie wysyłając „seed” większy niż 0x0000 przy pomocy usługi pozytywnej odpowiedzi *SecurityAccess*.

CPR_036 Jeżeli przyrząd rejestrujący nie jest gotowy do przyjęcia numeru PIN z testera, albo z tego powodu, że włożona karta warsztatowa nie jest ważna lub nie włożono żadnej karty warsztatowej lub przyrząd rejestrujący oczekuje na wprowadzenie numeru PIN inną metodą, odpowiada na żądanie wysyłając kod negatywnej odpowiedzi ustawiony na *conditionsNotCorrectOrRequestSequenceError*.

CPR_037 Następnie tester, ewentualnie, używa komunikatu *SecurityAccess „sendKey”* do przesłania numeru PIN do przyrządu rejestrującego. Aby karta miała wystarczający czas na przeprowadzenie uwierzytelnienia, VU w celu przedłużenia czasu oczekiwania na odpowiedź używa kodu negatywnej odpowiedzi *requestCorrectlyReceived-ResponsePending*. Maksymalny czas oczekiwania na odpowiedź nie przekracza pięciu minut. Gdy tylko żądana usługa zostaje zakończona, VU wysyła komunikat pozytywnej odpowiedzi lub komunikat negatywnej odpowiedzi z kodem odpowiedzi różnym od tego pierwszego kodu. VU może powtórzyć ten kod negatywnej odpowiedzi *requestCorrectlyReceived-ResponsePending* aż do zakończenia usługi i wysłania komunikatu ostatecznej odpowiedzi.

CPR_038 Przyrząd rejestrujący odpowiada na to żądanie przy pomocy pozytywnej odpowiedzi na żądanie usługi SecurityAccess jedynie wtedy gdy jest w TRYBIE KALIBRACYJNYM.

CPR_039 W następujących przypadkach przyrząd rejestrujący odpowiada na to żądanie negatywną odpowiedzią z następującą wartością kodu odpowiedzi:

- subFunctionNotSupported: niedozwolony format dla parametru podfunkcji (accessType),
- conditionsNotCorrectOrRequestSequenceError: przyrząd rejestrujący nie jest gotowy do przyjęcia numeru PIN,
- invalidKey: nieprawidłowy numer PIN i nie przekroczono dozwolonej liczby prób sprawdzania numeru PIN,
- exceededNumberOfAttempts: nieprawidłowy numer PIN i przekroczona dozwolona liczba prób sprawdzania numeru PIN,
- generalReject: prawidłowy numer PIN ale nieudane wzajemne uwierzytelnienie z kartą warsztatową.

5.2.2. **Format komunikatu — SecurityAccess — requestSeed**

CPR_040 Formaty komunikatu dla prymitywów SecurityAccess „requestSeed” opisano szczegółowo w poniższych tabelach:

Tabela 18

Żądanie SecurityAccess — komunikat requestSeed

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu — adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	EE	TGT
#3	Bajt adresu źródłowego	tt	SRC
#4	Dodatkowy bajt długości	02	LEN
#5	SecurityAccess ID usługi żądania	27	SA
#6	accessType — requestSeed	7D	AT_RSD
#7	Suma kontrolna	00-FF	CS

Tabela 19

SecurityAccess — requestSeed komunikat pozytywnej odpowiedzi

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu — adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT
#3	Bajt adresu źródłowego	EE	SRC
#4	Dodatkowy bajt długości	04	LEN
#5	SecurityAccess Id pozytywna odpowiedź na żądanie usługi	67	SAPR
#6	accessType — requestSeed	7D	AT_RSD
#7	Seed High	00-FF	SEEDH
#8	Seed Low	00-FF	SEEDL
#9	Suma kontrolna	00-FF	CS

Tabela 20

SecurityAccess komunikat negatywnej odpowiedzi

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu — adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT
#3	Bajt adresu źródłowego	EE	SRC
#4	Dodatkowy bajt długości	03	LEN
#5	ID usługi negatywnej odpowiedzi	7F	NR
#6	SecurityAccess ID żądania usługi	27	SA
#7	Kod odpowiedzi = (conditionsNotCorrectOrRequestSequenceError incorrectMessageLength)	22	RC_CNC
		13	RC_IML
#8	Suma kontrolna	00-FF	CS

5.2.3. **Format komunikatu — SecurityAccess — sendKey**

CPR_041 Formaty komunikatu dla prymitywów SecurityAccess „sendKey” opisano szczegółowo w poniższych tabelach:

Tabela 21

Komunikat żądania bezpiecznego dostępu — sendKey

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu — adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	EE	TGT
#3	Bajt adresu źródłowego	tt	SRC
#4	Dodatkowy bajt długości	m+2	LEN
#5	SecurityAccess ID usługi żądania	27	SA
#6	accessType — sendKey	7E	AT_SK
#7 to #m+6	Key#1 (najwyższy)	xx	KEY
	...	...	
	Key #m (niższy, m musi być minimum 4 i maksimum 8)	xx	
#m+7	Suma kontrolna	00-FF	CS

Tabela 22

Komunikat pozytywnej odpowiedzi SecurityAccess — sendKey

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu — adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT
#3	Bajt adresu źródłowego	EE	SRC
#4	Dodatkowy bajt długości	02	LEN
#5	SecurityAccess Id pozytywna odpowiedź na żądanie usługi	67	SAPR
#6	accessType — sendKey	7E	AT_SK
#7	Suma kontrolna	00-FF	CS

Tabela 23

SecurityAccess komunikat negatywnej odpowiedzi

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu — adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT
#3	Bajt adresu źródłowego	EE	SRC
#4	Dodatkowy bajt długości	03	LEN
#5	ID usługi negatywnej odpowiedzi	7F	NR
#6	SecurityAccess ID żądania usługi	27	SA
#7	Kod odpowiedzi = (generalReject subFunctionNotSupported incorrectMessageLength conditionsNotCorrectOrRequestSequenceError InvalidKey exceededNumberOfAttempts requestCorrectlyReceived-ResponsePending)	10 12 13 22 35 36 78	RC_GR RC_SFNS RC_IML RC_CNC RC_IK RC_ENA RC_RCR_RP
#8	Suma kontrolna	00-FF	CS

6. USŁUGI PRZESYŁANIA DANYCH

Dostępne usługi wyszczególniono w poniższej tabeli:

Tabela 24

Usługi przesyłania danych

Nazwa usługi	Opis
ReadDataByIdentifier	Klient żąda przesłania bieżącej wartości zapisu z dostępem poprzez recordDataIdentifier
WriteDataByIdentifier	Klient żąda zapisu z dostępem poprzez recordDataIdentifier

6.1. Usługa ReadDataByIdentifier**6.1.1. Opis komunikatu**

CPR_050 Klient używa usługi ReadDataByIdentifier do żądania wartości zapisów danych z serwera. Dane są identyfikowane przez recordDataIdentifier. Producent VU odpowiada za spełnienie warunków serwera przy wykonywaniu tej usługi.

6.1.2. Format komunikatu

CPR_051 Formaty komunikatu dla prymitywów ReadDataByIdentifier opisano szczegółowo w poniższych tabelach:

Tabela 25

Komunikat żądania ReadDataByIdentifier

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu — adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	EE	TGT
#3	Bajt adresu źródłowego	tt	SRC
#4	Dodatkowy bajt długości	03	LEN
#5	ID żądania usługi ReadDataByIdentifier	22	RDBI
#6 i #7	recordDataIdentifier = (wartość z tabela 28)	xxxx	RDI_...
#8	Suma kontrolna	00-FF	CS

Tabela 26

Komunikat pozytywnej odpowiedzi dla ReadDataByIdentifier

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu — adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT
#3	Bajt adresu źródłowego	EE	SRC
#4	Dodatkowy bajt długości	m+3	LEN
#5	ID żądania usługi ReadDataByIdentifier	62	RDBIPR
#6 i #7	recordDataIdentifier = (wartość z tabeli 28)	xxxx	RDI_...
#8 do #m+7	dataRecord() = (data#1 : data#m)	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Suma kontrolna	00-FF	CS

Tabela 27

Komunikat negatywnej odpowiedzi dla ReadDataByIdentifier

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu — adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT
#3	Bajt adresu źródłowego	EE	SRC
#4	Dodatkowy bajt długości	03	LEN
#5	ID usługi negatywnej odpowiedzi	7F	NR
#6	ID żądania usługi ReadDataByIdentifier	22	RDBI
#7	Kod odpowiedzi = (requestOutOfRange incorrectMessageLength conditionsNotCorrect)	31 13 22	RC_ROOR RC_IML RC_CNC
#8	Suma kontrolna	00-FF	CS

6.1.3. Definicja parametru

CPR_052 Parametr recordDataIdentifier (RDI_) w komunikacie żądania ReadDataByIdentifier wskazuje zapis danych.

CPR_053 Wartości recordDataIdentifier zdefiniowane w tym dokumencie pokazano w tabeli poniżej.

Tabela recordDataIdentifier składa się z czterech kolumn i wielu rzędów.

- Pierwsza kolumna (Hex) zawiera „wartość heksadecymalną” przypisaną identyfikatorowi recordDataIdentifier z trzeciej kolumny.
- Druga kolumna (Element danych) określa element danych z dodatku 1, na którym oparty jest identyfikator recordDataIdentifier (czasami niezbędne jest przekodowanie).
- Trzecia kolumna (Opis) podaje nazwę odpowiadającego identyfikatora recordDataIdentifier.
- Czwarta kolumna (Mnemonik) podaje mnemonik tego identyfikatora recordDataIdentifier.

Tabela 28

Definicja wartości identyfikatora recordDataIdentifier

Hex	Element danych	Nazwa recordDataIdentifier (patrz format w sekcji 8.2)	Mnemonik
F90B	CurrentDateTime	TimeDate	RDI_TD
F912	HighResOdometer	HighResolutionTotalVehicleDistance	RDI_HRTVD
F918	K-ConstantOfRecordingEquipment	Kfactor	RDI_KF
F91C	L-TyreCircumference	LfactorTyreCircumference	RDI_LF
F91D	W-VehicleCharacteristicConstant	WvehicleCharacteristicFactor	RDI_WVCF
F921	TyreSize	TyreSize	RDI_TS
F922	nextCalibrationDate	NextCalibrationDate	RDI_NCD
F92C	SpeedAuthorised	SpeedAuthorised	RDI_SA
F97D	vehicleRegistrationNation	RegisteringMemberState	RDI_RMS
F97E	VehicleRegistrationNumber	VehicleRegistrationNumber	RDI_VRN
F190	VehicleIdentificationNumber	VIN	RDI_VIN

CPR_054 Parametr dataRecord (DREC_) używany jest w komunikacie pozytywnej odpowiedzi ReadDataByIdentifier do dostarczania wartości zapisu danych wskazanego klientowi (testerowi) identyfikatorem recordDataIdentifier. Formaty danych określono w sekcji 8. Można wprowadzić dodatkowe opcjonalne dataRecords użytkownika obejmujące szczególne dane wejściowe, wewnętrzne i wyjściowe VU, ale nie są one zdefiniowane w tym dokumencie.

6.2. Usługa WriteDataByIdentifier**6.2.1. Opis komunikatu**

CPR_056 Usługa WriteDataByIdentifier używana jest przez klienta do zapisania wartości zapisu danych w serwerze. Dane wskazuje się identyfikatorem recordDataIdentifier. Producent VU odpowiada za spełnienie warunków serwera przy wykonywaniu tej usługi. Aby aktualizować parametry wymienione w tabeli 28 VU musi być w trybie kalibracyjnym.

6.2.2. Format komunikatu

CPR_057 Formaty komunikatu dla prymitywów WriteDataByIdentifier opisano szczegółowo w poniższych tabelach:

Tabela 29

Komunikat żądania WriteDataByIdentifier

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu — adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	EE	TGT
#3	Bajt adresu źródłowego	tt	SRC
#4	Dodatkowy bajt długości	m+3	LEN
#5	ID żądania usługi WriteDataByIdentifier	2E	WDBI
#6 i #7	recordDataIdentifier = (wartość z tabeli 28)	xxxx	RDI_...
#8 do #m+7	dataRecord() = (data#1 : data#m)	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Suma kontrolna	00-FF	CS

Tabela 30

Komunikat pozytywnej odpowiedzi dla WriteDataByIdentifier

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu — adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT
#3	Bajt adresu źródłowego	EE	SRC
#4	Dodatkowy bajt długości	03	LEN
#5	Id pozytywnej odpowiedzi na żądanie usługi WriteDataByIdentifier	6E	WDBIPR
#6 i #7	recordDataIdentifier = (ta sama wartość jak bajtów #6 i #7 w tabeli 29)	xxxx	RDI_...
#8	Suma kontrolna	00-FF	CS

Tabela 31

Komunikat negatywnej odpowiedzi dla WriteDataByIdentifier

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu — adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT
#3	Bajt adresu źródłowego	EE	SRC
#4	Dodatkowy bajt długości	03	LEN
#5	ID usługi negatywnej odpowiedzi	7F	NR
#6	ID żądania usługi WriteDataByIdentifier	2E	WDBI
#7	ResponseCode = (requestOutOfRange incorrectMessageLength conditionsNotCorrect)	31	RC_ROOR
		13	RC_IML
		22	RC_CNC
#8	Suma kontrolna	00-FF	CS

6.2.3. Definicja parametru

Parametr recordDataIdentifier (RDI_) zdefiniowano w tabeli 28.

Parametr dataRecord (DREC_) używany jest w komunikacie żądania WriteDataByIdentifier dostarczenia wartości zapisu danych wskazanego serwerowi (VU) przez recordDataIdentifier. Formaty danych określono w sekcji 8.

7. STEROWANIE IMPULSAMI TESTUJĄCYMI — JEDNOSTKA FUNKCYJALNA STEROWANIA WE/WY

Dostępne usługi opisano w poniższej tabeli:

Tabela 32

Jednostka funkcjonalna sterowania we/wy

Nazwa usługi	Opis
InputOutputControlByIdentifier	Klient żąda sterowania we/wy specyficznego dla serwera

7.1. Opis komunikatu**7.1.1. Opis komunikatu**

Przez przednie gniazdo zestawione jest połączenie, które umożliwia sterowanie lub monitorowanie impulsów testowych przy pomocy odpowiedniego testera.

CPR_058 Tę linię sygnałową we/wy kalibracji można skonfigurować poleceniem K-line posługując się usługą InputOutputControlByIdentifier w celu wybrania dla linii wymaganej funkcji wejścia lub wyjścia. Linia może przyjmować następujące stany:

- nieczynna,
- speedSignalInput, w którym linia sygnałowa we/wy kalibracji używana jest do wprowadzenia sygnału prędkości (sygnał testowy) zastępującego sygnał prędkości z czujnika ruchu,
- realTimeSpeedSignalOutputSensor, w którym linia sygnałowa we/wy kalibracji używana jest do wyprowadzenia sygnału prędkości z czujnika ruchu,
- RTCTOutput, w którym linia sygnałowa we/wy kalibracji używana jest do wyprowadzenia sygnału zegarowego UTC.

CPR_059 Przyrząd rejestrujący musi być wprowadzony do sesji regulacji i być w trybie kalibracyjnym w celu skonfigurowania stanu linii. Na zakończenie sesji regulacji lub trybu kalibracyjnego przyrząd rejestrujący musi zapewnić, że linia sygnałowa we/wy kalibracji powróci do stanu „disabled” (nieczynna — stan domyślny).

CPR_060 Jeżeli impulsy prędkości odbierane są w czasie rzeczywistym z linii sygnału wejściowego prędkości w VU, natomiast linia sygnałowa we/wy kalibracji jest ustawiona na wyjście, to linia sygnałowa we/wy kalibracji zostanie ustawiona na wyjście lub powróci do stanu „disabled” (nieczynna).

CPR_061 Kolejność czynności jest następująca:

- uruchomienie komunikacji usługą StartCommunication
- otwarcie sesji regulacji usługą StartDiagnosticSession i wejście do trybu kalibracyjnego (kolejność tych dwóch czynności nie ma znaczenia).
- zmiana stanu wyjścia usługą InputOutputControlByIdentifier.

7.1.2. **Format komunikatu**

CPR_062 Formaty komunikatu dla prymitywów InputOutputControlByIdentifier opisano szczegółowo w poniższych tabelach:

Tabela 33

Komunikat żądania InputOutputControlByIdentifier

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu — adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	EE	TGT
#3	Bajt adresu źródłowego	tt	SRC
#4	Dodatkowy bajt długości	xx	LEN
#5	SID żądania InputOutputControlByIdentifier	2F	IOCBI
#6 i #7	InputOutputIdentifier = (CalibrationInputOutput)	F960	IOI_CIO
#8 lub #8 do #9	ControlOptionRecord = (inputOutputControlParameter — wartość z tabeli 36 controlState — wartość z tabeli 38 (patrz uwaga poniżej))	xx xx	COR_... IOCP_... CS_...
#9 lub #10	Suma kontrolna	00-FF	CS

Uwaga: parametr controlState występuje tylko w określonych przypadkach (patrz 7.1.3).

Tabela 34

Komunikat pozytywnej odpowiedzi dla InputOutputControlByIdentifier

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu — adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT
#3	Bajt adresu źródłowego	EE	SRC
#4	Dodatkowy bajt długości	xx	LEN
#5	SID pozytywnej odpowiedzi na żądanie inputOutputControlByIdentifier	6F	IOCBIPR
#6 i #7	inputOutputIdentifier = (CalibrationInputOutput)	F960	IOI_CIO
#8 lub #8 do #9	controlStatusRecord = (inputOutputControlParameter (wartość jak dla bajtu #8 w tabeli 33) controlState (wartość jak dla bajtu #9 w tabeli 33)) (gdy dotyczy)	xx xx	CSR_ IOCP_... CS_...
#9 lub #10	Suma kontrolna	00-FF	CS

Tabela 35

Komunikat negatywnej odpowiedzi dla InputOutputControlByIdentifier

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu — adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT
#3	Bajt adresu źródłowego	EE	SRC
#4	Dodatkowy bajt długości	03	LEN
#5	ID usługi negatywnej odpowiedzi	7F	NR
#6	SId żądania inputOutputControlByIdentifier	2F	IOCBI
#7	Kod odpowiedzi = (incorrectMessageLength conditionsNotCorrect RequestOutOfRange deviceControlLimitsExceeded)	13 22 31 7A	RC_IML RC_CNC RC_ROOR RC_DCLE
#8	Suma kontrolna	00-FF	CS

7.1.3. Definicja parametru

CPR_064 Parametr inputOutputControlParameter (IOCP_) zdefiniowano w poniższej tabeli:

Tabela 36

Definicja wartości parametru inputOutputControlParameter

Hex	Opis	Mnemonik
00	ReturnControlToECU Wartość ta wskazuje serwerowi (VU), że tester już nie steruje linią sygnału we/wy kalibracji.	RCTECU
01	ResetToDefault Wartość ta wskazuje serwerowi (VU), że wymagane jest przełączenie linii sygnału we/wy kalibracji do stanu domyślnego.	RTD
03	ShortTermAdjustment Wartość ta wskazuje serwerowi (VU), że wymagane jest przełączenie linii sygnału we/wy kalibracji do żądanej wartości w celu wyregulowania parametru controlState.	STA

CPR_065 Parametr controlState występuje jedynie wtedy, gdy parametr inputOutputControlParameter jest ustawiony na ShortTermAdjustment i przyjmuje wartości zdefiniowane w poniższej tabeli:

Tabela 37

Definicja wartości stanu controlState

Tryb	Wartość heksadecymalna	Opis
wyłączony	00	linia we/wy wyłączona (stan domyślny)
włączony	01	włącz linię sygnału we/wy kalibracji jako speedSignalInput
włączony	02	włącz linię sygnału we/wy kalibracji jako realTimeSpeedSignalOutputSensor
włączony	03	włącz linię sygnału we/wy kalibracji jako RTCTOutput

8. FORMAT ZAPISÓW DANYCH

W tej sekcji opisano szczegółowo:

- ogólne zasady odnoszące się do szeregu parametrów wysyłanych przez przyrząd rejestrujący do testera,
- formaty, które należy stosować dla danych przesyłanych poprzez usługi przesyłania danych opisane w sekcji 6.

CPR_067 VU obsługuje wszystkie wyszczególnione parametry.

CPR_068 Dane wysyłane przez przyrząd rejestrujący do testera w odpowiedzi na komunikat żądania są typu pomiarowego (tj. bieżąca wartość żadanego parametru pomierzona lub stwierdzona przez VU).

8.1. Zakresy przesyłanych parametrów

CPR_069 W tabeli 38 podano wartości zakresów używane do sprawdzania poprawności przesłanego parametru.

CPR_070 Wartości w zakresie „wskaźnik błędu” umożliwiają przyrządowi rejestrującemu niezwłoczne wskazanie, że poprawne dane parametryczne nie są dostępne w bieżącym czasie wskutek pewnego typu błędu w urządzeniu rejestrującym.

CPR_071 Wartości w zakresie „nieodpowiednie” umożliwiają przyrządowi rejestrującemu wysłanie komunikatu zawierającego parametr, który nie jest dostępny bądź nie jest obsługiwany w tym module. Wartości w zakresie „nieżądane” umożliwiają przyrządowi wysłanie komunikatu polecenia i wskazanie tych parametrów, w przypadku gdy od urządzenia odbierającego oczekiwany jest brak odpowiedzi.

CPR_072 Jeżeli usterka elementu składowego uniemożliwia wysłanie prawidłowych danych dla parametru, zamiast danych parametru używa się wskaźnika błędu opisanego w tabeli 38. Jednak jeżeli dane pomierzone lub obliczone dają wartość, która jest poprawna, ale wychodzi poza zdefiniowany zakres parametru, nie należy używać wskaźnika błędu. Dane przesyłane są używając odpowiednio wartości minimalnej lub maksymalnej parametru.

Tabela 38

Zakresy zapisów dataRecords

Nazwa zakresu	1 bajt (wartość heksadecymalna)	2 bajty (wartość heksadecymalna)	4 bajty (wartość heksadecymalna)	ASCII
Prawidłowy sygnał	00 to FA	0000 to FAFF	00000000 to FFFFFFFF	1 do 254
Szczególny wskaźnik parametru	FB	FB00 to FBFF	FB000000 to FBFFFFFF	brak
Zastrzeżony zakres do wykorzystania w przyszłości	FC to FD	FC00 to FDFF	FC000000 to FDFFFFFF	brak
Wskaźnik błędu	FE	FE00 to FEFF	FE000000 to FEFFFFFF	0
Niedostępne lub nieządane	FF	FF00 to FFFF	FF000000 to FFFFFFFF	FF

CPR_073 Dla parametrów kodowanych w ASCII, znak ASCII „*” jest zastrzeżony jako ogranicznik.

8.2. Format dataRecords

W tabelach 40-44 opisano szczegółowo formaty używane przez usługi ReadDataByIdentifier i WriteDataByIdentifier.

CPR_074 W tabeli 40 podano długość, rozdzielczość i zakres roboczy dla każdego parametru identyfikowanego przez recordDataIdentifier:

Tabela 39

Format rekordów dataRecords

Nazwa parametru	Długość danych (w bajtach)	Rozdzielczość	Zakres roboczy
TimeDate	8	szczegółowy opis w tabeli 40	
HighResolutionTotalVehicleDistance	4	5 m/bit, offset 0 m	0 do + 21 055 406 km
Kfactor	2	0,001 impulsu/m/bit, offset 0	0 do 64,255 impulsu /m
LfactorTyreCircumference	2	0,123 10 ⁻³ /bit gain, offset 0	0 d 8 031 m
WvehicleCharacteristicFactor	2	0,001 impulsu/m/bit gain, offset 0	0 d 64,255 impulsu/m
TyreSize	15	ASCII	ASCII
NextCalibrationDate	3	szczegółowy opis w tabeli 41	
SpeedAuthorised	2	1/256 km/h/bit gain, offset 0	0 d 250 996 km/h
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	szczegółowy opis w tabeli 44	
VIN	17	ASCII	ASCII

CPR_075 W tabeli 40 zamieszczono szczegółowy opis formatów poszczególnych bajtów parametru TimeDate:

Tabela 40

Szczegółowy opis formatu TimeDate (wartość recordDataIdentifier F00B)

Bajt	Definicja parametru	Rozdzielczość	Zakres roboczy
1	sekundy	0,25 s/bit, offset 0 s	0 do 59,75 s
2	minuty	1 minuta/bit, offset 0 minut	0 do 59 minut
3	godziny	1 h/bit, offset 0 h	0 do 23 h
4	miesiąc	1 miesiąc/bit, offset 0 miesięcy	1 do 12 miesięcy
5	dzień	0,25 dnia/bit, offset 0 dni (patrz uwaga pod tabelą 41)	0,25 do 31,75 dnia
6	rok	1 rok/bit, + offset rok 1985 (patrz uwaga pod tabelą 41)	lata od 1985 do 2235
7	lokalne przesunięcie dla minut	1 minuta/bit, offset –125 minut	–59 do 59 minut
8	lokalne przesunięcie dla godzin	1 h/bit, offset –125	–23 do + 23 h

CPR_076 W tabeli 41 zamieszczono szczegółowy opis formatów poszczególnych bajtów parametru NextCalibrationDate:

Tabela 41

Szczegółowy opis formatu NextCalibrationDate (wartość recordDataIdentifier F022)

Bajt	Definicja parametru	Rozdzielczość	Zakres roboczy
1	miesiąc	1 miesiąc/bit, offset 0 miesięcy	1 do 12 miesięcy
2	dzień	0,25 dzień/bit, offset 0 dni (patrz uwaga pod tabelą)	0,25 do 31,75 dnia
3	rok	1 rok/bit, offset +1985 (patrz uwaga pod tabelą)	lata od 1985 do 2235

Uwagi dotyczące zastosowania parametru „dzień”:

1. Wartość 0 dla daty nie istnieje. Wartości 1, 2, 3 i 4 są stosowane do oznaczenia pierwszego dnia miesiąca; 5, 6, 7 i 8 – do oznaczenia drugiego dnia miesiąca, etc.
2. Ten parametr nie ma wpływu na, ani nie zmienia parametru „godzina”.

Uwaga dotycząca zastosowania parametru „rok”:

Wartość 0 dla roku oznacza rok 1985, wartość 1 oznacza rok 1986, etc.

CPR_078 W tabeli 42 zamieszczono szczegółowy opis formatów poszczególnych bajtów parametru VehicleRegistrationNumber:

Tabela 42

Szczegółowy opis formatu VehicleRegistrationNumber (wartość recordDataIdentifier F07E)

Bajt	Definicja parametru	Rozdzielczość	Zakres roboczy
1	Strona kodowa (zdefiniowana w dodatku 1)	ASCII	01 do 0A
2 do 14	Numer rejestracyjny pojazdu (zdefiniowany w dodatku 1)	ASCII	ASCII

Dodatek 9

HOMOLOGACJA TYPU — WYKAZ MINIMUM WYMAGANYCH TESTÓW

SPIS TREŚCI

1.	Wprowadzenie	469
1.1.	Homologacja typu	469
1.2.	Odniesienia	469
2.	Badania funkcjonalności przyrządu rejestrującego	470
3.	Czujnik ruchu badania funkcjonalności	473
4.	Badania funkcjonalności kart do tachografów	475
5.	Badania interoperacyjności	476

1. WPROWADZENIE

1.1. Homologacja typu

Homologacja typu EWG urządzenia rejestrującego (lub części składowej) lub karty do tachografów opiera się na następujących dokumentach:

- świadectwo zabezpieczenia, wystawione przez organ ITSEC na podstawie kryteriów bezpieczeństwa w pełni zgodnych z przedstawionymi w dodatku 10 do niniejszego załącznika,
- świadectwo funkcjonalności wystawione przez organ Państwa Członkowskiego i zaświadczaające, że zbadane urządzenie spełnia wymagania niniejszego Załącznika pod względem wykonywanych funkcji, dokładności pomiarów i charakterystyk środowiskowych,
- świadectwo interoperacyjności wystawione przez właściwy organ i zaświadczaające, że urządzenie rejestrujące (lub karta do tachografów) w pełni współpracuje z niezbędnymi modelami kart do tachografów (lub urządzenia rejestrującego) (patrz rozdział VIII niniejszego Załącznika).

Niniejszy dodatek określa, które testy, jako minimum, musi przeprowadzić organ Państwa Członkowskiego w ramach badania funkcjonalności, i które testy, jako minimum, musi przeprowadzić właściwy organ w ramach badania interoperacyjności. Nie określa się procedur przeprowadzania tych badań ani ich typów.

Niniejszy dodatek nie obejmuje aspektów świadectwa zabezpieczenia. Jeżeli niektóre badania wymagane dla homologacji typu przeprowadza się przy ocenie bezpieczeństwa i w ramach procesu certyfikacyjnego, to badań tych nie trzeba przeprowadzać ponownie. W takim przypadku mogą być zbadane tylko wyniki tych badań bezpieczeństwa. Do celów informacyjnych wymagania, których badań oczekuje się (lub ściśle wiążą się z badaniami, których przeprowadzenia oczekuje się) w ramach badań dla potrzeb świadectwa zabezpieczenia, są w niniejszym dodatku oznaczone symbolem »*«.

Niniejszy dodatek zajmuje się oddzielnie homologacją typu czujnika ruchu i przyrządu rejestrującego, jako części składowych urządzenia rejestrującego. Nie wymaga się współdziałania między każdym modelem czujnika ruchu i każdym modelem przyrządu rejestrującego, dlatego też homologacja typu dla czujnika ruchu może być wydane tylko w połączeniu z homologacją typu dla przyrządu rejestrującego i vice versa.

1.2. Odniesienia

W niniejszym dodatku używa się następujących odniesień:

IEC 68-2-1	Badania środowiskowe — część 2: Badania — Badania A: Zimne. 1990 + zmiana 2: 1994 r.
IEC 68-2-2	Badania środowiskowe — część 2: Badania — Badania B: Suche gorące. 1974 r. + zmiana 2: 1994 r.
IEC 68-2-6	Podstawowe procedury badań środowiskowych — Metody badania — Badanie Fc i przewodnik: Drgania (sinusoidalna). Wydanie szóste: 1985 r.
IEC 68-2-14	Podstawowe procedury badań środowiskowych — Metody badania — Badanie N: Zmiana temperatury. Zmiana 1: 1986 r.
IEC 68-2-27	Podstawowe procedury badań środowiskowych — Metody badania — Badanie Ea i przewodnik: Udar. Wydanie trzecie: 1987 r.
IEC 68-2-30	Podstawowe procedury badań środowiskowych — Metody badania — Badanie Db i przewodnik: Wilgotne gorąco, cykliczne (cykl 12 + 12 godzin). Zmiana 1: 1985 r.
IEC 68-2-35	Podstawowe procedury badań środowiskowych — Metody badania — Badanie Fda: Drgania losowe szerokopasmowe — wysoka powtarzalność. Zmiana 1: 1983 r.
IEC 529	Stopnie ochrony zapewniane przez obudowy (kod IP). Wydanie drugie: 1989 r.
IEC 61000-4-2	Kompatybilność elektromagnetyczna (EMC) — Techniki badawcze i pomiarowe — Badanie odporności na wyładowania elektrostatyczne: 1995/zmiana 1: 1998 r.
ISO 7637-1	Pojazdy drogowe — Zakłócenia elektryczne spowodowane przewodzeniem i sprzężeniem — część 1: Samochody osobowe i lekkie pojazdy samochodowe do eksploatacji handlowej z nominalnym 12 V napięciem zasilającym — Przewodzenie elektrycznych przebiegów przejściowych tylko przez linie zasilające. Wydanie drugie: 1990 r.

- ISO 7637-2 Pojazdy drogowe — Zakłócenia elektryczne spowodowane przewodzeniem i sprzężeniem — część 1: Samochody osobowe i lekkie pojazdy samochodowe do eksploatacji handlowej z nominalnym 12 V napięciem zasilającym — Przewodzenie elektrycznych przebiegów przejściowych tylko przez linie zasilające. Wydanie drugie: 1990 r.
- ISO 7637-3 Pojazdy drogowe — Zakłócenia elektryczne spowodowane przewodzeniem i sprzężeniem — część 3: Pojazdy samochodowe z 12 V lub 24 V napięciem zasilającym — Przenoszenie elektrycznych przebiegów przejściowych przez sprzężenia pojemnościowe i indukcyjne przez linie inne niż linie zasilające. Wydanie pierwsze: 1995 r. + sprostowania 1: 1995 r.
- ISO/IEC 7816-1 Identyfikacja kart — Karty z układem(ami) scalonym z wyprowadzeniami — część 1: Charakterystyki fizyczne. Wydanie pierwsze: 1998 r.
- ISO/IEC 7816-2 Informatyka — Identyfikacja kart — Karty z układem(ami) scalonym z wyprowadzeniami — część 2: Wymiary i rozmieszczenie styków. Wydanie pierwsze: 1999 r.
- ISO/IEC 7816-3 Informatyka — Identyfikacja kart — Karty z układem(ami) scalonym z wyprowadzeniami — część 3: Sygnały elektryczne i protokół komunikacyjny. Wydanie drugie: 1997 r.
- ISO/IEC 10373 Identyfikacja kart — Metody badania. Wydanie pierwsze: 1993 r.

2. BADANIA FUNKCJONALNOŚCI PRZYRZĄDU REJESTRUJĄCEGO

nr	Badanie	Wyszczególnienie	Wymagania związane
1.	Badanie administracyjne		
1.1.	Dokumentacja	Dokładność dokumentacji	
1.2.	Wyniki badań producenta	Wyniki badań producenta przeprowadzonych podczas integracji. Pokaz dokumentów papierowych	070, 071, 073
2.	Kontrola wizualna		
2.1.	Zgodność z dokumentacją		
2.2.	Identyfikacja/oznakowanie		168, 169
2.3.	Materiały		163–167
2.4.	Plombowanie		251
2.5.	Interfejsy zewnętrzne		
3.	Badania funkcjonalności		
3.1.	Obsługiwane funkcje		002, 004, 244
3.2.	Tryby pracy		006*, 007*, 008*, 009*, 106, 107
3.3.	Prawa dostępu do funkcji i danych		010*, 011*, 240, 246, 247
3.4.	Monitorowanie wkładania i wyjmowania kart		013, 014, 015*, 016*, 106
3.5.	Pomiar prędkości i odległości		017–026
3.6.	Pomiar czasu (badanie przeprowadzone w temperaturze 20 °C)		027–032
3.7.	Monitorowanie czynności kierowcy		033–043, 106
3.8.	Monitorowanie stanu prowadzenia pojazdu		044, 045, 106
3.9.	Pozycje wprowadzane ręcznie		046–050b
3.10.	Zarządzanie blokadami firmowymi		051–055
3.11.	Monitorowanie czynności kontrolnych		056, 057
3.12.	Wykrywanie zdarzeń i/lub usterek		059–069, 106

nr	Badanie	Wyszczególnienie	Wymagania związane
3.13.	Dane identyfikujące sprzęt		075*, 076*, 079
3.14.	Dane dotyczące wkładania i wyjmowania karty kierowcy		081*–083*
3.15.	Dane dotyczące czynności kierowcy		084*–086*
3.16.	Dane dotyczące miejsc		087*–089*
3.17.	Dane dotyczące licznika kilometrów		090*–092*
3.18.	Szczegółowe dane dotyczące prędkości		093*
3.19.	Dane dotyczące zdarzeń		094*, 095
3.20.	Dane dotyczące usterek		096*
3.21.	Dane dotyczące kalibracji		097*, 098*
3.22.	Dane dotyczące regulacji czasu		100*, 101*
3.23.	Dane dotyczące czynności kontrolnej		102*, 103*
3.24.	Dane dotyczące blokad firmowych		104*
3.25.	Dane dotyczące czynności wczytywania		105*
3.26.	Dane dotyczące warunków szczególnych		105a*, 105b*
3.27.	Rejestrowanie i przechowywanie danych na kartach do tachografów		108, 109*, 109a*, 110*, 111, 112
3.28.	Wyświetlanie		072, 106, 113 t–128, PIC_001, DIS_001
3.29.	Drukowanie		072, 106, 129–138, PIC_001, PRT_001–PRT_012
3.30.	Ostrzeganie		106, 139–148, PIC_001
3.31.	Wczytywanie danych na nośnik zewnętrzny		072, 106, 149–151
3.32.	Wyprowadzanie danych do dodatkowych urządzeń zewnętrznych		152, 153
3.33.	Kalibracja		154*, 155*, 156*, 245
3.34.	Regulacja czasu		157*, 158*
3.35.	Niezakłócanie funkcji dodatkowych		003, 269

nr	Badanie	Wyszczególnienie	Wymagania związane
4.	Badania środowiskowe		
4.1.	Temperatura	Sprawdzenie funkcjonalności: — IEC 68-2-1, test Ad, z czasem trwania testu 72 godziny w niższej temperaturze (-20°C), 1 godzinę urządzenie pracuje, 1 godzinę urządzenie nie pracuje, — IEC 68-2-2, test Bd, z czasem trwania testu 72 godziny w wyższej temperaturze (70°C), 1 godzinę urządzenie pracuje, 1 godzinę urządzenie nie pracuje. Cykle temperaturowe: sprawdzenie odporności przyrządu rejestrującego na gwałtowne zmiany temperatury otoczenia testem Na wg normy IEC 68-2-14, 20 cykli, każdy z temperaturą zmieniającą się od niższej temperatury (-20°C) do wyższej temperatury (70°C) i 2 godziny pozostawiania w obu temperaturach niższej i wyższej. Można przeprowadzić zredukowany zestaw testów (spośród tych zdefiniowanych w sekcji 3 niniejszej tabeli) w niższej temperaturze, wyższej temperaturze i w czasie cykli temperaturowych.	159
4.2.	Wilgotność	Sprawdzenie odporności przyrządu rejestrującego na cykliczne zmiany wilgotności (test gorący) testem Db wg normy IEC 68-2-30, sześć 24-godzinnych cykli, w każdym zmieniające się temperatura od 25°C do 55°C i wilgotność względna 97 % w 25°C i równa 93 % w 55°C	160
4.3.	Drgania	1. Drgania harmoniczne: Sprawdzenie odporności przyrządu rejestrującego na drgania harmoniczne o następujących charakterystykach: stałe przemieszczenie przy częstotliwości między 5 a 11 Hz: 10 mm amplituda stałe przyspieszenie przy częstotliwości między 11 a 300 Hz: 5 g Wymaganie to sprawdza się testem Fc wg normy IEC 68-2-6, z minimalnym czasem trwania testu 3×12 godzin (12 godzin na oś) 2. Drgania swobodne: Sprawdzenie odporności przyrządu rejestrującego na drgania swobodne o następujących charakterystykach: częstotliwość 5-150 Hz, poziom $0,02 \text{ g}^2/\text{Hz}$ Wymaganie to sprawdza się testem Ffda wg normy IEC 68-2-35, z minimalnym czasem trwania testu 3×12 godzin (12 godzin na oś), 1 godzinę urządzenie pracuje, 1 godzinę urządzenie nie pracuje. Dwa opisane powyżej testy przeprowadza się na dwóch, różnych próbkach urządzeń poddawanych testom.	163
4.4.	Ochrona przed wodą i ciałami obcymi	Sprawdzenie czy stopień ochrony przyrządu rejestrującego wg normy IEC 529 jest przynajmniej IP 40, dla urządzenia zainstalowanego w warunkach eksploatacyjnych w pojeździe.	164, 165
4.5.	Zabezpieczenie nadmiarowo-napięciowe	Sprawdzenie odporności przyrządu rejestrującego napięcie zasilania: wersje 24V: 34 V przy 40°C przez 1 godzinę wersje 12V: 17 V przy 40°C przez 1 godzinę	161
4.6.	Zabezpieczenie przed odwróceniem polaryzacji	Sprawdzenie odporności przyrządu rejestrującego na odwrócenie biegunów napięcia zasilającego.	161

nr	Badanie	Wyszczególnienie	Wymagania związane
4.7.	Zabezpieczenie zwarciowe	Sprawdzenie czy sygnały wyjściowe są zabezpieczone przed zwarciem do napięcia zasilającego i do masy.	161
5.	Badania kompatybilności elektromagnetycznej		
5.1.	Emisje radiacyjne i wrażliwość na radiację	Zgodność z dyrektywą 95/54/EWG	162
5.2.	Rozładowanie elektrostatische	Zgodność z normą IEC 61000-4-2, ± 2 kV (poziom 1)	162
5.3.	Wrażliwość na stany nieustalone w zasilaniu	Dla wersji 24V: zgodność z normą ISO 7637-2: impuls 1a: $V_s = -100$ V, $R_i = 10$ omów impuls 2: $V_s = +100$ V, $R_i = 10$ omów impuls 3a: $V_s = -100$ V, $R_i = 50$ omów impuls 3b: $V_s = +100$ V, $R_i = 50$ omów impuls 4: $V_s = -16$ V $V_a = -12$ V, $t_6 = 100$ ms impuls 5: $V_s = +120$ V, $R_i = 2,2$ oma, $t_d = 250$ ms Dla wersji 12V: zgodność z normą ISO 7637-1: impuls 1: $V_s = -100$ V, $R_i = 10$ omów impuls 2: $V_s = +100$ V, $R_i = 10$ omów impuls 3a: $V_s = -100$ V, $R_i = 50$ omów impuls 3b: $V_s = +100$ V, $R_i = 50$ omów impuls 4: $V_s = -6$ V, $V_a = -5$ V, $t_6 = 15$ ms impuls 5: $V_s = +65$ V, $R_i = 3$ omy, $t_d = 100$ ms Impuls 5 należy testować tylko dla przyrządów rejestrujących skonstruowanych do zainstalowania w pojazdach, w których nie zainstalowano zewnętrznego, wspólnego zabezpieczenia przed spadkiem obciążenia.	162

3. CZUJNIK RUCHU BADANIA FUNKCJONALNOŚCI

nr	Test	Wyszczególnienie	Wymagania związane
1.	Badanie administracyjne		
1.1.	Dokumentacja	Dokładność dokumentacji	
2.	Kontrola wizualna		
2.1.	Zgodność z dokumentacją		
2.2.	Identyfikacja/oznakowanie		169, 170
2.3.	Materiały		163–167
2.4.	Plombowanie		251
3.	Badania funkcjonalności		
3.1.	Dane identyfikacyjne czujnika		077*
3.2.	Parowanie czujnik ruchu — przyrząd rejestrujący		099*, 155
3.3.	Wykrywanie ruchu		
	Dokładność pomiaru ruchu		022–026

nr	Test	Wyszczególnienie	Wymagania związane
4.	Badania środowiskowe		
4.1.	Temperatura pracy	Sprawdzenie funkcjonalności (zdefiniowanej w teście nr 3.3) w zakresie temperatur $[-40 \text{ — } 135 \text{ °C}]$: — testem Ad wg normy IEC 68-2-1, z czasem trwania testu 96 godzin w najniższej temperaturze $T_{\min}$ — testem Bd wg normy IEC 68-2-2, z czasem trwania testu 96 godzin w najwyższej temperaturze $T_{\max}$	159
4.2.	Cykle temperaturowe	Sprawdzenie funkcjonalności (zdefiniowanej w teście nr 3.3) testem Na wg normy IEC 68-2-14, 20 cykli, każdy z temperaturą zmieniającą się od niższej temperatury (-40 °C) do wyższej temperatury (135 °C) i pozostawianiem przez 2 godziny zarówno w niższej jak i wyższej temperaturze Można przeprowadzić zredukowany zestaw testów (spośród tych zdefiniowanych w teście 3.3) w niższej temperaturze, wyższej temperaturze i w czasie cykli temperaturowych.	159
4.3.	Cykle wilgotności	Sprawdzenie funkcjonalności (zdefiniowanej w teście nr 3.3) testem Db wg normy IEC 68-2-30, sześć 24-godzinnych cykli, w każdym zmieniające się temperatura od $25 \text{ do } 55 \text{ °C}$ i wilgotność względna $97 \% \text{ w } 25 \text{ °C}$ i równa $93 \% \text{ w } 55 \text{ °C}$	160
4.4.	Drgania	Sprawdzenie funkcjonalności (zdefiniowanej w teście nr) testem Fc wg normy IEC 68-2-6, z testem obejmującym 100 cykli częstotliwości: stałe przemieszczenie przy częstotliwości między $10 \text{ a } 57 \text{ Hz}$: amplituda $1,5 \text{ mm}$, stałe szczytowe przyspieszenie dla częstotliwości między $57 \text{ a } 500 \text{ Hz}$: 20 g .	163
4.5.	Udar mechaniczny	Sprawdzenie funkcjonalności (zdefiniowanej w teście nr 3.3) test Ea wg normy IEC 68-2-27, 3 udary w obu kierunkach po 3 prostopadłych osiach.	163
4.6.	Ochrona przed wodą i ciałami obcymi	Sprawdzenie czy stopień ochrony przyrządu rejestrującego wg normy IEC 529 jest przynajmniej IP 64, dla urządzenia zainstalowanego w warunkach eksploatacyjnych w pojeździe.	165
4.7.	Zabezpieczenie przed odwróceniem polaryzacji	Sprawdzenie odporności czujnika ruchu na odwrócenie biegunów napięcia zasilającego.	161
4.8.	Zabezpieczenie zwarcia	Sprawdzenie czy sygnały wyjściowe są zabezpieczone przed zwarciem do napięcia zasilającego i do masy.	161
5.	Badania kompatybilności elektromagnetycznej		
5.1.	Emisje radiacyjne i wrażliwość na radiację	Sprawdzenie zgodności z dyrektywą 95/54/EWG	162
5.2.	Rozładowanie elektrostyczne	Zgodność z normą IEC 61000-4-2, $\pm 2 \text{ kV}$ (poziom 1)	162
5.3.	Wrażliwość na stany nieustalone na liniach danych	Zgodność z normą ISO 7637-3 (poziom III)	162

4. BADANIA FUNKCJONALNOŚCI KART DO TACHOGRAFÓW

nr	Test	Wyszczególnienie	Wymagania związane
1.	Badanie administracyjne		
1.1.	Dokumentacja	Dokładność dokumentacji	
2.	Kontrola wizualna		
2.1.		Sprawdzenie czy wszystkie zabezpieczenia i widoczne dane są prawidłowo wydrukowane i zgodne z wymaganiami	171–181
3.	Badania fizyczne		
3.1.		Sprawdzenie wymiarów karty i rozmieszczenia styków	184 ISO/IEC 7816-1 ISO/IEC 7816-2
4.	Testy protokołów		
4.1.	ATR	Sprawdzenie zgodności ATR.	ISO/IEC 7816-3 TCS 304, 307, 308
4.2.	T=0	Sprawdzenie zgodności protokołu T=0.	ISO/IEC 7816-3 TCS 302, 303, 305
4.3.	PTS	Sprawdzenie zgodności polecenia PTS przez ustawienie T=1 z T=0.	ISO/IEC 7816-3 TCS 309–311
4.4.	T=1	Sprawdzenie zgodności protokołu T=1.	ISO/IEC 7816-3 TCS 303, / 306
5.	Struktura karty		
5.1.		Sprawdzenie zgodności struktury plików na karcie przez sprawdzenie czy na karcie są wymagane pliki oraz sprawdzenie warunków dostępu do plików.	TCS 312 TCS 400*, 401, 402, 403*, 404, 405*, 406, 407, 408*, 409, 410*, 411, 412, 413*, 414, 415*, 416, 417, 418*, 419
6.	Badania funkcjonalności		
6.1.	Normalne przetwarzanie	Sprawdzenie przynajmniej raz każdego, dozwolonego użycia każdego polecenia (np.: sprawdzenie polecenia UPDATE BINARY z CLA = '00', CLA = '0C' i z różnymi parametrami P1, P2 i Lc). Sprawdzenie czy karta rzeczywiście wykonuje czynności (np.: odczytując plik poleceniem wykonywanym na tym pliku).	TCS 313–TCS 379
6.2.	Komunikaty błędów	Sprawdzenie przynajmniej raz każdego komunikatu błędów (określonego w dodatku 2) dla każdego polecenia. Sprawdzenie przynajmniej raz każdego błędów ogólnego (z wyjątkiem błędów integralności '6400' sprawdzanych w ramach badań na świadectwo zabezpieczenia).	
7.	Badania środowiskowe		
7.1.		Sprawdzenie czy karty pracują w granicach warunków zdefiniowanych zgodnie z normą ISO/IEC 10373	185–188 ISO/IEC 7816-1

5. BADANIA INTEROPERACYJNOŚCI

nr	Test	Wyszczególnienie
1.	Wzajemne uwierzytelnienie	Sprawdzenie czy wzajemne uwierzytelnienie między przyrządem rejestrującym a kartą do tachografów przebiega normalnie
2.	Testy zapis/odczyt	Wykonanie scenariusza typowej czynności na przyrządzie rejestrującym. Scenariusz dostosowany jest do typu badanej karty i obejmować zapis na karcie tak wielu EF jak możliwe. Sprawdzenie poprzez wczytywanie danych z karty czy wszystkie odpowiednie zapisy są zrobione prawidłowo. Sprawdzenie poprzez dzienny wydruk z karty czy wszystkie odpowiednie zapisy mogą być odczytane prawidłowo.

Dodatek 10

OGÓLNE CELE ZABEZPIECZENIA

Niniejszy dodatek określa minimalne wymagania dotyczące celów zabezpieczenia czujnika ruchu, przyrządu rejestrującego i karty do tachografów.

W celu nadania kształtu celom zabezpieczenia, które stanowią podstawę do uzyskania świadectwa zabezpieczenia, producenci przygotowują i kompletują niezbędne dokumenty bez poprawiania i usuwania istniejących zagrożeń, celów, środków proceduralnych i specyfikacji funkcji realizujących zabezpieczenia.

SPIS TREŚCI

Ogólny cel zabezpieczenia czujnika ruchu

1.	Wprowadzenie	482
2.	Skróty, definicje i odniesienia	482
2.1.	Skróty	482
2.2.	Definicje	482
2.3.	Odniesienia	483
3.	Podstawy racjonalne produktu	483
3.1.	Opis i metoda użycia czujnika ruchu	483
3.2.	Cykl istnienia czujnika ruchu	484
3.3.	Zagrożenia	484
3.3.1.	Zagrożenia związane z polityką kontroli dostępu	484
3.3.2.	Zagrożenia związane z konstrukcją	485
3.3.3.	Zagrożenia zorientowane na eksploatację	485
3.4.	Cele zabezpieczenia	485
3.5.	Informatyczne cele zabezpieczenia	485
3.6.	Środki fizyczne, osobowe lub proceduralne	486
3.6.1.	Konstrukcja urządzenia	486
3.6.2.	Dostawa urządzenia	486
3.6.3.	Generowanie danych bezpieczeństwa i dostawa	486
3.6.4.	Instalacja, kalibracja i inspekcja urządzenia rejestrującego	486
3.6.5.	Kontrola wdrażania prawa	486
3.6.6.	Aktualizacje oprogramowania	486
4.	Funkcje realizujące zabezpieczenie	486
4.1.	Identyfikacja i uwierzytelnienie	486
4.2.	Kontrola dostępu	487
4.2.1.	Polityka kontroli dostępu	487
4.2.2.	Prawa dostępu do danych	487
4.2.3.	Struktura pliku i warunki dostępu	487
4.3.	Identyfikacja czujnika ruchu	487

4.4.	Audyt	488
4.5.	Dokładność	488
4.5.1.	Polityka kontroli przepływu informacji	488
4.5.2.	Wewnętrzne przesyłanie danych	488
4.5.3.	Integralność przechowywanych danych	488
4.6.	Wiarygodność usługi	488
4.6.1.	Testy	488
4.6.2.	Oprogramowanie	489
4.6.3.	Ochrona fizyczna	489
4.6.4.	Przerwy zasilania	489
4.6.5.	Warunki zerujące	489
4.6.6.	Dostępność danych	489
4.6.7.	Obsługa wielu aplikacji	489
4.7.	Wymiana danych	489
4.8.	Wsparcie kryptograficzne	489
5.	Definicja mechanizmów zabezpieczenia	490
6.	Minimalna siła mechanizmów zabezpieczenia	490
7.	Poziom gwarancji zabezpieczenia	490
8.	Podstawy racjonalne	490

Ogólny cel zabezpieczenia przyrządu rejestrującego

1.	Wprowadzenie	492
2.	Skróty, definicje i odniesienia	492
2.1.	Skróty	492
2.2.	Definicje	492
2.3.	Odniesienia	492
3.	Podstawy racjonalne produktu	492
3.1.	Opis i metoda użycia przyrządu rejestrującego	492
3.2.	Cykl istnienia przyrządu rejestrującego	494
3.3.	Zagrożenia	494
3.3.1.	Zagrożenia dla polityki identyfikacji i kontroli dostępu	494
3.3.2.	Zagrożenia związane z konstrukcją	495
3.3.3.	Zagrożenia zorientowane na eksploatację	495
3.4.	Cele zabezpieczenia	495
3.5.	Informatyczne cele zabezpieczenia	496
3.6.	Środki fizyczne, osobowe lub proceduralne	496
3.6.1.	Konstrukcja urządzenia	496
3.6.2.	Dostawa i aktywacja urządzenia	496

3.6.3. Generowanie danych bezpieczeństwa i dostawa	496
3.6.4. Dostawa kart	497
3.6.5. Instalacja, kalibracja i inspekcja urządzenia rejestrującego	497
3.6.6. Eksploatacja urządzenia	497
3.6.7. Kontrola wdrażania prawa	497
3.6.8. Aktualizacje oprogramowania	497
4. Funkcje realizujące zabezpieczenie	497
4.1. Identyfikacja i uwierzytelnienie	497
4.1.1. Identyfikacja i uwierzytelnienie czujnika ruchu	497
4.1.2. Identyfikacja i uwierzytelnienie użytkownika	498
4.1.3. Identyfikacja i uwierzytelnienie zdalnie przyłączonej firmy	499
4.1.4. Identyfikacja i uwierzytelnienie urządzenia zarządzającego	499
4.2. Kontrola dostępu	499
4.2.1. Polityka kontroli dostępu	499
4.2.2. Prawa dostępu do funkcji	499
4.2.3. Prawa dostępu do danych	499
4.2.4. Struktura pliku i warunki dostępu	500
4.3. Wiarygodność	500
4.4. Audyt	500
4.5. Powtórne wykorzystanie obiektu	501
4.6. Dokładność	501
4.6.1. Polityka kontroli przepływu informacji	501
4.6.2. Wewnętrzne przesyłanie danych	501
4.6.3. Integralność przechowywanych danych	501
4.7. Wiarygodność usługi	501
4.7.1. Testy	501
4.7.2. Oprogramowanie	502
4.7.3. Ochrona fizyczna	502
4.7.4. Przerwy zasilania	502
4.7.5. Warunki zerujące	502
4.7.6. Dostępność danych	502
4.7.7. Obsługa wielu aplikacji	502
4.8. Wymiana danych	502
4.8.1. Wymiana danych z czujnikiem ruchu	502
4.8.2. Wymiana danych z kartami do tachografów	503
4.8.3. Wymiana danych z zewnętrznymi nośnikami gromadzenia danych (funkcja ładowania danych)	503
4.9. Wsparcie kryptograficzne	503

5.	Definicja mechanizmów zabezpieczenia	503
6.	Minimalna siła mechanizmów zabezpieczenia	503
7.	Poziom gwarancji zabezpieczenia	503
8.	Podstawy racjonalne	504

Ogólny cel zabezpieczenia karty do tachografów

1.	Wprowadzenie	508
2.	Skróty, definicje i odniesienia	508
2.1.	Skróty	508
2.2.	Definicje	508
2.3.	Odniesienia	509
3.	Podstawy racjonalne produktu	509
3.1.	Opis i metoda użycia karty do tachografów	509
3.2.	Cykl życia karty do tachografów	509
3.3.	Zagrożenia	510
3.3.1.	Końcowe cele	510
3.3.2.	Ścieżki ataku	510
3.4.	Cele zabezpieczenia	510
3.5.	Informatyczne cele zabezpieczenia	510
3.6.	Środki fizyczne, osobowe lub proceduralne	510
4.	Funkcje realizujące zabezpieczenie	511
4.1.	Zgodność z profilami ochrony	511
4.2.	Identyfikacja i uwierzytelnienie użytkownika	511
4.2.1.	Identyfikacja użytkownika	511
4.2.2.	Uwierzytelnienie użytkownika	511
4.2.3.	Błędy uwierzytelnienia	511
4.3.	Kontrola dostępu	412
4.3.1.	Polityka kontroli dostępu	412
4.3.2.	Funkcje kontroli dostępu	412
4.4.	Wiarygodność	412
4.5.	Audyt	412
4.6.	Dokładność	412
4.6.1.	Integralność przechowywanych danych	412
4.6.2.	Podstawowe uwierzytelnienie danych	412
4.7.	Wiarygodność usługi	513
4.7.1.	Testy	513
4.7.2.	Oprogramowanie	513
4.7.3.	Zasilanie	513

4.7.4.	Warunki zerujące	513
4.8.	Wymiana danych	513
4.8.1.	Wymiana danych z przyrządem rejestrującym	513
4.8.2.	Eksport danych gdzie indziej niż do przyrządu rejestrującego (funkcja ładowania danych)	513
4.9.	Wsparcie kryptograficzne	513
5.	Definicja mechanizmów zabezpieczenia	513
6.	Minimalna siła mechanizmów zabezpieczenia	514
7.	Poziom gwarancji zabezpieczenia	514
8.	Podstawy racjonalne	514

OGÓLNY CEL ZABEZPIECZENIA CZUJNIKA RUCHU

1. Wprowadzenie

Niniejszy dokument zawiera opis czujnika ruchu, zagrożeń, którym czujnik ruchu musi być w stanie przeciwdziałać i celów zabezpieczenia, które musi osiągnąć. Niniejszy dokument określa wymagane funkcje realizujące zabezpieczenia, podaje wymaganą, minimalną siłę mechanizmów ochrony i wymagany poziom zapewnienia rozwoju i oceny.

Wymaganiami, określone w tym dokumencie, są te znajdujące się w treści załącznika I B. W celu zwiększenia czytelności czasami pojawia się powielanie wymagań znajdujących się w treści załącznika I B i wymagań celu zabezpieczenia. W przypadku niezgodności między wymaganiami celu zabezpieczenia a wymaganiami znajdującymi się w treści załącznika I B, do których odwołuje się wymaganie celu zabezpieczenia, obowiązuje wymaganie z treści załącznika I B.

Wymagania znajdujące się w treści załącznika I B, do których nie odwołują się cele zabezpieczenia, nie są przedmiotem funkcji realizujących zabezpieczenia.

Zagrożeniom, celom, środkom proceduralnym i specyfikacjom funkcji realizujących zabezpieczenia nadano unikalne etykiety w celu umożliwienia odtworzenia historii produktu w dokumentach rozwoju i oceny.

2. Skróty, definicje i odniesienia**2.1. Skróty**

ROM	pamięć stała (nieulotna)
SEF	funkcja realizująca zabezpieczenia
TBD	określi
TOE	cel oceny
VU	przyrząd rejestrujący.

2.2. Definicje

Cyfrowy tachograf	urządzenie rejestrujące
Jednostka	urządzenie przyłączone do czujnika ruchu
Dane ruchowe	dane wymieniane z VU, reprezentujące prędkość i przebytą odległość
Fizycznie odrębne części	fizyczne części składowe czujnika ruchu, które są rozmieszczone w pojeździe, w odróżnieniu od fizycznych części składowych znajdujących się we wnętrzu obudowy czujnika ruchu
Dane związane z zabezpieczeniem	swoiste dane potrzebne do wspierania funkcji realizujących zabezpieczenia (np. klucze kryptograficzne)
System	sprzęt, ludzie lub organizacje uwikłani w jakikolwiek sposób w urządzenie rejestrujące
Użytkownik	człowiek używający czujnika ruchu (gdy nie jest użyty w wyrażeniu »dane użytkownika«)
Dane użytkownika	wszelkie dane inne niż dane dotyczące ruchu i dane związane z zabezpieczeniem, rejestrowane lub gromadzone przez czujnik ruchu.

2.3. Odniesienia

ITSEC ITSEC Informatyka — kryteria oceny zabezpieczeń 1991 r.

3. Podstawy racjonalne produktu

3.1. Opis i metoda użycia czujnika ruchu

Czujnik ruchu przeznaczony jest do instalowania w pojazdach używanych w transporcie drogowym. Jego zadaniem jest dostarczanie VU chronionych danych ruchowych reprezentujących prędkość pojazdu i przebytą odległość.

Czujnik ruchu jest mechanicznie połączony z poruszającą się częścią pojazdu, której ruch może reprezentować prędkość pojazdu i przebytą odległość. Może być umieszczony w skrzyni biegów lub innej części pojazdu.

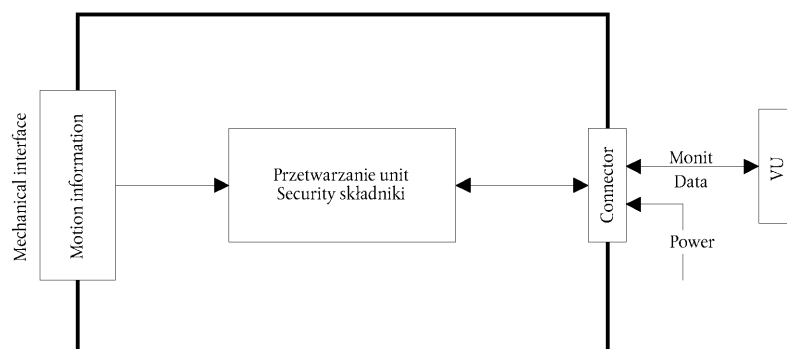
W trybie eksploatacyjnym czujnik ruchu połączony jest z VU.

Czujnik ruchu może być także połączony z innym sprzętem dla potrzeb zarządzania (do zdefiniowania przez producenta).

Typowy czujnik ruchu zobrazowano na poniższym rysunku:

Rysunek 1

Typowy czujnik ruchu

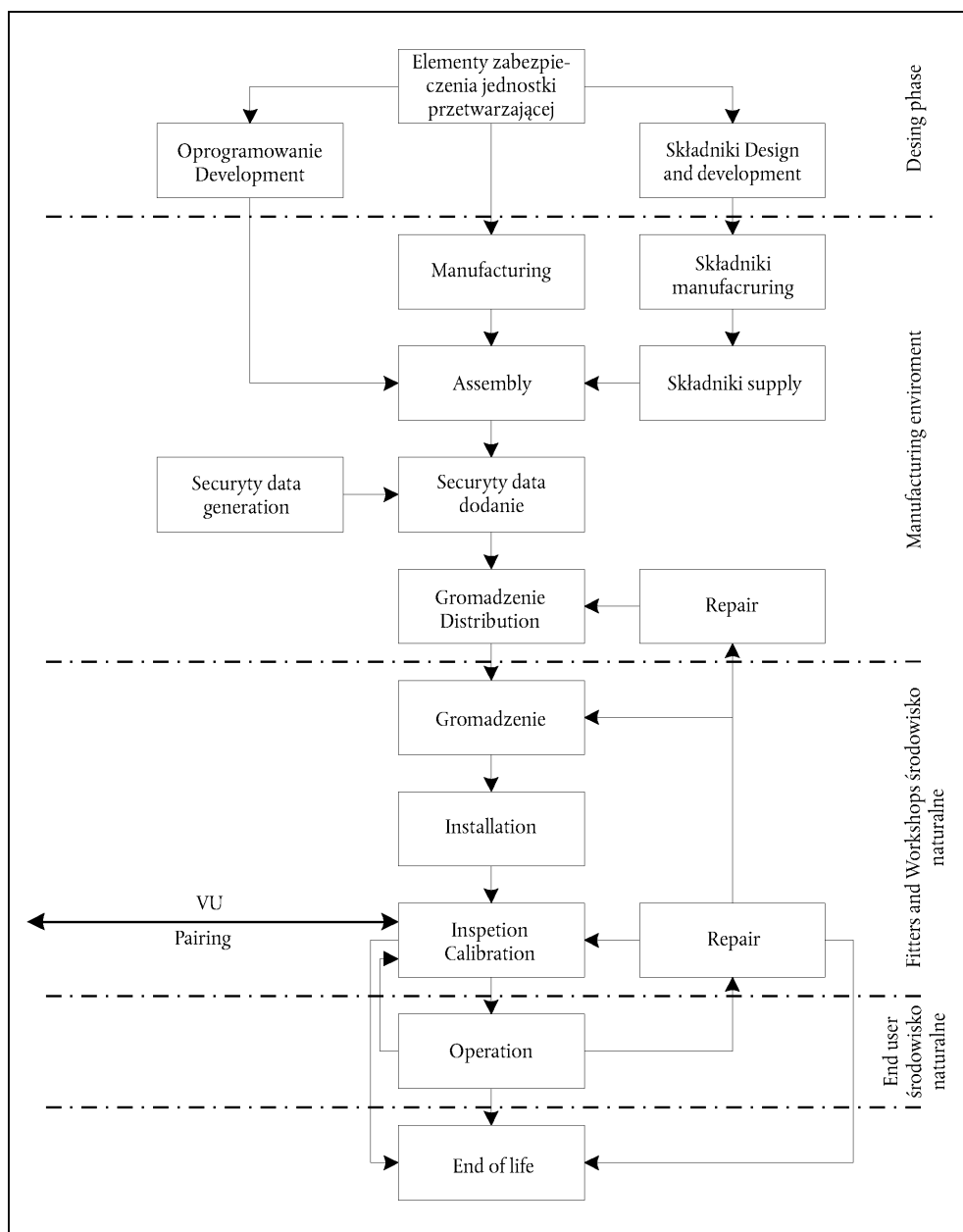


3.2. Cykl istnienia czujnika ruchu

Typowy cykl istnienia czujnika ruchu pokazano na poniższym rysunku:

Rysunek 2

Typowy cykl istnienia czujnika ruchu



3.3. Zagrożenia

W niniejszym punkcie opisano zagrożenia, na jakie czujnik ruchu może być narażony.

3.3.1. Zagrożenia związane z polityką kontroli dostępu

T.Access

Użytkownicy mogą usiłować uzyskać niedozwolony dostęp do funkcji.

3.3.2. Zagrożenia związane z konstrukcją

T.Faults	Usterki sprzętu, oprogramowania, procedur komunikacyjnych mogą spowodować, że czujnik ruchu znajdzie się w stanie naruszającym jego bezpieczeństwo.
T.Tests	Użycie nieunieważnionych trybów testowania lub istniejących tylnych drzwi może naruszyć bezpieczeństwo czujnika ruchu.
T.Design	Użytkownicy mogą próbować pozyskać nielegalną wiedzę dotyczącą konstrukcji albo z materiałów producenta (poprzez kradzież, przekupstwo, ...) lub metodą reverse engineering.

3.3.3. Zagrożenia zorientowane na eksploatację

T.Environment	Użytkownicy mogą naruszyć bezpieczeństwo czujnika ruchu atakami środowiskowymi (termicznymi, elektromagnetycznymi, optycznymi, chemicznymi, mechanicznymi, ...)
T.Hardware	Użytkownicy mogą próbować modyfikować sprzęt czujnika ruchu.
T.Mechanical_Origin	Użytkownicy mogą próbować manipulować przy wejściu czujnika ruchu (np. odkręcając czujnik ruchu od skrzyni biegów, ...)
T.Motion_Data	Użytkownicy mogą próbować zmieniać dane dotyczące ruchu pojazdu (dodanie, modyfikowanie, usuwanie, replikowanie sygnału).
T.Power_Supply	Użytkownicy mogą próbować pokonać cele zabezpieczenia czujnika ruchu modyfikując (odcinając, obniżając, podwyższając) zasilanie czujnika ruchu.
T.Security_Data	Użytkownicy mogą próbować pozyskać nielegalną wiedzę dotyczącą danych bezpieczeństwa w czasie gdy dane bezpieczeństwa są generowane lub transportowane lub gromadzone w sprzęcie.
T.Software	Użytkownicy mogą próbować modyfikować oprogramowanie czujnika ruchu.
T.Stored_Data	Użytkownicy mogą próbować modyfikować zgromadzone dane (dane bezpieczeństwa lub dane dotyczące użytkownika).

3.4. Cele zabezpieczenia

Główny cel zabezpieczenia dla systemu urządzenia rejestrującego jest następujący:

O.Main	Dane przeznaczone do sprawdzenia przez organ kontrolny muszą być dostępne oraz w pełni i dokładnie odzwierciedlać czynności kontrolowanych kierowców i pojazdów, czas prowadzenia pojazdu, pracy, dyspozycyjności odpoczynku oraz prędkość pojazdu.
--------	---

Tym samym celem zabezpieczenia dla czujnika ruchu, przyczyniającym się do ogólnego celu zabezpieczenia, jest:

O.Sensor_Main	Dane transmitowane przez czujnik ruchu muszą być dostępne dla VU, tak aby umożliwić VU pełne i dokładne ustalenie ruchu pojazdu, jego prędkości i przebytej odległości.
---------------	---

3.5. Informatyczne cele zabezpieczenia

Swoiste informatyczne cele zabezpieczenia dla czujnika ruchu, przyczyniające się do jego głównego celu zabezpieczenia, są następujące:

O.Access	Czujnik ruchu musi kontrolować dostęp przyłączonych »jednostek« do funkcji i danych.
O.Audit	Czujnik ruchu musi rejestrować dla potrzeb kontroli próby naruszenia jego bezpieczeństwa i powinien umożliwić powiązanie ich z jednostkami.
O.Authentication	Czujnik ruchu musi uwierzytelniać przyłączone jednostki.

O.Processing	Czujnik ruchu musi zapewniać, że przetwarzanie sygnału wejściowego w celu wyprowadzenia danych ruchowych jest dokładne.
O.Reliability	Czujnik ruchu musi być niezawodny w eksploatacji.
O.Secured_Data_Exchange	Czujnik ruchu musi zapewniać wymianę danych z VU.

3.6. Środki fizyczne, osobowe lub proceduralne

W punkcie tym opisano wymagania fizyczne, osobowe lub proceduralne składające się na bezpieczeństwo czujnika ruchu.

3.6.1. Konstrukcja urządzenia

M.Development	Konstruktorzy czujnika ruchu muszą zapewnić, że przydział obowiązków w czasie projektowania jest zorganizowany w sposób zapewniający zachowanie bezpieczeństwa informatycznego.
M.Manufacturing	Producenci czujnika ruchu muszą zapewnić, że przydział obowiązków w czasie wytwarzania jest zorganizowany w sposób zapewniający zachowanie bezpieczeństwa informatycznego i że w czasie procesu wytwarzania czujnik ruchu jest chroniony przed atakami fizycznymi, które mogłyby naruszyć bezpieczeństwo informatyczne.

3.6.2. Dostawa urządzenia

M.Delivery	Producenci czujnika ruchu, producenci pojazdów i instalatorzy lub warsztaty muszą zapewnić, że manipulowanie czujnikiem ruchu jest zorganizowane w sposób zapewniający zachowanie bezpieczeństwa informatycznego.
------------	---

3.6.3. Generowanie danych bezpieczeństwa i dostawa

M.Sec_Data_Generation	Algorytmy generowania danych bezpieczeństwa muszą być dostępne wyłącznie dla upoważnionych i zaufanych osób.
M.Sec_Data_Transport	Dane bezpieczeństwa muszą być generowane, transportowane i wprowadzane do czujnika ruchu w sposób zapewniający zachowanie odpowiedniej poufności i integralności.

3.6.4. Instalacja, kalibracja i inspekcja urządzenia rejestrującego

M.Approved_Workshops	Instalację, kalibrację i naprawę urządzenia rejestrującego muszą przeprowadzać zaufani i uprawnieni instalatorzy lub warsztaty
M.Mechanical_Interface	Muszą być zapewnione środki (np. plomby) umożliwiające wykrycie fizycznego manipulowania przy interfejsie mechanicznym.
M.Regular_Inspections	Urządzenie rejestrujące musi być okresowo kontrolowane i kalibrowane.

3.6.5. Kontrola wdrażania prawa

M.Controls	Kontrola wdrażania prawa musi być przeprowadzana regularnie i losowo oraz musi obejmować audyty bezpieczeństwa.
------------	---

3.6.6. Aktualizacje oprogramowania

M.Software_Upgrade	Wersje oprogramowania muszą uzyskać świadectwo zabezpieczenia przed zainstalowaniem ich w czujniku ruchu.
--------------------	---

4. Funkcje realizujące zabezpieczenie

4.1. Identyfikacja i uwierzytelnienie

UIA_101 Czujnik ruchu jest w stanie ustalić, dla każdej interakcji, tożsamość przyłączonej do niego jednostki.

UIA_102 Na tożsamość przyłączonej jednostki składają się następujące informacje:

- grupa jednostek:
 - VU,
 - urządzenie zarządzające,
 - inne,
- ID jednostki (tylko VU).

UIA_103 ID jednostki przyłączonego VU oznacza numer homologacji VU i numer fabryczny VU.

UIA_104 Czujnik ruchu jest w stanie dokonać uwierzytelnienia VU lub urządzenia zarządzającego, do którego jest przyłączony:

- w chwili przyłączania jednostki,
- w chwili przywracania zasilania.

UIA_105 Czujnik ruchu jest w stanie okresowo powtarzać uwierzytelnienie VU, do którego jest przyłączony.

UIA_106 Czujnik ruchu wykrywa i uniemożliwia użycie danych wykorzystywanych do uwierzytelnienia, które są skopiowane bądź odtwarzane.

UIA_107 Po wykryciu (ilości ustalonej przez producenta, ale nie więcej niż 20) kolejnych nieudanych prób uwierzytelnienia, funkcja SEF:

- generuje rekord audytu dla zdarzenia,
- ostrzega jednostkę,
- kontynuuje eksport danych ruchowych w trybie bez zabezpieczenia.

4.2. Kontrola dostępu

Kontrola dostępu zapewnia, że informacje są odczytane, stworzone lub zmienione w celu TOE tylko przez tych, którzy są do tego upoważnieni.

4.2.1. Polityka kontroli dostępu

ACC_101 Czujnik ruchu kontroluje prawa dostępu do funkcji i danych.

4.2.2. Prawa dostępu do danych

ACC_102 Czujnik ruchu zapewnia, że dane identyfikacyjne czujnika ruchu mogą być zapisane tylko raz (wymaganie 078).

ACC_103 Czujnik ruchu akceptuje i/lub zachowuje dane dotyczące użytkownika pochodzące tylko z uwierzytelnionych jednostek.

ACC_104 Czujnik ruchu wdraża odpowiednie prawa dostępu do odczytu i zapisu dla danych bezpieczeństwa.

4.2.3. Struktura pliku i warunki dostępu

ACC_105 Aplikacje i struktura pliku danych oraz warunki dostępu są stwarzane podczas procesu produkcji i następnie blokowane w sposób uniemożliwiający ich modyfikację lub usunięcie w późniejszym czasie.

4.3. Identyfikacja czujnika ruchu

ACT_101 Czujnik ruchu przechowuje w pamięci swoje dane identyfikacyjne (wymaganie 077).

ACT_102 Czujnik ruchu przechowuje w pamięci dane instalacyjne (wymaganie 099).

ACT_103 Czujnik ruchu ma możliwość wyprowadzenia danych dotyczących swojej tożsamości uwierzytelnionym jednostkom na ich żądanie.

4.4. **Audyt**

AUD_101 Czujnik ruchu, dla zdarzeń naruszających jego bezpieczeństwo, generuje zdarzenia rekordów audytu.

AUD_102 Następujące zdarzenia godzą w bezpieczeństwo czujnika ruchu:

- próba naruszenia zabezpieczeń,
- błąd uwierzytelnienia,
- błąd integralności przechowywanych danych,
- błąd wewnętrznego przesyłania danych,
- nieupoważnione otwarcie obudowy,
- uszkodzenie sprzętu.
- usterka czujnika.

AUD_103 Rekordy audytu zawierają następujące dane:

- data i godzina zdarzenia,
- typ zdarzenia,
- tożsamość przyłączonej jednostki.

w przypadku gdy wymagane dane nie są dostępne, wprowadzane są odpowiednie dane domyślne (określa producent).

AUD_104 Czujnik ruchu wysyła wygenerowane rekordy audytu do VU, może też przechowywać je w pamięci.

AUD_105 W przypadku gdy czujnik ruchu przechowuje rekordy audytu, zapewnia by 20 rekordów audytu było utrzymywane niezależnie od wyczerpania możliwości gromadzenia audytu oraz ma możliwość wyprowadzania przechowywanych rekordów audytu uwierzytelnionym jednostkom na ich żądanie.

4.5. **Dokładność**

4.5.1. *Polityka kontroli przepływu informacji*

ACR_101 Czujnik ruchu zapewnia by dane ruchowe mogły być przetwarzane i pobierane wyłącznie z mechanicznego wejścia czujnika.

4.5.2. *Wewnętrzne przesyłanie danych*

Wymagania tego punktu stosuje się tylko wtedy, gdy czujnik ruchu składa się z fizycznie oddzielonych części.

ACR_102 Jeżeli dane przesyła się między fizycznie oddzielnymi częściami czujnika ruchu, dane te są zabezpieczone przed modyfikacją.

ACR_103 W przypadku wykrycia błędu przesyłania danych podczas wewnętrznego przesyłania danych, transmisja jest powtarzana a funkcja SEF generuje rekord audytu.

4.5.3. *Integralność przechowywanych danych*

ACR_104 Czujnik ruchu sprawdza dane użytkownika przechowywane w jego pamięci pod względem błędów integralności.

ACR_105 W przypadku wykrycia błędu integralności przechowywanych danych użytkownika, funkcja SEF generuje rekord audytu.

4.6. **Wiarygodność usługi**

4.6.1. *Testy*

RLB_101 Wszystkie polecenia, czynności lub punkty testowe przeznaczone dla potrzeb testowania w fazie produkcyjnej są blokowane lub usuwane przed zakończeniem fazy produkcyjnej. Przywrócenie ich do wykorzystania w późniejszym czasie jest niemożliwe.

RLB_102 Czujnik ruchu uruchamia auto testy, w czasie początkowego uruchomienia i w czasie normalnej pracy, w celu zweryfikowania prawidłowego funkcjonowania. Auto testy czujnika ruchu obejmują weryfikację integralności danych bezpieczeństwa przechowywanych w kodzie wynikowym, (jeżeli nie w pamięci ROM).

RLB_103 W przypadku wykrycia wewnętrznej usterki w czasie auto testu funkcja SEF generuje rekord audytu (usterka czujnika).

4.6.2. Oprogramowanie

RLB_104 Analizowanie lub testowanie oprogramowania czujnika ruchu nie jest możliwe w warunkach polowych.

RLB_105 Wejścia z zewnętrznych źródeł nie przyjmują kodu wykonywalnego.

4.6.3. Ochrona fizyczna

RLB_106 Jeżeli konstrukcja czujnika ruchu umożliwia otwarcie obudowy, czujnik ruchu wykrywa każde otwarcie obudowy nawet bez zewnętrznego zasilania przez okres przynajmniej 6 miesięcy. W takim przypadku funkcja SEF generuje zdarzenie rekordu audytu (dopuszcza się, że rekord audytu jest generowany i zapamiętywany po ponownym przyłączeniu zasilania).

Jeżeli konstrukcja czujnika ruchu nie pozwala na otwieranie go, jest tak skonstruowany, aby umożliwić łatwe wykrycie wszelkich prób manipulowania przy nim (np. przez kontrolę wizualną).

RLB_107 Czujnik ruchu wykrywa określone (przez producenta) uszkodzenia sprzętu.

RLB_108 W opisanym powyżej przypadku funkcja SEF generuje rekord audytu a czujnik ruchu: (określa producent).

4.6.4. Przerwy zasilania

RLB_109 Czujnik ruchu utrzymuje bezpieczny stan w czasie odcięcia lub zmian zasilania.

4.6.5. Warunki zerujące

RLB_110 W przypadku przerwy zasilania lub gdy transakcja jest zatrzymana przez zakończeniem lub w przypadku zaistnienia innych warunków zerujących (reset), czujnik ruchu daje się łatwo zerować.

4.6.6. Dostępność danych

RLB_111 Czujnik ruchu zapewnia uzyskanie dostępu do zasobów, gdy jest to potrzebne, zapewnia także to, że zasoby nie są niepotrzebnie żądane ani zachowywane.

4.6.7. Obsługa wielu aplikacji

RLB_112 Jeżeli czujnik ruchu obsługuje aplikacje inne niż aplikacja tachograficzna, wszystkie aplikacje są rozdzielone każda od pozostałych fizycznie i/lub logicznie. Aplikacje te nie współdzielą danych bezpieczeństwa. Jednocześnie jest aktywne tylko jedno zadanie.

4.7. Wymiana danych

DEX_101 Czujnik ruchu eksportuje dane ruchowe do VU razem ze związanymi atrybutami bezpieczeństwa, tak by VU był w stanie zweryfikować integralność i autentyczność tych danych.

4.8. Wsparcie kryptograficzne

Wymagania tego punktu stosuje się tylko tam gdzie potrzeba, w zależności od zastosowanych mechanizmów bezpieczeństwa i rozwiązań producenta.

CSP_101 Wszelkie operacje kryptograficzne wykonywane przez czujnik ruchu są zgodne z ustalonym algorytmem i używają klucza o ustalonej długości.

CSP_102 Jeżeli czujnik ruchu generuje klucze kryptograficzne, to robi to zgodnie z ustalonymi algorytmami generowania kluczy kryptograficznych, a klucze kryptograficzne mają ustaloną długość.

CSP_103 Jeżeli czujnik ruchu rozprowadza klucze kryptograficzne, to robi to zgodnie z ustalonymi metodami rozprowadzania kluczy kryptograficznych.

CSP_104 Jeżeli czujnik ruchu ma dostęp do kluczy kryptograficznych, jest to zgodne z ustalonymi metodami dostępu do kluczy kryptograficznych.

CSP_105 Jeżeli czujnik ruchu niszczy klucze kryptograficzne, to robi to zgodnie z ustalonymi metodami niszczenia kluczy kryptograficznych.

5. Definicja mechanizmów zabezpieczenia

Mechanizmy zabezpieczenia wypełniające funkcje realizujące zabezpieczenia czujnika ruchu definiują producenci czujnika ruchu.

6. Minimalna siła mechanizmów zabezpieczenia

Minimalna siła mechanizmów zabezpieczenia czujnika ruchu jest »wysoka« według definicji ITSEC.

7. Poziom gwarancji zabezpieczenia

Docelowym poziomem gwarancji zabezpieczenia dla czujnika ruchu jest poziom E3 według definicji ITSEC.

8. Podstawy racjonalne

W tabeli poniżej zamieszczono podstawy racjonalne dla funkcji SEF pokazując przy tym:

- które funkcje SEF lub środki są skierowane przeciw którym zagrożeniom,
- które funkcje SEF realizują które informatyczne cele zabezpieczenia.

	Zagrożenia												Cele informatyczne					
	Dostęp	Usterki	Testy	Konstrukcja	Środowisko	Sprzęt	Pochodzenie mechaniczne	Dane ruchowe	Zasilanie	Dane bezpieczeństwa	Oprogramowanie	Przechowywane dane	Dostęp	Audyt	Uwierzytelnienie	Przetwarzanie	Wiarygodność	Bezpieczna wymiana danych
Środki fizyczne, osobowe i proceduralne																		
Projektowanie		x	x	x														
Wytwarzanie			x	x														
Dostawa						x					x	x						
Generowanie danych bezpieczeństwa										x								
Transport danych bezpieczeństwa										x								
Zatwierdzone warsztaty							x											
Interfejs mechaniczny							x											
Regularne przeglądy						x	x		x		x							
Kontrole wdrażania prawa					x	x	x		x	x	x							
Aktualizacje oprogramowania											x							
Funkcje realizujące zabezpieczenie																		
Identyfikacja i uwierzytelnienie																		
UIA_101 Identyfikacja jednostek	x							x					x		x			x
UIA_102 Tożsamość jednostek	x												x		x			
UIA_103 Tożsamość VU														x				
UIA_104 Uwierzytelnienie jednostek	x							x					x		x			x
UIA_105 Uwierzytelnienie powtórne	x							x					x		x			x
UIA_106 Uwierzytelnienie niewymazywalne	x							x					x		x			
UIA_107 Błąd uwierzytelnienia								x						x			x	
Kontrola dostępu																		
ACC_101 Polityka kontroli dostępu	x									x		x	x					
ACC_102 ID czujnika ruchu												x	x					

[illegible]

OGÓLNY CEL ZABEZPIECZENIA PRZYRZĄDU REJESTRUJĄCEGO

1. Wprowadzenie

Niniejszy dokument zawiera opis przyrządu rejestrującego, zagrożeń, którym przyrząd rejestrujący musi być w stanie przeciwdziałać i celów zabezpieczenia, które musi osiągnąć. Niniejszy dokument określa wymagane funkcje realizujące zabezpieczenia. Podaje wymaganą, minimalną siłę mechanizmów ochrony i wymagany poziom zapewnienia rozwoju i oceny.

Wymaganiami, określonych w tym dokumencie, są te znajdujące się w treści załącznika I B. W celu zwiększenia czytelności czasami pojawia się powielanie wymagań znajdujących się w treści załącznika I B i wymagań celu zabezpieczenia. W przypadku niezgodności między wymaganiami celu zabezpieczenia a wymaganiami znajdującymi się w treści załącznika I B, do których odwołuje się wymaganie celu zabezpieczenia, obowiązuje wymaganie podane w treści załącznika I B.

Wymagania znajdujące się w treści załącznika I B, do których nie odwołują się cele zabezpieczenia, nie są przedmiotem funkcji realizujących zabezpieczenia.

Zagrożeniom, celom, środkom proceduralnym i specyfikacjom funkcji realizujących zabezpieczenia nadano unikalne etykiety w celu umożliwienia odtworzenia historii produktu w dokumentach rozwoju i oceny.

2. Skróty, definicje i odniesienia**2.1. Skróty**

PIN	osobisty numer identyfikacyjny
ROM	pamięć stała
SEF	funkcja realizująca zabezpieczenia
TBD	określa
TOE	cel oceny
VU	przyrząd rejestrujący.

2.2. Definicje

Cyfrowy tachograf	urządzenie rejestrujące
Dane ruchowe	dane wymieniane z czujnikiem ruchu, reprezentujące prędkość i przebytą odległość
Części oddzielone fizycznie	fizyczne części składowe VU, które są rozmieszczone w pojeździe, w odróżnieniu od fizycznych części składowych znajdujących się we wnętrzu obudowy VU
Dane bezpieczeństwa	swoiste dane potrzebne do wspierania funkcji realizujących zabezpieczenia (np. klucze kryptograficzne)
System	sprzęt, ludzie lub organizacje związani w jakikolwiek sposób z urządzeniem rejestrującym
Użytkownik	pod pojęciem użytkownika rozumie się człowieka używającego sprzętu. Do normalnych użytkowników VU zalicza się kierowców, kontrolerów, warsztaty i firmy
Dane użytkownika	wszelkie dane inne niż dane związane z zabezpieczeniem, rejestrowane lub gromadzone przez VU, zgodne z wymaganiami ustanowionymi w pkt 12 w rozdziale III.

2.3. Odniesienia

ITSEC ITSEC Informatyka — kryteria oceny zabezpieczeń 1991 r.

3. Podstawy racjonalne produktu**3.1. Opis i metoda użycia przyrządu rejestrującego**

VU przeznaczony jest do instalowania w pojazdach używanych w transporcie drogowym. Jego zadaniem jest rejestrowanie, przechowywanie, prezentowanie, drukowanie i wyprowadzanie danych dotyczących czynności kierowcy.

VU jest połączony z czujnikiem ruchu, z którym wymienia dane ruchowe dotyczące pojazdu.

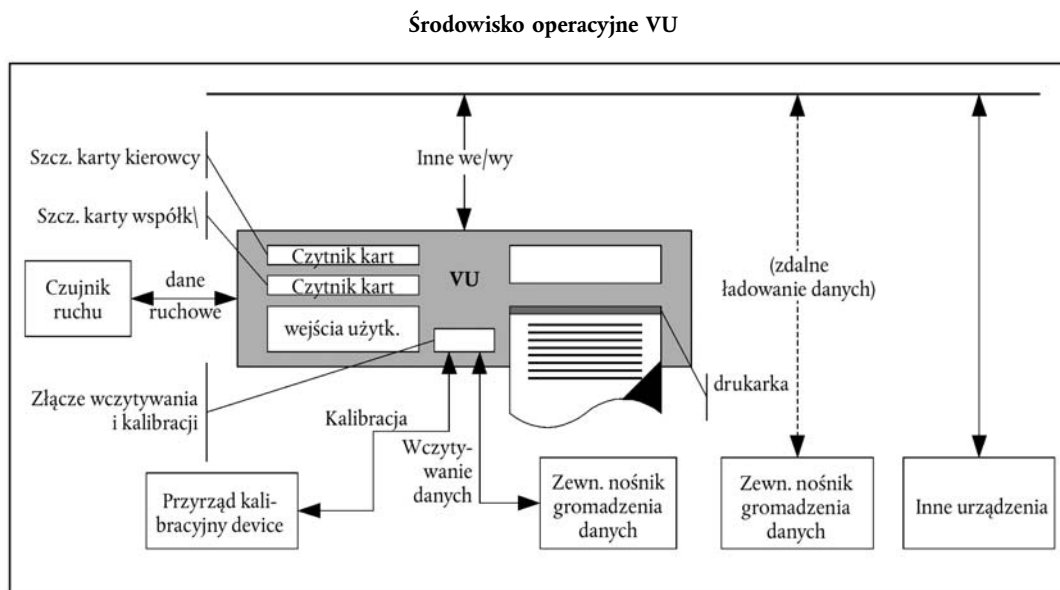
Użytkownicy identyfikują się w VU przy pomocy kart do tachografów.

VU rejestruje i przechowuje w swojej pamięci dane dotyczące czynności użytkownika a także rejestruje czynności użytkownika na kartach do tachografów.

Dane z VU mogą być prezentowane na wyświetlaczu, drukowane na drukarce i przesyłane do urządzeń zewnętrznych.

Środowisko operacyjne przyrządu rejestrującego zainstalowanego w pojeździe zobrazowano na poniższym rysunku:

Rysunek 1

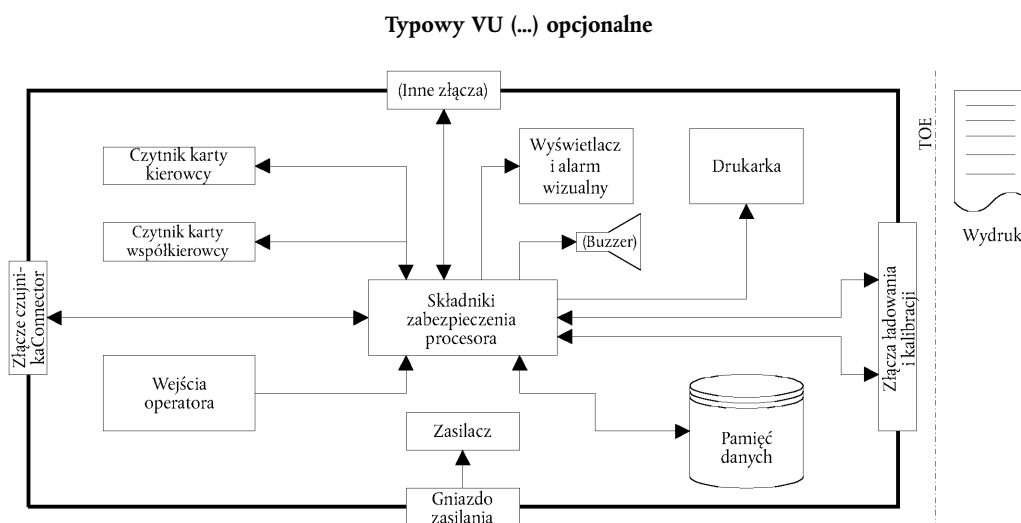


Charakterystyki ogólne VU, funkcje i tryb pracy opisano w rozdziale II załącznika I B.

Wymagania funkcjonalne dla VU określono w rozdziale III załącznika I B.

Typowy VU zobrazowano na poniższym rysunku:

Rysunek 2



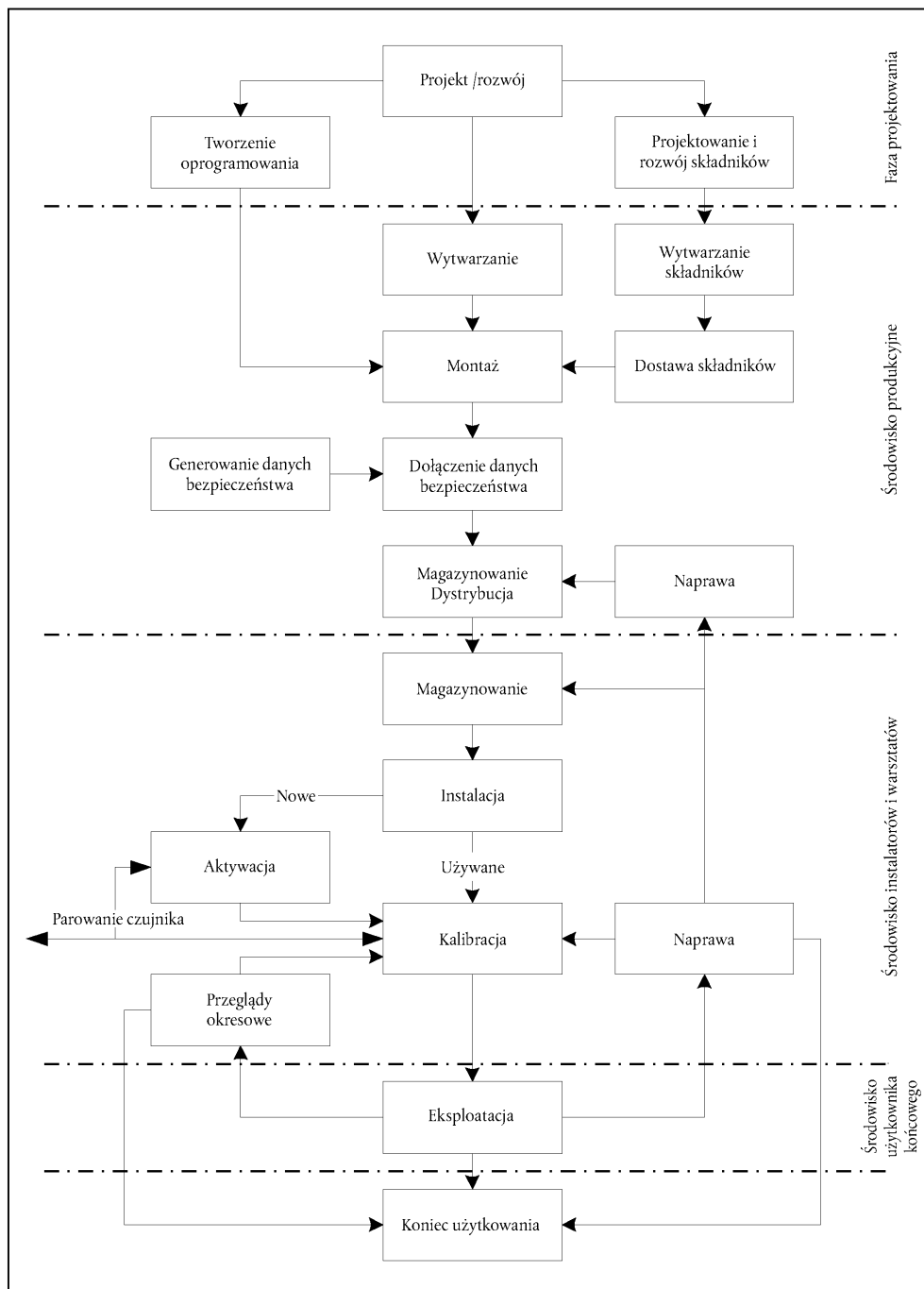
Mimo iż mechanizm drukarki jest częścią TOE, to wydrukowany dokument papierowy już nią nie jest.

3.2. Cykl istnienia przyrządu rejestrującego

Typowy cykl istnienia VU pokazano na poniższym rysunku:

Rysunek 3

Typowy cykl istnienia VU



3.3. Zagrożenia

W niniejszym punkcie opisano zagrożenia, na jakie VU może być narażony.

3.3.1. Zagrożenia dla polityki identyfikacji i kontroli dostępu

T.Access

Użytkownicy mogą usiłować uzyskać niedozwolony dostęp do funkcji (np. kierowcy mogą usiłować uzyskać dostęp do funkcji kalibracji).

T.Identification

Użytkownicy mogą próbować używać kilku identyfikacji lub wykonywać działania bez identyfikacji.

3.3.2. Zagrożenia związane z konstrukcją

T.Faults	Usterki sprzętu, oprogramowania, procedur komunikacyjnych mogą spowodować, że VU znajdzie się w stanie naruszającym jego bezpieczeństwo.
T.Tests	Użycie nieunieważnionych trybów testowania lub istniejących tylnych drzwi może naruszyć bezpieczeństwo VU.
T.Design	Użytkownicy mogą próbować pozyskać nielegalną wiedzę dotyczącą konstrukcji albo z materiałów producenta (poprzez kradzież, przekupstwo,...) albo metodą reverse engineering.

3.3.3. Zagrożenia zorientowane na eksploatację

T.Calibration_Parameters	Użytkownicy mogą próbować używać nieprawidłowo wykalibrowanego urządzenia (zmieniając dane dotyczące kalibracji lub wykorzystując słabości organizacyjne).
T.Card_Data_Exchange	Użytkownicy mogą próbować modyfikować dane podczas wymiany danych między VU a kartami do tachografów (dodanie, modyfikowanie, usuwanie, replikowanie sygnału).
T.Clock	Użytkownicy mogą próbować modyfikować wewnętrzny zegar.
T.Environment	Użytkownicy mogą naruszyć bezpieczeństwo VU ruchy atakami środowiskowymi (termicznymi, elektromagnetycznymi, optycznymi, chemicznymi, mechanicznymi,...)
T.Fake_Devices	Użytkownicy mogą próbować przyłączyć fałszywe urządzenia (czujnik ruchu, karty inteligentne) do VU.
T.Hardware	Użytkownicy mogą próbować modyfikować sprzęt VU.
T.Motion_Data	Użytkownicy mogą próbować zmieniać dane dotyczące ruchu pojazdu (dodanie, modyfikowanie, usuwanie, replikowanie sygnału)
T.Non_Activated	Użytkownicy mogą usiłować używać urządzeń nieaktywowanych.
T.Output_Data	Użytkownicy mogą próbować modyfikować dane wyjściowe (wydruk, wyświetlacz lub wczytywanie).
T.Power_Supply	Użytkownicy mogą próbować pokonać cele zabezpieczenia czujnika ruchu modyfikując (odcinając, obniżając, podwyższając) zasilanie VU.
T.Security_Data	Użytkownicy mogą próbować pozyskać nielegalną wiedzę dotyczącą danych bezpieczeństwa w czasie, gdy dane bezpieczeństwa są generowane lub transportowane bądź gromadzone w sprzęcie.
T.Software	Użytkownicy mogą próbować modyfikować oprogramowanie VU.
T.Stored_Data	Użytkownicy mogą próbować modyfikować zgromadzone dane (dane bezpieczeństwa lub dane dotyczące użytkownika).

3.4. Cele zabezpieczenia

Główny cel zabezpieczenia systemu urządzenia rejestrującego jest następujący:

O.Main	Dane przeznaczone do sprawdzenia przez organ kontrolny muszą być dostępne oraz w pełni i dokładnie odzwierciedlać czynności kontrolowanych kierowców i pojazdów, czas prowadzenia pojazdu, pracy, dyspozycyjności i odpoczynku oraz prędkość pojazdu.
--------	---

Tym samym celem zabezpieczenia VU, przyczyniającym się do ogólnego celu zabezpieczenia jest:

O.VU_Main	Dane, które mają być mierzone i rejestrowane oraz następnie kontrolowane przez organy kontrolne muszą być dostępne oraz w pełni i dokładnie odzwierciedlać czynności kontrolowanych kierowców i pojazdów, czas prowadzenia pojazdu, pracy, dyspozycyjności odpoczynku i prędkość pojazdu.
O.VU_Export	VU musi być w stanie eksportować dane do zewnętrznych nośników gromadzenia danych w taki sposób, by umożliwić weryfikację ich integralności i autentyczności.

3.5. Informatyczne cele zabezpieczenia

Swoiste informatyczne cele zabezpieczenia VU, przyczyniające się do jego głównego celu zabezpieczenia, są następujące:

O.Access	VU musi kontrolować dostęp użytkownika do funkcji i danych
O.Accountability	VU musi zbierać dokładne, wiarygodne dane.
O.Audit	VU musi rejestrować dla potrzeb kontroli próby naruszenia jego bezpieczeństwa i powinien umożliwić powiązanie ich z użytkownikami.
O.Authentication	VU musi uwierzytelniać użytkowników i przyłączone jednostki, (gdy między jednostkami trzeba utworzyć bezpieczną ścieżkę).
O.Integrity	VU musi utrzymywać integralność przechowywanych danych.
O.Output	VU musi zapewniać, że dane wyjściowe dokładnie odzwierciedlają dane pomierzone lub zgromadzone.
O.Processing	VU musi zapewniać dokładne przetwarzanie sygnałów wejściowych w celu uzyskania danych dotyczących użytkownika.
O.Reliability	VU musi być niezawodny w eksploatacji.
O.Secured_Data_Exchange	VU musi zapewniać wymianę danych z czujnikiem ruchu i kartami do tachografów.

3.6. Środki fizyczne, osobowe lub proceduralne

W punkcie tym opisano wymagania fizyczne, osobowe lub proceduralne składające się na bezpieczeństwo VU.

3.6.1. Konstrukcja urządzenia

M.Development	Konstruktorzy VU muszą zapewnić, że przydział obowiązków w czasie projektowania jest zorganizowany w sposób zapewniający zachowanie bezpieczeństwa informatycznego.
M.Manufacturing	Producenci VU muszą zapewnić, że przydział obowiązków w czasie wytwarzania jest zorganizowany w sposób zapewniający zachowanie bezpieczeństwa informatycznego i że w czasie procesu wytwarzania VU jest chroniony przed atakami fizycznymi, które mogłyby naruszyć bezpieczeństwo informatyczne.

3.6.2. Dostawa i aktywacja urządzenia

M.Delivery	Producenci VU, producenci pojazdów i instalatorzy lub warsztaty muszą zapewnić, że manipulowanie przy nieaktywowanych urządzeniach rejestracyjnych odbywa się w sposób zapewniający zachowanie bezpieczeństwa informatycznego.
M.Activation	Producenci pojazdów, instalatorzy lub warsztaty muszą aktywować VU po instalacji zanim pojazd opuści obiekt, w którym wykonuje się instalację.

3.6.3. Generowanie danych bezpieczeństwa i dostawa

M.Sec_Data_Generation	Algorytmy generowania danych bezpieczeństwa muszą być dostępne wyłącznie dla upoważnionych i zaufanych osób.
M.Sec_Data_Transport	Dane bezpieczeństwa muszą być generowane, transportowane i wprowadzone do VU w sposób zapewniający zachowanie odpowiedniej poufności i integralności.

3.6.4. Dostawa kart

M.Card_Availability	Karty do tachografów muszą być dostępne i dostarczane wyłącznie upoważnionemu personelowi.
M.Driver_Card_Uniqueness	Kierowcy mogą mieć jednocześnie tylko jedną ważną kartę kierowcy.
M.Card_Traceability	Dostawa kart musi umożliwiać odtworzenie historii produktu (białe listy, czarne listy), a w przy wykonywaniu audytów bezpieczeństwa należy korzystać z czarnych list.

3.6.5. Instalacja, kalibracja i inspekcja urządzenia rejestrującego

M.Approved_Workshops	Instalację, kalibrację i naprawę urządzenia rejestrującego muszą przeprowadzać zaufani i uprawnieni instalatorzy lub warsztaty.
M.Regular_Inpections	Urządzenie rejestrujące musi być okresowo kontrolowane i kalibrowane.
M.Faithful_Calibration	W czasie kalibracji uprawnieni instalatorzy i warsztaty muszą wprowadzać do urządzenia rejestrującego prawidłowe parametry.

3.6.6. Eksploatacja urządzenia

M.Faithful_Drivers	Kierowcy muszą postępować zgodnie z zasadami i odpowiedzialnie (np. używając swoich kart kierowcy prawidłowo wybierać czynności, które wprowadzają ręcznie,...).
--------------------	--

3.6.7. Kontrola wdrażania prawa

M.Controls	Kontrola wdrażania prawa musi być przeprowadzana regularnie i losowo oraz musi obejmować audyty bezpieczeństwa.
------------	---

3.6.8. Aktualizacje oprogramowania

M.Software_Upgrade	Przed zainstalowaniem ich w VU wersje oprogramowania muszą uzyskać świadectwo zabezpieczenia.
--------------------	---

4. Funkcje realizujące zabezpieczenie

4.1. Identyfikacja i uwierzytelnienie

4.1.1. Identyfikacja i uwierzytelnienie czujnika ruchu

UIA_201 VU jest w stanie ustalić, dla każdej interakcji, tożsamość czujnika ruchu, do którego jest przyłączony.

UIA_202 Na tożsamość czujnika ruchu składają się numer homologacji czujnika i numer fabryczny czujnika.

UIA_203 VU uwierzytelnia czujnik ruchu, do którego jest przyłączony:

- przy przyłączaniu czujnika ruchu,
- przy każdej kalibracji urządzenia rejestrującego,
- przy przywróceniu zasilania.

Uwierzytelnianie jest wzajemne i uaktywniane przez VU.

UIA_204 VU okresowo (okres ustali producent, ale częściej niż raz na godzinę) powtarza identyfikację i uwierzytelnienie czujnika ruchu, do którego jest przyłączony i sprawdza czy czujnik ruchu zidentyfikowany podczas ostatniej kalibracji urządzenia rejestrującego nie jest zmieniony.

UIA_205 VU wykrywa i uniemożliwia wykorzystanie danych uwierzytelniających, które są kopiowane i odtwarzane.

UIA_206 Po wykryciu (ilość ustali producent, ale nie więcej niż 20) kolejnych nieudanych prób uwierzytelnienia i/lub po wykryciu nieautoryzowanej zmiany tożsamości czujnika ruchu (tj. dokonanej w innym czasie niż podczas kalibracji urządzenia rejestrującego), funkcja SEF:

- generuje rekord audytu dla zdarzenia,
- ostrzega użytkownika,
- nadal akceptuje i używa w trybie bez zabezpieczenia danych ruchowych wysłanych przez czujnik ruchu.

4.1.2. Identyfikacja i uwierzytelnienie użytkownika

UIA_207 VU ustawicznie i wybiórczo śledzi historię tożsamości dwóch użytkowników poprzez monitorowanie kart do tachografów włożonych odpowiednio do szczeliny karty kierowcy i szczeliny karty współkierowcy urządzenia.

UIA_208 Na tożsamość użytkownika składają się następujące dane:

- grupa użytkowników:
 - KIEROWCA (karta kierowcy),
 - KONTROLER (karta kontrolna),
 - WARSZTAT (karta warsztatowa),
 - FIRMA (karta firmowa),
 - NIEOKREŚLONA (brak karty),
- ID użytkownika składające się z następujących danych:
 - kod Państwa Członkowskiego wydającego i numer karty,
 - NIEOKREŚLONE, jeżeli grupa użytkownika jest NIEOKREŚLONA.

Tożsamości NIEOKREŚLONE mogą być znane jawnie lub niejawnie.

UIA_209 VU przeprowadza uwierzytelnienie swoich użytkowników przy wkładaniu karty.

UIA_210 VU powtarza uwierzytelnienie swoich użytkowników:

- przy przywróceniu zasilania,
- okresowo lub po zajściu szczególnych zdarzeń (ustalają producenci, ale częściej niż raz dziennie).

UIA_211 Uwierzytelnienie polega na sprawdzeniu czy włożona karta jest ważną kartą do tachografów z danymi bezpieczeństwa, które może rozpowszechniać tylko system. Uwierzytelnienie jest wzajemne a stroną inicjującą jest VU.

UIA_212 W dodatku do powyższego od warsztatów wymaga się dalszego uwierzytelnienia przez wprowadzenie numeru PIN. Numery PIN mają przynajmniej 4 znaki.

Uwaga: W przypadku przesyłania numeru PIN do VU z zewnętrznego urządzenia znajdującego się w pobliżu VU, przy przesyłaniu nie wolno naruszyć poufności numeru PIN.

UIA_213 VU wykrywa i uniemożliwia użycie danych wykorzystywanych do uwierzytelnienia, które są kopiowane bądź odtwarzane

UIA_214 Po wykryciu 5 kolejnych nieudanych prób uwierzytelnienia, funkcja SEF:

- generuje rekord audytu dla zdarzenia,
- ostrzega użytkownika,
- przyjmuje że użytkownik jest NIEOKREŚLONY, a karta nie jest ważna (definicja z) i wymaganie 007).

4.1.3. Identyfikacja i uwierzytelnienie zdalnie przyłączonej firmy

Możliwość zdalnego przyłączenia firmy jest opcjonalna. Tym samym przepisy niniejszego punktu stosuje się tylko wtedy, gdy w urządzenie ma tę funkcję.

- UIA_215 Dla każdej interakcji ze zdalnie przyłączoną firmą VU jest w stanie ustalić tożsamość firmy.
- UIA_216 Na tożsamość zdalnie przyłączonej firmy składają się kod Państwa Członkowskiego, które wydało kartę firmową i numer karty firmowej.
- UIA_217 VU pomyślnie uwierzytelnia zdalnie przyłączoną firmę zanim dopuści eksport jakichkolwiek danych do tej firmy.
- UIA_218 Uwierzytelnienie polega na sprawdzeniu czy włożona karta jest ważną kartą firmową z danymi bezpieczeństwa, które może rozpowszechniać tylko system.
- UIA_219 VU wykrywa i uniemożliwia użycie danych wykorzystywanych do uwierzytelnienia, które są kopiowane bądź odtwarzane.
- UIA_220 Po wykryciu 5 kolejnych nieudanych prób uwierzytelnienia, funkcja SEF:
- ostrzega zdalnie przyłączoną firmę.

4.1.4. Identyfikacja i uwierzytelnienie urządzenia zarządzającego

Producenci VU mogą umożliwić stosowanie specjalnych, przeznaczonych do tego celu urządzeń wykonujących dodatkowe funkcje zarządzające VU (np. aktualizowanie oprogramowania, powtórne ładowanie danych bezpieczeństwa,...). Tym samym niniejszy punkt stosuje się tylko wtedy, gdy takie funkcje są wdrożone.

- UIA_221 Dla każdej interakcji z urządzeniem zarządzającym VU jest w stanie ustalić tożsamość tego urządzenia.
- UIA_222 Przed dopuszczeniem do jakichkolwiek dalszych interakcji VU pomyślnie uwierzytelnia urządzenie zarządzające.
- UIA_223 VU wykrywa i uniemożliwia użycie danych wykorzystywanych do uwierzytelnienia, które są kopiowane bądź odtwarzane.

4.2. Kontrola dostępu

Kontrole dostępu zapewniają, że tylko upoważnieni mogą odczytywać, tworzyć lub modyfikować informacje w TOE.

Należy zwrócić uwagę, że dane użytkownika zarejestrowane przez VU, chociaż wiążą się z wrażliwymi aspektami prywatności i handlowymi, nie mają charakteru poufnego. Dlatego wymaganie funkcjonalne dotyczące prawa dostępu do odczytu tych danych (wymaganie 011) nie jest objęte funkcją realizującą zabezpieczenie.

4.2.1. Polityka kontroli dostępu

- ACC_201 VU zarządza i sprawdza prawa dostępu do funkcji i danych.

4.2.2. Prawa dostępu do funkcji

- ACC_202 VU stosuje zasady wyboru trybu pracy (wymagania 006 do 009).
- ACC_203 VU wykorzystuje tryb pracy do wdrażania zasad kontroli dostępu do funkcji (wymaganie 010).

4.2.3. Prawa dostępu do danych

- ACC_204 VU stosuje zasady dostępu do zapisu danych identyfikacyjnych VU (wymaganie 076).
- ACC_205 VU stosuje zasady dostępu do zapisu danych identyfikacyjnych sparowanego czujnika ruchu (wymagania 079 i 155).
- ACC_206 Po aktywacji VU, VU zapewnia, że dane dotyczące kalibracji mogą być wprowadzane do VU i przechowywane w jego pamięci danych tylko w trybie kalibracyjnym (wymagania 154 i 156).
- ACC_207 Po aktywacji VU, VU stosuje zasady dostępu do zapisu i usuwania danych kalibracyjnych (wymaganie 097).

ACC_208 Po aktywacji VU, VU zapewnia, że dane dotyczące regulacji czasu mogą być wprowadzane do VU i przechowywane w jego pamięci danych tylko w trybie kalibracyjnym (wymagania tego nie stosuje się przy małych regulacjach czasu dozwolonych w wymaganiach 157 i 158).

ACC_209 Po aktywacji VU, VU stosuje zasady dostępu do zapisu i usuwania danych dotyczących regulacji czasu (wymaganie 100).

ACC_210 VU stosuje odpowiednie prawa dostępu do odczytu i zapisu danych bezpieczeństwa (wymaganie 080).

4.2.4. Struktura pliku i warunki dostępu

ACC_211 Aplikacje i struktura plików danych i warunki dostępu są tworzone w czasie procesu wytwarzania i następnie blokowane w sposób uniemożliwiający jakiegokolwiek późniejsze modyfikacje lub usunięcie.

4.3. Wiarygodność

ACT_201 VU umożliwia rozliczenie kierowców z wykonywanych przez nich czynności (wymagania 081, 084, 087, 105a, 105b, 109 i 109a).

ACT_202 VU przechowuje trwale dane identyfikacyjne (wymaganie 075).

ACT_203 VU umożliwia rozliczenie warsztatów z wykonywanych przez nich czynności (wymagania 098, 101 i 109).

ACT_204 VU umożliwia rozliczenie kontrolerów z wykonywanych przez nich czynności (wymagania 102, 103 i 109).

ACT_205 VU rejestruje dane dotyczące licznika kilometrów (wymaganie 090) i szczegółowe dane dotyczące prędkości (wymaganie 093).

ACT_206 VU zapewnia, że po zarejestrowaniu danych użytkownika dotyczących wymagań 081 do 093 i 102 do 105b nie można zmienić, wyjąwszy sytuację gdy najstarsze ze zgromadzonych danych zastępuje się nowymi danymi.

ACT_207 VU zapewnia, że danych zapisanych już na karcie do tachografów nie można zmienić (wymagania 109 i 109a) z wyjątkiem zastąpienia najstarszych danych nowymi danymi (wymaganie 110) lub przypadku opisanego w dodatku 1 w uwadze przy pkt 2.1.

4.4. Audyt

Audytem obowiązkowo obejmują tylko te zdarzenia, które mogą wskazywać na manipulowanie lub próby naruszenia zabezpieczenia. Audyt nie jest wymagany dla normalnego wykonywania praw, nawet gdy wiąże się to z bezpieczeństwem.

AUD_201 VU, dla zdarzeń naruszających jego bezpieczeństwo, rejestruje te zdarzenia wraz ze związanymi danymi (wymagania 094, 096 i 109).

AUD_202 Następujące zdarzenia godzą w bezpieczeństwo VU:

- próba naruszenia zabezpieczeń,
- błąd uwierzytelnienia czujnika ruchu,
- błąd uwierzytelnienia karty do tachografów,
- nieupoważniona zmiana w czujniku ruchu,
- błąd integralności wprowadzania danych na kartę,
- błąd integralności przechowywanych danych użytkownika,
- błąd wewnętrznego przesyłania danych,
- nieupoważnione otwarcie obudowy,
- uszkodzenia sprzętu,

- sesja ostatniej karty niezamknięta prawidłowo,
- zdarzenie błędu danych o ruchu,
- zdarzenie przerwy zasilania,
- wewnętrzna usterka VU.

AUD_203 VU stosuje zasady gromadzenia rekordów audytu (wymagania 094 i 096).

AUD_204 VU przechowuje w swojej pamięci danych rekordy audytu generowane przez czujnik ruchu.

AUD_205 Możliwe jest wydrukowanie, wyświetlenie i wczytanie rekordów audytu.

4.5. **Powtórne wykorzystanie obiektu**

REU_201 VU zapewnia czasowe gromadzenie obiektów, które mogą być powtórnie wykorzystane, w sposób niepociągający za sobą niedopuszczalnego przepływu informacji.

4.6. **Dokładność**

4.6.1. *Polityka kontroli przepływu informacji*

ACR_201 VU zapewnia, że dane użytkownika wiążące się z wymaganiami 081, 084, 087, 090, 093, 102, 104, 105, 105a i 109 mogą być przetwarzane tylko wtedy, gdy pochodzą z prawidłowych źródeł:

- dane ruchowe pojazdu,
- zegar czasu rzeczywistego VU,
- parametry kalibracyjne urządzenia rejestrującego,
- karty do tachografów,
- wejścia użytkownika.

ACR_201a VU zapewnia, że dane użytkownika dotyczące wymagania 109a można wprowadzać tylko za okres ostatniego wyjęcia — bieżącego włożenia karty (wymaganie 050a).

4.6.2. *Wewnętrzne przesyłanie danych*

Wymagania tego punktu stosuje się tylko wtedy, gdy VU korzysta z fizycznie oddzielonych części.

ACR_202 Jeżeli dane przesyła się między fizycznie oddzielnymi częściami VU, dane te są zabezpieczone przed modyfikacją.

ACR_203 W przypadku wykrycia błędu przesyłania danych podczas wewnętrznego przesyłania danych, transmisja jest powtarzana a funkcja SEF generuje rekord audytu.

4.6.3. *Integralność przechowywanych danych*

ACR_204 VU sprawdza dane użytkownika przechowywane w jego pamięci pod względem błędów integralności.

ACR_205 W przypadku wykrycia błędu integralności przechowywanych danych użytkownika, funkcja SEF generuje rekord audytu.

4.7. **Wiarygodność usługi**

4.7.1. *Testy*

RLB_201 Wszystkie polecenia, czynności lub punkty testowe przeznaczone dla potrzeb testowania w fazie produkcyjnej VU są zablokowane lub usunięte przed aktywacją VU. Przywrócenie ich do wykorzystania w późniejszym czasie nie jest możliwe.

RLB_202 VU uruchamia auto testy w czasie początkowego uruchomienia i w czasie normalnej pracy w celu zweryfikowania prawidłowego funkcjonowania. Auto testy VU obejmują weryfikację integralności danych bezpieczeństwa i weryfikację integralności przechowywanego kodu wynikowego, (jeżeli nie w pamięci ROM).

RLB_203 W przypadku wykrycia wewnętrznej usterki w czasie auto testu funkcja SEF:

- generuje rekord audytu (wyjawszy pracę w trybie kalibracyjnym) (wewnętrzna usterka VU),
- zachowuje integralność przechowywanych danych.

4.7.2. Oprogramowanie

RLB_204 Po aktywacji VU analizowanie lub testowanie oprogramowania nie jest możliwe w warunkach polowych.

RLB_205 Wejścia z zewnętrznych źródeł nie przyjmują kodu wykonywalnego.

4.7.3. Ochrona fizyczna

RLB_206 Jeżeli konstrukcja VU pozwala na otwarcie obudowy, VU wykrywa każde otwarcie obudowy, wyjąwszy pracę w trybie kalibracyjnym, nawet przy braku zewnętrznego zasilania przez okres przynajmniej 6 miesięcy. W takim przypadku funkcja SEF generuje rekord audytu (dopuszcza się, że rekord audytu jest generowany i zapamiętywany po ponownym przyłączeniu zasilania).

Jeżeli konstrukcja VU nie pozwala na otwieranie go, VU jest tak skonstruowane, aby umożliwić łatwe wykrycie wszelkich prób ataku zewnętrznego (np. przez kontrolę wizualną).

RLB_207 Po aktywacji, VU wykrywa określone (przez producenta) uszkodzenia sprzętu.

RLB_208 W opisanym powyżej przypadku funkcja SEF generuje rekord audytu a VU: (określa producent).

4.7.4. Przerwy zasilania

RLB_209 VU wykrywa odchylenia od nominalnych wartości zasilania, z odcięciem włączanie.

RLB_210 W przypadku opisanym powyżej funkcja SEF:

- generuje rekord audytu (w szczególności, gdy jest w trybie kalibracyjnym),
- utrzymuje bezpieczny stan VU,
- utrzymuje funkcje zabezpieczające dla składników lub procesów w stanie operacyjnym,
- zachowuje integralność przechowywanych danych.

4.7.5. Warunki zerujące

RLB_211 W przypadku przerwy zasilania lub, gdy transakcja jest zatrzymana przez zakończeniem lub w przypadku zaistnienia innych warunków zerujących (reset), VU daje się łatwo zerować.

4.7.6. Dostępność danych

RLB_212 VU zapewnia uzyskanie dostępu do zasobów, gdy są potrzebne, oraz by zasoby nie były niepotrzebnie żądane ani zachowywane.

RLB_213 VU musi zapewniać, że kart nie da się wyjąć przed zapisaniem na nich stosownych danych (wymagania 015 and 016).

RLB_214 W przypadku opisanym powyżej, funkcja SEF generuje zdarzenia rekordu audytu.

4.7.7. Obsługa wielu aplikacji

RLB_215 Jeżeli VU obsługuje aplikacje inne niż aplikacja tachograficzna, wszystkie aplikacje są rozdzielone każda od pozostałych fizycznie i/lub logicznie. Aplikacje te nie współdzielą danych bezpieczeństwa. Jednocześnie może być aktywne tylko jedno zadanie.

4.8. Wymiana danych

Niniejszy punkt dotyczy wymiany danych między VU i przyłączonymi urządzeniami.

4.8.1. Wymiana danych z czujnikiem ruchu

DEX_201 VU weryfikuje integralność i autentyczność danych ruchowych importowanych z czujnika ruchu

DEX_202 W przypadku wykrycia błędu integralności lub autentyczności danych ruchowych funkcja SEF:

- generuje rekord audytu,
- kontynuuje używanie importowanych danych.

4.8.2. Wymiana danych z kartami do tachografów

DEX_203 VU weryfikuje integralność i autentyczność danych ruchowych importowanych z kart do tachografów.

DEX_204 W przypadku wykrycia błędu integralności lub autentyczności danych z karty funkcja SEF:

- generuje rekord audytu,
- nie używa tych danych.

DEX_205 VU eksportuje dane do inteligentnych kart do tachografów razem ze skojarzonymi atrybutami bezpieczeństwa, tak aby karta była w stanie zweryfikować integralność i autentyczność tych danych.

4.8.3. Wymiana danych z zewnętrznymi nośnikami gromadzenia danych (funkcja ładowania danych)

DEX_206 VU generuje informacje o pochodzeniu danych wczytywanych na zewnętrzne nośniki.

DEX_207 VU zapewnia adresatowi możliwość weryfikowania informacji o pochodzeniu wczytanych danych.

DEX_208 VU wczytuje dane na zewnętrzne nośniki gromadzenia razem ze skojarzonymi atrybutami bezpieczeństwa, tak aby umożliwić weryfikację integralności i autentyczności tych danych.

4.9. Wsparcie kryptograficzne

Wymagania tego punktu stosuje się tylko tam gdzie potrzeba, w zależności od zastosowanych mechanizmów bezpieczeństwa i rozwiązań producenta.

CSP_201 Wszelkie operacje kryptograficzne wykonywane przez VU są zgodne z ustalonym algorytmem i używają klucza o ustalonej długości.

CSP_202 Jeżeli VU generuje klucze kryptograficzne, to robi to zgodnie z ustalonymi algorytmami generowania kluczy kryptograficznych a klucze kryptograficzne mają ustaloną długość.

CSP_203 Jeżeli VU rozprowadza klucze kryptograficzne, to robi to zgodnie z ustalonymi metodami rozprowadzania kluczy kryptograficznych.

CSP_204 Jeżeli VU ma dostęp do kluczy kryptograficznych, to robi to zgodnie z ustalonymi metodami dostępu do kluczy kryptograficznych.

CSP_205 Jeżeli VU niszczy klucze kryptograficzne, to robi to zgodnie z ustalonymi metodami niszczenia kluczy kryptograficznych.

5. Definicja mechanizmów zabezpieczenia

Wymagane mechanizmy zabezpieczenia opisano w dodatku 11.

Wszystkie pozostałe mechanizmy zabezpieczenia definiują producenci.

6. Minimalna siła mechanizmów zabezpieczenia

Minimalna siła mechanizmów zabezpieczenia VU jest wysoka, według definicji ITSEC.

7. Poziom gwarancji zabezpieczenia

Docelowym poziomem gwarancji zabezpieczenia dla czujnika ruchu jest poziom E3, według definicji ITSEC.

8. Podstawy racjonalne

W tabelach poniżej zamieszczono podstawy racjonalne dla funkcji SEF pokazując przy tym:

- które funkcje SEF lub środki są skierowane przeciw którym zagrożeniom,
- które funkcje SEF realizują które informatyczne cele zabezpieczenia.

	Zagrożenia																Cele informatyczne											
	Dostęp	Identyfikacja	Usterki	Testy	Konstrukcja	Parametry kalibracyjne	Wymiana danych z kartą	Zegar	Środowisko	Urządzenia fałszywe	Sprzęt	Dane ruchowe	Nieaktywowane	Dane wyjściowe	Zasilanie	Dane bezpieczeństwa	Oprogramowanie	Przechowywane dane	Dostęp	Wiarygodność	Audyt	Uwierzytelnienie	Integralność	Wyjście	Przetwarzanie	Wiarygodność	Bezpieczna wymiana danych	
Środki fizyczne, osobowe i proceduralne																												
Projektowanie			x	x	x																							
Wytwarzanie				x	x																							
Dostawa													x															
Aktywacja	x											x																
Generowanie danych bezpieczeństwa																	x											
Transport danych bezpieczeństwa																	x											
Dostępność karty		x																										
Jedna karta kierowcy		x																										
Możliwość odtworzenia historii karty		x																										
Zatwierdzone warsztaty						x		x																				
Regularne przeglądy kalibracyjne						x		x				x	x			x												
Wiarygodne warsztaty						x		x																				
Wiarygodni kierowcy		x																										
Kontrole wdrażania prawa		x				x		x	x		x		x		x		x	x										
Aktualizacja oprogramowania																		x										
Funkcje realizujące zabezpieczenie																												
Identyfikacja i uwierzytelnienie																												
UIA_201 Identyfikacja czujnika										x		x											x					x
UIA_202 Tożsamość czujnika										x		x											x					x
UIA_203 Uwierzytelnienie czujnika										x		x											x					x
UIA_204 Powtórna identyfikacja i uwierzytelnienie czujnika										x		x											x					x
UIA_205 Uwierzytelnienie niewymazywalne										x		x											x					
UIA_206 Błąd uwierzytelnienia										x		x											x				x	
UIA_207 Identyfikacja użytkowników	x	x								x									x				x					x
UIA_208 Tożsamość użytkownika	x	x								x									x				x					x
UIA_209 Uwierzytelnienie użytkownika	x	x								x									x				x					x
UIA_210 Powtórne uwierzytelnienie użytkownika	x	x								x									x				x					x
UIA_211 Środki uwierzytelniania	x	x								x									x				x					
UIA_212 Kontrole kodu PIN	x	x				x		x											x				x					
UIA_213 Uwierzytelnienie niewymazywalne	x	x								x									x				x					

	Zagrożenia																	Cele informatyczne										
	Dostęp	Identyfikacja	Usterki	Testy	Konstrukcja	Parametry kalibracyjne	Wymiana danych z kartą	Zegar	Środowisko	Urządzenia fałszywe	Sprzęt	Dane ruchowe	Nieaktywowane	Dane wyjściowe	Zasilanie	Dane bezpieczeństwa	Oprogramowanie	Przechowywane dane	Dostęp	Wiarygodność	Audyt	Uwierzytelnienie	Integralność	Wyjście	Przetwarzanie	Wiarygodność	Bezpieczna wymiana danych	
UIA_214 Błąd uwierzytelnienia	x	x							x											x								
UIA_215 Identyfikacja zdalnego użytkownika	x	x																x			x							x
UIA_216 Tożsamość zdalnego użytkownika	x	x																x			x							
UIA_217 Uwierzytelnienie zdalnego użytkownika	x	x																x			x							x
UIA_218 Środki uwierzytelnienia	x	x																x			x							
UIA_219 Uwierzytelnienie niewymazywalne	x	x																x			x							
UIA_220 Błąd uwierzytelnienia	x	x																										
UIA_221 Identyfikacja urządzenia zarządzającego	x	x																	x			x						
UIA_222 Uwierzytelnienie urządzenia zarządzającego	x	x																	x			x						
UIA_223 Uwierzytelnienie niewymazywalne	x	x																	x			x						
Kontrola dostępu																												
ACC_201 Polityka kontroli dostępu	x					x		x									x		x	x								
ACC_202 Prawa dostępu do funkcji	x					x		x												x								
ACC_203 Prawa dostępu do funkcji	x					x		x												x								
ACC_204 ID VU																			x	x								
ACC_205 ID przyłączonego czujnika										x									x	x								
ACC_206 Dane dotyczące kalibracji	x					x													x	x								
ACC_207 Dane dotyczące kalibracji						x													x	x								
ACC_208 Dane dotyczące regulacji czasu								x											x	x								
ACC_209 Dane dotyczące regulacji czasu								x											x	x								
ACC_210 Dane bezpieczeństwa																	x		x	x								
ACC_211 Struktura pliku i warunki dostępu	x					x											x		x	x								
Wiarygodność																												
ACT_201 Rozliczanie kierowców																				x								
ACT_202 Dane identyfikacyjne VU																				x	x							
ACT_203 Rozliczanie warsztatów																				x								
ACT_204 Rozliczanie kontrolerów																				x								
ACT_205 Rozliczanie ruchu pojazdu																				x								
ACT_206 Modyfikacja danych rozliczeniowych																			x					x			x	
ACT_207 Modyfikacja danych rozliczeniowych																			x					x			x	

[illegible]

[illegible]

OGÓLNY CEL ZABEZPIECZENIA KARTY DO TACHOGRAFÓW

1. Wprowadzenie

Niniejszy dokument zawiera opis karty do tachografów, zagrożeń, którym karta do tachografów musi być w stanie przeciwdziałać i celów zabezpieczenia, które musi osiągnąć. Niniejszy dokument określa wymagane funkcje realizujące zabezpieczenia. Podaje wymaganą, minimalną siłę mechanizmów zabezpieczenia i wymagany poziom zapewnienia rozwoju i oceny.

Wymaganiami, o których mowa w tym dokumencie, są te znajdujące się w treści załącznika I B. W celu zwiększenia czytelności czasami pojawia się dublowanie wymagań znajdujących się w treści załącznika I B i wymagań celu zabezpieczenia. W przypadku niezgodności między wymaganiami celu zabezpieczenia a wymaganiami znajdującymi się w treści załącznika I B, do których odwołuje się wymaganie celu zabezpieczenia, obowiązuje wymaganie z treści załącznika I B.

Wymagania znajdujące się w treści załącznika I B, do których nie odwołują się cele zabezpieczenia, nie są przedmiotem funkcji realizujących zabezpieczenia.

Karta do tachografów jest standardową kartą inteligentną z dedykowaną aplikacją tachograficzną i jest zgodna z nowoczesnymi wymaganiami funkcjonalnymi i zapewnienia bezpieczeństwa, które stosuje się do kart inteligentnych. Tym samym ten cel zabezpieczenia wnosi tylko dodatkowe wymagania bezpieczeństwa wymagane dla aplikacji tachograficznej.

Zagrożeniom, celom, środkom proceduralnym i specyfikacjom funkcji realizujących zabezpieczenia nadano unikalne etykiety w celu umożliwienia odtworzenia historii produktu w dokumentach rozwoju i oceny.

2. Skróty, definicje i odniesienia**2.1. Skróty**

IC	układ scalony (element elektroniczny przeznaczony do realizowania funkcji przetwarzania i/lub pamięci)
OS	system operacyjny
PIN	osobisty numer identyfikacyjny
ROM	pamięć stała
SFP	polityka funkcji realizujących zabezpieczenia
TBD	określi
TOE	cel oceny
TSF	funkcji realizujących zabezpieczenia TOE
VU	przyrząd rejestrujący.

2.2. Definicje

Cyfrowy tachograf	urządzenie rejestrujące.
Wrażliwe dane	dane przechowywane przez kartę do tachografów wymagające ochrony pod względem integralności, nieautoryzowanej modyfikacji i poufności (gdzie stosowne dla danych bezpieczeństwa). Wrażliwymi danymi są dane bezpieczeństwa i dane użytkownika.
Dane bezpieczeństwa	szczególne dane potrzebne do wspierania funkcji realizujących zabezpieczenie (np. klucze kryptograficzne).
System	sprzęt, ludzie lub organizacje związane w jakikolwiek sposób z urządzeniem rejestrującym.
Użytkownik	pod pojęciem użytkownika rozumie się jednostkę (człowieka lub zewnętrzną jednostkę informatyczną) zewnętrzną w stosunku do TOE, która przeprowadza interakcje, z TOE (gdy nieużywane w wyrażeniu »dane użytkownika«).

Dane użytkownika	wrażliwe dane przechowywane na karcie do tachografów, inne niż dane bezpieczeństwa. Danymi użytkownika są dane identyfikacyjne i dane dotyczące aktywności.
Dane identyfikacyjne	danymi identyfikacyjnymi są dane identyfikacyjne karty i dane identyfikacyjne posiadacza karty.
Dane identyfikacyjne karty	dane użytkownika dotyczące identyfikacji karty zdefiniowane w wymaganiach 190, 191, 192, 194, 215, 231 i 235.
Dane identyfikacyjne posiadacza karty	dane użytkownika dotyczące identyfikacji posiadacza karty zdefiniowane w wymaganiach 195, 196, 216, 232 i 236.
Dane dotyczące aktywności	danymi dotyczącymi aktywności są dane dotyczące czynności posiadacza karty, dane dotyczące zdarzeń i usterek oraz dane dotyczące czynności kontrolnej.
Dane dotyczące czynności posiadacza karty	dane użytkownika dotyczące czynności wykonywanych przez posiadacza karty zdefiniowane w wymaganiach 197, 199, 202, 212, 212a, 217, 219, 221, 226, 227, 229, 230a, 233 i 237.
Dane dotyczące zdarzeń i usterek	dane użytkownika dotyczące zdarzeń i usterek zdefiniowane w wymaganiach 204, 205, 207, 208 i 223.
Dane dotyczące czynności kontrolnej	dane użytkownika dotyczące kontroli wdrażania prawa zdefiniowane w wymaganiach 210 i 225.

2.3. Odniesienia

ITSEC	ITSEC Informatyka — kryteria oceny zabezpieczeń 1991 r.
IC PP	Profil zabezpieczenia układu scalonego dla kart inteligentnych — wersja 2.0 — wydanie z września 1998 r. Zarejestrowane we francuskiej jednostce certyfikacyjnej pod numerem PP/9806
ES PP	Profil zabezpieczenia układu scalonego dla kart inteligentnych z wbudowanym oprogramowaniem — wersja 2.0 — wydanie z czerwca 1999 r. Zarejestrowane we francuskiej jednostce certyfikacyjnej pod numerem PP/9911

3. Podstawy racjonalne produktu

3.1. Opis i metoda użycia karty do tachografów

Karta do tachografów jest kartą inteligentną, jak opisano w (IC PP) i (ES PP), zawierającą aplikację przeznaczoną do używania z urządzeniem rejestrującym.

Podstawowymi funkcjami karty do tachografów są:

- przechowywanie danych identyfikacyjnych karty i posiadacza karty. Danymi tych używa przyrząd rejestrujący do identyfikacji posiadacza karty, udostępniania związanych praw dostępu do funkcji i danych, i zapewnienia rozliczenia posiadacza karty z jego czynności,
- przechowywanie danych dotyczących czynności posiadacza karty, danych dotyczące zdarzeń i usterek oraz danych dotyczących czynności kontrolnych dotyczących posiadacza karty.

Tak więc karta do tachografów jest przewidziana do czytnika kart w przyrządzie rejestrującym. Może być też używana w dowolnym, innym czytniku kart (np. w komputerze osobistym), który powinien mieć pełne prawa odczytu danych użytkownika.

W czasie fazy eksploatacyjnej w cyklu życia karty do tachografów (faza 7 cyklu życia opisana w (ES PP)), tylko przyrządy rejestrujące mogą zapisywać dane użytkownika na karcie.

Wymagania funkcjonalne dla karty do tachografów określono w treści załącznika I B i dodatku 2.

3.2. Cykl życia karty do tachografów

Cykl życia karty do tachografów jest zgodny z cyklem życia karty inteligentnej opisanym w (ES PP).

3.3. Zagrożenia

W dodatku do ogólnych zagrożeń dla karty inteligentnej wymienionych w (ES PP) i (IC PP), karta do tachografów może być narażona na następujące zagrożenia:

3.3.1. Końcowe cele

Końcowym celem atakujących będzie zmodyfikowanie danych użytkownika zgromadzonych w TOE.

T.Ident_Data	Pomyślnie wprowadzona zmiana danych identyfikacyjnych przechowywanych przez TOE (np. typ karty lub data ważności karty lub dane identyfikacyjne CardHolder) umożliwiłaby użycie TOE niezgodne z przeznaczeniem i stanowiłaby poważne zagrożenie dla ogólnego celu zabezpieczenia systemu.
T.Activity_Data	Pomyślnie wprowadzona zmiana danych dotyczących aktywności przechowywanych w TOE stanowiłaby zagrożenie dla bezpieczeństwa TOE.
T.Data_Exchange	Pomyślnie wprowadzona zmiana danych dotyczących aktywności (dodanie, usunięcie, zmiana) podczas importu lub eksportu danych stanowiłaby zagrożenie dla bezpieczeństwa TOE.

3.3.2. Ścieżki ataku

Zasoby TOE mogą być zaatakowane następującymi sposobami:

- próba uzyskania nielegalnej wiedzy dotyczącej konstrukcji sprzętu i oprogramowania TOE w szczególności jego funkcji realizujących zabezpieczenie lub danych bezpieczeństwa. Nielegalną wiedzę można pozyskać atakami na konstruktora lub producenta materiału (kradzież, przekupstwo,...) lub przez bezpośrednie badania samego TOE (próby fizyczne, analiza zakłóceń,...),
- wykorzystanie słabości konstrukcji lub wykonania TOE (błędy eksploatacyjne sprzętu, błędy oprogramowania, usterki transmisji, błędy wprowadzone do TOE wskutek stresów środowiskowych, słabości eksploatacyjne funkcji realizujących zabezpieczenie takich jak procedury uwierzytelnienia, kontrola dostępu do danych, czynności kryptograficzne,...),
- modyfikowanie TOE lub jego funkcji realizujących zabezpieczenie przed atakami fizycznymi, elektrycznymi lub logicznymi lub ich kombinacją.

3.4. Cele zabezpieczenia

Główny cel zabezpieczenia całego systemu urządzenia rejestrującego jest następujący:

O.Main	Dane przeznaczone do sprawdzenia przez organ kontrolny muszą być dostępne oraz w pełni i dokładnie odzwierciedlać czynności kontrolowanych kierowców i pojazdów, czas prowadzenia pojazdu, pracy, dyspozycyjności i odpoczynku oraz prędkość pojazdu.
--------	---

Tym samym głównymi celami zabezpieczenia dla TOE, przyczyniającymi się do ogólnego celu zabezpieczenia, są:

O.Card_Identification_Data	TOE musi zachować dane identyfikacyjne karty i dane identyfikacyjne posiadacza karty zgromadzone podczas procesu personalizacji karty,
O.Card_Activity_Storage	TOE musi zachować dane użytkownika zapisane na karcie przez przyrządy rejestrujące.

3.5. Informatyczne cele zabezpieczenia

Dodatkowo do ogólnych celów zabezpieczenia karty inteligentnej wyszczególnionych w (ES PP) i (IC PP), szczególne, informatyczne cele zabezpieczenia TOE przyczyniające się do jego głównych celów zabezpieczenia w czasie fazy eksploatacyjnej w cyklu życia są następujące:

O.Data_Access	TOE musi ograniczać prawa zapisu danych użytkownika do uwierzytelnionych przyrządów rejestrujących,
O.Secure_Communications	TOE musi być w stanie wspierać bezpieczne protokoły i procedury komunikacyjne między kartą a czytnikiem kart, gdy jest to wymagane przez aplikację.

3.6. Środki fizyczne, osobowe lub proceduralne

Wymagania dotyczące środków fizycznych, osobowych lub proceduralnych przyczyniające się do bezpieczeństwa TOE wyszczególniono w (ES PP) i (IC PP) (Rozdziały o celach zabezpieczenia dla środowiska).

4. Funkcje realizujące zabezpieczenie

W punkcie tym sprecyzowano niektóre z dozwolonych czynności, takich jak przyporządkowanie lub wybór (ES PP) oraz podano dodatkowe wymagania funkcjonalne dla funkcji SEF.

4.1. Zgodność z profilami ochrony

CPP_301 TOE jest zgodny z (IC PP).

CPP_302 TOE jest zgodny z (ES PP) w sposób dalej sprecyzowany.

4.2. Identyfikacja i uwierzytelnienie użytkownika

Karta musi identyfikować jednostkę, do której jest włożona i wiedzieć, czy jest to uwierzytelniony przyrząd rejestrujący czy nie. Karta może eksportować wszelkie dane użytkownika niezależnie od jednostki, do której jest przyłączona, z wyjątkiem karty kontrolnej, która może eksportować dane identyfikacyjne posiadacza karty tylko do uwierzytelnionych przyrządów rejestrujących (tak by kontroler miał pewność, że przyrząd rejestrujący nie jest przyrządem fałszywym widząc jego nazwę na wyświetlaczu lub wydruku).

4.2.1. Identyfikacja użytkownika

Przyporządkowanie (FIA_UID.1.1) Wykaz pośrednich czynności funkcji TSF: brak.

Przyporządkowanie (FIA_ATD.1.1) Wykaz atrybutów bezpieczeństwa::

USER_GROUP VEHICLE_UNIT, NON_VEHICLE_UNIT,

USER_ID numer rejestracyjny pojazdu (VRN) i kod Państwa Członkowskiego rejestracji (USER_ID znany jest tylko USER_GROUP = VEHICLE_UNIT).

4.2.2. Uwierzytelnienie użytkownika

Przyporządkowanie (FIA_UAU.1.1) Wykaz pośrednich czynności funkcji TSF:

- karty kierowcy i warsztatowe: eksport danych użytkownika z atrybutami bezpieczeństwa (funkcja wczytywania danych z karty),
- karta kontrolna: eksport danych użytkownika bez atrybutów bezpieczeństwa z wyjątkiem danych identyfikacyjnych posiadacza karty.

UIA_301 Uwierzytelnienie przyrządu rejestrującego odbywa się poprzez wykazanie, że przyrząd rejestrujący dysponuje danymi bezpieczeństwa, które mógł dystrybuować tylko system.

Wybór (FIA_UAU.3.1 i FIA_UAU.3.2): zapobiec.

Przyporządkowanie (FIA_UAU.4.1) Identyfikowany mechanizm(y) uwierzytelniający: dowolny mechanizm uwierzytelniający.

UIA_302 Karta warsztatowa udostępnia dodatkowy mechanizm uwierzytelniający poprzez kontrolę numeru PIN (mechanizm ten przeznaczony jest dla przyrządu rejestrującego w celu kontroli tożsamości posiadacza karty, zadaniem jego nie jest ochrona zawartości karty warsztatowej).

4.2.3. Błędy uwierzytelnienia

Poniższe przyporządkowania opisują odpowiedź karty na każdy pojedynczy błąd uwierzytelnienia użytkownika.

Przyporządkowanie (FIA_AFL.1.1) Numer: 1, wykaz zdarzeń uwierzytelnienia: uwierzytelnienie urządzenia interfejsu kart.

Przyporządkowanie (FIA_AFL.1.2) Wykaz czynności:

- ostrzec przyłączoną jednostkę,
- przyjąć założenie, że użytkownikiem jest NON_VEHICLE_UNIT.

Poniższe przyporządkowania opisują odpowiedź karty w przypadku błędu mechanizmu dodatkowego uwierzytelnienia wymaganego w UIA_302.

Przyporządkowanie (FIA_AFL.1.1) Numer: 5, wykaz zdarzeń uwierzytelnienia: kontrole PIN (karta warsztatowa).

Przyporządkowanie (FIA_AFL.1.2) Wykaz czynności::

- ostrzec przyłączoną jednostkę,
- zablokować procedurę kontroli PIN w taki sposób, by wszelkie dalsze próby kontroli PIN dały wynik negatywny,
- być w stanie wskazać kolejnym użytkownikom przyczynę zablokowania.

4.3. Kontrola dostępu**4.3.1. Polityka kontroli dostępu**

W czasie fazy eksploatacji w cyklu użycia karty do tachografów podlega ona jednej polityce funkcji zabezpieczenia realizującej kontrolę dostępu (SFP) zwanej AC_SFP.

Przyporządkowanie (FDP_ACC.2.1) Kontrola dostępu SFP: AC_SFP.**4.3.2. Funkcje kontroli dostępu****Przyporządkowanie** (FDP_ACF.1.1) Kontrola dostępu SFP: AC_SFP.**Przyporządkowanie** (FDP_ACF.1.1) Nazwana grupa atrybutów bezpieczeństwa: USER_GROUP.

Przyporządkowanie (FDP_ACF.1.2) Reguły rządzące dostępem stosowane między kontrolowanymi przedmiotami a kontrolowanymi obiektami wykorzystujące kontrolowane czynności wykonywane na kontrolowanych obiektach:

GENERAL_READ:	Dane użytkownika może odczytać z TOE dowolny użytkownik, z wyłączeniem danych identyfikacyjnych posiadacza karty, które tylko VEHICLE_UNIT może odczytać z kart kontrolnych.
IDENTIF_WRITE:	Dane identyfikacyjne można zapisać tylko raz i przed końcem fazy 6 cyklu życia karty. Żaden użytkownik nie może zapisać ani zmienić danych identyfikacyjnych w okresie eksploatacji w cyklu życia karty.
ACTIVITY_WRITE:	Dane dotyczące czynności może zapisywać do TOE tylko VEHICLE_UNIT.
SOFT_UPGRADE:	Żaden użytkownik nie może aktualizować oprogramowania TOE.
FILE_STRUCTURE:	Struktura plików i warunki dostępu są utworzone przed końcem fazy 6 cyklu życia TOE i następnie zablokowane w sposób uniemożliwiający w przyszłości ich zmianę lub wymazanie.

4.4. Wiarygodność

ACT_301 TOE trwale przechowuje dane identyfikacyjne.

ACT_302 Godzina i data personalizacji TOE są zapisane. Zmiana tych danych nie jest możliwa.

4.5. Audyt

TOE musi monitorować zdarzenia, które wskazują na potencjalne naruszenie jego zabezpieczenia.

Przyporządkowanie (FAU_SAA.1.2) Podzbiór zdefiniowanych zdarzeń uwzględnianych w audycie:

- błąd uwierzytelnienia CardHolder (5 kolejnych błędnych wprowadzeń kodu PIN),
- błąd auto testu,
- błąd integralności przechowywanych danych,
- błąd integralności danych wejściowych dotyczących aktywności.

4.6. Dokładność**4.6.1. Integralność przechowywanych danych****Przyporządkowanie** (FDP_SDI.2.2) Podejmowane czynności: ostrzec przyłączoną jednostkę,**4.6.2. Podstawowe uwierzytelnienie danych****Przyporządkowanie** (FDP_DAU.1.1) Wykaz obiektów lub typów informacji: dane dotyczące czynności.**Przyporządkowanie** (FDP_DAU.1.2) Wykaz przedmiotów: dowolna.

4.7. **Wiarygodność usługi**

4.7.1. Testy

Wybór (FPT_TST.1.1): podczas początkowego uruchomienia, okresowo w czasie normalnej pracy.

Uwaga: podczas początkowego uruchomienia oznacza przed wykonaniem kodu (i niekoniecznie w czasie wykonywania procedury zerowania ATR).

- RLB_301 Auto testy TOE obejmują weryfikację integralności kodu oprogramowania nieprzechowywanego w pamięci ROM.
- RLB_302 W przypadku wykrycia błędu przez auto test funkcja TSF ostrzega przyłączoną jednostkę.
- RLB_303 Po zakończeniu testowania OS wszystkie swoje dla testowania polecenia i czynności należy zablokować lub usunąć. Obejście tych kontroli i przywrócenie ich do działania nie jest możliwe. Polecenia związane z jednym wyłącznie stanem cyklu życia nie są dostępne w żadnym innym stanie.

4.7.2. Oprogramowanie

- RLB_304 Analizowanie, testowanie ani modyfikowanie oprogramowania TOE nie jest możliwe w warunkach polowych.
- RLB_305 Wejścia z zewnętrznych źródeł nie przyjmują kodu wykonywalnego.

4.7.3. Zasilanie

- RLB_306 TOE zachowuje bezpieczny stan w czasie zaniku lub zmian zasilania.

4.7.4. Warunki zerujące

- RLB_307 W przypadku przerwy zasilania (lub wystąpienia wahań zasilania) TOE, lub gdy transakcja jest zatrzymana przed zakończeniem lub w przypadku zaistnienia innych warunków zerujących, TOE daje się łatwo zerować.

4.8. **Wymiana danych**

4.8.1. Wymiana danych z przyrządem rejestrującym

- DEX_301 TOE weryfikuje integralność i autentyczność danych importowanych z przyrządu rejestrującego.
- DEX_302 W przypadku wykrycia błędu integralności importowanych danych TOE:
- ostrzega jednostkę wysyłając dane,
 - nie używa tych danych.

- DEX_303 TOE eksportuje dane użytkownika do przyrządu rejestrującego razem ze skojarzonymi atrybutami bezpieczeństwa, tak aby przyrząd rejestrujący był w stanie zweryfikować integralność i autentyczność odebranych danych.

4.8.2. Eksport danych gdzie indziej niż do przyrządu rejestrującego (funkcja ładowania danych)

- DEX_304 TOE generuje informacje o pochodzeniu danych wczytywanych na zewnętrzne media.
- DEX_305 TOE zapewnia adresatowi możliwość weryfikowania informacji o pochodzeniu wczytanych danych.
- DEX_306 TOE wczytuje dane na zewnętrzne nośniki gromadzenia razem ze skojarzonymi atrybutami bezpieczeństwa, tak aby umożliwić weryfikację integralności tych danych.

4.9. **Wsparcie kryptograficzne**

- CSP_301 Jeżeli funkcja TSF generuje klucze kryptograficzne, to robi to zgodnie z ustalonymi algorytmami generowania kluczy kryptograficznych a klucze kryptograficzne mają ustaloną długość. Liczba możliwych użyć generowanych kluczy kryptograficznych sesji jest ograniczona (i ustalona przez producenta, ale nie większa niż 240).
- CSP_302 Jeżeli funkcja TSF rozprowadza klucze kryptograficzne, to robi to zgodnie z ustalonymi metodami rozprowadzania kluczy kryptograficznych.

5. **Definicja mechanizmów zabezpieczenia**

Wymagane mechanizmy zabezpieczenia opisano w dodatku 11.

Wszystkie pozostałe mechanizmy zabezpieczenia definiuje producent.

6. Minimalna siła mechanizmów zabezpieczenia

Minimalna siła mechanizmów zabezpieczenia VU jest wysoka, według definicji ITSEC.

7. Poziom gwarancji zabezpieczenia

Docelowym poziomem gwarancji zabezpieczenia karty do tachografów jest poziom E3, według definicji ITSEC.

8. Podstawy racjonalne

W tabelach poniżej podano podstawy racjonalne dodatkowych funkcji SEF, pokazując przy tym:

- które funkcje SEF są skierowane przeciw którym zagrożeniom,
- które funkcje SEF realizują które informatyczne cele zabezpieczenia.

	Zagrożenia										Cele informatyczne									
	T.CLON*	T.DIS_ES2	T.T_ES	T.T_CMD	T.MOD_SOFT*	T.MOD_LOAD	T.MOD_EXE	T.MOD_SHARE	Ident_Data	Activity_Data	Data_Exchange	O.TAMPER_ES	O.CLON*	O.OPERATE*	O.FLAW*	O.DIS_MECHANISM2	O.DIS_MEMORY*	O.MOD_MEMORY*	Data_Access	Bezpieczna wymiana komunikatów
UIA_301 Środki uwierzytelnienia																			x	
UIA_302 Kontrole numeru PIN																			x	
ACT_301 Dane identyfikacyjne																				
ACT_302 Data personalizacji																				
RLB_301 Integralność oprogramowania												x		x						
RLB_302 Auto testy												x		x						
RLB_303 Testy fabryczne					x	x						x		x						
RLB_304 Analizowanie oprogramowania					x		x	x				x		x						
RLB_305 Ładowanie oprogramowania					x	x		x				x		x						
RLB_306 Zasilanie									x	x		x		x						
RLB_307 Warunki zerujące												x		x						
DEX_301 Bezpieczny import danych											x									x
DEX_302 Bezpieczny import danych											x									x
DEX_303 Bezpieczny eksport danych do VU											x									x
DEX_304 Informacje o pochodzeniu											x									x
DEX_305 Informacje o pochodzeniu											x									x
DEX_306 Bezpieczny eksport do zewnętrznego medium											x									x
CSP_301 Generowanie klucza												x								x
CSP_302 Rozprowadzanie klucza												x								x

Dodatek 11

WSPÓLNE MECHANIZMY ZABEZPIECZENIA

SPIS TREŚCI

1.	Informacje ogólne	516
1.1.	Odniesienia	516
1.2.	Notacje i skróty	517
2.	Systemy i algorytmy kryptograficzne	518
2.1.	Systemy kryptograficzne	518
2.2.	Algorytmy kryptograficzne	518
2.2.1.	Algorytm RSA	518
2.2.2.	Algorytm skrótu	518
2.2.3.	Algorytm szyfrowania danych	518
3.	Klucze i certyfikaty	518
3.1.	Generowanie i dystrybucja kluczy	518
3.1.1.	Generowanie i dystrybucja kluczy RSA	518
3.1.2.	Klucze testowe RSA	520
3.1.3.	Klucze czujnika ruchu	520
3.1.4.	Generowanie i dystrybucja kluczy sesji T-DES	520
3.2.	Klucze	520
3.3.	Certyfikaty	520
3.3.1.	Treść certyfikatu	521
3.3.2.	Wydane certyfikaty	522
3.3.3.	Weryfikacja i rozpakowanie certyfikatu	523
4.	Mechanizm wzajemnego uwierzytelnienia	523
5.	Poufność, integralność i mechanizmy uwierzytelniania przesyłania danych między VU a kartami ..	526
5.1.	Bezpieczna wymiana komunikatów	526
5.2.	Obsługa błędów w bezpiecznej wymianie komunikatów	527
5.3.	Algorytm obliczania kryptograficznych sum kontrolnych	528
5.4.	Algorytm obliczania kryptogramów dla poufnych obiektów danych	528
6.	Mechanizmy cyfrowego podpisu dla wczytywania danych	529
6.1.	Generowanie podpisu	529
6.2.	Sprawdzenie podpisu	529

1. INFORMACJE OGÓLNE

W niniejszym dodatku opisano mechanizmy zabezpieczenia zapewniające:

- wzajemne uwierzytelnienie między VU a kartami do tachografów, z uzgodnieniem klucza sesji włącznie,
- poufność, integralność i uwierzytelnienie danych przesyłanych między VU a kartami do tachografów,
- integralność i uwierzytelnienie danych wczytywanych z VU do zewnętrznych nośników gromadzenia danych,
- integralność i uwierzytelnienie danych wczytywanych z kart do tachografów do zewnętrznych nośników gromadzenia danych.

1.1. Odniesienia

W niniejszym dodatku używa się następujących odniesień:

SHA-1	National Institute of Standards and Technology (NIST). FIPS Publikacja 180-1: Bezpieczny standard skrótu. Kwiecień 1995 r.
PKCS1	RSA Laboratories. PKCS # 1: Standard szyfrowania RSA. Wersja 2.0. Październik 1998 r.
TDES	National Institute of Standards and Technology (NIST). FIPS Publikacja 46-3: Standard szyfrowania danych. Projekt 1999 r.
TDES-OP	ANSI X9.52, Tryby pracy algorytmu trzyetapowego szyfrowania danych. 1998 r.
ISO/IEC 7816-4	Informatyka — Identyfikacja kart — karty z układem(ami) scalonym(i) ze stykami — część 4: Międzybranżowe polecenia wymiany informacji. Wydanie pierwsze: 1995 + zmiana 1: 1997 r.
ISO/IEC 7816-6	Informatyka — Identyfikacja kart — karty z układem(ami) scalonym(i) ze stykami — część 6: Międzybranżowe elementy danych. Wydanie pierwsze: 1996 + zmiana 1: 1998 r.
ISO/IEC 7816-8	Informatyka — Identyfikacja kart — karty z układem(ami) scalonym(i) ze stykami — część 8: Międzybranżowe polecenia związane z bezpieczeństwem. Wydanie pierwsze 1999 r.
ISO/IEC 9796-2	Informatyka — Techniki zabezpieczeń — Metody podpisu cyfrowego z odzyskiwaniem komunikatu — część 2: Mechanizmy używające funkcji skrótu. Wydanie pierwsze: 1997 r.
ISO/IEC 9798-3	Informatyka — Techniki zabezpieczeń — Mechanizmy uwierzytelnienia jednostki — część 3: Uwierzytelnienie jednostki przy użyciu algorytmu klucza publicznego. Wydanie drugie: 1998 r.
ISO 16844-3	Pojazdy drogowe — Systemy tachograficzne — część 3: Interfejs czujnika ruchu.

1.2. Notacje i skróty

W niniejszym dodatku używa się następujących notacji i skrótów:

(K_a, K_b, K_c)	wiązka kluczy używanych w algorytmie trzyetapowego szyfrowania danych
CA	jednostka certyfikująca
CAR	odesłanie do jednostki certyfikującej
CC	kryptograficzna suma kontrolna
CG	kryptogram
CH	nagłówek polecenia
CHA	uprawnienie posiadacza certyfikatu
CHR	odesłanie do posiadacza certyfikatu
D()	deszyfracja DES
DE	element danych
DO	obiekt danych
d	klucz prywatny RSA, wykładnik prywatny
e	klucz publiczny RSA, wykładnik publiczny
E()	szyfrowanie DES
EQT	urządzenia
Hash()	skrót, wartość wyjściowa funkcji skrótu
Hash	funkcja skrótu
KID	identyfikator klucza
Km	klucz TDES. Klucz główny wg normy ISO 16844-3
Km_{vu}	klucz TDES wstawiony do przyrządu rejestrującego
Km_{wc}	klucz TDES wstawiony do kart warsztatowych
m	reprezentacja komunikatu, liczba całkowita z przedziału od 0 do $n-1$
n	klucze RSA, moduły
PB	bajty wypełnienia
PI	bajt wskaźnik wypełnienia (do zastosowania w kryptogramie dla poufności DO)
PV	wartość odkryta
s	reprezentacja podpisu, liczba całkowita z przedziału od 0 do $n-1$
SSC	licznik sekwencji nadawania
SM	bezpieczna wymiana komunikatów
TCBC	blok szyfrowy TDEA zmieniający tryb pracy
TDEA	algorytm trzyetapowego szyfrowania danych
TLV	wartość długości znacznika
VU	przyrząd rejestrujący
X.C	certyfikat użytkownika X wydany przez jednostkę certyfikującą
X.CA	jednostka certyfikująca użytkownika X
X.CA.PK ₀ X.C	operacja rozpakowania certyfikatu w celu uzyskania klucza publicznego. Jest to operator wzrostkowy, którego argumentem lewostronnym jest klucz publiczny jednostki certyfikującej, a argumentem prawostronnym jest certyfikat wydany przez tę jednostkę certyfikującą. Wynikiem jest klucz publiczny użytkownika X, którego certyfikat jest argumentem prawostronnym,

X.PK	klucz publiczny użytkownika X
X.PK[I]	szyfrowanie RSA pewnych informacji kluczem publicznym I użytkownika X
X.SK	klucz prywatny RSA użytkownika X
X.SK[I]	szyfrowanie RSA pewnych informacji kluczem prywatnym I użytkownika X
'xx'	wartość heksadecymalna
	operator konkatencji.

2. SYSTEMY I ALGORYTMY KRYPTOGRAFICZNE

2.1. Systemy kryptograficzne

CSM_001 Przyrządy rejestrujące i karty do tachografów używają klasycznego systemu kryptograficznego RSA z kluczem publicznym do realizowania następujących mechanizmów zabezpieczających:

- uwierzytelnienie między przyrządami rejestrującymi a kartami,
- transport kluczy sesji Triple-DES między przyrządami rejestrującymi a kartami do tachografów,
- podpis cyfrowy danych wczytywanych z przyrządów rejestrujących lub kart do tachografów do zewnętrznych mediów.

CSM_002 Przyrządy rejestrujące i karty do tachografów używają symetrycznego systemu kryptograficznego Triple-DES do zrealizowania mechanizmu zapewniającego integralność danych w czasie wymiany danych użytkownika między przyrządami rejestrującymi a kartami do tachografów i zapewnienia, gdzie stosowne, poufności wymiany danych między przyrządami rejestrującymi a kartami do tachografów.

2.2. Algorytmy kryptograficzne

2.2.1. Algorytm RSA

CSM_003 Algorytm RSA w pełni definiują następujące relacje:

$$\begin{aligned} X.SK[m] &= s = m^d \bmod n \\ X.PK[s] &= m = s^e \bmod n \end{aligned}$$

Bardziej wyczerpujący opis funkcji RSA można znaleźć w odesłaniach (PKCS1).

Wykładnik publiczny e dla obliczeń RSA jest różny od 2 we wszystkich generowanych kluczach RSA.

2.2.2. Algorytm skrótu

CSM_004 Mechanizmy podpisu cyfrowego używają algorytmu skrótu SHA-1 zdefiniowanego w odesłaniu (SHA-1).

2.2.3. Algorytm szyfrowania danych

CSM_005 Algorytmy oparte na algorytmie DES są używane w trybie pracy Cipher Block Chaining.

3. KLUCZE I CERTYFIKATY

3.1. Generowanie i dystrybucja kluczy

3.1.1. Generowanie i dystrybucja kluczy RSA

CSM_006 Klucze RSA są generowane na trzech hierarchicznych poziomach funkcjonalnych:

- poziom europejski,
- poziom Państwa Członkowskiego,
- poziom urzędzenia.

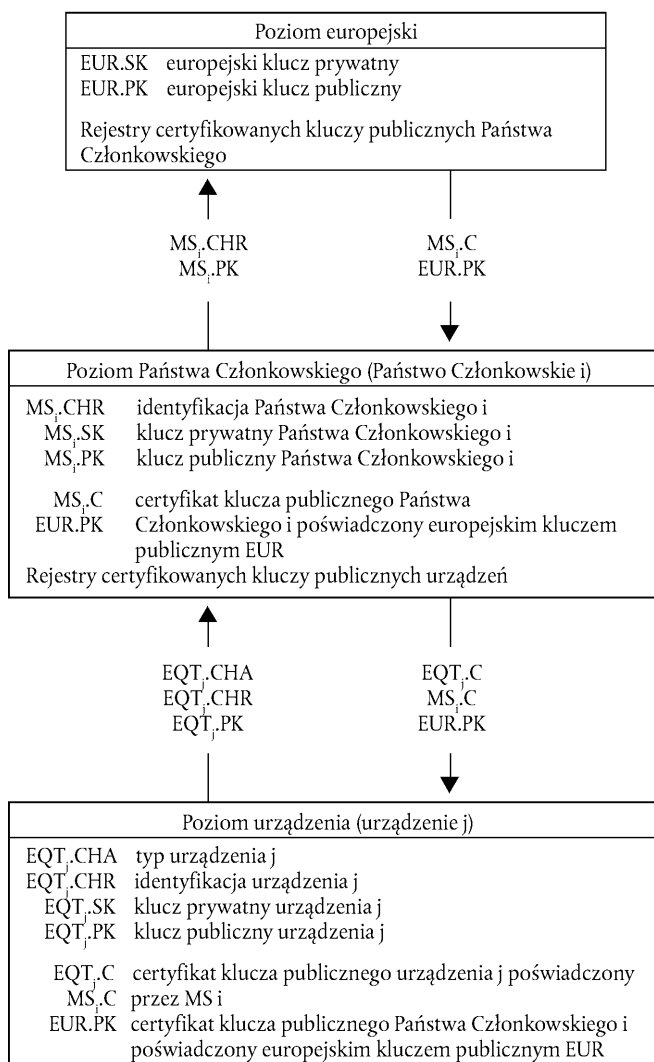
CSM_007 Na poziomie europejskim generuje się jedną parę kluczy europejskich (EUR.SK i EUR.PK). Do poświadczania kluczy publicznych Państw Członkowskich służy europejski klucz prywatny. Należy prowadzić rejestry wszystkich certyfikowanych kluczy. Organem realizującym za te zadania jest europejska jednostka certyfikująca, działająca z upoważnienia i na odpowiedzialność Komisji Europejskiej.

CSM_008 Na poziomie Państwa Członkowskiego generuje się parę kluczy Państwa Członkowskiego (MS.SK i MS.PK). Klucze publiczne Państwa Członkowskiego certyfikuje europejska jednostka certyfikująca. Klucza prywatnego Państwa Członkowskiego używa się do certyfikowania kluczy publicznych umieszczanych w urządzeniach (w przyrządzie rejestrującym lub karcie do tachografów). Należy prowadzić rejestry wszystkich certyfikowanych kluczy publicznych wraz z identyfikacją urządzeń, dla których są przewidziane. Organem realizującym te zadania jest jednostka certyfikująca Państwa Członkowskiego. Państwo Członkowskie może okresowo zmieniać swoją parę kluczy.

CSM_009 Na poziomie urządzenia generuje się jedną parę kluczy (EQT.SK i EQT.PK), którą wprowadza się do każdego urządzenia. Klucze publiczne urządzenia certyfikuje jednostka certyfikująca Państwa Członkowskiego. Zadanie te mogą realizować producenci urządzeń, jednostki personalizujące urządzenia lub organy Państwa Członkowskiego. Ta para kluczy służy do uwierzytelniania, składania podpisu cyfrowego i szyfrowania.

CSM_010 W czasie generowania, transportu (ewentualnego) i przechowywania należy zachować poufność kluczy prywatnych.

Na poniższym rysunku zobrazowano obieg danych zachodzący w tym procesie:



3.1.2. Klucze testowe RSA

CSM_011 Do celów testowania urządzeń (włącznie z testami współdziałania) europejska jednostka certyfikująca generuje różniące się pary kluczy, jedną europejską parę kluczy testowych i przynajmniej dwie pary kluczy testowych Państwa Członkowskiego, których klucze publiczne są poświadczone europejskim testowym kluczem prywatnym. Producenci umieszczają w urządzeniach przechodzących testy homologacji typu klucze testowe certyfikowane jednym z tych kluczy testowych Państwa Członkowskiego.

3.1.3. Klucze czujnika ruchu

W czasie generowania, transportu (ewentualnego) i przechowywania stosownie zachowuje się poufność trzech kluczy TDES opisanych poniżej

W celu wspierania urządzeń rejestrujących zgodnych z normą ISO 16844, europejska jednostka certyfikująca i organ certyfikacyjny Państwa Członkowskiego dodatkowo zapewniają, co następuje:

CSM_036 Europejska jednostka certyfikująca generuje $K_{m_{VU}}$ i $K_{m_{WC}}$, dwa niezależne i unikalne klucze Triple DES oraz generuje K_m jako:

$$K_m = K_{m_{VU}} \text{ XOR } K_{m_{WC}}$$

Europejska jednostka certyfikująca przesyła te klucze, z zachowaniem stosownych procedur bezpieczeństwa, organom certyfikacyjnym Państw Członkowskich na ich wniosek.

CSM_037 Organy certyfikacyjne Państw Członkowskich:

- używają K_m do szyfrowania danych czujnika ruchu wymaganych przez producentów czujników ruchu (dane są zaszyfrowane kluczem K_m w sposób zdefiniowany w normie ISO 16844-3),
- przesyłają klucz $K_{m_{VU}}$ producentom przyrządów rejestrujących, z zachowaniem stosownych procedur bezpieczeństwa, z przeznaczeniem do umieszczenia w przyrządach rejestrujących,
- zapewniają, że klucz $K_{m_{WC}}$ jest umieszczony we wszystkich kartach warsztatowych (*SensorInstallationSecData* w pliku elementarnym *Sensor_Installation_Data*) w czasie personalizacji kart.

3.1.4. Generowanie i dystrybucja kluczy sesji T-DES

CSM_012 Przyrządy rejestrujące i karty do tachografów, w ramach procesu wzajemnego uwierzytelnienia, generują i wymieniają niezbędne dane w celu uzyskania wspólnego klucza sesji Triple DES. Poufność tej wymiany informacji jest chroniona mechanizmem kryptograficznym RSA.

CSM_013 Klucz ten stosuje się we wszystkich późniejszych czynnościach kryptograficznych używając bezpiecznej wymiany komunikatów. Ważność tego klucza wygasa z końcem sesji (wyjęcie karty lub wyzerowanie karty) i/lub po 240 użyciach (jedno użycie klucza = jedno polecenie używające bezpiecznej wymiany komunikatów wysłane do karty i związana z tym odpowiedź).

3.2. Klucze

CSM_014 Długości kluczy RSA (niezależnie od poziomu) są następujące: moduł n 1024 bity, wykładnik publiczny e maksymalnie 64 bity, wykładnik prywatny d 1024 bity.

CSM_015 Klucze Triple DES są w postaci (K_a, K_b, K_c) , gdzie K_a i K_b są niezależnymi 64-bitowymi kluczami. Żadnych bitów wykrywania błędów parzystości nie wolno ustawiać.

3.3. Certyfikaty

CSM_016 Certyfikaty klucza publicznego RSA są certyfikatami »niesamoopisującymi« »Card Verifiable« (patrz norma: ISO/IEC 7816-8).

3.3.1. **Treść certyfikatu**

CSM_017 Certyfikaty klucza publicznego RSA zawierają następujące dane w określonym poniżej porządku:

Dane	Format	Bajty	Opis
CPI	INTEGER	1	Identyfikator profilu certyfikatu («01» dla tej wersji)
CAR	OCTET STRING	8	Odniesienie do jednostki certyfikującej
CHA	OCTET STRING	7	Upoważnienie posiadacza certyfikatu
EOV	TimeReal	4	Koniec terminu ważności certyfikatu. Opcjonalny, gdy nieużywany, wypełniony »FF«
CHR	OCTET STRING	8	Odniesienie do posiadacza certyfikatu
<i>n</i>	OCTET STRING	128	Klucz publiczny (moduł)
<i>e</i>	OCTET STRING	8	Klucz publiczny (wykładnik publiczny)
		164	

Uwagi:

1. »Identyfikator profilu certyfikatu« (CPI) wyznacza dokładną strukturę certyfikatu uwierzytelniania. Można go używać jako wewnętrznego identyfikatora urządzenia w stosownej liście nagłówkowej, która opisuje konkatencję elementów danych w certyfikacie.

Wykaz nagłówków związanych z treścią certyfikatu jest następujący:

„4D”	„16”	„5F 29”	„01”	„42”	„08”	„5F 4B”	„07”	„5F 24”	„04”	„5F 20”	„08”	„7F 49”	„05”	„81”	„81 80”	„82”	„08”
Znacznik rozszerzonej listy nagłówkowej	Długość listy nagłówkowej	Znacznik CPI	Długość CPI	Znacznik CAR	Długość CAR	Znacznik CHA	Długość CHA	Znacznik EOV	Długość EOV	Znacznik CHR	Długość CHR	Znacznik klucza publicznego (zbudowany)	Długość dalszych DO	Znacznik modułu	Długość modułu	Znacznik wykładnika publicznego	Długość wykładnika publicznego

2. »Odniesienie do jednostki certyfikującej« (CAR) ma na celu identyfikację CA wydającej certyfikat, w taki sposób, że ten element danych może być użyty jednocześnie jako identyfikator klucza organu w celu odniesienia do klucza publicznego jednostki certyfikującej (kodowanie — patrz Identyfikator klucza poniżej).
3. »Upoważnienie posiadacza certyfikatu« ((CHA) służy do identyfikowania praw posiadacza certyfikatu. Składa się z ID aplikacji tachograficznej i typu urządzenia, dla którego certyfikat jest przeznaczony (zgodnie z elementem danych EquipmentType, »00« dla Państwa Członkowskiego).
4. »Odniesienie do posiadacza certyfikatu« (CHR) ma na celu jednoznaczną identyfikację posiadacza certyfikatu, w taki sposób, że ten element danych może być użyty jednocześnie jako identyfikator klucza podmiotu w celu odniesienia do posiadacza certyfikatu klucza publicznego.
5. Identyfikatory kluczy jednoznacznie identyfikują posiadacza certyfikatu lub organy certyfikujące. Są one kodowane w następujący sposób:

5.1. Urządzenie (VU lub karta):

Dane	Numer fabryczny urządzenia	Data	Typ	Producent
Długość	4 bajty	2 bajty	1 bajt	1 bajt
wartość	integer	mm rr w kodzie BCD	swoisty dla producenta	kod producenta

W przypadku VU producent, gdy wnioskuję o certyfikaty, może, ale nie musi znać identyfikację urządzenia, do którego mają być wstawione klucze.

W pierwszym przypadku producent wysyła identyfikację urządzenia z kluczem publicznym do organu certyfikacyjnego swojego Państwa Członkowskiego. W tym przypadku certyfikat zawiera identyfikację urządzenia i producent musi zapewnić, że klucze i certyfikat są wstawione do przewidzianego urządzenia. Identyfikator klucza ma postać pokazaną powyżej.

W drugim przypadku producent musi tylko identyfikować każdy wniosek o certyfikat i wysłać tę identyfikację z kluczem publicznym do organu certyfikacyjnego swojego Państwa Członkowskiego. W tym przypadku certyfikat zawiera wnioskowaną identyfikację. Po zainstalowaniu klucza w urządzeniu producent musi zawiadomić zwrótnie organ certyfikacyjny swojego Państwa Członkowskiego o przyporządkowaniu klucza do urządzenia (tj. podać identyfikację wniosku o certyfikat, identyfikację urządzenia). Identyfikator klucza ma postać pokazaną poniżej:

Dane	Numer fabryczny wniosku o certyfikat	Data	Typ	Producent
Długość	4 bajty	2 bajty	1 bajt	1 bajt
Wartość	kod BCD	mm rr w kodzie BCD	'FF'	kod producenta

5.2. Jednostka certyfikująca::

Dane	Identyfikacja organu	Numer fabryczny klucza	Dodatkowe informacje	Identyfikator
Długość	4 bajty	1 bajt	2 bajty	1 bajt
Wartość	1-bajtowy kod numeryczny państwa 3-bajtowy kod alfanumeryczny państwa	Integer	dodatkowe informacje (swoista dla CA) 'FF FF' gdy nie jest używany	'01'

Numer fabryczny klucza służy do rozróżniania różnych kluczy Państwa Członkowskiego, w przypadku zmiany klucza.

- Urządzenia kontrolne wiedzą niejawnie, że certyfikowany klucz publiczny jest kluczem RSA właściwym do uwierzytelnienia, sprawdzenia podpisu cyfrowego i szyfrowania dla poufnych usług (certyfikat nie zawiera identyfikatora obiektu, który by to określał).

3.3.2. Wydane certyfikaty

CSM_018 Wydany certyfikat jest podpisem cyfrowym z częściowym odzyskiwaniem treści certyfikatu zgodnie z normą ISO/IEC 9796-2, z dołączonym »odniesieniem do jednostki certyfikującej«.

$$X.C = X.CA.SK['6A' || C_r || Hash(Cc) || 'BC'] || C_n || X.CAR$$

$$\text{z treścią certyfikatu} \quad = Cc = \begin{matrix} C_r \\ 106 \text{ Bytes} \end{matrix} || \begin{matrix} C_n \\ 58 \text{ Bytes} \end{matrix}$$

Uwagi:

- Ten certyfikat zawiera 194 bajty.
- CAR, utajniony podpisem, jest również dołączony do podpisu, tak że do weryfikacji certyfikatu można wybrać klucz publiczny jednostki certyfikującej.
- Urządzenia kontrolne znają niejawnie algorytm użyty przez jednostkę certyfikującą do podpisania certyfikatu.

4. Wykaz nagłówków związanych z wydanym certyfikatem jest następujący:

„7F 21”	„09”	„5F 37”	„81 80”	„5F 38”	„3A”	„42”	„08”
Znacznik certyfikatu CV (budowany)	Długość następnego DO	Znacznik podpisu	Długość podpisu	Znacznik reszty	Długość reszty	Znacznik CAR	Długość CAR

3.3.3. Weryfikacja i rozpakowanie certyfikatu

Weryfikacja i rozpakowanie certyfikatu obejmuje sprawdzenie podpisu zgodnie z normą ISO/IEC 9796-2, odzyskanie treści certyfikatu i klucza publicznego: $X.PK = X.CA.PK.X.C$, oraz sprawdzenie ważności certyfikatu.

CSM_019 Wykonuje się to w następujących krokach:

weryfikacja podpisu i odzyskanie treści:

- z $X.C$ odzyskaj $Sign$, C_n i CAR' :

$$X.C = \begin{matrix} Sign \\ 128 \text{ Bytes} \end{matrix} \parallel \begin{matrix} C_n' \\ 58 \text{ Bytes} \end{matrix} \parallel \begin{matrix} CAR' \\ 8 \text{ Bytes} \end{matrix}$$
- z CAR' wybierz odpowiednio klucz publiczny jednostki certyfikującej (jeżeli nie uzyskano go wcześniej innymi środkami)
- odtwórz $Sign$ z klucza publicznego CA : $Sr' = X.CA.PK [Sign]$,
- sprawdź czy Sr' zaczyna się od '6A' i kończy 'BC'
- oblicz Cr' i H' z:

$$Sr' = \begin{matrix} '6A' \\ 106 \text{ Bytes} \end{matrix} \parallel \begin{matrix} Cr' \\ 106 \text{ Bytes} \end{matrix} \parallel \begin{matrix} H' \\ 20 \text{ Bytes} \end{matrix} \parallel \begin{matrix} 'BC' \end{matrix}$$
- odzyskaj treść certyfikatu $C' = C_r' \parallel C_n'$,
- sprawdź $Hash(C') = H'$

Jeżeli kontrole są OK, certyfikat jest prawdziwy, treścią certyfikatu jest C' .

Sprawdzenie ważności z C' :

- gdy dotyczy, sprawdź koniec daty ważności,

odzyskaj i zachowaj klucz publiczny, identyfikator klucza, upoważnienie posiadacza certyfikatu i koniec ważności certyfikatu z C' :

- $X.PK = n \parallel e$,
- $X.KID = CHR$
- $X.CHA = CHA$
- $X.EOV = EOV$.

4. MECHANIZM WZAJEMNEGO UWIERZYTELNIENIA

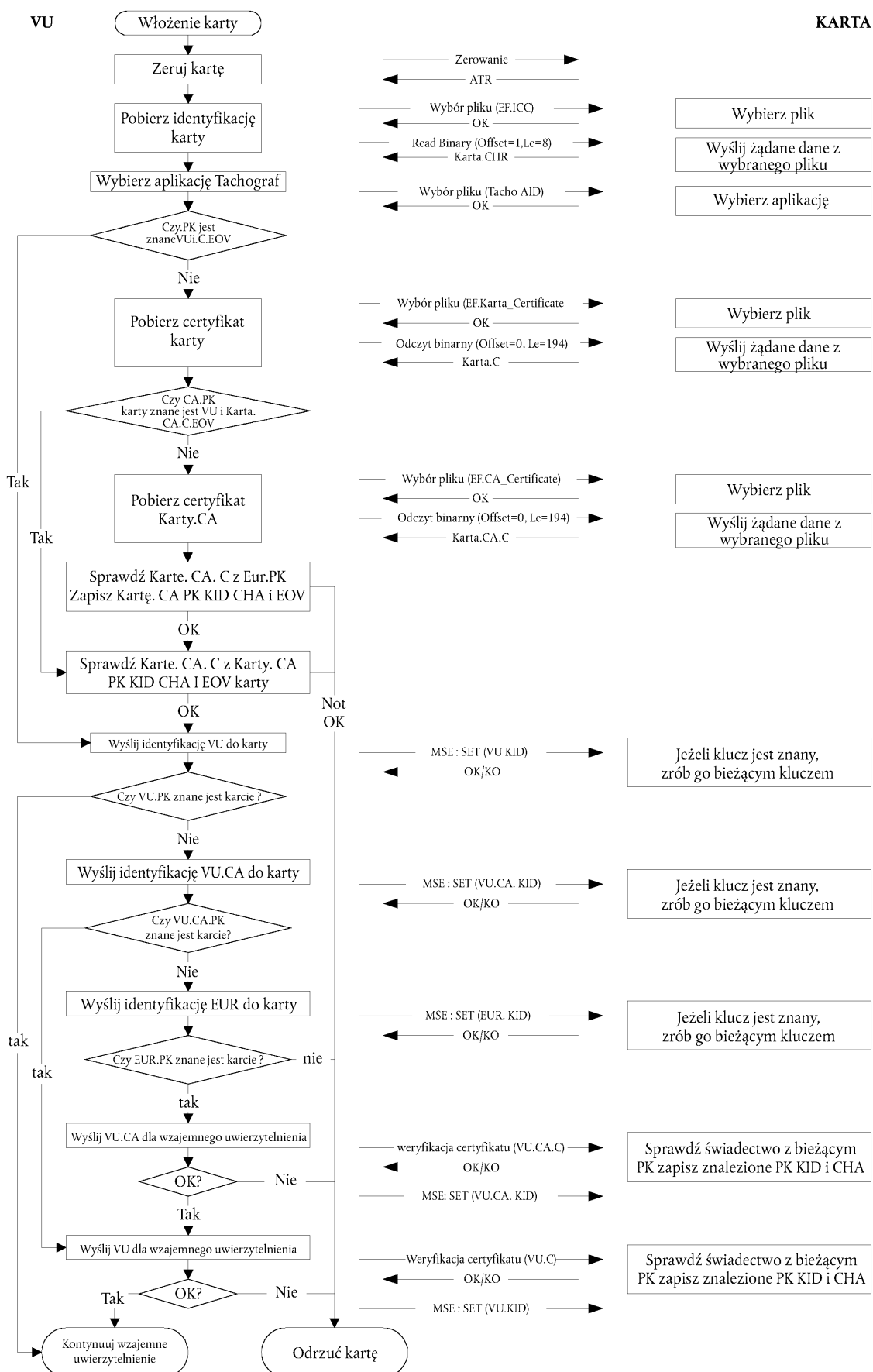
Wzajemne uwierzytelnienie między kartami a urządzeniami VU odbywa się według opisanej poniżej zasady:

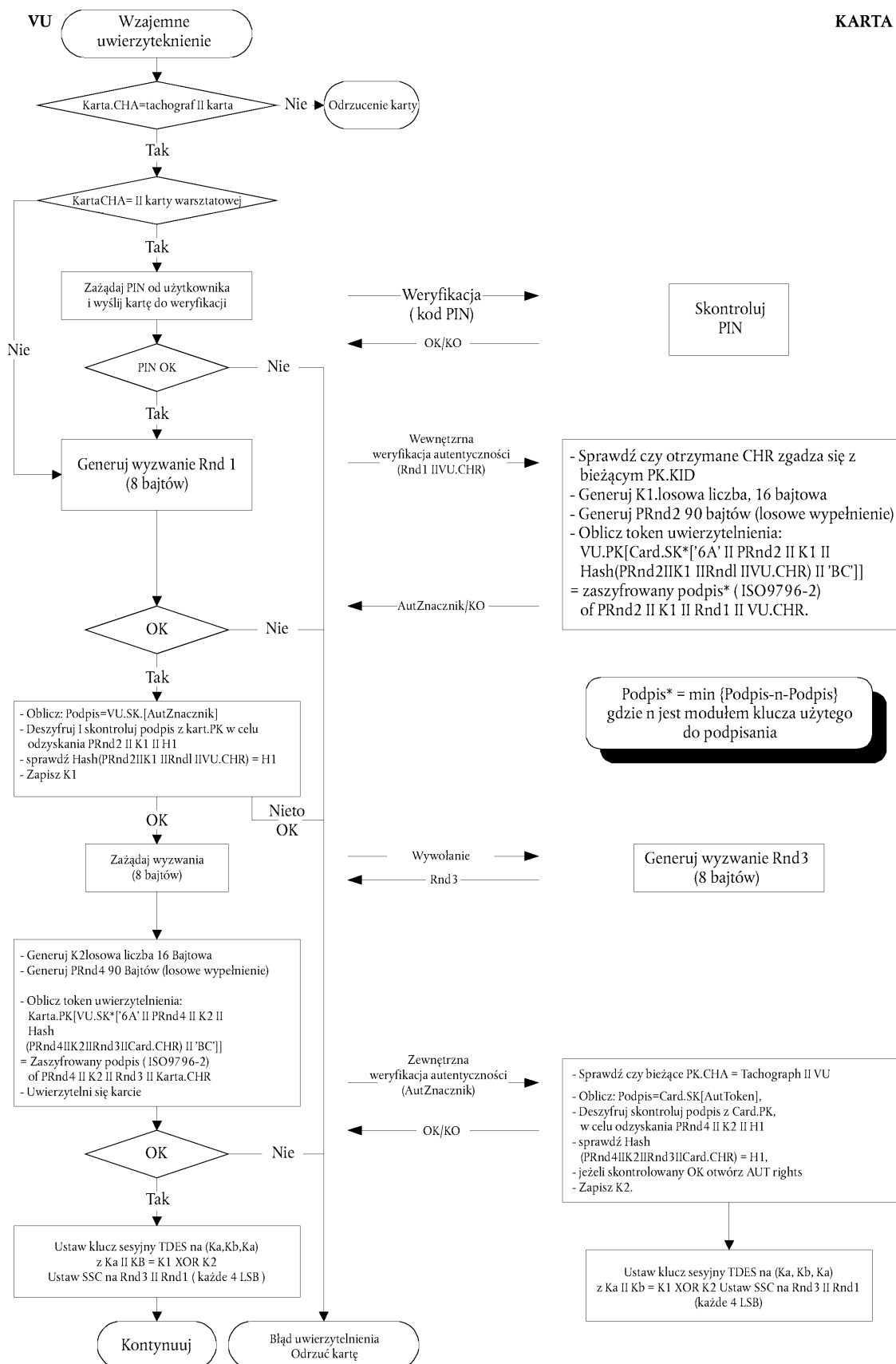
Każda strona wykazuje drugiej, że posiada ważną parę kluczy, z której klucz publiczny jest certyfikowany przez jednostkę certyfikującą Państwa Członkowskiego, która jest certyfikowana przez europejską jednostkę certyfikującą.

Wykazanie polega na podpisaniu kluczem prywatnym losowej liczby przysłanej przez drugą stronę, która musi odzyskać tę liczbę przy sprawdzaniu tego podpisu.

VU uruchamia ten mechanizm uruchomiony przy wkładaniu karty. Rozpoczyna się od wymiany certyfikatów i rozpakowaniu kluczy publicznych i kończy ustaleniem klucza sesyjnego.

CSM_020 W procesie tym stosuje się następujący protokół (strzałki oznaczają polecenia i wymianę danych (patrz dodatek 2)):





5. POUFNOŚĆ, INTEGRALNOŚĆ I MECHANIZMY UWIERZYTELNIANIA PRZESYŁANIA DANYCH MIĘDZY VU A KARTAMI

5.1. Bezpieczna wymiana komunikatów

- CSM_021 Bezpieczna wymiana komunikatów chroni integralność przesyłania danych VU-karty zgodnie z normami (ISO/IEC 7816-4) i (ISO/IEC 7816-8).
- CSM_022 Gdy dane powinny być chronione podczas przesyłania, do obiektów danych wysyłanych w poleceniu lub odpowiedzi dołącza się obiekt danych z kryptograficzną sumą kontrolną. Kryptograficzną sumę kontrolną weryfikuje odbiorca.
- CSM_023 Kryptograficzna suma kontrolna danych wysyłanych w poleceniu integruje nagłówek polecenia i wszystkie wysłane obiekty danych (= > CLA = '0C', a wszystkie obiekty danych są hermetycznie zamknięte ze znacznikami, w których b1 = 1).
- CSM_024 Bajty statusu-informacyjne odpowiedzi są chronione przez kryptograficzną sumę kontrolną, gdy w odpowiedzi nie ma pola danych.
- CSM_025 Kryptograficzne sumy kontrolne składają się z czterech bajtów.

Struktura poleceń i odpowiedzi, gdy przesyłane są przy użyciu bezpiecznej wymiany komunikatów, jest następująca:

Używane obiekty DO są częściowym zbiorem DO bezpiecznej wymiany komunikatów opisanej w normie ISO/IEC 7816-4:

Znacznik	Mnemonik	Znaczenie
'81'	T _{PV}	Odkryta wartość danych niekodowanych w BER-TLV (chroniona przez CC)
'97'	T _{LE}	Wartość Le w niechronionym poleceniu (chroniona przez CC)
'99'	T _{SW}	Status-Info (chronione przez CC)
'8E'	T _{CC}	Kryptograficzna suma kontrolna
'87'	T _{PI CG}	Bajt wskaźnika wypełniania Kryptogram (odkryta wartość niekodowana w BER-TLV)

Dla danej pary niechronionych polecenia — odpowiedzi:

Nagłówek polecenia	Treść polecenia
CLA INS P1 P2	(L _c -pole)(pole danych) (L _c -pole)
cztery bajty	L bajtów, oznaczone B ₁ do B _L

Treść odpowiedzi	Stopka odpowiedzi
(Pole danych)	SW1 SW2
L _r bajty danych	dwa bajty

Odpowiadającą parą chronionych polecenia — odpowiedzi jest:

Chronione polecenie:

Nagłówek polecenia (CH)				Treść polecenia										
CLA	INS	P1	P2	(nowe pole L _C)	(nowe pole danych)							(nowe pole L _C)		
'OC'				Długość nowego pola danych	T _{PV}	L _{PV}	PV	T _{LE}	L _{LE}	L _e	T _{CC}	L _{CC}	CC	'00'
					'81'	L _c	pole danych	'97'	'01'	L _e	'8E'	'04'	CC	

Dane integrowane w sumie kontrolnej = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_c || PB

PB = bajty wypełniające (80.. 00) zgodnie z normami ISO-IEC 7816-4 i ISO 9797 metoda 1.

Obiekty DO PV i LE występują tylko wtedy gdy są pewne odpowiednia dane w niechronionym poleceniu.

Chroniona odpowiedź:

1. Przypadek, gdy pole danych odpowiedzi nie jest puste i nie wymaga ochrony poufności:

Treść odpowiedzi						Stopka odpowiedzi
(nowe pole danych)						nowe SW1 SW2
T _{PV}	L _{PV}	PV	T _{CC}	L _{CC}	CC	
'81'	L _r	pole danych	'8E'	'04'	CC	

Dane zintegrowane w sumie kontrolnej = T_{PV} || L_{PV} || PV || PB

2. Przypadek, gdy pole danych odpowiedzi nie jest puste i wymaga ochrony poufności:

Treść odpowiedzi						Stopka odpowiedzi
(nowe pole danych)						nowe SW1 SW2
T _{PI CG}	L _{PI CG}	PI CG	T _{CC}	L _{CC}	CC	
'87'		PI CG	'8E'	'04'	CC	

Dane przenoszone przez CG: dane niekodowane w BER-TLV i bajty wypełnienia.

Dane zintegrowane w sumie kontrolnej = T_{PI CG} || L_{PI CG} || PI CG || PB

3. Przypadek, gdy pole danych odpowiedzi jest puste:

Treść odpowiedzi						Stopka odpowiedzi
(nowe pole danych)						nowe SW1 SW2
T _{SW}	L _{SW}	SW	T _{CC}	L _{CC}	CC	
'99'	'02'	New SW1 SW2	'8E'	'04'	CC	

Dane zintegrowane w sumie kontrolnej = T_{SW} || L_{SW} || SW || PB

5.2. Obsługa błędów w bezpiecznej wymianie komunikatów

CSM_026 Gdy karta do tachografów wykryje błąd SM podczas interpretowania polecenia, w odpowiedzi musi zwrócić bajty stanu bez SM. Zgodnie z normą ISO/IEC 7816-4, błędy SM wskazuje się następującymi bajtami stanu:

- '66 88' błąd sprawdzenia kryptograficznej sumy kontrolnej,
- '69 87' brak oczekiwanych obiektów danych SM,
- '69 88' nieprawidłowe obiekty danych SM.

CSM_027 W przypadku, gdy karta do tachografów zwraca bajty stanu bez obiektów danych, SM lub z błędnym obiektem danych SM, VU musi przerwać sesję.

5.3. Algorytm obliczania kryptograficznych sum kontrolnych

CSM_028 Kryptograficzne sumy kontrolne tworzy się przy pomocy jednokierunkowej funkcji skrótu MAC zgodnie z normą ANSI X9.19 z DES:

- etap początkowy: początkowy blok kontrolny y_0 jest $E(K_a, SSC)$.
- etap sekwencyjny: bloki kontrolne $y_1, \dots, y_n$ oblicza się przy pomocy K_a .
- etap końcowy: kryptograficzną sumę kontrolną oblicza się z ostatniego bloku y_n jako: $E(K_a, D(K_b, y_n))$.

gdzie $E()$ oznacza szyfrowanie DES, a $D()$ oznacza deszyfrowanie DES.

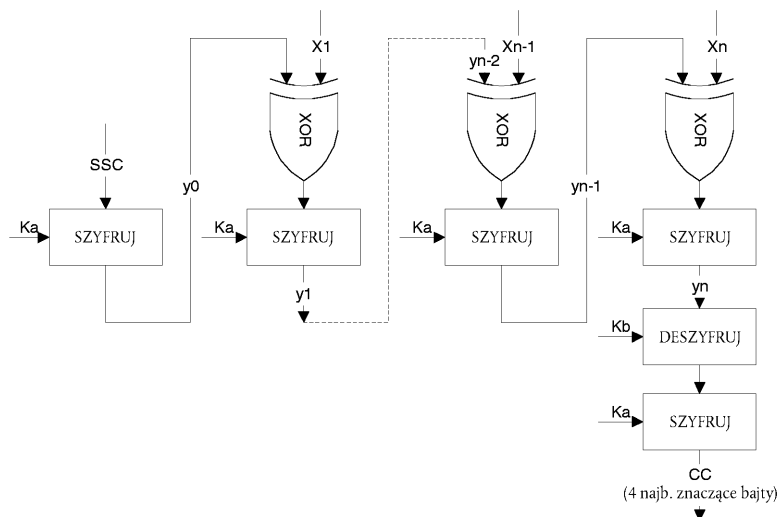
Cztery najbardziej znaczące bajty kryptograficznej sumy kontrolnej są przesyłane.

CSM_029 Licznik sekwencji wysyłania (SSC) jest inicjowany podczas procedury uzgadniania klucza:

początkowy SSC: Rnd3 (4 najmniej znaczące bajty) || Rnd1 (4 najmniej znaczące bajty).

CSM_030 Licznik SSC zwiększa się za każdym razem o 1 przed obliczeniem MAC (tj. SSC dla pierwszego polecenia będzie początkowy SSC + 1, SSC dla pierwszej odpowiedzi będzie początkowy SSC + 2).

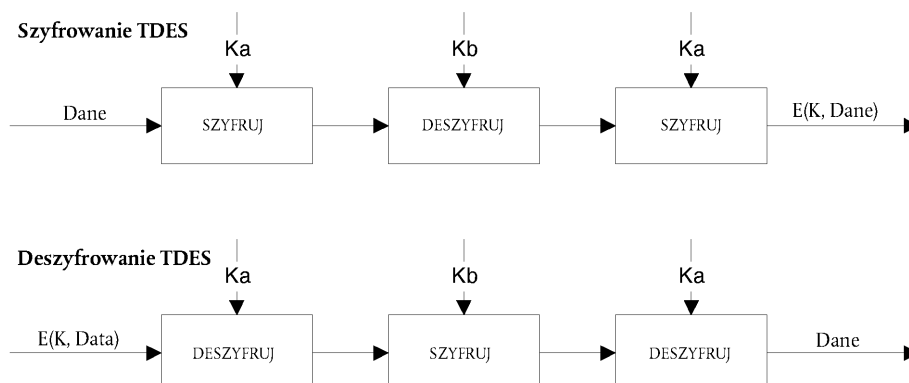
Na poniższym rysunku pokazano obliczenie skrótu MAC:



5.4. Algorytm obliczania kryptogramów dla poufnych obiektów danych

CSM_031 Kryptogramy oblicza się przy pomocy TDEA w trybie pracy TCBC zgodnie z odniesieniami (TDES) i (TDES-OP) i wektorem zerowym jako blokiem wartości początkowych.

Na poniższym rysunku pokazano zastosowanie kluczy w TDES:



6. MECHANIZMY CYFROWEGO PODPISU DLA WCZYTYWANIA DANYCH

CSM_032 Inteligentne urządzenie dedykowane (IDE) przechowuje dane otrzymane z urządzenia (VU lub karty) podczas jednej sesji wczytywania w fizycznie jednym pliku danych. Plik ten musi zawierać certyfikaty MSi.C i EQT.C. Plik zawiera podpisy cyfrowe bloków danych zgodnie z opisem znajdującym się w dodatku 7 Protokoły wczytywania danych.

CSM_033 Podpisy cyfrowe wczytanych danych korzystają ze schematu podpisu cyfrowego z tym że gdy trzeba, wczytane dane można odczytać bez deszyfrowania.

6.1. Generowanie podpisu

CSM_034 Urządzenie generuje podpis danych zgodnie ze schematem podpisu z dodatkiem zdefiniowanym w (PKCS1) z funkcją skrótu SHA-1:

$$\text{Podpis} = \text{EQT.SK}[\text{'00'} \parallel \text{'01'} \parallel \text{PS} \parallel \text{'00'} \parallel \text{DER}(\text{SHA-1}(\text{Data}))]$$

PS Wypełnienie łańcuchem oktetów z wartością 'FF' do długości 128.

DER(SHA-1(M)) jest identyfikatorem algorytmu kodującego dla funkcji skrótu a wartość skrótu jest wartością w ASN.1 typu DigestInfo (wyróżnione reguły kodowania):

'30' || '21' || '30' || '09' || '06' || '05' || '2B' || '0E' || '03' || '02' || '1A' || '05' || '00' || '04' || '14' || Hash Value.

6.2. Sprawdzenie podpisu

CSM_035 Sprawdzenie podpisu danych dla wczytanych danych odbywa się zgodnie ze schematem podpisu z dodatkiem zdefiniowanym w (PKCS1) z funkcją skrótu SHA-1.

Urządzenie kontrolne musi znać niezależnie (powierzony) europejski klucz publiczny EUR.PK.

Na schemacie poniżej zilustrowano protokół przenoszenia IDE, z którego może korzystać karta kontrolna przy sprawdzaniu integralności danych wczytanych i zapisanych na zewnętrznym nośniku ESM. Karta kontrolna służy do deszyfrowania podpisów cyfrowych. W tym przypadku ta funkcja nie musi być zaimplementowana w IDE.

Urządzenie, które wczytuje i podpisuje dane przeznaczone do analizowania, oznaczono EQT.

