

II

(Akty o charakterze nieustawodawczym)

ROZPORZĄDZENIA

ROZPORZĄDZENIE wykonawcze Komisji (UE) 2018/502

z dnia 28 lutego 2018 r.

zmieniające rozporządzenie wykonawcze Komisji (UE) 2016/799 ustanawiające wymogi dotyczące budowy, sprawdzania, instalacji, użytkowania i naprawy tachografów oraz ich elementów składowych

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 165/2014 z dnia 4 lutego 2014 r. w sprawie tachografów stosowanych w transporcie drogowym ⁽¹⁾, w szczególności jego art. 11 i art. 12 ust. 7,

a także mając na uwadze, co następuje:

- (1) Rozporządzeniem (UE) nr 165/2014 wprowadzono tachografy inteligentne, stanowiące drugą generację tachografów cyfrowych, które obejmują połączenie z urządzeniem globalnego systemu nawigacji satelitarnej („GNSS”), urządzenie wczesnego wykrywania na odległość oraz fakultatywny interfejs do inteligentnych systemów transportowych.
- (2) Wymogi techniczne dotyczące budowy, sprawdzania, instalacji, użytkowania i naprawy tachografów oraz ich elementów składowych określono w rozporządzeniu wykonawczym Komisji (UE) 2016/799 ⁽²⁾.
- (3) Zgodnie z art. 8, 9 i 10 rozporządzenia (UE) nr 165/2014 tachografy instalowane w pojazdach zarejestrowanych po raz pierwszy w dniu 15 czerwca 2019 r. lub po tej dacie muszą być tachografami inteligentnymi. Należy zatem zmienić rozporządzenie wykonawcze (UE) 2016/799, aby określone w nim przepisy techniczne miały zastosowanie począwszy od powyższej daty.
- (4) W celu spełnienia wymogów określonych w art. 8 rozporządzenia (UE) nr 165/2014, określającym, że położenie pojazdu musi być zapisywane co trzy godziny skumulowanego czasu prowadzenia pojazdu, należy zmienić rozporządzenie wykonawcze (UE) 2016/799, aby umożliwić przechowywanie informacji o położeniu pojazdu z częstotliwością 3 godzin, przy użyciu wskaźnika, którego nie można zerować, oraz aby uniknąć pomylenia z „nieprzerwanym czasem prowadzenia pojazdu”, który jest wskaźnikiem o innej funkcji.
- (5) Przyrząd rejestrujący może być pojedynczą jednostką lub kilkoma jednostkami rozmieszczonymi w pojeździe. Urządzenia GNSS i wydzielonej łączności krótkiego zasięgu („DSRC”) mogą zatem być zewnętrzne lub wewnętrzne w stosunku do jednostki głównej przyrządu rejestrującego. W przypadku gdy są one zewnętrzne, powinna istnieć możliwość, aby zarówno urządzenia, jak i jednostka główna przyrządu rejestrującego mogły uzyskać homologację typu jako elementy składowe w celu dostosowania procesu homologacji typu tachografów inteligentnych do potrzeb rynku.
- (6) Należy zmodyfikować przepisy dotyczące zdarzeń konfliktu czasu i korekt czasu w celu rozróżnienia automatycznych korekt czasu uruchamianych w następstwie ewentualnej próby manipulacji tachografem bądź jego wadliwego działania, jak i korekt czasu spowodowanych innymi przyczynami, np. konserwacją.
- (7) Identyfikatory danych powinny być w stanie dokonać rozróżnienia danych pobranych z tachografu inteligentnego i danych pobranych w tachografu wcześniejszej generacji.

⁽¹⁾ Dz.U. L 60 z 28.2.2014, s. 1.

⁽²⁾ Rozporządzenie wykonawcze Komisji (UE) 2016/799 z dnia 18 marca 2016 r. w sprawie wykonania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 165/2014 ustanawiającego wymogi dotyczące budowy, sprawdzania, instalacji, użytkowania i naprawy tachografów oraz ich elementów składowych (Dz.U. L 139 z 26.5.2016, s. 1).

- (8) Okres ważności karty firmowej należy przedłużyć z dwóch do pięciu lat, aby ujednoczyć go z okresem ważności karty kierowcy.
- (9) Należy lepiej doprecyzować opis pewnych usterek i zdarzeń, zatwierdzanie wpisów miejsc rozpoczęcia lub zakończenia dziennych okresów pracy, wykorzystywanie zgody kierowcy dotyczącej interfejsu do inteligentnego systemu transportowego („ITS”) odnośnie do danych przekazywanych przez przyrząd rejestrujący za pośrednictwem sieci pojazdu, a także inne kwestie techniczne.
- (10) W celu zapewnienia uaktualnienia certyfikacji plomb tachografu należy je dostosować do nowej normy dotyczącej zabezpieczeń plomb mechanicznych stosowanych w tachografach.
- (11) Niniejsze rozporządzenie dotyczy budowy, sprawdzania, instalacji i użytkowania systemów, w skład których wchodzi również urządzenia radiowe podlegające przepisom dyrektywy Parlamentu Europejskiego i Rady 2014/53/UE ⁽¹⁾. We wspomnianej dyrektywie uregulowano kwestie udostępniania na rynku i oddawania do użytku urządzeń elektronicznych i elektrycznych wykorzystujących fale radiowe na potrzeby komunikacji lub radiolokacji na poziomie horyzontalnym, ze szczególnym uwzględnieniem bezpieczeństwa elektrycznego, zgodności z innymi systemami, dostępu do widma radiowego, dostępu do służb ratunkowych lub wszelkich dodatkowych przepisów delegowanych. W celu zagwarantowania efektywnego korzystania z widma radiowego, unikania szkodliwych zakłóceń, zapewnienia bezpieczeństwa i kompatybilności elektromagnetycznej urządzeń radiowych oraz dopuszczenia wszelkich innych specjalnych wymogów delegowanych niniejsze rozporządzenie nie powinno naruszać przepisów wspomnianej dyrektywy.
- (12) Należy zatem zmienić rozporządzenie wykonawcze (UE) 2016/799.
- (13) Środki przewidziane w niniejszym rozporządzeniu są zgodne z opinią komitetu, o którym mowa w art. 42 ust. 3 rozporządzenia (UE) nr 165/2014,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

W rozporządzeniu wykonawczym (UE) 2016/799 wprowadza się następujące zmiany:

1) w art. 1 wprowadza się następujące zmiany:

a) ustępy 2 i 3 otrzymują brzmienie:

„2. Budowa, sprawdzanie, instalacja, kontrola, użytkowanie i naprawa tachografów inteligentnych i ich elementów składowych muszą być zgodne z wymogami technicznymi określonymi w załączniku IC do niniejszego rozporządzenia.

3. Tachografy inne niż tachografy inteligentne muszą nadal spełniać, jeśli chodzi o ich budowę, sprawdzanie, instalację, kontrolę, użytkowanie i naprawę, wymogi zawarte w załączniku I do rozporządzenia (UE) nr 165/2014 albo w załączniku IB do rozporządzenia Rady (EWG) nr 3821/85 ^(*), stosownie do przypadku.

^(*) Rozporządzenie Rady (EWG) nr 3821/85 z dnia 20 grudnia 1985 r. w sprawie urządzeń rejestrujących stosowanych w transporcie drogowym (Dz.U. L 370 z 31.12.1985, s. 8).”;

b) dodaje się ust. 5 w brzmieniu:

„5. Niniejsze rozporządzenie nie narusza przepisów dyrektywy Parlamentu Europejskiego i Rady 2014/53/UE ^(*).

^(*) Dyrektywa Parlamentu Europejskiego i Rady 2014/53/UE z dnia 16 kwietnia 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich dotyczących udostępniania na rynku urządzeń radiowych i uchylająca dyrektywę 1999/5/WE (Dz.U. L 153 z 22.5.2014, s. 62).”;

2) w art. 2 wprowadza się następujące zmiany:

a) definicja 3 otrzymuje brzmienie:

„3) »folder informacyjny« oznacza pełny folder, w formie elektronicznej lub papierowej, zawierający wszystkie informacje dostarczone przez producenta lub jego przedstawiciela organowi udzielającemu homologacji typu na potrzeby homologacji typu tachografu lub jego elementu składowego, w tym certyfikaty, o których mowa w art. 12 ust. 3 rozporządzenia (UE) nr 165/2014, wyniki testów przewidzianych w załączniku IC do niniejszego rozporządzenia, a także rysunki, fotografie i inne istotne dokumenty”;

⁽¹⁾ Dyrektywa Parlamentu Europejskiego i Rady 2014/53/UE z dnia 16 kwietnia 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich dotyczących udostępniania na rynku urządzeń radiowych i uchylająca dyrektywę 1999/5/WE, Dz.U. L 153 z 22.5.2014, s. 62.

b) definicja 7 otrzymuje brzmienie:

„7) »tachograf inteligentny« lub »tachograf drugiej generacji« oznacza tachograf cyfrowy spełniający wymogi art. 8, 9 i 10 rozporządzenia (UE) nr 165/2014 oraz załącznika IC do niniejszego rozporządzenia;”;

c) definicja 8 otrzymuje brzmienie:

„8) »element składowy tachografu« oznacza dowolny z następujących elementów: przyrząd rejestrujący, czujnik ruchu, wykresówka, urządzenie zewnętrzne GNSS oraz zewnętrzne urządzenie wczesnego wykrywania na odległość;”;

d) dodaje się następującą definicję 10:

„10) »przyrząd rejestrujący« oznacza tachograf bez czujnika ruchu i przewodów do przyłączenia czujnika ruchu.

Może to być pojedyncza jednostka lub kilka jednostek rozmieszczonych w pojeździe, składających się z jednostki przetwarzającej, pamięci danych, funkcji pomiaru czasu, dwóch czytników kart inteligentnych (dla kierowcy i współkierowcy), drukarki, wyświetlacza, złącz i urządzeń do wprowadzania danych przez użytkownika, odbiornika GNSS i urządzenia do łączności na odległość.

Przyrząd rejestrujący może się składać z następujących elementów składowych podlegających homologacji typu:

- urządzenie rejestrujące jako jeden element składowy (obejmujący odbiornik GNSS i urządzenie do łączności na odległość),
- jednostka główna przyrządu rejestrującego (obejmująca urządzenie do łączności na odległość) i urządzenie zewnętrzne GNSS,
- jednostka główna przyrządu rejestrującego (obejmująca odbiornik GNSS) i zewnętrzne urządzenie do łączności na odległość,
- jednostka główna przyrządu rejestrującego, urządzenie zewnętrzne GNSS i zewnętrzne urządzenie do łączności na odległość.

Jeżeli przyrząd rejestrujący składa się z kilku jednostek rozmieszczonych w pojeździe, jednostką główną przyrządu rejestrującego jest jednostka zawierająca jednostkę przetwarzającą, pamięć danych i funkcję pomiaru czasu.

Określenie »przyrząd rejestrujący« stosuje się w odniesieniu do »przyrządu rejestrującego« lub »jednostki głównej przyrządu rejestrującego«.”;

3) w art. 6 akapit trzeci otrzymuje brzmienie:

„Załącznik IC stosuje się jednak od dnia 15 czerwca 2019 r., z wyjątkiem dodatku 16, który stosuje się od dnia 2 marca 2016 r.”;

4) w załączniku IC wprowadza się zmiany zgodnie z załącznikiem I do niniejszego rozporządzenia;

5) w załączniku II wprowadza się zmiany zgodnie z załącznikiem II do niniejszego rozporządzenia.

Artykuł 2

Wejście w życie

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia 28 lutego 2018 r.

W imieniu Komisji
Jean-Claude JUNCKER
Przewodniczący

ZAŁĄCZNIK I

W załączniku IC do rozporządzenia (UE) 2016/799 wprowadza się następujące zmiany:

1) w spisie treści wprowadza się następujące zmiany:

a) punkt 3.12.5. otrzymuje brzmienie:

„3.12.5. Miejsca i pozycje, w których zaczynają się i kończą dzienne okresy pracy lub w których osiągnięto 3 godziny skumulowanego czasu prowadzenia pojazdu”;

b) pkt 4.5.3.2.16 otrzymuje brzmienie:

„4.5.3.2.16 Dane miejsc, w których minęły trzy godziny skumulowanego czasu prowadzenia pojazdu”;

c) pkt 4.5.4.2.14 otrzymuje brzmienie:

„4.5.4.2.14 Dane miejsc, w których minęły trzy godziny skumulowanego czasu prowadzenia pojazdu”;

d) pkt 6.2 otrzymuje brzmienie:

„6.2. Kontrola techniczna elementów składowych nowych i po naprawie”;

2) w pkt 1 wprowadza się następujące zmiany:

a) definicja ll) otrzymuje brzmienie:

„ll) »urządzenie do łączności na odległość« lub »urządzenie wczesnego wykrywania na odległość« oznacza:

wyposażenie przyrządu rejestrującego, które jest używane do przeprowadzania ukierunkowanych kontroli drogowych;”;

b) definicja tt) otrzymuje brzmienie:

„tt) »korekta czasu« oznacza:

korektę bieżącego czasu; może ona być automatyczna w regularnych odstępach z wykorzystaniem czasu podawanego przez odbiornik GNSS jako odniesienia lub wykonywana w trybie kalibracyjnym;”;

c) tiret pierwsze definicji yy) otrzymuje brzmienie:

„— które jest zainstalowane i stosowane wyłącznie w pojazdach kategorii M1 i N1 (określonych w załączniku II do dyrektywy 2007/46/WE Parlamentu Europejskiego i Rady (*) z późniejszymi zmianami);”;

d) dodaje się nową definicję fff):

„(fff) »skumulowany czas prowadzenia pojazdu« oznacza:

wartość odpowiadającą łącznej skumulowanej liczbie minut prowadzenia danego pojazdu.

Wartość skumulowanego czasu prowadzenia pojazdu to nieprzerwana liczba wszystkich minut uznanych przez funkcję monitorowania czynności prowadzenia pojazdu urządzenia rejestrującego za PROWADZENIE POJAZDU i jest wykorzystywana wyłącznie do uruchomienia rejestracji pozycji pojazdu za każdym razem, gdy upłynie wielokrotność trzech godzin skumulowanego czasu prowadzenia pojazdu. Skumulowany czas zaczyna biec w momencie uruchomienia urządzenia rejestrującego. Nie mają na niego wpływu jakiegokolwiek inne warunki, np. poza zakresem lub przeprawa promowa/przejazd kolejowy.

Nie przewiduje się wyświetlania, drukowania lub pobierania skumulowanego czasu prowadzenia pojazdu;”;

3) pkt 2.3 ppkt 13 akapit ostatni otrzymuje brzmienie:

„— normalny okres ważności operacji przyrządów rejestrujących wynosi 15 lat, począwszy od daty wejścia w życie świadectwa przyrządu rejestrującego, ale przyrządy rejestrujące mogą być wykorzystywane przez kolejne 3 miesiące wyłącznie do pobierania danych.”;

4) pkt 2.4 akapit pierwszy otrzymuje brzmienie:

„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, ochrona integralności i autentyczności danych wymienianych między przyrządem rejestrującym a ewentualnym urządzeniem zewnętrznym GNSS, ochrona poufności, integralności i autentyczności danych wymienianych w ramach wczesnego wykrywania na odległość na potrzeby kontroli oraz sprawdzenie integralności i autentyczności pobieranych danych.”;

5) w pkt 3.2 ppkt 27 tiret drugie otrzymuje brzmienie:

„— pozycji, w których skumulowany czas prowadzenia pojazdu osiągnie wielokrotność trzech godzin.”;

6) w pkt 3.4 ppkt 49 otrzymuje brzmienie:

„49) Jeżeli w czasie 120 sekund od automatycznej zmiany na PRACĘ, wskutek zatrzymania pojazdu, nastąpi zmiana czynności na PRZERWA/ODPOCZYNEK lub GOTOWOŚĆ, przyjmuje się, że pierwsza taka zmiana zaistniała w czasie postoju pojazdu (w ten sposób można anulować zmianę czynności na PRACA).”;

7) w pkt 3.6.1 ppkt 59 otrzymuje brzmienie:

„59) Kierowca wprowadza wówczas bieżące miejsce pojazdu, a wpis ten uznaje się za tymczasowy.

W poniższych warunkach wpis tymczasowy wykonany przy ostatnim wyjęciu karty zostaje zatwierdzony (tj. nie będzie go już można nadpisać):

— wpis miejsca, w którym rozpoczyna się obecny dzienny okres pracy, w trakcie ręcznego wprowadzania zgodnie z wymogiem 61;

— następny wpis miejsca, w którym rozpoczyna się obecny dzienny okres pracy, jeśli posiadacz karty nie wpisze żadnego miejsca rozpoczęcia lub zakończenia okresu pracy w trakcie ręcznego wprowadzania zgodnie z wymogiem 61.

W poniższych warunkach wpis tymczasowy wykonany przy ostatnim wyjęciu karty jest nadpisany i zatwierdzona zostaje nowa wartość:

— następny wpis miejsca zakończenia obecnego dziennego okresu pracy, jeśli posiadacz karty nie wpisze żadnego miejsca rozpoczęcia lub zakończenia okresu pracy w trakcie ręcznego wprowadzania zgodnie z wymogiem 61.”;

8) w pkt 3.6.2 tiret szóste i siódme otrzymują brzmienie:

„— miejsca, w którym zakończył się poprzedni dzienny okres pracy powiązany z jednośmym czasem (czyli nadpisania i zatwierdzenia wpisu przy ostatnim wyjęciu karty),

— miejsca, w którym rozpoczyna się obecny dzienny okres pracy powiązany z jednośmym czasem (czyli zatwierdzenia wpisu tymczasowego przy ostatnim wyjęciu karty).”;

9) pkt 3.9.15 otrzymuje brzmienie:

„3.9.15 Zdarzenie „konflikt czasu»

86) **Z wyjątkiem trybu kalibracyjnego**, zdarzenie to uruchamia się, jeżeli przyrząd rejestrujący wykryje rozbieżność większą niż 1 min. między czasem określonym przez funkcję pomiaru czasu w przyrządzie rejestrującym a czasem pochodzącym z odbiornika GNSS. Zdarzenie to jest rejestrowane wraz z wartością wyświetlaną na wewnętrznym zegarze przyrządu rejestrującego i wiąże się z automatyczną korektą czasu. Po uruchomieniu zdarzenia konfliktu czasu przyrząd rejestrujący nie generuje innych zdarzeń konfliktu czasu przez kolejnych 12 godzin. Zdarzenie nie zostanie wywołane w przypadkach, w których odbiornik GNSS nie mógł wykryć prawidłowego sygnału GNSS przez co najmniej 30 dni.”;

10) w pkt 3.9.17 dodaje się tiret w brzmieniu:

„— usterka interfejsu ITS (w stosownych przypadkach).”;

11) w pkt 3.10 wprowadza się następujące zmiany:

(i) tekst przed tabelą w pkt 89 otrzymuje brzmienie:

„Urządzenie rejestrujące wykrywa usterki, wykonując autotesty i testy wbudowane, zgodnie z poniższą tabelą.”;

(ii) w tabeli dodaje się wiersz w brzmieniu:

„Interfejs ITS (fakultatywnie)	Prawidłowa praca”	
--------------------------------	-------------------	--

12) w pkt 3.12 tiret drugie otrzymuje brzmienie:

„— średnia liczba pozycji na dzień jest definiowana jako co najmniej 6 pozycji, w których rozpoczyna się dzienny okres pracy, 6 pozycji, w których skumulowany czas prowadzenia pojazdu osiąga wielokrotność trzech godzin, oraz 6 pozycji, w których kończy się dzienny okres pracy, tak więc »365 dni« obejmuje co najmniej 6570 pozycji.”;

13) w pkt 3.12.5 wprowadza się następujące zmiany:

a) nagłówek i pkt 108 otrzymują brzmienie:

„3.12.5. Miejsca i pozycje, w których zaczynają się i kończąienne okresy pracy lub w których osiągnięto 3 godziny skumulowanego czasu prowadzenia pojazdu”;

108) Urządzenie rejestrujące rejestruje i przechowuje w pamięci następujące dane:

- miejsca i pozycje, w których kierowca lub współkierowca rozpoczynają dzienny okres pracy;
- pozycje, w których skumulowany czas prowadzenia pojazdu osiągnie wielokrotność trzech godzin;
- miejsca i pozycje, w których kierowca lub współkierowca kończą dzienny okres pracy.”;

b) w pkt 110 tiret czwarte otrzymuje brzmienie:

„— rodzaj wpisu (rozpoczęcie, zakończenie lub 3 godziny skumulowanego czasu prowadzenia pojazdu).”;

c) pkt 111 otrzymuje brzmienie:

„111) Pamięć danych wystarcza do przechowywania miejsc i pozycji, w których zaczynają się i kończąienne okresy pracy lub w których osiągnięto 3 godziny skumulowanego czasu prowadzenia pojazdu, przez co najmniej 365 dni.”;

14) w pkt 3.12.7 ppkt 116 otrzymuje brzmienie:

„116) Urządzenie rejestrujące rejestruje i przechowuje w pamięci danych prędkość chwilową pojazdu wraz z datą i godziną, rejestrowane co sekundę przez okres co najmniej ostatnich 24 godzin, w których pojazd był w ruchu.”;

15) w tabeli w pkt 3.12.8 wprowadza się następujące zmiany:

a) między zdarzenia „Brak informacji o pozycji z odbiornika GNSS” i „Błąd danych dotyczących ruchu” dodaje się zdarzenie w brzmieniu:

„Błąd połączenia z urządzeniem zewnętrznym GNSS	<ul style="list-style-type: none"> — najdłuższe zdarzenie w każdym z ostatnich 10 dni ich występowania — 5 najdłuższych zdarzeń w ciągu ostatnich 365 dni 	<ul style="list-style-type: none"> — data i godzina początku zdarzenia — data i godzina końca zdarzenia — typ karty, numer, państwo członkowskie wydające kartę i generacja dla każdej karty wprowadzonej na początku lub pod koniec zdarzenia — liczba podobnych zdarzeń w tym dniu”
---	---	---

b) zdarzenie „Konflikt czasu” otrzymuje brzmienie:

„Konflikt czasu	<ul style="list-style-type: none"> — najpoważniejsze zdarzenie w każdym z 10 ostatnich dni ich występowania (tj. zdarzenia z największymi różnicami pomiędzy datą i godziną z urządzenia rejestrującego a datą i godziną z GNSS), — 5 najpoważniejszych zdarzeń w ciągu ostatnich 365 dni 	<ul style="list-style-type: none"> — data i godzina z urządzenia rejestrującego — data i godzina z GNSS — typ karty, numer, państwo członkowskie wydające kartę i generacja dla każdej karty wprowadzonej na początku lub pod koniec zdarzenia — liczba podobnych zdarzeń w tym dniu”
-----------------	---	---

16) w pkt 3.20 ppkt 200 otrzymuje brzmienie:

„200) Urządzenie rejestrujące może być również wyposażone w znormalizowane interfejsy pozwalające na wykonywanie przez urządzenie zewnętrzne danych rejestrowanych lub generowanych przez tachograf w trybie operacyjnym lub kalibracyjnym.

W dodatku 13 określono i podano normę dla opcjonalnego interfejsu ITS. Inne podobne interfejsy przyrządu rejestrującego mogą współistnieć, pod warunkiem że są w pełni zgodne z wymogami określonymi w dodatku 13 w odniesieniu do minimalnego wykazu danych, zabezpieczeń i zgody kierowcy.

Zgoda kierowcy nie ma zastosowania do danych przekazywanych przez urządzenie rejestrujące do sieci pojazdu. W przypadku gdy dane osobowe wprowadzone do sieci pojazdu są dalej przetwarzane poza siecią pojazdu, producent pojazdu jest zobowiązany do zapewnienia zgodności procedury przetwarzania danych osobowych z rozporządzeniem (UE) 2016/679 (ogólne rozporządzenie o ochronie danych).

Zgoda kierowcy nie ma zastosowania do danych z tachografu pobranych zdalnie przez firmę (wymóg 193), ponieważ taka sytuacja jest monitorowana przez prawo dostępu karty firmowej.

Następujące wymagania mają zastosowanie do danych ITS udostępnianych za pośrednictwem tego interfejsu:

- dane te stanowią zbiór wybranych istniejących danych ze słownika danych tachografu (dodatek 1),
- podzbiór tych wybranych danych jest oznaczony jako »dane osobowe«,
- podzbiór »danych osobowych« jest dostępny jedynie w przypadku, gdy włączona jest opcja podlegającej weryfikacji zgody kierowcy na wyprowadzenie jego danych osobowych z sieci pojazdu,
- w dowolnym momencie istnieje możliwość potwierdzenia lub wycofania zgody kierowcy przez wybranie polecenia w menu, pod warunkiem że karta kierowcy jest włożona,
- zbiór i podzbiór danych są przekazywane za pośrednictwem protokołu bezprzewodowego Bluetooth w promieniu kabiny pojazdu, z częstotliwością odświeżania co 1 minutę,
- sparowanie urządzenia zewnętrznego z interfejsem ITS jest zabezpieczone dedykowanym losowym kodem PIN składającym się z co najmniej 4 cyfr, zapisywanym i dostępnym przez wyświetlacz każdego przyrządu rejestrującego,
- w żadnych okolicznościach obecność interfejsu ITS nie może zakłócać prawidłowego funkcjonowania i bezpieczeństwa przyrządu rejestrującego ani oddziaływać na niego.

Można wyprowadzać również inne dane oprócz zbioru wybranych istniejących danych, uznawanych za wykaz minimalny, pod warunkiem że nie można ich uważać za dane osobowe.

Urządzenie rejestrujące musi posiadać zdolność do podawania statusu zgody kierowcy innym platformom w sieci pojazdu.

Przy włączonym zapłonie pojazdu dane te udostępniane są nieprzerwanie.”;

17) w pkt 3.23 ppkt 211 otrzymuje brzmienie:

„211) Ustawienia czasu zegara wewnętrznego przyrządu rejestrującego są automatycznie korygowane co 12 godzin. Jeżeli korekta nie jest możliwa, ponieważ sygnał GNSS nie jest dostępny, ustawienie czasu wprowadza się, jak tylko przyrząd rejestrujący uzyska dostęp do prawidłowego czasu z odbiornika GNSS, zależnie od stanu włączenia zapłonu pojazdu. Czasem odniesienia dla automatycznego ustawienia wewnętrznego zegara przyrządu rejestrującego jest czas pobrany z odbiornika GNSS.”;

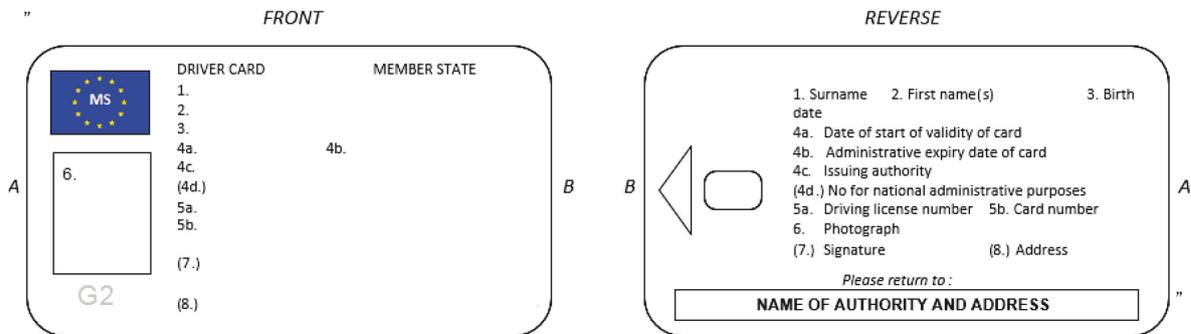
18) w pkt 3.26 ppkt 225 i 226 otrzymują brzmienie:

„225) Do każdego odrębnego elementu składowego urządzenia rejestrującego jest przymocowana tabliczka zawierająca następujące informacje:

- nazwa i adres producenta,
- numer części producenta i rok produkcji,
- numer seryjny,
- znak homologacji typu.

226) Jeżeli dostępna powierzchnia nie wystarcza do umieszczenia wszystkich powyższych informacji, na tabliczce umieszcza się przynajmniej: nazwę producenta lub jego logo i numer części.”;

19) w pkt 4.1 rysunek odpowiadający awersowi i rewersowi karty kierowcy zastępuje się następującym rysunkiem:



20) w pkt 4.5.3.1.8 ppkt 263 tiret pierwsze otrzymuje brzmienie:

„— usterka karty (w przypadku gdy dana karta jest przedmiotem usterki);”;

21) w pkt 4.5.3.2.8 ppkt 288 tiret pierwsze otrzymuje brzmienie:

„— usterka karty (w przypadku gdy dana karta jest przedmiotem usterki);”;

22) pkt 4.5.3.2.16 otrzymuje brzmienie:

„4.5.3.2.16 Dane miejsc, w których minęły trzy godziny skumulowanego czasu prowadzenia pojazdu

305) Karta kierowcy umożliwia przechowywanie następujących danych dotyczących pozycji pojazdu, w których skumulowany czas prowadzenia pojazdu osiąga wielokrotność trzech godzin:

- data i godzina, o której skumulowany czas prowadzenia pojazdu osiąga wielokrotność trzech godzin,
- pozycja pojazdu,
- dokładność GNSS, data i godzina określenia pozycji,
- stan licznika kilometrów.

306) Karta kierowcy umożliwia przechowywanie co najmniej 252 takich rekordów danych.”;

23) pkt 4.5.4.2.14 otrzymuje brzmienie:

„4.5.4.2.14 Dane miejsc, w których minęły trzy godziny skumulowanego czasu prowadzenia pojazdu

353) Karta warsztatowa umożliwia przechowywanie następujących danych dotyczących pozycji pojazdu, w których skumulowany czas prowadzenia pojazdu osiąga wielokrotność trzech godzin:

- data i godzina, o której skumulowany czas prowadzenia pojazdu osiąga wielokrotność trzech godzin,

- pozycja pojazdu,
- dokładność GNSS, data i godzina określenia pozycji,
- stan licznika kilometrów.

354) Karta warsztatowa umożliwia przechowywanie co najmniej 18 takich rekordów danych.”;

24) w pkt 5.2 ppkt 396 otrzymuje brzmienie:

„396) Tabliczka zawiera co najmniej następujące dane:

- nazwa, adres lub nazwa handlowa zatwierdzonego instalatora lub warsztatu,
- współczynnik charakterystyczny pojazdu, w postaci »w = ...imp/km«,
- stała urządzenia rejestrującego, w postaci »k = ...imp/km«,
- obwód toczny opon, w postaci „l = ...mm”,
- rozmiar opon,
- data pomiaru współczynnika charakterystycznego pojazdu i obwodu tocznego opon,
- numer identyfikacyjny pojazdu,
- obecność (lub brak) urządzenia zewnętrznego GNSS,
- numer seryjny urządzenia zewnętrznego GNSS, w stosownych przypadkach,
- numer seryjny urządzenia do łączności na odległość, jeżeli występuje,
- numer seryjny wszystkich założonych plomb,
- część pojazdu, w której zamontowany jest ewentualny adapter,
- część pojazdu, w której zamontowany jest czujnik ruchu, jeżeli nie jest podłączony do skrzyni biegów lub w przypadku niezastosowania adaptera,
- kolor przewodu łączącego adapter z częścią pojazdu, z której dochodzą impulsy,
- numer seryjny czujnika ruchu wbudowanego w adapter.”;

25) w pkt 5.3 wprowadza się następujące zmiany:

a) po ppkt 398 dodaje się nowy ppkt 398a w brzmieniu:

„398a Plomby, o których mowa powyżej, muszą być certyfikowane zgodnie z normą EN 16882:2016.”;

b) w ppkt 401 akapit drugi otrzymuje brzmienie:

„Ten niepowtarzalny numer identyfikacyjny jest określony w następujący sposób: MMNNNNNNNNN w formie niedającego się usunąć oznakowania, gdzie MM to jednoznaczny identyfikator producenta (numer w bazie danych prowadzonej przez KE), a NNNNNNNNN to numer alfanumeryczny plomby, niepowtarzalny dla danego producenta.”;

c) ppkt 403 otrzymuje brzmienie:

„403) Producenci plomb muszą być zarejestrowani w specjalnej bazie danych, gdy otrzymują model plomby certyfikowany zgodnie z normą EN 16882:2016, i muszą udostępniać publicznie numery identyfikacyjne plomb w procedurze, którą ma określić Komisja Europejska.”;

d) ppkt 404 otrzymuje brzmienie:

„404) Zatwierdzone warsztaty i producenci pojazdów korzystają, w ramach rozporządzenia (UE) nr 165/2014, wyłącznie z plomb certyfikowanych zgodnie z normą EN 16882:2016 od producentów plomb zapisanych w bazie danych, o której mowa powyżej.”;

26) pkt 6.2 otrzymuje brzmienie:

„6.2. Kontrola techniczna elementów składowych nowych lub po naprawie

407) Każdy przyrząd, tak nowy, jak i po naprawie, jest kontrolowany pod względem prawidłowego funkcjonowania oraz dokładności odczytów i rejestracji, w granicach określonych w rozdziałach 3.2.1, 3.2.2, 3.2.3 oraz 3.3.”;

27) w pkt 6.3 ppkt 408 otrzymuje brzmienie:

„408) Po zainstalowaniu w pojeździe cała instalacja (włącznie z urządzeniem rejestrującym) musi być zgodna z przepisami dotyczącymi maksymalnych tolerancji ustanowionymi w rozdziałach 3.2.1, 3.2.2, 3.2.3 i 3.3. Cała instalacja musi być zaplombowana zgodnie z rozdziałem 5.3 i musi obejmować kalibrację.”;

28) w pkt 8.1 wprowadza się następujące zmiany:

a) w pkt 8.1 tekst wprowadzający przed ppkt 425 otrzymuje brzmienie:

„Do celów niniejszego rozdziału wyrażenie »urządzenie rejestrujące« oznacza »urządzenie rejestrujące lub jego elementy składowe«. Homologacji typu nie wymaga się dla przewodu(-ów) łączącego(-ych) czujnik ruchu z przyrządem rejestrującym, urządzenie zewnętrzne GNSS z przyrządem rejestrującym lub zewnętrzne urządzenie do łączności na odległość z przyrządem rejestrującym. Papier używany przez urządzenie rejestrujące uważa się za element składowy urządzenia rejestrującego.

Każdy producent może zwrócić się o homologację typu elementów składowych urządzenia rejestrującego z wszelkimi innymi elementami składowymi urządzenia rejestrującego, pod warunkiem że każdy element składowy jest zgodny z wymogami niniejszego załącznika. Producenci mogą również zwrócić się o homologację typu urządzenia rejestrującego.

Jak opisano w definicji 10 w art. 2 niniejszego rozporządzenia, przyrządy rejestrujące mają różne warianty zespołów elementów składowych. Bez względu na wariant zespołu elementów składowych przyrządu rejestrującego, antena zewnętrzna i rozdzielacz antenowy podłączony do odbiornika GNSS lub do urządzenia do łączności na odległość nie stanowią części homologacji typu przyrządu rejestrującego.

Niemniej jednak po uzyskaniu homologacji typu urządzenia rejestrującego producenci prowadzą powszechnie dostępny wykaz anten i rozdzielaczy kompatybilnych z każdym homologowanym przyrządem rejestrującym, urządzeniem zewnętrznym GNSS i zewnętrznym urządzeniem do łączności na odległość.”;

b) ppkt 427 otrzymuje brzmienie:

„427) Organy homologacji typu w państwach członkowskich nie wydają świadectwa homologacji typu, dopóki nie otrzymają:

— świadectwa bezpieczeństwa (jeżeli jest ono wymagane na podstawie niniejszego załącznika),

— świadectwa funkcjonalności,

— świadectwa interoperacyjności (jeżeli jest ono wymagane na podstawie niniejszego załącznika),

dla urządzenia rejestrującego lub kart do tachografów, dla których złożono wnioski o homologację typu.”;

29) w dodatku 1 wprowadza się następujące zmiany:

a) w spisie treści wprowadza się następujące zmiany:

(i) pkt 2.63 otrzymuje brzmienie:

„2.63. Zarezerwowany dla przyszłego użytku.”;

(ii) pkt 2.78 otrzymuje brzmienie:

„2.78. GNSSAccumulatedDriving”;

(iii) pkt 2.79 otrzymuje brzmienie:

„2.79. GNSSAccumulatedDrivingRecord”;

(iv) pkt 2.111 otrzymuje brzmienie:

„2.111. NoOfGNSSADRecords”;

(v) pkt 2.160 otrzymuje brzmienie:

„2.160. Zarezerwowany dla przyszłego użytku.”;

(vi) pkt 2.203 otrzymuje brzmienie:

„2.203. VuGNSSADRecord”;

(vii) pkt 2.204 otrzymuje brzmienie:

„2.204. VuGNSSADRecordArray”;

(viii) pkt 2.230 otrzymuje brzmienie:

„2.230. Zarezerwowany dla przyszłego użytku.”;

(ix) pkt 2.231 otrzymuje brzmienie:

„2.231. Zarezerwowany dla przyszłego użytku.”;

b) w pkt 2 dodaje się przed pkt 2.1 tekst w brzmieniu:

„W przypadku typów danych karty używanych do aplikacji generacji 1 i generacji 2, wielkość określona w niniejszym dodatku to wielkość dla aplikacji generacji 2. Wielkość dla aplikacji generacji 1 powinna być już znana dla czytelnika. Numery wymogów dotyczących takich typów danych określone w załączniku IC obejmują zarówno aplikacje generacji 1, jak i generacji 2.”;

c) pkt 2.19 otrzymuje brzmienie:

„2.19. **CardEventData**

Generacja 1:

Informacje przechowywane na karcie kierowcy lub warsztatowej dotyczące zdarzeń związanych z posiadaczem karty (wymagania 260 i 318 określone w załączniku IC).

```
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 rekordów związanych z próbami naruszenia zabezpieczeń, które gromadzone są w ostatnim zbiorze sekwencji).

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

Generacja 2:

Informacje przechowywane na karcie kierowcy lub warsztatowej dotyczące zdarzeń związanych z posiadaczem karty (wymagania 285 i 341 określone w załączniku IC).

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

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

cardEventRecords jest zbiorem rekordów ze zdarzeniami dla danego typu zdarzenia (lub kategorii prób naruszeń zabezpieczenia).”

d) pkt 2.30 otrzymuje brzmienie:

„2.30. **CardRenewalIndex**

Numer odnowienia karty (definicja i)).

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

Przypisanie wartości: (zob. rozdział 7 niniejszego załącznika).

»0« Wydanie pierwsze.

Kolejność zwiększania: »0, ..., 9, A, ..., Z «”;

- e) w pkt 2.61 tekst po nagłówku „Generacja 2” otrzymuje brzmienie:

```

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

```

Oprócz generacji 1 używane są następujące elementy danych:

noOfGNSSADRecords jest liczbą rekordów skumulowanego czasu prowadzenia pojazdu z GNSS, które mogą być zapisane na karcie.

noOfSpecificConditionRecords jest liczbą rekordów warunków szczególnych, które mogą być zapisane na karcie.

noOfCardVehicleUnitRecords jest liczbą rekordów używanych przyrządów rejestrujących, które mogą być zapisane na karcie.”;

- f) pkt 2.63 otrzymuje brzmienie:

„2.63. **Zarezerwowany dla przyszłego użytku.**”;

- g) w pkt 2.67 tekst pod nagłówkiem „Generacja 2” otrzymuje brzmienie:

„Takie same wartości jak w przypadku generacji 1 z następującymi uzupełnieniami:

```

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

```

Uwaga 1: Wartości generacji 2 dla tabliczki, adaptera, połączenia zewnętrznego GNSS, a także wartości generacji 1 dla przyrządu rejestrującego oraz czujnika ruchu mogą być, w stosownych przypadkach, używane w SealRecord.

Uwaga 2: W polu CardHolderAuthorisation (CHA) świadectwa generacji 2, wartości (1), (2) i (6) należy interpretować jako wskazujące na świadectwo wzajemnego uwierzytelnienia dla danego typu urządzenia. W celu wskazania danego certyfikatu na potrzeby podpisu cyfrowego należy użyć wartości (17), (18) lub (19).”;

h) w pkt 2.70 tekst pod nagłówkiem „Generacja 2” otrzymuje brzmienie:

„Generacja 2:

' 0x' H	zdarzenia ogólne,
' 00' H	brak dalszych szczegółów,
' 01' H	włożenie nieważnej karty,
' 02' H	konflikt kart,
' 03' H	nakładające się czasy,
' 04' H	przewodzenie pojazdu bez prawidłowej karty,
' 05' H	włożenie karty podczas prowadzenia pojazdu,
' 06' H	sesja ostatniej karty niezamknięta prawidłowo,
' 07' H	przekroczenie prędkości,
' 08' H	przerwa w zasilaniu,
' 09' H	błąd danych dotyczących ruchu,
' 0A' H	konflikt ruchu pojazdu,
' 0B' H	konflikt czasowy (między GNSS a wewnętrznym zegarem VU),
' 0C' H	błąd połączenia z urządzeniem do łączności na odległość,
' 0D' H	brak informacji o pozycji z odbiornika GNSS,
' 0E' H	błąd połączenia z urządzeniem zewnętrznym GNSS,
' 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	wykrycie ingerencji w GNSS,
' 1A' H	błąd uwierzytelnienia urządzenia zewnętrznego GNSS,
' 1B' H	wygaśnięcie certyfikatu urządzenia zewnętrznego GNSS,
' 1C' 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	usterki urządzenia rejestrującego,
' 30' H	brak dalszych szczegółów,
' 31' H	usterka wewnętrzna VU,
' 32' H	usterka drukarki,
' 33' H	usterka wyświetlacza,
' 34' H	usterka pobierania danych,
' 35' H	usterka czujnika,
' 36' H	wewnętrzny odbiornik GNSS,
' 37' H	urządzenie zewnętrzne GNSS,
' 38' H	urządzenie do łączności na odległość,
' 39' H	interfejs ITS,
' 3A' 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.”;

i) pkt 2.71 otrzymuje brzmienie:

„2.71. **ExtendedSealIdentifier**

Generacja 2:

Rozszerzony identyfikator plomby jednoznacznie identyfikuje plombę (wymaganie 401 określone w załączniku IC).

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

manufacturerCode: jest kodem producenta plomby.

sealIdentifier jest identyfikatorem plomby, który jest niepowtarzalny dla producenta.”;

j) pkt 2.78 i 2.79 otrzymują brzmienie:

„2.78. **GNSSAccumulatedDriving**

Generacja 2:

Informacje zapisane na karcie kierowcy lub na karcie warsztatowej dotyczące położenia pojazdu z GNSS, jeżeli skumulowany czas prowadzenia pojazdu osiągnie wielokrotność trzech godzin (wymagania 306 i 354 określone w załączniku IC).

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

gnssADPointerNewestRecord jest indeksem ostatniego uaktualnionego rekordu skumulowanego prowadzenia pojazdu z GNSS.

Value assignment to liczba odpowiadająca stanowi licznika rekordu GNSS dotyczącego skumulowanego prowadzenia pojazdu, rozpoczynając od »0« dla pierwszego wystąpienia w strukturze rekordu GNSS dotyczącego skumulowanego czasu prowadzenia pojazdu.

gnssAccumulatedDrivingRecords jest zbiorem rekordów zawierających datę i godzinę, kiedy skumulowany czas prowadzenia pojazdu osiąga wielokrotność trzech godzin i informacji na temat położenia pojazdu.

2.79. **GNSSAccumulatedDrivingRecord**

Generacja 2:

Informacje zapisane na karcie kierowcy lub na karcie warsztatowej dotyczące położenia pojazdu z GNSS, jeżeli skumulowany czas prowadzenia pojazdu osiągnie wielokrotność trzech godzin (wymagania 305 i 353 określone w załączniku IC)

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

timeStamp to data i godzina, o której skumulowany czas prowadzenia pojazdu osiąga wielokrotność trzech godzin.

gnssPlaceRecord zawiera informacje dotyczące położenia pojazdu.

vehicleOdometerValue to wartość stanu licznika kilometrów, przy której skumulowany czas prowadzenia pojazdu osiąga wielokrotność trzech godzin.”;

k) pkt 2.86 otrzymuje brzmienie:

„2.86. 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, karty do tachografu lub urządzenia zewnętrznego GNSS.

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

Trzecia pozycja jest odpowiednia przy odesłaniu do klucza publicznego państwa członkowskiego.”;

l) pkt 2.92 otrzymuje brzmienie:

„2.92. MAC

Generacja 2:

Kryptograficzna suma kontrolna o długości 8, 12 lub 16 bajtów odpowiadającej mechanizmowi szyfrowania określonym w dodatku 11.

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

m) pkt 2.111 otrzymuje brzmienie:

„2.111. NoOfGNSSADRecords

Generacja 2:

Liczba rekordów skumulowanego czasu prowadzenia pojazdu z GNSS, które mogą być przechowywane na karcie.

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

Przypisanie wartości: zob. dodatek 2.”;

n) w pkt 2.120 przypisanie wartości „16H” otrzymuje brzmienie:

```
„'16'H VuGNSSADRecord”;
```

o) pkt 2.160 otrzymuje brzmienie:

„2.160. Zarezerwowany dla przyszłego użytku.”;

p) pkt 2.162 otrzymuje brzmienie:

„2.162. **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. UTC.

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

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

Maksymalna możliwa data/godzina wypada w 2106 r.”;

q) pkt 2.179 otrzymuje brzmienie:

„2.179. **VuCardRecord**

Generacja 2:

Informacje przechowywane w przyrządzie rejestrującym dotyczące używanej karty do tachografu (wymagania 132 określone w załączniku IC).

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

cardNumberAndGenerationInformation jest pełnym numerem karty i generacji dla użytej karty (typ danych 2.74).

cardExtendedSerialNumber odczytany z pliku EF_ICC w ramach pliku głównego karty.

cardStructureVersion odczytane z pliku EF_Application_Identification w ramach pliku DF_Tachograph_G2.

cardNumber odczytane z pliku EF_Identification w ramach pliku DF_Tachograph_G2.”;

r) pkt 2.203 i 2.204 otrzymują brzmienie:

„2.203. **VuGNSSADRecord**

Generacja 2:

Informacje przechowywane w przyrządzie rejestrującym dotyczące położenia pojazdu z GNSS, jeżeli skumulowany czas prowadzenia pojazdu osiągnie wielokrotność trzech godzin (wymagania 108 i 110 określone w załączniku IC).

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

timeStamp to data i godzina, o której skumulowany czas prowadzenia pojazdu osiąga wielokrotność trzech godzin.

cardNumberAndGenDriverSlot identyfikuje kartę, w tym jej generację, włożoną do szczeliny karty kierowcy.

cardNumberAndGenCodriverSlot identyfikuje kartę, w tym jej generację, włożoną do szczeliny karty współkierowcy.

gnssPlaceRecord zawiera informacje dotyczące położenia pojazdu.

vehicleOdometerValue to wartość stanu licznika kilometrów, przy której skumulowany czas prowadzenia pojazdu osiąga wielokrotność trzech godzin.

2.204. **VuGNSSADRecordArray**

Generacja 2:

Informacje przechowywane w przyrządzie rejestrującym dotyczące położenia pojazdu z GNSS, jeżeli skumulowany czas prowadzenia pojazdu osiągnie wielokrotność trzech godzin (wymagania 108 i 110 określone w załączniku IC).

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

recordType oznacza typ rekordu (VuGNSSADRecord).

Value Assignment: zob. RecordType

recordSize to wielkość VuGNSSADRecord w bajtach.

noOfRecords jest liczbą rekordów w zbiorze.

records jest zbiorem rekordów skumulowanego czasu prowadzenia pojazdu z GNSS.”;

- s) pkt 2.230 i 2.231 otrzymują brzmienie:

„2.230. Zarezerwowany dla przyszłego użytku.

2.231. Zarezerwowany dla przyszłego użytku.”;

- t) w pkt 2.234 tekst pod nagłówkiem „Generacja 2” otrzymuje brzmienie:

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

Oprócz generacji 1 używane są następujące elementy danych:

noOfGNSSCDRecords jest liczbą rekordów skumulowanego czasu prowadzenia pojazdu z GNSS, które mogą być zapisane na karcie.

noOfSpecificConditionRecords jest liczbą rekordów warunków szczególnych, które mogą być zapisane na karcie.

noOfCardVehicleUnitRecords jest liczbą rekordów używanych przyrządów rejestrujących, które mogą być zapisane na karcie.”;

30) w dodatku 2 wprowadza się następujące zmiany:

a) w pkt 1.1 dodaje się następujące skróty:

„CHA upoważnienie posiadacza certyfikatu

DO obiekt danych”;

b) w pkt 3.3 wprowadza się następujące zmiany:

(i) punkt TCS_24 otrzymuje brzmienie:

„TCS_24 Przedmiotowe warunki zabezpieczenia mogą być powiązane ze sobą w następujący sposób:

AND: muszą zostać spełnione wszystkie warunki zabezpieczenia

OR: musi zostać spełniony przynajmniej jeden warunek zabezpieczenia

Zasady dostępu dla systemu plików, tzn. polecenia SELECT, READ BINARY oraz UPDATE BINARY, zostały określone w rozdziale 4. Zasady dostępu dla pozostałych poleceń zostały określone w poniższych tabelach. Określenie »nie dotyczy« jest stosowane w przypadku braku wymogu obsługi danego polecenia. W takim przypadku polecenie może być lub nie być obsługiwane, ale warunek dostępu jest wyłączony z zakresu zastosowania.”;

(ii) w pkt TCS_25 tabela otrzymuje brzmienie:

„Polecenie	Karta kierowcy	Karta warsztatowa	Karta kontrolna	Karta firmowa
External Authenticate				
— dla uwierzytelnienia 1. generacji	ALW	ALW	ALW	ALW
— dla uwierzytelnienia 2. generacji	ALW	PWD	ALW	ALW
Internal Authenticate	ALW	PWD	ALW	ALW
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	nie dotyczy	nie dotyczy	nie dotyczy	nie dotyczy
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	nie dotyczy	nie dotyczy
PSO: Hash	nie dotyczy	nie dotyczy	ALW	nie dotyczy

Polecenie	Karta kierowcy	Karta warsztatowa	Karta kontrolna	Karta firmowa
PERFORM HASH of FILE	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	nie dotyczy	nie dotyczy
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	nie dotyczy	nie dotyczy	ALW	nie dotyczy
Verify	nie dotyczy	ALW	nie dotyczy	nie dotyczy ”

(iii) w pkt TCS_26 tabela otrzymuje brzmienie:

„Polecenie	Karta kierowcy	Karta warsztatowa	Karta kontrolna	Karta firmowa
External Authenticate				
— dla uwierzytelnienia 1. generacji	nie dotyczy	nie dotyczy	nie dotyczy	nie dotyczy
— dla uwierzytelnienia 2. generacji	ALW	PWD	ALW	ALW
Internal Authenticate	nie dotyczy	nie dotyczy	nie dotyczy	nie dotyczy
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	nie dotyczy	ALW	ALW	nie dotyczy
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	nie dotyczy	nie dotyczy
PSO: Hash	nie dotyczy	nie dotyczy	ALW	nie dotyczy
PERFORM HASH of FILE	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	nie dotyczy	nie dotyczy
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	nie dotyczy	nie dotyczy	ALW	nie dotyczy
Verify	nie dotyczy	ALW	nie dotyczy	nie dotyczy”

(iv) w pkt TCS_27 tabela otrzymuje brzmienie:

„Polecenie	Karta kierowcy	Karta warsztatowa	Karta kontrolna	Karta firmowa
External Authenticate				
— dla uwierzytelnienia 1. generacji	nie dotyczy	nie dotyczy	nie dotyczy	nie dotyczy
— dla uwierzytelnienia 2. generacji	ALW	PWD	ALW	ALW
Internal Authenticate	nie dotyczy	nie dotyczy	nie dotyczy	nie dotyczy
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	nie dotyczy	nie dotyczy	nie dotyczy	nie dotyczy
PSO: Compute Digital Signature	nie dotyczy	nie dotyczy	nie dotyczy	nie dotyczy
PSO: Hash	nie dotyczy	nie dotyczy	nie dotyczy	nie dotyczy
PERFORM HASH of FILE	nie dotyczy	nie dotyczy	nie dotyczy	nie dotyczy
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	nie dotyczy	nie dotyczy	nie dotyczy	nie dotyczy
Verify	nie dotyczy	ALW	nie dotyczy	nie dotyczy ”

c) w pkt 3.4 ppkt TCS_29 otrzymuje brzmienie:

„TCS_29 Słowa stanu SW1 i 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	00	Nieudane uwierzytelnienie (ostrzeżenie)
63	CX	Nieprawidłowe CHV (PIN). »X« oznacza licznik pozostałych prób.

SW1	SW2	Znaczenie
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 uwierzytelnienia) lub nieprawidłowy podpis (w czasie weryfikacji podpisu)
67	00	Nieprawidłowa długość (nieprawidłowe Lc lub Le)
68	83	Oczekiwane ostatnie polecenie łańcucha
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	80	Nieprawidłowe parametry w polu danych
6A	82	Nie znaleziono pliku.
6A	86	Nieprawidłowe parametry P1-P2.
6A	88	Nie znaleziono powołanych danych.
6B	00	Nieprawidłowe parametry (przesunięcie poza EF).
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

Dodatkowe słowa stanu zdefiniowane w normie ISO/IEC 7816-4 mogą być zwracane, jeżeli ich zachowanie nie jest wyraźnie wymienione w niniejszym dodatku.

Przykładowo następujące słowa stanu mogą być zwracane opcjonalnie:

6881: Kanał logiczny nieobsługiwany

6882: Bezpieczna wymiana komunikatów nieobsługiwana”;

d) w pkt 3.5.1.1 tiret ostatnie pozycji TCS_38 otrzymuje brzmienie:

„— Jeżeli wybrana aplikacja uznana jest za uszkodzoną (znaleziony błąd integralności w atrybutach pliku), zwróconym stanem przetwarzania jest »6400« lub »6500«.”;

e) w pkt 3.5.1.2 tiret ostatnie pozycji TCS_41 otrzymuje brzmienie:

„— Jeżeli wybrany plik uznany jest za uszkodzony (znaleziony błąd integralności w atrybutach pliku), zwróconym stanem przetwarzania jest »6400« lub »6500«.”;

f) w pkt 3.5.2.1 tiret szóste pozycji TCS_43 otrzymuje brzmienie:

„— Jeżeli błąd integralności zostaje wykryty w atrybutach pliku, karta uznaje, że plik jest uszkodzony i nienaprawialny, a zwróconym stanem przetwarzania jest »6400« lub »6500«.”;

g) w pkt 3.5.2.1.1 wprowadza się następujące zmiany:

(i) w pozycji TCS_45 tabela otrzymuje brzmienie:

„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 L _e). L ma 2 bajty, jeżeli L _{pv} >127 bajtów
#(2+L) - #(1+L+NN)	NN	»XX..XXh«	Wartość danych odkrytych
#(2+L+NN)	1	»99h«	Znacznik stanu przetwarzania (SW1-SW2) – opcjonalnie dla bezpiecznej wymiany komunikatów 1. generacji
#(3+L+NN)	1	»02h«	Długość stanu przetwarzania – opcjonalnie dla bezpiecznej wymiany komunikatów 1. generacji
#(4+L+NN) - #(5+L+NN)	2	»XX XXh«	Stan przetwarzania niechronionej odpowiedzi APDU – opcjonalnie dla bezpiecznej wymiany komunikatów 1. generacji
#(6+L+NN)	1	»8Eh«	TCC: znacznik kryptograficznej sumy kontrolnej
#(7+L+NN)	1	»XXh«	LCC: długość znajdującej się dalej kryptograficznej sumy kontrolnej »04h« dla bezpiecznej wymiany komunikatów 1. generacji (zob. dodatek 11 część A) »08h«, »0Ch« lub »10h«, w zależności od długości klucza AES, dla bezpiecznej wymiany komunikatów 2. generacji (zob. dodatek 11 część B)

Bajt	Długość	Wartość	Opis
#(8+L+NN)-#(7+M+L+NN)	M	»XX..XXh«	Kryptograficzna suma kontrolna
SW	2	»XXXXh«	Słowa stanu (SW1, SW2)”

(ii) w pozycji TCS_46 tabela otrzymuje brzmienie:

„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 LPI CG > 127 bajtów
#(2+L)-#(1+L+MM)	MM	»01XX..XXh«	dane szyfrowane: wskaźnik wypełnienia i kryptogram
#(2+L+MM)	1	»99h«	Znacznik stanu przetwarzania (SW1-SW2) – opcjonalnie dla bezpiecznej wymiany komunikatów 1. generacji
#(3+L+MM)	1	»02h«	Długość stanu przetwarzania – opcjonalnie dla bezpiecznej wymiany komunikatów 1. generacji
#(4+L+MM) - #(5+L+MM)	2	»XX XXh«	Stan przetwarzania niechronionej odpowiedzi APDU – opcjonalnie dla bezpiecznej wymiany komunikatów 1. generacji
#(6+L+MM)	1	»8Eh«	TCC: znacznik kryptograficznej sumy kontrolnej
#(7+L+MM)	1	»XXh«	LCC: długość znajdującej się dalej kryptograficznej sumy kontrolnej »04h« dla bezpiecznej wymiany komunikatów 1. generacji (zob. dodatek 11 część A) »08h«, »0Ch« lub »10h«, w zależności od długości klucza AES, dla bezpiecznej wymiany komunikatów 2. generacji (zob. dodatek 11 część B)
#(8+L+MM)- #(7+N+L+MM)	N	»XX..XXh«	Kryptograficzna suma kontrolna
SW	2	»XXXXh«	Słowa stanu (SW1, SW2)”

h) w pkt 3.5.2.2 tiret szóste pozycji TCS_50 otrzymuje brzmienie:

„— Jeżeli błąd integralności zostaje wykryty w atrybutach pliku, karta uznaje, że plik jest uszkodzony i nienaprawialny, a zwróconym stanem przetwarzania jest »6400« lub »6500«.”;

i) w pkt 3.5.2.3 w pozycji TCS_52 wprowadza się następujące zmiany:

(i) wiersz ostatni tabeli otrzymuje brzmienie:

„Le	1	»XXh«	zgodnie ze specyfikacją w normie ISO/IEC 7816-4”
-----	---	-------	--

(ii) dodaje się zdanie w brzmieniu:

„W przypadku gdy $T=0$, karta przyjmuje wartość $Le = »00h«$, jeżeli nie stosuje się bezpiecznej wymiany komunikatów.

W przypadku gdy $T = 1$, zwróconym stanem przetwarzania jest $»6700«$, jeżeli $Le = »01h«$.”;

j) w pkt 3.5.2.3 tiret szóste pozycji TCS_53 otrzymuje brzmienie:

„— Jeżeli błąd integralności zostaje wykryty w atrybutach pliku, karta uznaje, że plik jest uszkodzony i nienaprawialny, a zwróconym stanem przetwarzania jest $»6400«$ lub $»6500«$.”;

k) w pkt 3.5.3.2 tiret szóste pozycji TCS_63 otrzymuje brzmienie:

„— Jeżeli błąd integralności zostaje wykryty w atrybutach pliku, karta uznaje, że plik jest uszkodzony i nienaprawialny, a zwróconym stanem przetwarzania jest $»6400«$ lub $»6500«$.”;

l) w pkt 3.5.5 pozycja TCS_72 otrzymuje brzmienie:

„TCS_72 PIN wprowadzony przez użytkownika musi być kodowany w ASCII i prawidłowo wypełniony przez IFD bajtami $»FFh«$ do długości 8 bajtów (zob. również typ danych WorkshopCardPIN w dodatku 1).”;

m) w pkt 3.5.8 pozycja TCS_95 otrzymuje brzmienie:

„TCS_95 Jeżeli uwierzytelnienie poleceniem INTERNAL AUTHENTICATE jest pomyślne, klucz bieżącej sesji 1. generacji (o ile istnieje) zostaje skasowany i nie jest dalej dostępny. W celu uzyskania nowego klucza sesji 1. generacji konieczne jest pomyślne wykonanie uwierzytelnienia poleceniem EXTERNAL AUTHENTICATE dla mechanizmu uwierzytelnienia 1. generacji.

Uwaga: Zob. dodatek 11 pozycje CSM_193 i CSM_195 odnośnie do kluczy sesji 2. generacji. Jeżeli ustanowiono klucze sesji 2. generacji, a karta do tachografu otrzymuje odkryte polecenie APDU INTERNAL AUTHENTICATE, przerywa sesję bezpiecznej wymiany komunikatów 2. generacji i niszczy klucze sesji 2. generacji.”;

n) w pkt 3.5.9 pozycja TCS_97 otrzymuje brzmienie:

„TCS_97 Wariant polecenia dla wzajemnego uwierzytelnienia VU – karta drugiej generacji można wykonać w MF, DF Tachograph i DF Tachograph_G2 (zob. również TCS_34). Jeżeli uwierzytelnienie poleceniem 2. generacji EXTERNAL AUTHENTICATE jest pomyślne, klucz bieżącej sesji 1. generacji (o ile istnieje) zostaje skasowany i nie jest dalej dostępny.

Uwaga: Zob. dodatek 11 pozycje CSM_193 i CSM_195 odnośnie do kluczy sesji 2. generacji. Jeżeli ustanowiono klucze sesji 2. generacji, a karta do tachografu otrzymuje odkryte polecenie APDU EXTERNAL AUTHENTICATE, przerywa sesję bezpiecznej wymiany komunikatów 2. generacji i niszczy klucze sesji 2. generacji.”;

o) w pkt 3.5.10 w tabeli w pozycji TCS_101 dodaje się wiersz w brzmieniu:

„5 + L + 1	1	»00h«	zgodnie ze specyfikacją w normie ISO/IEC 7816-4”
------------	---	-------	--

p) w pkt 3.5.11.2.3 w pozycji TCS_114 dodaje się następujące akapity:

„- Jeżeli currentAuthenticatedTime karty jest późniejszy niż data upływu ważności wybranego klucza publicznego, zwróconym stanem przetwarzania jest »6A88«.

Uwaga: W przypadku polecenia MSE: SET AT na potrzeby uwierzytelnienia VU powołany klucz to klucz publiczny VU_MA. Karta ustawia klucz publiczny VU_MA do użytku, jeżeli jest on dostępny w jej pamięci, który pokrywa się z odniesieniem do posiadacza certyfikatu (CHR) podanym w polu danych dotyczących polecenia (karta może zidentyfikować klucze publiczne VU_MA za pomocą pola CHA certyfikatu). Karta zwraca »6A88« temu poleceniu, w przypadku gdy jest dostępny jedynie klucz publiczny VU_Sign lub nie jest dostępny żaden klucz publiczny przyrządu rejestrującego. Zob. definicja pola CHA w dodatku 11 i typu danych equipmentType w dodatku 1.

Analogicznie w przypadku polecenia MSE: SET DST odwołującego się do EQT (tzn. przyrządu rejestrującego lub karty), które jest przesyłane do karty kontrolnej, zgodnie z CSM_234 powołany klucz to zawsze klucz EQT_Sign, który musi być stosowany na potrzeby weryfikacji podpisu cyfrowego. Zgodnie z rys. 13 w dodatku 11 karta kontrolna będzie zawsze przechowywać odpowiedni klucz publiczny EQT_Sign. W pewnych przypadkach karta kontrolna może przechowywać odpowiadający klucz publiczny EQT_MA. Karta kontrolna musi zawsze ustawiać klucz publiczny EQT_Sign do użytku, gdy otrzyma polecenie MSE: SET DST.”;

q) w pkt 3.5.13 wprowadza się następujące zmiany:

(i) pozycja TCS_121 otrzymuje brzmienie:

„TCS_121 Tymczasowo zachowana wartość skrótu pliku jest usuwana, jeżeli nowa wartość skrótu zostaje obliczona za pomocą polecenia PERFORM HASH of FILE, jeżeli DF jest wybrany oraz jeżeli karta do tachografu jest zresetowana.”;

(ii) pozycja TCS_123 otrzymuje brzmienie:

„TCS_123 Aplikacja tachograficzna 2. generacji musi obsługiwać algorytm SHA-2 (SHA-256, SHA-384 lub SHA-512), określony za pomocą mechanizmu szyfrowania w dodatku 11 część B dla klucza podpisu karty Card_Sign.”;

(iii) tabela w pozycji TCS_124 otrzymuje brzmienie:

„Bajt	Długość	Wartość	Opis
CLA	1	»80h«	CLA
INS	1	»2Ah«	wykonanie operacji zabezpieczającej
P1	1	»90h«	znacznik: Hash
P2	1	»00h«	algorytm niejawnie znany W przypadku aplikacji tachograficznej 1. generacji: SHA-1 W przypadku aplikacji tachograficznej 2. generacji: algorytm SHA-2 (SHA-256, SHA-384 lub SHA-512) zdefiniowany za pomocą mechanizmu szyfrowania w dodatku 11 część B dla klucza podpisu karty Card_Sign”

r) w pkt 3.5.14 wprowadza się następujące zmiany:

tekst pod nagłówkiem aż do pozycji TCS_126 otrzymuje brzmienie:

„Polecenia tego używa się do obliczania podpisu cyfrowego z obliczonego wcześniej kodu skrótu (zob. polecenie PERFORM HASH of FILE, pkt 3.5.13).

Tylko karta kierowcy i karta warsztatowa są zobowiązane obsługiwać to polecenie w DF Tachograph i DF Tachograph_G2.

Inne rodzaje kart do tachografów mogą, ale nie muszą realizować tego polecenia. W przypadku aplikacji tachograficznej 2. generacji jedynie karta kierowcy i karta warsztatowa mają klucz podpisu 2. generacji, inne karty nie mają możliwości skutecznego wykonania polecenia i kończą je odpowiednim kodem błędu.

Polecenie może, ale nie musi być dostępne w MF. Jeżeli polecenie nie jest dostępne w MF, zostaje zakończone odpowiednim kodem błędu.

Polecenie to jest zgodne z normą ISO/IEC 7816-8. Zastosowanie tego polecenia jest ograniczone w porównaniu z poleceniem zdefiniowanym w tej normie.”;

s) w pkt 3.5.15 wprowadza się następujące zmiany:

(i) tabela w pozycji TCS_133 otrzymuje brzmienie:

„Bajt	Długość	Wartość	Opis
CLA	1	»00h«	CLA
INS	1	»2Ah«	wykonanie operacji zabezpieczającej
P1	1	»00h«	
P2	1	»A8h«	Znacznik: pole danych zawiera obiekty DO stosowne do weryfikacji
Lc	1	»XXh«	Lc długość następnego pola danych
#6	1	»9Eh«	znacznik dla podpisu cyfrowego
#7 lub #7-#8	L	»NNh« lub »81 NNh«	Długość podpisu cyfrowego (L ma 2 bajty, jeżeli podpis cyfrowy jest dłuższy niż 127 bajtów): 128 bajtów kodowanych zgodnie z dodatkiem 11 część A dla aplikacji tachograficznej 1. generacji. w zależności od wybranej krzywej dla aplikacji tachograficznej 2. generacji (zob. dodatek 11 część B).
#(7+L)-#(6+L+NN)	NN	»XX..XXh«	treść podpisu cyfrowego”

(ii) w pozycji TCS_134 dodaje się tiret w brzmieniu:

„— Jeżeli wybrany klucz publiczny (używany do weryfikacji podpisu cyfrowego) ma CHA.LSB (Certificate-HolderAuthorisation.equipmentType), które nie jest odpowiednie dla weryfikacji podpisu cyfrowego zgodnie z dodatkiem 11, zwróconym stanem przetwarzania jest »6985«.”;

t) w pkt 3.5.16 wprowadza się następujące zmiany:

(i) w tabeli w pozycji TCS_138 dodaje się wiersz w brzmieniu:

„5 + L + 1	1	»00h«	zgodnie ze specyfikacją w normie ISO/IEC 7816-4”
------------	---	-------	--

(ii) w pozycji TCS_139 dodaje się akapit w brzmieniu:

„— »6985« wskazuje, że 4-bajtowy znacznik czasu podany w polu danych dotyczących polecenia jest wcześniejszy niż cardValidityBegin lub późniejszy niż cardExpiryDate.”;

u) w pkt 4.2.2 wprowadza się następujące zmiany:

(i) w strukturze danych w pozycji TCS_154 wiersze od DF Tachograph G2 do EF CardMA_Certificate oraz wiersze od EF GNSS_Places do końca tego podpunktu otrzymują brzmienie:

„

Plik / element danych	Liczba rekordów	Wielkość (w bajtach)		Wartości domyślne
		Min.	Maks.	
└ DF Tachograph_G2		20268	40316	
└ EF Application_Identification		17	17	
└└ DriverCardApplicationIdentification		17	17	
└└└ typeOfTachographCardId		1	1	{00}
└└└ cardStructureVersion		2	2	{00 00}
└└└ noOfEventsPerType		1	1	{00}
└└└ noOfFaultsPerType		1	1	{00}
└└└ activityStructureLength		2	2	{00 00}
└└└ noOfCardVehicleRecords		2	2	{00 00}
└└└ noOfCardPlaceRecords		2	2	{00 00}
└└└ noOfGNSSADRecords		2	2	{00 00}
└└└ noOfSpecificConditionRecords		2	2	{00 00}
└└└ noOfCardVehicleUnitRecords		2	2	{00 00}
└ EF CardMA_Certificate		204	341	

...

EF GNSS_Places		4538	6050	
└ GNSSContinuousDriving		4538	6050	
└└ gnssADPointerNewestRecord		2	2	{00 00}
└└ gnssAccumulatedDrivingRecords		4536	6048	
└└└ GNSSContinuousDrivingRecord	n ₈	18	18	
└└└└ timeStamp		4	4	{00..00}
└└└└ gnssPlaceRecord		14	14	
└└└└└ timeStamp		4	4	{00..00}
└└└└└ gnssAccuracy		1	1	{00}
└└└└└ geoCoordinates		6	6	{00..00}
└└└└└ vehicleOdometerValue		3	3	{00..00}

„

(ii) w pozycji TCS_155 element NoOfGNSSCDRecords w tabeli otrzymuje brzmienie:

„n ₈ ”	NoOfGNSSADRecords	252	336”
-------------------	-------------------	-----	------

v) w pkt 4.3.1 tekst towarzyszący skrótowi SC4 w pozycji TCS_156 otrzymuje brzmienie:

„**SC4** Dla polecenia READ BINARY z parzystym bajtem INS:

(SM-C-MAC-G1 AND SM-R-ENC-MAC-G1) OR

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

Dla polecenia READ BINARY z nieparzystym bajtem INS (jeżeli obsługiwane): NEV”;

w) w pkt 4.3.2 wprowadza się następujące zmiany:

(i) w strukturze danych w pozycji TCS_162 wiersze od DF Tachograph G2 do EF CardMA_Certificate, wiersze od EF Calibration do extendedSealIdentifier oraz wiersze od EF GNSS_Places do vehicleOdometerValue otrzymują brzmienie:

”

Plik / element danych	Liczba rekordów w	Wielkość (w bajtach)		Wartości domyślne
		Min	Max	
DF Tachograph_G2	1878	49787		
EF Application_Identification	19	19		
L WorkshopCardApplicationIdentificatio	19	19		
typeOfTachographCardId	1	1		{00}
cardStructureVersion	2	2		{00 00}
noOfEventsPerType	1	1		{00}
noOfFaultsPerType	1	1		{00}
activityStructureLength	2	2		{00 00}
noOfCardVehicleRecords	2	2		{00 00}
noOfCardPlaceRecords	2	2		{00 00}
noOfCalibrationRecords	2	2		{00 00}
noOfGNSSADRecords	2	2		{00 00}
noOfSpecificConditionRecords	2	2		{00 00}
noOfCardVehicleUnitRecords	2	2		{00 00}
EF CardMA_Certificate	204	341		
...				
EF Calibration	15668	45394		
L WorkshopCardCalibrationData	15668	45394		
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		2	2	{00}
calibrationRecords	15664	45390		
L WorkshopCardCalibrationRecord	n ₅	178	178	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}
oldTimeValue		4	4	{00..00}
newTimeValue		4	4	{00..00}
nextCalibrationDate		4	4	{00..00}
vuPartNumber		16	16	{20..20}
vuSerialNumber		8	8	{00..00}
sensorSerialNumber		8	8	{00..00}
sensorGNSSSerialNumber		8	8	{00..00}
rcmSerialNumber		8	8	{00..00}
vuAbility		1	1	{00}
sealDataCard		56	56	
noOfSealRecords		1	1	{00}
SealRecords		55	55	
L SealRecord	5	11	11	
equipmentType		1	1	{00}
extendedSealIdentifier		10	10	{00..00}

...

EF	GNSS_Places		326	434	
	└ GNSSContinuousDriving		326	434	
	└ gnssADPointerNewestRecord		2	2	{00 00}
	└ gnssAccumulatedDrivingRecords		324	432	
	└ GNSSContinuousDrivingRecord	n ₈	18	18	
	└ timeStamp		4	4	{00..00}
	└ gnssPlaceRecord		14	14	
	└ timeStamp		4	4	{00..00}
	└ gnssAccuracy		1	1	{00}
	└ geoCoordinates		6	6	{00..00}
	└ vehicleOdometerValue		3	3	{00..00}

„

(ii) w pozycji TCS_163 element NoOfGNSSCDRecords w tabeli otrzymuje brzmienie:

„n ₈	NoOfGNSSADRecords	18	24”
-----------------	-------------------	----	-----

31) w pkt 2 dodatku 3 wprowadza się następujące zmiany:

- a) po wierszu z piktogramami „miejsce rozpoczęcia dziennego okresu pracy” i „miejsce zakończenia dziennego okresu pracy” dodaje się wiersz w brzmieniu:

„ położenie po 3 godzinach skumulowanego czasu prowadzenia pojazdu”;

- b) kombinacja piktogramów „korekta czasu (w warsztacie)” otrzymuje brzmienie:

„  konflikt czasu lub korekta czasu (w warsztacie)”;

- c) do wykazu zdarzeń dodaje się następujące kombinacje piktogramów:

„ brak informacji o pozycji z odbiornika GNSS lub błąd połączenia z urządzeniem zewnętrznym GNSS;

!  błąd połączenia z urządzeniem do łączności na odległość”;

32) w dodatku 4 wprowadza się następujące zmiany:

- a) w pkt 2 wprowadza się następujące zmiany:

(i) blok nr 11.4 otrzymuje brzmienie:

„11.4 Wprowadzanie miejsca rozpoczęcia lub zakończenia dziennego okresu pracy

pi = piktogram miejsca rozpoczęcia / zakończenia, godzina,
kraj, region
długość geograficzna zarejestrowanej pozycji
szerokość geograficzna zarejestrowanej pozycji
znacznik momentu określenia pozycji
Stan licznika kilometrów

pihh:mm Cou Reg
lon ±DDD°MM.M'
lat ± DD°MM.M'
hh:mm
x xxx xxx km”

(ii) blok nr 11.5 otrzymuje brzmienie:

„11.5 Położenia po 3 godzinach skumulowanego czasu prowadzenia pojazdu”;
pi = położenie po 3 godzinach skumulowanego czasu prowadzenia pojazdu;

godzina
długość geograficzna zarejestrowanej pozycji
szerokość geograficzna zarejestrowanej pozycji
znacznik momentu określenia pozycji
Stan licznika kilometrów

pihh:mm
lon ± DDD°MM.M'
lat ± DD°MM.M'
hh:mm
x xxx xxx km'

b) w pkt 3.1 pozycja 11.15 formatu dziennego wydruku otrzymuje brzmienie:

„11.5	Położenia po 3 godzinach skumulowanego czasu prowadzenia pojazdu w kolejności chronologicznej”
-------	--

c) w pkt 3.2 format dziennego wydruku otrzymuje brzmienie:

„1	Data i godzina drukowania dokumentu
2	Typ wydruku
3	Identyfikacja posiadacza karty (dla wszystkich kart włożonych do VU + GEN)
4	Identyfikacja pojazdu (tego, dla którego sporządzany jest wydruk)
5	Identyfikacja VU (z którego uzyskano wydruk +GEN)
6	Ostatnia kalibracja tego VU
7	Ostatnia kontrola tego tachografu
9	Ogranicznik czynności kierowcy
10	Ogranicznik szczeliny czytnika karty kierowcy (szczelina 1)
10 a	Stan poza zakresem na początku danego dnia
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Czynności w kolejności chronologicznej (szczelina czytnika karty kierowcy)
10	Ogranicznik szczeliny czytnika karty współkierowcy (szczelina 2)
10a	Stan poza zakresem na początku danego dnia
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Czynności w kolejności chronologicznej (szczelina czytnika karty współkierowcy)
11	Ogranicznik dziennego zestawienia
11.1	Zestawienie okresów bez karty w szczelinie czytnika karty kierowcy
11.4	Miejsca wprowadzone w kolejności chronologicznej
11.5	Położenia po 3 godzinach skumulowanego czasu prowadzenia pojazdu w kolejności chronologicznej
11.7	Podsumowania dla czynności
11.2	Zestawienie okresów bez karty w szczelinie czytnika karty współkierowcy
11.4	Miejsca wprowadzone w kolejności chronologicznej
11.5	Położenia po 3 godzinach skumulowanego czasu prowadzenia pojazdu w kolejności chronologicznej

11.8	Podsumowania dla czynności
11.3	Zestawienie czynności dla kierowcy z uwzględnieniem obu szczelin czytnika kart
11.4	Miejsca wprowadzone przez danego kierowcę w kolejności chronologicznej
11.5	Położenia po 3 godzinach skumulowanego czasu prowadzenia pojazdu w kolejności chronologicznej
11.9	Podsumowania dla czynności danego kierowcy
13.1	Ogranicznik zdarzeń/ usterek
13.4	Rekordy zdarzeń/ usterek (5 ostatnich zdarzeń lub usterek zapisanych lub trwających na VU)
22.1	Miejsce kontroli
22.2	Podpis kontrolera
22.3	Od godziny (miejsce przeznaczone dla kierowcy bez karty w celu wskazania
22.4	Do godziny dotyczących go okresów)
22.5	Podpis kierowcy”

d) w pkt 3.7 pozycja PRT_014 otrzymuje brzmienie:

„PRT_014 Wydruk historii włożonych kart jest zgodny z poniższym formatem:

1	Data i godzina drukowania dokumentu
2	Typ wydruku
3	Identyfikacja posiadacza karty (dla wszystkich kart włożonych do przyrządu rejestrującego)
23	Karta ostatnio włożona do VU
23.1	Włożone karty (maks. 88 rekordów)
12.3	Ogranicznik usterek”

33) w dodatku 7 wprowadza się następujące zmiany:

a) pkt 1.1 otrzymuje brzmienie:

„1.1. **Zakres**

Dane mogą być pobierane na ESM:

- z przyrządu rejestrującego za pośrednictwem inteligentnego urządzenia dedykowanego (IDE) przyłączonego do VU,
- z karty do tachografu za pośrednictwem IDE spasowanego z czytnikiem karty (IFD),
- z karty do tachografu za pośrednictwem przyrządu rejestrującego poprzez IDE przyłączone do VU.

Aby umożliwić weryfikację autentyczności i integralności pobranych danych przechowywanych na ESM, dane są pobierane razem z dołączonym podpisem, zgodnie z dodatkiem 11 »Wspólne mechanizmy zabezpieczenia«. Razem z danymi pobierane są również identyfikacja urządzenia źródłowego (VU lub karta) i jego świadectwa bezpieczeństwa (państwo członkowskie i urządzenie). Niezależnie od tego weryfikator danych musi mieć zaufany europejski klucz publiczny.

Dane pobrane z przyrządu rejestrującego są podpisywane przy użyciu wspólnych mechanizmów zabezpieczeń określonych w dodatku 11 część B (System tachografu drugiej generacji), z wyjątkiem sytuacji, gdy kontrolę kierowców przeprowadza organ kontrolny spoza UE, używając karty kontrolnej pierwszej generacji, w którym to przypadku dane są podpisywane przy użyciu wspólnych mechanizmów zabezpieczeń określonych w dodatku 11 część A (System tachografu pierwszej generacji), zgodnie z wymogiem określonym w dodatku 15 »Migracja«, wymóg MIG_015.

Niniejszy dodatek określa zatem dwa typy pobrań danych z VU:

- pobranie danych z VU typu 2. generacji, zapewniające strukturę danych 2. generacji, podpisanych przy użyciu wspólnych mechanizmów zabezpieczeń określonych w dodatku 11 część B,
- pobranie danych z VU typu 1. generacji, zapewniające strukturę danych 1. generacji, podpisanych przy użyciu wspólnych mechanizmów zabezpieczeń określonych w dodatku 11 część A,

Analogicznie występują dwa typy pobrań danych z kart kierowcy 2. generacji włożonych do przyrządu rejestrującego, jak określono w pkt 3 i 4 niniejszego dodatku.”;

b) w pkt 2.2.2 wprowadza się następujące zmiany:

(i) tabela otrzymuje brzmienie:

„Struktura komunikatu		Maks. 4 bajty Nagłówek				Maks. 255 bajtów Dane			1 bajt Suma kontrolna
IDE ->	<- VU	FMT	TGT	SRC	LEN	SID	DS_ / TRTP	DANE	CS
Start Communication Request		81	EE	F0		81			E0
Positive Response Start Communication		80	F0	EE	03	C1		EA, 8F	9B
Start Diagnostic Session Request		80	EE	F0	02	10	81		F1
Positive Response Start Diagnostic		80	F0	EE	02	50	81		31
Link Control Service									
Verify Baud Rate (stage 1)									
9 600 Bd		80	EE	F0	04	87		01,01,01	EC
19 200 Bd		80	EE	F0	04	87		01,01,02	ED
38 400 Bd		80	EE	F0	04	87		01,01,03	EE
57 600 Bd		80	EE	F0	04	87		01,01,04	EF
115 200 Bd		80	EE	F0	04	87		01,01,05	F0
Positive Response Verify Baud Rate		80	F0	EE	02	C7		01	28
Transition Baud Rate (stage 2)		80	EE	F0	03	87		02,03	ED
Request Upload		80	EE	F0	0A	35		00,00,00,0-0,00,FF,FF,FF,FF	99
Positive Response Request Upload		80	F0	EE	03	75		00,FF	D5
Transfer Data Request									
Overview		80	EE	F0	02	36	01 lub 21		97
Activities		80	EE	F0	06	36	02 lub 22	Date	CS
Events & Faults		80	EE	F0	02	36	03 lub 23		99
Detailed Speed		80	EE	F0	02	36	04 lub 24		9A
Technical Data		80	EE	F0	02	36	05 lub 25		9B
Card download		80	EE	F0	02	36	06	Slot	CS

Struktura komunikatu	Maks. 4 bajty Nagłówek				Maks. 255 bajtów Dane			1 bajt Suma kontrolna		
	IDE ->	<- VU	FMT	TGT	SRC	LEN	SID	DS_ / TRTP	DANE	CS
Positive Response Transfer Data			80	F0	EE	Len	76	TREP	Data	CS
Request Transfer Exit			80	EE	F0	01	37			96
Positive Response Request Transfer Exit			80	F0	EE	01	77			D6
Stop Communication Request			80	EE	F0	01	82			E1
Positive Response Stop Communication			80	F0	EE	01	C2			21
Acknowledge sub message			80	EE	F0	Len	83		Data	CS
Negative responses										
General reject			80	F0	EE	03	7F	Sid Req	10	CS
Service not supported			80	F0	EE	03	7F	Sid Req	11	CS
Sub function not supported			80	F0	EE	03	7F	Sid Req	12	CS
Incorrect Message Length			80	F0	EE	03	7F	Sid Req	13	CS
Conditions not correct or Request sequence error			80	F0	EE	03	7F	Sid Req	22	CS
Request out of range			80	F0	EE	03	7F	Sid Req	31	CS
Upload not accepted			80	F0	EE	03	7F	Sid Req	50	CS
Response pending			80	F0	EE	03	7F	Sid Req	78	CS
Data not available			80	F0	EE	03	7F	Sid Req	FA	CS"

(ii) do uwag pod tabelą dodaje się tiret w brzmieniu:

„— TRTP 21–25 używa się w przypadku żądań pobrania danych z przyrządu rejestrującego typu 2. generacji, TRTP 01–05 używa się w przypadku żądań pobrania danych z przyrządu rejestrującego typu 1. generacji, które mogą zostać zaakceptowane przez przyrząd rejestrujący w ramach kontroli kierowcy przeprowadzanej przez organ kontrolny spoza UE przy użyciu karty kontrolnej 1. generacji,

— TRTP 11–19 oraz 31–39 są zarezerwowane dla żądań pobrania swoistych dla producenta.”;

c) w pkt 2.2.2.9 wprowadza się następujące zmiany:

(i) punkt DDP_011 otrzymuje brzmienie:

„DDP_011 IDE wysyła żądanie »Transfer Data Request« w celu wskazania VU typu danych, które mają być pobierane. Jednobajtowy parametr »Transfer Request Parameter« (TRTP) wskazuje typ przesyłania.

Rozróżnia się sześć typów przesyłania danych: Na potrzeby pobierania danych z przyrządu rejestrującego dla każdego typu transferu można użyć dwóch różnych wartości TRTP:

Typ transferu danych	Wartość TRTP w przypadku żądań pobrania danych z przyrządu rejestrującego typu 1. generacji	Wartość TRTP w przypadku żądań pobrania danych z przyrządu rejestrującego typu 2. generacji
Przegląd	01	21
Czynności o określonej dacie	02	22
Zdarzenia i usterki	03	23
Szczegółowe dane dotyczące prędkości	04	24
Dane techniczne	05	25

Typ transferu danych	Wartość TRTP
Pobieranie danych z karty	06"

(ii) pozycja DDP_054 otrzymuje brzmienie:

„DDP_054 IDE musi obowiązkowo zażądać przesłania danych Informacje ogólne (TRTP 01 lub 21) w czasie sesji pobierania, ponieważ tylko to zagwarantuje, że certyfikaty VU są zarejestrowane w pobieranym pliku (i umożliwi weryfikację podpisu cyfrowego).

W drugim przypadku (TRTP 02 lub 22) w komunikacie »Transfer Data Request« znajduje się informacja o dniu kalendarzowym (format TimeReal), dla którego dane mają być pobrane.”;

d) w pkt 2.2.2.10 pozycja DDP_055 otrzymuje brzmienie:

„DDP_055 W pierwszym przypadku (TREP 01 lub 21) VU wyśle dane pomagające operatorowi IDE w wyborze danych, które chce dalej pobrać. Komunikat ten zawiera następujące informacje:

- świadectwa bezpieczeństwa,
- identyfikacja pojazdu,
- bieżąca data i godzina VU,
- minimalna i maksymalna data, dla której można dokonać pobrania (dane z VU),
- sygnalizacja obecności kart w VU,
- poprzednie pobranie dla firmy,
- blokady firmowe,
- poprzednie kontrole.”;

e) w pkt 2.2.2.16 tiret ostatnie pozycji DDP_018 otrzymuje brzmienie:

„— FA brak dostępnych danych

Obiekt danych żądania transferu danych nie jest dostępny w przyrządzie rejestrującym (np. karta nie jest włożona, zażądano pobrania danych z przyrządu rejestrującego typu generacji 1 poza ramami kontroli kierowców przez organ kontrolny spoza UE ...).”;

f) w pkt 2.2.6.1 wprowadza się następujące zmiany:

(i) pozycja DDP_029 akapit pierwszy otrzymuje brzmienie:

„Pole danych w komunikacie „Positive Response Transfer Data Overview” zawiera następujące dane w określonej tu kolejności pod SID 76 Hex, TREP 01 lub 21 Hex z odpowiednim podziałem na podkomunikaty i licznikami.”;

(ii) nagłówek „Struktura danych 1. generacji” otrzymuje brzmienie:

„Struktura danych 1. generacji (TREP 01 Hex)”;

(iii) nagłówek „Struktura danych 2. generacji” otrzymuje brzmienie:

„Struktura danych 2. generacji (TREP 21 Hex)”;

g) w pkt 2.2.6.2 wprowadza się następujące zmiany:

(i) pozycja DDP_030 akapit pierwszy otrzymuje brzmienie:

„Pole danych w komunikacie »Positive Response Transfer Data Activities« zawiera następujące dane w określonej tu kolejności pod SID 76 Hex, TREP 02 lub 22 Hex z odpowiednim podziałem na podkomunikaty i licznikami:”;

(ii) nagłówek „Struktura danych 1. generacji” otrzymuje brzmienie:

„Struktura danych 1. generacji (TREP 02 Hex)”;

(iii) nagłówek „Struktura danych 2. generacji” otrzymuje brzmienie:

„Struktura danych 2. generacji (TREP 22 Hex)”;

(iv) element VuGNSSCDRecordArray pod nagłówkiem „Struktura danych 2. generacji (TREP 22 Hex)” otrzymuje brzmienie:

„VuGNSSADRecordArray

Pozycje GNSS dla pojazdu, gdy skumulowany czas prowadzenia pojazdu osiągnie wielokrotność trzech godzin. Jeżeli sekcja jest pusta, wysłany jest nagłówek tablicy z noOfRecords = 0.”

h) w pkt 2.2.6.3 wprowadza się następujące zmiany:

(i) pozycja DDP_031 akapit pierwszy otrzymuje brzmienie:

„Pole danych w komunikacie »Positive Response Transfer Data Events and Faults« zawiera następujące dane w określonej tu kolejności pod SID 76 Hex, TREP 03 lub 23 Hex, z odpowiednim podziałem na podkomunikaty i z licznikami:”;

(ii) nagłówek „Struktura danych 1. generacji” otrzymuje brzmienie:

„Struktura danych 1. generacji (TREP 03 Hex)”;

(iii) nagłówek „Struktura danych 2. generacji” otrzymuje brzmienie:

„Struktura danych 2. generacji (TREP 23 Hex)”;

(iv) skreśla się element VuTimeAdjustmentGNSSRecordArray pod nagłówkiem „Struktura danych 2. generacji (TREP 23 Hex)”;

i) w pkt 2.2.6.4 wprowadza się następujące zmiany:

(i) pozycja DDP_032 akapit pierwszy otrzymuje brzmienie:

„Pole danych w komunikacie »Positive Response Transfer Data Detailed Speed« zawiera następujące dane w określonej tu kolejności pod SID 76 Hex, TREP 04 lub 24 Hex z odpowiednim podziałem na podkomunikaty i licznikami:”;

- (ii) nagłówek „Struktura danych 1. generacji” otrzymuje brzmienie:
- „Struktura danych 1. generacji (TREP 04)”;
- (iii) nagłówek „Struktura danych 2. generacji” otrzymuje brzmienie:
- „Struktura danych 2. generacji (TREP 24)”;
- j) w pkt 2.2.6.5 wprowadza się następujące zmiany:
- (i) pozycja DDP_033 akapit pierwszy otrzymuje brzmienie:
- „Pole danych w komunikacie »Positive Response Transfer Data Technical Data« zawiera następujące dane w określonej tu kolejności pod SID 76 Hex, TREP 05 lub 25 Hex z odpowiednim podziałem na podkomunikaty i licznikami:”;
- (ii) nagłówek „Struktura danych 1. generacji” otrzymuje brzmienie:
- „Struktura danych 1. generacji (TREP 05)”;
- (iii) nagłówek „Struktura danych 2. generacji” otrzymuje brzmienie:
- „Struktura danych 2. generacji (TREP 25)”;
- k) w pkt 3.3 pozycja DDP_035 otrzymuje brzmienie:
- „DDP_035 Pobieranie danych z karty do tachografu obejmuje następujące kroki:
- Pobieranie wspólnych informacji zawartych na karcie w plikach EF ICC oraz IC Dane te są nieobowiązkowe i nie są chronione podpisem cyfrowym.
 - (w przypadku kart do tachografów pierwszej i drugiej generacji) Pobieranie w plikach EF w Tachograph DF:
 - Wczytanie plików EF Card_Certificate i CA_Certificate Dane te nie są chronione podpisem cyfrowym.
- Pobranie tych plików jest obowiązkowe dla każdej sesji pobierania.
- wczytanie plików EF zawierających inne dane aplikacyjne (w Tachograph DF) z wyłączeniem EF Card_Download Informacje takie są zabezpieczone podpisem cyfrowym przy użyciu wspólnych mechanizmów zabezpieczenia określonych w dodatku 11 część A.
 - Pobranie przynajmniej plików EF Application_Identification i Identification jest obowiązkowe dla każdej sesji pobierania.
 - Przy pobieraniu danych z karty kierowcy obowiązkowe jest pobranie także następujących plików EF:
 - Events_Data,
 - Faults_Data,

- Driver_Activity_Data,
 - Vehicles_Used,
 - Places,
 - Control_Activity_Data,
 - Specific_Conditions,
- (w przypadku wyłącznie kart do tachografów drugiej generacji) Z wyjątkiem sytuacji gdy pobranie danych z karty kierowcy włożonej do przyrządu rejestrującego odbywa się w trakcie kontroli kierowców przeprowadzanej przez organ kontrolny spoza UE przy użyciu karty kontrolnej pierwszej generacji, pobieranie w plikach EF Tachograph_G2 DF:

- Pobieranie w plikach EF CardSignCertificate, CA_Certificate oraz Link_Certificate (jeżeli występują). Dane te nie są chronione podpisem cyfrowym.

Pobranie tych plików jest obowiązkowe dla każdej sesji pobierania.

- Wczytanie plików EF zawierających inne dane aplikacyjne (w Tachograph_G2 DF) z wyłączeniem EF Card_Download Informacje takie są zabezpieczone podpisem cyfrowym przy użyciu wspólnych mechanizmów zabezpieczenia określonych w dodatku 11 część B.
- Pobranie przynajmniej plików EF Application_Identification i Identification jest obowiązkowe dla każdej sesji pobierania.
- Przy pobieraniu danych z karty kierowcy obowiązkowe jest pobranie także następujących plików EF:

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

- Przy wczytywaniu danych z karty kierowcy aktualizowana jest data LastCardDownload w pliku EF Card_Download w DF Tachograph i, w stosownych przypadkach, Tachograph_G2
- Przy pobieraniu danych z karty warsztatowej zerowany jest licznik kalibracji w pliku EF Card_Download w DF Tachograph i, w stosownych przypadkach, Tachograph_G2

— Przy pobieraniu danych z karty warsztatowej pliki EF Sensor_Installation_Data w DF Tachograph i, w stosownych przypadkach, Tachograph_G2 nie mogą być pobierane.”;

l) pkt 3.3.2 pozycja DDP_037 akapit pierwszy otrzymuje brzmienie:

„Sekwencja pobierania plików elementarnych ICC, IC, Card_Certificate (lub CardSignCertificate dla DF Tachograph_G2), CA_Certificate i Link_Certificate (wyłącznie dla DF Tachograph_G2) jest następująca.”;

m) w pkt 3.3.3 tabela otrzymuje brzmienie:

„Karta	Kierunek	IDE/IFD	Znaczenie / Uwagi
	←	Select File	
OK	⇒		
	←	Perform Hash of File	— Oblicza wartość skrótu dla danych wybranego pliku przy pomocy wymaganego algorytmu skrótu zgodnie z dodatkiem 11 część A lub B. Polecenie to nie jest poleceniem ISO.
oblicz skrót pliku i czasowo zachowaj wartość skrótu			
OK	⇒		
	←	Read Binary	Jeżeli wielkość danych w pliku jest większa od pojemności bufora czytnika lub karty, polecenie musi być powtarzane aż do odczytania całego pliku.
File Data OK	⇒	zapisz odebrane dane na ESM	zgodnie z 3.4 Data storage format
	←	PSO: Compute Digital Signature	
wykonaj operację zabezpieczającą »Compute Digital Signature«, używając czasowo zachowaną wartość skrótu			
Signature OK	⇒	dołącz dane do poprzednio zapisanych danych na ESM	zgodnie z 3.4 Data storage format”

n) w pkt 3.4.2 pozycja DDP_046 otrzymuje brzmienie:

„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 EF (FID) w DF Tachograph lub wspólnych informacji zawartych na karcie	3 bajty
FID (2 bajty) »01«	Znacznik podpisu pliku EF (FID) w DF Tachograph	3 bajty
FID (2 bajty) »02«	Znacznik podpisu pliku EF (FID) w DF Tachograph_G2	3 bajty
FID (2 bajty) »03«	Znacznik podpisu pliku EF (FID) w DF Tachograph_G2	3 bajty
xx xx	długość pola wartości	2 bajty

Przykładowe dane w pliku pobranym na ESM:

Znacznik	Długość	Wartość
00 02 00	00 11	— Dane pliku EF ICC
C1 00 00	00 C2	— Dane pliku EF Card_Certificate
		— ...
05 05 00	0A 2E	Dane pliku EF Vehicles_Used (w DF Tachograph)
05 05 01	00 80	Podpis pliku EF Vehicles_Used (w DF Tachograph)
05 05 02	0A 2E	Dane pliku EF Vehicles_Used w DF Tachograph_G2
05 05 03	xx xx	Podpis pliku EF Vehicles_Used_Used w DF Tachograph_G2 ”

o) w pkt 4 pozycja DDP_049 otrzymuje brzmienie:

„DDP_049 Karty kierowcy pierwszej generacji: Dane pobiera się przy użyciu protokołu pobierania danych pierwszej generacji, a pobierane dane muszą mieć taki sam format jak dane pobierane z przyrządu rejestrującego pierwszej generacji.

Karty kierowcy drugiej generacji: Następnie VU pobiera wszystkie dane z karty, plik po pliku, zgodnie z protokołem pobierania danych z karty zdefiniowanym w pkt 3, oraz przekazuje wszystkie dane odebrane z karty do IDE w odpowiednim formacie pliku TLV (zob. 3.4.2) i zapakowane w komunikacie »Positive Response Transfer Data«.”;

34) w dodatku 8 w pkt 2 akapit pod nagłówkiem „Odniesienia” otrzymuje brzmienie:

„ISO 14230-2: Pojazdy drogowe – Systemy diagnostyczne – Protokół słowa kluczowego 2000 – część 2: Warstwa łącza danych.

Wydanie pierwsze: 1999.”;

35) w dodatku 9 wprowadza się następujące zmiany:

a) pkt 6 spisu treści otrzymuje brzmienie:

„6. BADANIA ZEWNĘTRZNEGO URZĄDZENIA DO ŁĄCZNOŚCI NA ODLEGŁOŚĆ”;

b) w pkt 1.1 tiret pierwsze otrzymuje brzmienie:

„— **świadczenie bezpieczeństwa**, opartym na specyfikacjach normy »Common Criteria«, w odniesieniu do celu bezpieczeństwa w pełni zgodnego z celami przedstawionymi w dodatku 10 do niniejszego załącznika.”;

c) w pkt 2 tabela dotycząca badań funkcjonalności przyrządu rejestrującego otrzymuje brzmienie:

„Nr	Badanie	Opis	Powiązane wymogi
1	Badanie administracyjne		
1.1	Dokumentacja	Prawidłowość dokumentacji	
1.2	Wyniki badań producenta	Wyniki badań producenta przeprowadzonych podczas integracji. Przedstawienie dokumentów papierowych.	88, 89,91
2	Kontrola wizualna		
2.1	Zgodność z dokumentacją		
2.2	Identyfikacja/oznakowanie		224–226
2.3	Materiały		219–223
2.4	Plombowanie		398, 401–405
2.5	Interfejsy zewnętrzne		
3	Badania funkcjonalności		
3.1	Obsługiwane funkcje		02, 03, 04, 05, 07, 382
3.2	Tryby pracy		09–11*, 134, 135
3.3	Prawa dostępu do funkcji i danych		12* 13*, 382, 383, 386–389
3.4	Monitorowanie wkładania i wyjmowania kart		15, 16, 17, 18, 19*, 20*, 134
3.5	Pomiar prędkości i odległości		21–31
3.6	Pomiar czasu (badanie przeprowadzone w temperaturze 20 °C)		38–43
3.7	Monitorowanie czynności kierowcy		44–53, 134
3.8	Monitorowanie stanu prowadzenia pojazdu		54, 55, 134
3.9	Pozycje wprowadzane ręcznie		56–62
3.10	Zarządzanie blokadami firmowymi		63–68
3.11	Monitorowanie czynności kontrolnych		69, 70
3.12	Wykrywanie zdarzeń lub usterek		71–88, 134

Nr	Badanie	Opis	Powiązane wymogi
3.13	Dane identyfikujące urządzenie		93*, 94*, 97, 100
3.14	Dane dotyczące wkładania i wyjmowania karty kierowcy		102*–104*
3.15	Dane dotyczące czynności kierowcy		105*–107*
3.16	Dane dotyczące miejsc i położenia		108*–112*
3.17	Dane dotyczące licznika kilometrów		113*–115*
3.18	Szczegółowe dane dotyczące prędkości		116*
3.19	Dane dotyczące zdarzeń		117*
3.20	Dane dotyczące usterek		118*
3.21	Dane dotyczące kalibracji		119*–121*
3.22	Dane dotyczące korekty czasu		124*, 125*
3.23	Dane dotyczące czynności kontrolnej		126*, 127*
3.24	Dane dotyczące blokad firmowych		128*
3.25	Dane dotyczące czynności pobierania		129*
3.26	Dane dotyczące warunków szczególnych		130*, 131*
3.27	Rejestrowanie i przechowywanie danych na kartach do tachografu		136, 137, 138*, 139*, 141*, 142, 143 144, 145, 146*, 147*, 148*, 149, 150
3.28	Wyświetlanie		90, 134, 151–168 PIC_001, DIS_001
3.29	Drukowanie		90, 134, 169–181, PIC_001, PRT_001–PRT_014
3.30	Ostrzeganie		134, 182–191, PIC_001
3.31	Pobieranie danych na nośnik zewnętrzny		90, 134, 192–196
3.32	Łączność na odległość na potrzeby ukierunkowanych kontroli drogowych		197–199
3.33	Wyprowadzanie danych do dodatkowych urządzeń zewnętrznych		200, 201
3.34	Kalibracja		202–206*, 383, 384, 386–391
3.35	Drogowe kontrole kalibracji		207–209
3.36	Korekta czasu		210–212*
3.37	Niezakłócanie funkcji dodatkowych		06, 425

Nr	Badanie	Opis	Powiązane wymogi
3.38	Interfejs czujnika ruchu		02, 122
3.39	Urządzenie zewnętrzne GNSS		03, 123
3.40	Sprawdzenie, czy VU wykrywa, rejestruje i zapisuje zdarzenie (zdarzenia) lub usterkę (usterki) określone przez producenta VU, gdy sparowany czujnik ruchu reaguje na pola magnetyczne zaburzające wykrywanie ruchu pojazdu.		217
3.41	Pakiet szyfrów i standardowe parametry domeny		CSM_48, CSM_50
4	Badania środowiskowe		
4.1	Temperatura	<p>Sprawdzenie funkcjonalności za pomocą: badania zgodnie z normą ISO 16750-4, rozdział 5.1.1.2: Próba eksploatacyjna w niskiej temperaturze (72 h w temperaturze -20 °C).</p> <p>Badanie to odnosi się do normy IEC 60068-2-1: Badania środowiskowe – Część 2-1: Próby – Próba A: Zimno</p> <p>badania zgodnie z normą ISO 16750-4: Rozdział 5.1.2.2: Próba eksploatacyjna w wysokiej temperaturze (72 h w temperaturze 70 °C).</p> <p>Badanie to odnosi się do normy IEC 60068-2-2: Podstawowe procedury badań środowiskowych – Część 2: Próby – Próba B: Suche gorąco;</p> <p>badania zgodnie z normą ISO 16750-4: Rozdział 5.3.2: Nagła zmiana temperatury z określonym okresem przejściowym (-20 °C / 70 °C, 20 cykli, czas przebywania: 2 h w każdej temperaturze).</p> <p>Można przeprowadzić skrócony zestaw badań (spośród tych zdefiniowanych w sekcji 3 niniejszej tabeli) w niższej temperaturze, wyższej temperaturze i w czasie cykli temperaturowych.</p>	213
4.2	Wilgotność	<p>Sprawdzenie odporności przyrządu rejestrującego na cykliczne zmiany wilgotności (próba gorąca) za pomocą próby wg normy IEC 60068-2-30, w sześciu 24-godzinnych cyklach, w każdym ze zmieniającą się temperaturą od +25 °C do +55 °C i wilgotnością względną 97 % w temperaturze +25 °C i 93 % w temperaturze +55 °C</p>	214
4.3	M/echanika	<p>1. Drgania harmoniczne: sprawdzenie odporności przyrządu rejestrującego na drgania harmoniczne o następujących właściwościach: stałe przemieszczenie przy częstotliwości 5–11 Hz: 10-milimetrowa amplituda; stałe przyspieszenie przy częstotliwości 11–300 Hz: 5g.</p> <p>Wymóg ten sprawdza się za pomocą próby Fc wg normy IEC 60068-2-6, z minimalnym czasem trwania próby 3 × 12 h (12 h na oś).</p> <p>ISO 16750-3 nie wymaga przeprowadzenia badania drgań harmonicznych w przypadku urządzeń znajdujących się w oddzielnej kabinie pojazdu.</p>	219

Nr	Badanie	Opis	Powiązane wymogi
		<p>2. Drgania swobodne:</p> <p>Próba zgodnie z normą ISO 16750-3: Rozdział 4.1.2.8: Próba VIII: Pojazd użytkowy, oddzielna kabina pojazdu.</p> <p>Próba drgań swobodnych: 10...2000 Hz, wertykalna średnia kwadratowa 21,3 m/s², wzdłużna średnia kwadratowa 11,8 m/s², poprzeczna średnia kwadratowa 13,1 m/s², 3 osie, 32 h na oś, w tym cykl temperaturowy -20...70 °C.</p> <p>Badanie to odnosi się do normy IEC 60068-2-64: Badania środowiskowe – Część 2-64: Próby – Próba Fh: Wibracje szerokopasmowe losowe i wytyczne</p> <p>3. Udry:</p> <p>udar mechaniczny przy impulsie półsinusoidalnym 3 g wg normy ISO 16750.</p> <p>Opisane powyżej badania przeprowadza się na różnych próbkach urządzeń poddawanych badaniom.</p>	
4.4	Ochrona przed wodą i ciałami obcymi	Badanie zgodnie z normą ISO 20653: Pojazdy drogowe – Stopień ochrony (kod IP) – Ochrona urządzeń elektrycznych przed ciałami obcymi, wodą i dostępem (bez zmian parametrów); minimalna wartość IP – 40	220, 221
4.5	Zabezpieczenie nadnapięciowe	Sprawdzenie odporności przyrządu rejestrującego na napięcie zasilania: wersje 24 V: 34 V przy +40 °C przez 1 godzinę wersje 12 V: 17 V przy +40 °C przez 1 godzinę(ISO 16750-2)	216
4.6	Zabezpieczenie przed odwróceniem polaryzacji	Sprawdzenie odporności przyrządu rejestrującego na odwrócenie biegunów napięcia zasilającego. (ISO 16750-2)	216
4.7	Zabezpieczenie zwarciove	Sprawdzenie, czy sygnały wyjściowe są zabezpieczone przed zwarcie do napięcia zasilającego i do masy. (ISO 16750-2)	216
5	Badania EMC		
5.1	Emisje radiacyjne i wrażliwość na radiację	Zgodność z regulaminem nr 10 EKG ONZ	218
5.2	Wyładowania elektrostacyjne	Zgodność z normą ISO 10605:2008 + Sprostowanie techniczne:2010 + AMD1:2014: +/- 4kV w przypadku styku i +/- 8kV w przypadku rozładowania do powietrza	218

Nr	Badanie	Opis	Powiązane wymogi
5.3	Wrażliwość na stany nieustalone w zasilaniu	<p>W przypadku wersji 24 V: zgodność z normą ISO 7637-2 i wersją 3 regulaminu nr 10 EKG ONZ:</p> <p>impuls 1a: $V_s = -450 \text{ V}$, $R_i = 50 \text{ omów}$</p> <p>impuls 2a: $V_s = +37 \text{ V}$, $R_i = 2 \text{ omy}$</p> <p>impuls 2b: $V_s = +20 \text{ V}$, $R_i = 0,05 \text{ oma}$</p> <p>impuls 3a: $V_s = -150 \text{ V}$, $R_i = 50 \text{ omów}$</p> <p>impuls 3b: $V_s = +150 \text{ V}$, $R_i = 50 \text{ omów}$</p> <p>impuls 4: $V_s = -16 \text{ V}$, $V_a = -12 \text{ V}$, $t_6 = 100 \text{ ms}$</p> <p>impuls 5: $V_s = +120 \text{ V}$, $R_i = 2,2 \text{ oma}$, $t_d = 250 \text{ ms}$</p> <p>W przypadku wersji 12V: zgodność z normą ISO 7637-1 i wersją 3 regulaminu nr 10 EKG ONZ:</p> <p>impuls 1: $V_s = -75 \text{ V}$, $R_i = 10 \text{ omów}$</p> <p>impuls 2a: $V_s = +37 \text{ V}$, $R_i = 2 \text{ omy}$</p> <p>impuls 2b: $V_s = +10 \text{ V}$, $R_i = 0,05 \text{ oma}$</p> <p>impuls 3a: $V_s = -112 \text{ V}$, $R_i = 50 \text{ omów}$</p> <p>impuls 3b: $V_s = +75 \text{ V}$, $R_i = 50 \text{ omów}$</p> <p>impuls 4: $V_s = -6 \text{ V}$, $V_a = -5 \text{ V}$, $t_6 = 15 \text{ ms}$</p> <p>impuls 5: $V_s = +65 \text{ V}$, $R_i = 3 \text{ omy}$, $t_d = 100 \text{ ms}$</p> <p>Impuls 5 należy testować tylko w przypadku przyrządów rejestrujących przeznaczonych do zainstalowania w pojazdach, w których nie zainstalowano zewnętrznego, wspólnego zabezpieczenia przed spadkiem obciążenia.</p> <p>Aby uzyskać informacje na temat propozycji zabezpieczenia przed spadkiem obciążenia, zob. norma ISO 16750-2 wydanie 4, rozdział 4.6.4.</p>	218"

d) pkt 6 otrzymuje brzmienie:

„6. BADANIE ZEWNĘTRZNEGO URZĄDZENIA DO ŁĄCZNOŚCI NA ODLEGŁOŚĆ”;

Nr	Badanie	Opis	Powiązane wymogi
1.	Badanie administracyjne		
1.1	Dokumentacja	Prawidłowość dokumentacji	
2.	Kontrola wizualna		
2.1.	Zgodność z dokumentacją		
2.2.	Identyfikacja/oznakowanie		225, 226
2.3	Materiały		219–223
3.	Badania funkcjonalności		
3.1	Łączność na odległość na potrzeby ukierunkowanych kontroli drogowych		4, 197–199

Nr	Badanie	Opis	Powiązane wymogi
3.2	Rejestrowanie i przechowywanie w pamięci danych		91
3.3	Łączność z przyrządem rejestrującym		Dodatek 14 pozycje DSC_66–DSC_70, DSC_71–DSC_76
4.	Badania środowiskowe		
4.1	Temperatura	<p>Sprawdzenie funkcjonalności za pomocą: badania zgodnie z normą ISO 16750-4, rozdział 5.1.1.2: Próba eksploatacyjna w niskiej temperaturze (72 h w temperaturze -20 °C).</p> <p>Badanie to odnosi się do normy IEC 60068-2-1: Badania środowiskowe – Część 2-1: Próby – Próba A: Zimno</p> <p>Badanie zgodnie z normą ISO 16750-4: Rozdział 5.1.2.2: Próba eksploatacyjna w wysokiej temperaturze (72 h w temperaturze 70 °C).</p> <p>Badanie to odnosi się do normy IEC 60068-2-2: Podstawowe procedury badań środowiskowych – Część 2: Próby – Próba B: Suche gorąco;</p> <p>Badanie zgodnie z normą ISO 16750-4: Rozdział 5.3.2: Nagła zmiana temperatury z określonym okresem przejściowym (-20 °C/70 °C, 20 cykli, czas przebywania: 1 h w każdej temperaturze).</p> <p>Można przeprowadzić skrócony zestaw badań (spośród tych zdefiniowanych w sekcji 3 niniejszej tabeli) w niższej temperaturze, wyższej temperaturze i w czasie cykli temperaturowych.</p>	213
4.2	Ochrona przed wodą i ciałami obcymi	Badanie zgodnie z normą ISO 20653: Pojazdy drogowe – Stopień ochrony (kod IP) – Ochrona urządzeń elektrycznych przed ciałami obcymi, wodą i dostępem (wartość docelowa IP40)	220, 221
5	Badania EMC		
5.1	Emisje radiacyjne i wrażliwość na radiację	Zgodność z regulaminem nr 10 EKG ONZ	218
5.2	Wyładowania elektrostacyjne	Zgodność z normą ISO 10605:2008 + Sprostowanie techniczne: 2010 + AMD1:2014: +/- 4kV w przypadku styku i +/- 8kV w przypadku rozładowania do powietrza	218

Nr	Badanie	Opis	Powiązane wymogi
5.3	Wrażliwość na stany nieustalone w zasilaniu	<p>W przypadku wersji 24 V: zgodność z normą ISO 7637-2 i wersją 3 regulaminu nr 10 EKG ONZ:</p> <p>impuls 1a: $V_s = -450$ V, $R_i = 50$ omów</p> <p>impuls 2a: $V_s = +37$ V, $R_i = 2$ omy</p> <p>impuls 2b: $V_s = +20$ V, $R_i = 0,05$ oma</p> <p>impuls 3a: $V_s = -150$ V, $R_i = 50$ omów</p> <p>impuls 3b: $V_s = +150$ V, $R_i = 50$ omów</p> <p>impuls 4: $V_s = -16$ V, $V_a = -12$ V, $t_6 = 100$ ms</p> <p>impuls 5: $V_s = +120$ V, $R_i = 2,2$ oma, $t_d = 250$ ms</p> <p>W przypadku wersji 12 V: zgodność z normą ISO 7637-1 i wersją 3 regulaminu nr 10 EKG ONZ:</p> <p>impuls 1: $V_s = -75$ V, $R_i = 10$ omów</p> <p>impuls 2a: $V_s = +37$ V, $R_i = 2$ omy</p> <p>impuls 2b: $V_s = +10$ V, $R_i = 0,05$ oma</p> <p>impuls 3a: $V_s = -112$ V, $R_i = 50$ omów</p> <p>impuls 3b: $V_s = +75$ V, $R_i = 50$ omów</p> <p>impuls 4: $V_s = -6$ V, $V_a = -5$ V, $t_6 = 15$ ms</p> <p>impuls 5: $V_s = +65$ V, $R_i = 3$ omy, $t_d = 100$ ms</p> <p>Impuls 5 należy testować tylko w przypadku przyrządów rejestrujących przeznaczonych do zainstalowania w pojazdach, w których nie zainstalowano zewnętrznego, wspólnego zabezpieczenia przed spadkiem obciążenia.</p> <p>Aby uzyskać informacje na temat propozycji zabezpieczenia przed spadkiem obciążenia, zob. norma ISO 16750-2 wydanie 4, rozdział 4.6.4.</p>	218"

e) tabela w pkt 8 dotycząca badań interoperacyjności otrzymuje brzmienie:

„Nr	Badanie	Opis
8.1 Badania interoperacyjności między przyrządami rejestrującymi a kartami do tachografu		
1	Wzajemne uwierzytelnienie	Sprawdzenie, czy wzajemne uwierzytelnienie między przyrządem rejestrującym a kartą do tachografu przebiega normalnie.
2	Próby zapisu/odczytu	<p>Wykonanie scenariusza typowej czynności na przyrządzie rejestrującym. Scenariusz dostosowany jest do typu badanej karty i obejmuje zapis na karcie tak wielu EF, jak to możliwe.</p> <p>Sprawdzenie poprzez pobieranie danych z przyrządu rejestrującego, czy wszystkie odpowiednie zapisy zostały wykonane prawidłowo.</p> <p>Sprawdzenie poprzez pobieranie danych z karty, czy wszystkie odpowiednie zapisy zostały wykonane prawidłowo.</p> <p>Sprawdzenie poprzez dzienny wydruk z karty, czy wszystkie odpowiednie zapisy mogą być odczytane prawidłowo.</p>

Nr	Badanie	Opis
8.2 Badania interoperacyjności między przyrządami rejestrującymi a czujnikami ruchu		
1	Parowanie	Sprawdzenie, czy parowanie przyrządu rejestrującego z czujnikami ruchu przebiega normalnie.
2	Badania czynności	Wykonanie scenariusza typowej czynności na czujniku ruchu. Scenariusz obejmuje normalną czynność i wygenerowanie jak największej liczby zdarzeń lub usterek. Sprawdzenie poprzez pobieranie danych z przyrządu rejestrującego, czy wszystkie odpowiednie zapisy zostały wykonane prawidłowo. Sprawdzenie poprzez pobieranie danych z karty, czy wszystkie odpowiednie zapisy zostały wykonane prawidłowo. Sprawdzenie poprzez dzienny wydruk, czy wszystkie odpowiednie zapisy mogą być odczytane prawidłowo.
8.3 Badania interoperacyjności między przyrządami rejestrującymi a urządzeniem zewnętrznym GNSS (w stosownych przypadkach)		
1	Wzajemne uwierzytelnienie	Sprawdzenie, czy wzajemne uwierzytelnienie (połączenie) między przyrządem rejestrującym a zewnętrznym modułem GNSS przebiega normalnie.
2	Badania czynności	Wykonanie scenariusza typowej czynności na zewnętrznym urządzeniu GNSS. Scenariusz obejmuje normalną czynność i wygenerowanie jak największej liczby zdarzeń lub usterek. Sprawdzenie poprzez pobieranie danych z przyrządu rejestrującego, czy wszystkie odpowiednie zapisy zostały wykonane prawidłowo. Sprawdzenie poprzez pobieranie danych z karty, czy wszystkie odpowiednie zapisy zostały wykonane prawidłowo. Sprawdzenie poprzez dzienny wydruk, czy wszystkie odpowiednie zapisy mogą być odczytane prawidłowo."

36) w dodatku 11 wprowadza się następujące zmiany:

a) pkt 8.2.3 pozycja CSM_49 otrzymuje brzmienie:

„CSM_49 Przyrządy rejestrujące, karty do tachografu i urządzenia zewnętrzne GNSS obsługują algorytmy SHA-256, SHA-384 i SHA-512 określone w [SHS].”;

b) pkt 9.1.2 pozycja CSM_58 akapit pierwszy otrzymuje brzmienie:

„CSM_58 Ilekroć ERCA generuje nową parę europejskich kluczy głównych, tworzy certyfikat łączący dla nowego europejskiego klucza publicznego i podpisuje go za pomocą poprzedniego europejskiego klucza prywatnego. Okres ważności certyfikatu łączy wynosi 17 lat i 3 miesiące. Przedstawiono to również na rys. 1 w sekcji 9.1.7.”;

c) pkt 9.1.4 pozycja CSM_72 otrzymuje brzmienie:

„CSM_72 Dla każdego przyrządu rejestrującego generuje się dwie unikatowe pary kluczy ECC oznaczone jako VU_MA i VU_Sign. Zadanie to realizują producenci VU. Ilekroć generowana jest para kluczy VU, organ generujący klucz przekazuje klucz publiczny swojemu MSCA, aby uzyskać powiązany certyfikat VU podpisany przez MSCA. Klucz prywatny może być używany wyłącznie przez przyrząd rejestrujący.”;

d) w pkt 9.1.5 wprowadza się następujące zmiany:

(i) pozycja CSM_83 otrzymuje brzmienie:

„CSM_83 Dla każdej karty do tachografu generuje się jedną unikatową parę kluczy ECC oznaczoną jako Card_MA. Dla każdej karty kierowcy i karty warsztatowej generuje się dodatkowo drugą unikatową parę kluczy ECC oznaczoną jako Card_Sign. Zadanie to mogą realizować producenci kart lub instytucje dokonujące personalizacji kart. Ilekroć generowana jest para kluczy karty, organ generujący klucz przekazuje klucz publiczny swojemu MSCA, aby uzyskać powiązany certyfikat karty podpisany przez MSCA. Klucz prywatny może być używany wyłącznie przez kartę do tachografu.”;

(ii) pozycja CSM_88 otrzymuje brzmienie:

„CSM_88 Okres ważności certyfikatu Card_MA wynosi:

- w przypadku kart kierowcy: 5 lat,
- w przypadku kart firmowych: 5 lat,
- w przypadku kart kontrolnych: 2 lata,
- w przypadku kart warsztatowych: 1 rok.”;

(iii) w pozycji CSM_91 dodaje się tekst w brzmieniu:

„— Dodatkowo tylko w przypadku kart kontrolnych, kart firmowych i kart warsztatowych i tylko jeżeli takie karty zostały wydane w ciągu pierwszych trzech miesięcy okresu ważności nowego certyfikatu EUR: certyfikat EUR starszy o dwie generacje, jeżeli występuje.

Uwaga do tiret ostatniego: Przykładowo w pierwszych trzech miesiącach certyfikatu ERCA(3) (zob. rys. 1) wspomniane karty zawierają certyfikat ERCA(1). Uwzględnienie certyfikatu ERCA(1) jest konieczne w celu zapewnienia możliwości używania tych kart na potrzeby pobierania danych z przyrządów rejestrujących, których normalny okres użyteczności wynoszący 15 lat plus trzy miesiące okresu pobierania danych upływa w ciągu tych miesięcy; zob. tiret ostatnie wymogu 13 w załączniku IC.”;

e) w pkt 9.1.6 wprowadza się następujące zmiany:

(i) pozycja CSM_93 otrzymuje brzmienie:

„CSM_93 Dla każdego urządzenia zewnętrznego GNSS generuje się jedną unikatową parę kluczy ECC oznaczoną jako EGF_MA. Zadanie to realizują producenci urządzeń zewnętrznych GNSS. Ilekroć generowana jest para kluczy EGF_MA, organ generujący klucz przekazuje klucz publiczny swojemu MSCA, aby uzyskać powiązany certyfikat EGF_MA podpisany przez MSCA. Klucz prywatny może być używany wyłącznie przez urządzenie zewnętrzne GNSS.”;

(ii) pozycja CSM_95 otrzymuje brzmienie:

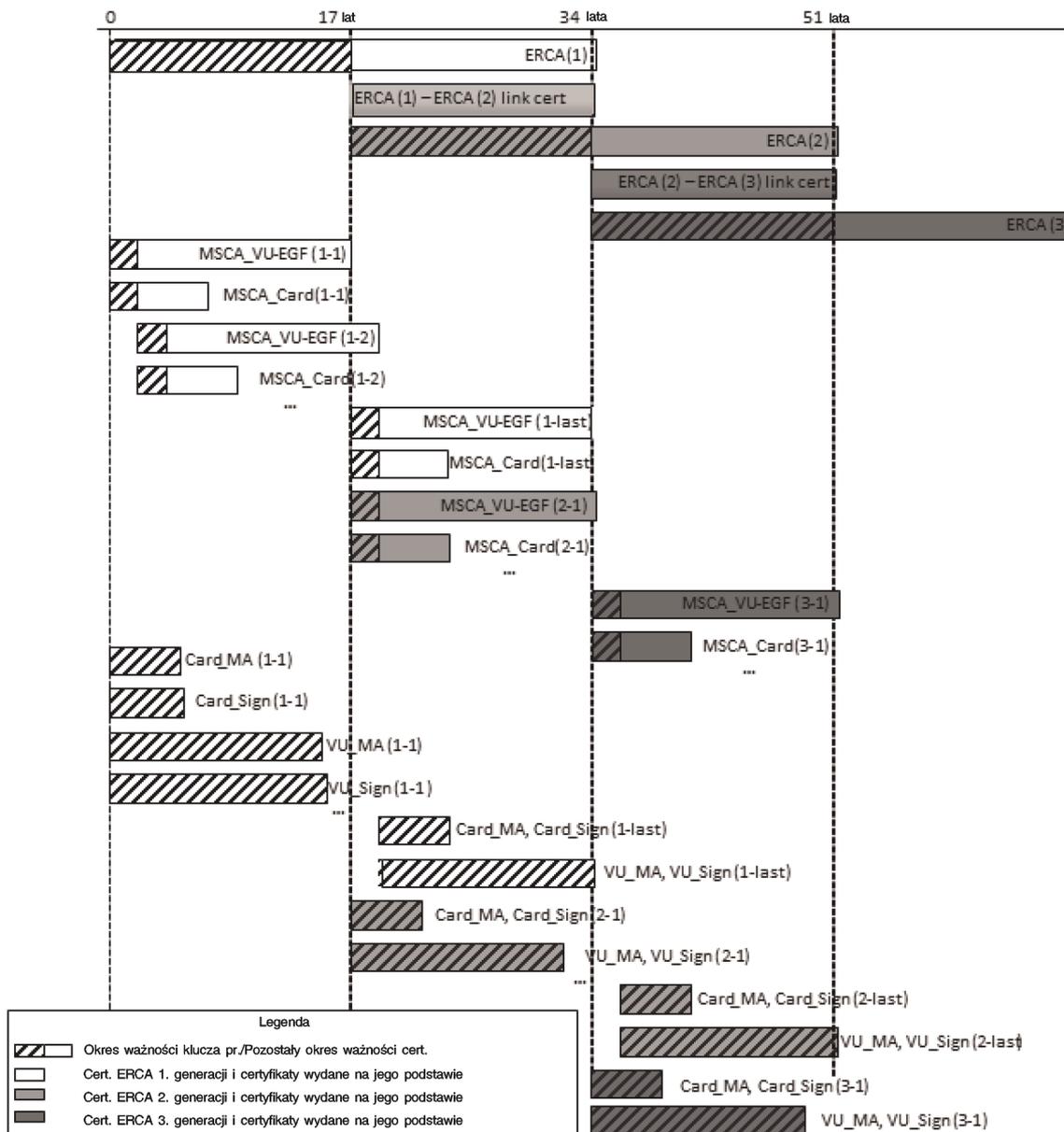
„CSM_95 Urządzenie zewnętrzne GNSS używa swojej pary kluczy EGF_MA, w której skład wchodzi klucz prywatny EGF_MA.SK i klucz publiczny EGF_MA.PK, wyłącznie do wzajemnego uwierzytelniania i uzgadniania klucza sesji w stosunku do przyrządów rejestrujących, jak określono w sekcji 11.4 niniejszego dodatku.”;

f) w pkt 9.1.7 wprowadza się następujące zmiany:

(i) rys. 1 zastępuje się następującym rysunkiem:

„Rysunek 1

Wydawanie i używanie różnych generacji certyfikatów głównych ERCA, certyfikatów łączących ERCA, certyfikatów MSCA i certyfikatów urzędzeń



(ii) pkt 6 w uwagach do rys. 1 otrzymuje brzmienie:

„6. aby zaoszczędzić miejsce, różnica w okresie ważności certyfikatów Card_MA i Card_Sign została podana wyłącznie dla certyfikatów pierwszej generacji.”;

g) w pkt 9.2.1.1 wprowadza się następujące zmiany:

(i) pozycja CSM_106 tiret pierwsze otrzymuje brzmienie:

„— w odniesieniu do 128-bitowych kluczy głównych czujnika ruchu: CV = »B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5D 83«”;

(ii) pozycja CSM_107 akapit pierwszy otrzymuje brzmienie:

„Każdy producent czujników ruchu generuje losowy i unikatowy klucz parowania K_p dla każdego czujnika ruchu i przesyła każdy klucz parowania organowi certyfikacji państwa członkowskiego (MSCA). MSCA szyfruje każdy klucz parowania oddzielnie za pomocą klucza głównego czujnika ruchu K_M i zwraca zaszyfrowany klucz producentowi czujników ruchu. W przypadku każdego zaszyfrowanego klucza MSCA powiadamia producenta czujników ruchu o numerze wersji powiązanego K_M .”;

(iii) pozycja CSM_108 otrzymuje brzmienie:

„CSM_108 Każdy producent czujników ruchu generuje unikatowy numer seryjny dla każdego czujnika ruchu i przesyła wszystkie numery seryjne swojemu organowi certyfikacji państwa członkowskiego. MSCA szyfruje każdy numer seryjny oddzielnie za pomocą klucza identyfikacyjnego K_{ID} i zwraca zaszyfrowany numer seryjny producentowi czujników ruchu. W przypadku każdego zaszyfrowanego numeru seryjnego MSCA powiadamia producenta czujników ruchu o numerze wersji powiązanego K_{ID} .”;

h) w pkt 9.2.2.1 wprowadza się następujące zmiany:

(i) pozycja CSM_123 otrzymuje brzmienie:

„CSM_123 W odniesieniu do każdego przyrządu rejestrującego producent takiego przyrządu tworzy unikatowy numer seryjny VU i przesyła taki numer swojemu organowi certyfikacji państwa członkowskiego we wniosku w celu uzyskania zestawu dwóch kluczy DSRC specyficznych dla VU. Numer seryjny VU posiada typ danych VuSerialNumber.

Uwaga:

- Taki numer seryjny VU musi być identyczny z elementem vuSerialNumber w VuIdentification (zob. dodatek 1) i z odniesieniem do posiadacza certyfikatu w certyfikatach VU.
- Numer seryjny VU może nie być znany w momencie żądania przez producenta przyrządu rejestrującego kluczy DSRC specyficznych dla VU. W takim przypadku producent VU wysyła zastępczo unikatowy identyfikator wniosku o certyfikat, którego użył, występując o certyfikaty VU. zob. CSM_153; Taki identyfikator wniosku o certyfikat musi być zatem identyczny z odniesieniem do posiadacza certyfikatu w certyfikatach VU.”;

(ii) w pozycji CSM_124 wymóg dotyczący informacji w kroku 2 otrzymuje brzmienie:

„info = numer seryjny VU lub identyfikator wniosku o certyfikat, jak określono w CSM_123”;

(iii) pozycja CSM_128 otrzymuje brzmienie:

„CSM_128 MSCA prowadzi rejestry wszystkich wygenerowanych kluczy DSRC specyficznych dla VU, ich numerów wersji i numerów seryjnych VU lub identyfikatorów wniosku o certyfikat wykorzystanych w celu ich wyprowadzenia.”;

i) pkt 9.3.1 pozycja CSM_135 akapit pierwszy otrzymuje brzmienie:

„Wyróżnione reguły kodowania (DER) zgodnie z [normą ISO 8825-1] wykorzystuje się do kodowania obiektów danych w ramach certyfikatów. W tabeli 4 przedstawiono pełne kodowanie świadectw, z uwzględnieniem wszystkich bajtów znaczników i długości.”;

j) w pkt 9.3.2.3 pozycja CSM_141 otrzymuje brzmienie:

„CSM_141 Upoważnienie posiadacza certyfikatu służy do identyfikowania rodzaju certyfikatu. Składa się ono z sześciu najbardziej znaczących bajtów identyfikatora aplikacji tachograficznej, połączonych z typem urządzenia, który wskazuje typ urządzenia, dla którego certyfikat jest przeznaczony. W przypadku certyfikatu VU, certyfikatu karty kierowcy lub certyfikatu karty warsztatowej typu urządzenia używa się również w celu rozróżnienia świadectwa wzajemnego uwierzytelnienia i certyfikatu na potrzeby tworzenia podpisu cyfrowego (zob. pkt 9.1 i dodatek 1, typ danych EquipmentType).”;

k) w pkt 9.3.2.5 w pozycji CSM_146 dodaje się następujący akapit:

„Uwaga: W przypadku certyfikatu karty wartość CHR musi być równa wartości cardExtendedSerialNumber w EF_ICC; zob. dodatek 2. W przypadku certyfikatu EGF wartość CHR musi być równa wartości sensorGNSSSerialNumber w EF_ICC; zob. dodatek 14. W przypadku certyfikatu VU wartość CHR musi być równa elementowi vuSerialNumber w Vuldentification (zob. dodatek 1), chyba że producent nie zna specyficznego dla danego producenta numeru seryjnego, w momencie gdy wystąpiono o certyfikat.”;

l) pkt 9.3.2.6 pozycja CSM_148 otrzymuje brzmienie:

„CSM_148 Data wejścia w życie certyfikatu określa datę i godzinę rozpoczęcia okresu ważności certyfikatu.”;

m) w pkt 9.3.3 wprowadza się następujące zmiany:

(i) pozycja CSM_151 akapit pierwszy otrzymuje brzmienie:

Składając wniosek o certyfikat, MSCA przesyła ERCA następujące dane:

(ii) pozycja CSM_153 otrzymuje brzmienie:

„CSM_153 Producent urządzenia przesyła MSCA następujące dane we wniosku o certyfikat, co umożliwi MSCA utworzenie odniesienia do posiadacza certyfikatu dla nowego certyfikatu urządzenia:

— numer seryjny urządzenia, unikalny dla producenta, typu urządzenia i miesiąc wyprodukowania, jeżeli dane te są znane (zob. CSM_154). W przeciwnym razie – unikatowy identyfikator wniosku o certyfikat,

— miesiąc i rok produkcji urządzenia lub miesiąc i rok sporządzenia wniosku o certyfikat.

Producent zapewnia, aby przedmiotowe dane były prawidłowe, a certyfikat zwrócony przez MSCA został umieszczony w przewidzianym urządzeniu.”;

n) w pkt 10.2.1 wprowadza się następujące zmiany:

(i) w pozycji CSM_157 tekst przed uwagami do rys. 4 otrzymuje brzmienie:

„Przyrządy rejestrujące używają protokołu przedstawionego na rys. 4 w celu weryfikacji łańcucha certyfikatów karty do tachografu. Dla każdego certyfikatu odczytywanego z karty przyrząd rejestrujący weryfikuje prawidłowość pola Upoważnienie Posiadacza Certyfikatu (CHA):

— Pole CHA certyfikatu karty wskazuje certyfikat karty na potrzeby wzajemnego uwierzytelnienia (zob. dodatek 1, typ danych EquipmentType).

— CHA certyfikatu Card.CA musi wskazywać MSCA.

— CHA certyfikatu Card.Link musi wskazywać ERCA.”;

(ii) w pozycji CSM_159 dodaje się zdanie w brzmieniu:

„Zważywszy że przechowywanie wszystkich pozostałych typów certyfikatu jest fakultatywne, VU musi przechowywać nowy certyfikat łączący przedstawiony przez kartę.”;

o) w pkt 10.2.2 wprowadza się następujące zmiany:

(i) w pozycji CSM_161 tekst przed rys. 5 otrzymuje brzmienie:

„Karty do tachografu używają protokołu przedstawionego na rys. 5 w celu weryfikacji łańcucha certyfikatów VU. Dla każdego certyfikatu przedstawionego przez przyrząd rejestrujący karta weryfikuje prawidłowość pola Upoważnienie Posiadacza Certyfikatu (CHA):

— CHA certyfikatu VU.Link musi wskazywać ERCA.

— CHA certyfikatu VU.CA musi wskazywać MSCA.

— Pole CHA certyfikatu VU wskazuje certyfikat VU na potrzeby wzajemnego uwierzytelnienia (zob. dodatek 1, typ danych EquipmentType).”;

(ii) pozycja CSM_165 otrzymuje brzmienie:

„CSM_165 Jeżeli polecenie MSE: Set AT jest skuteczne, karta ustawia wskazany VU.PK w celu późniejszego użycia podczas uwierzytelnienia przyrządu rejestrującego i tymczasowo zapisuje Comp(VU.PKeph). W przypadku wysłania co najmniej dwóch skutecznych poleceń MSE: Set AT przed uzgodnieniem klucza sesji karta zapisuje tylko ostatni otrzymany Comp(VU.PKeph). Karta zeruje Comp(VU.PKeph) po skutecznym poleceniu GENERAL AUTHENTICATE.”;

p) w pkt 10.3 wprowadza się następujące zmiany:

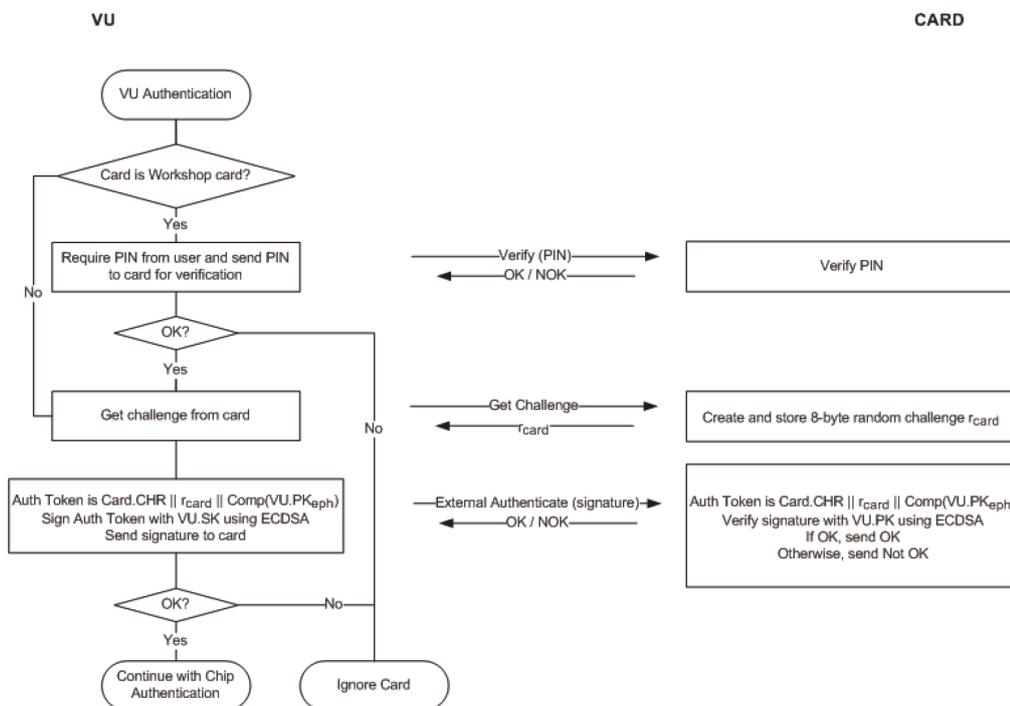
(i) pozycja CSM_170 akapit pierwszy otrzymuje brzmienie:

„Oprócz żądania karty VU umieszcza w podpisie odniesienie do posiadacza certyfikatu uzyskane z certyfikatu karty.”;

(ii) w pkt CSM_171 rys. 6 otrzymuje brzmienie:

„Rysunek 6

Protokół uwierzytelniania VU



(iii) pozycja CSM_174 otrzymuje brzmienie:

„CSM_174 Po otrzymaniu podpisu VU w poleceniu EXTERNAL AUTHENTICATE karta:

- oblicza token uwierzytelniania poprzez połączenie Card.CHR, żądania karty rcard i identyfikatora efemerycznego klucza publicznego VU $\text{Comp}(VU.PK_{eph})$;
- weryfikuje podpis VU za pomocą algorytmu ECDSA, używając algorytmu skrótu powiązanego z wielkością pary kluczy VU VU_MA , jak określono w CSM_50, w połączeniu z $VU.PK$ i obliczonym tokenem uwierzytelniania.”;

q) w pkt 10.4 pozycja CSM_176 wprowadza się następujące zmiany:

(i) ppkt 2 otrzymuje brzmienie:

„2. VU przesyła karcie punkt publiczny $VU.PK_{eph}$ swojej pary kluczy efemerycznych. Punkt publiczny przekształca się w ciąg oktetowy, jak określono w [TR-03111]. Stosuje się nieskompresowany format kodowania. Jak wyjaśniono w CSM_164, VU wygenerował tę parę kluczy efemerycznych przed zweryfikowaniem łańcucha certyfikatów VU. VU przesłał karcie identyfikator efemerycznego klucza publicznego $\text{Comp}(VU.PK_{eph})$ i karta zapisuje ten identyfikator”;

(ii) ppkt 6 otrzymuje brzmienie:

„6. za pomocą K_{MAC} , karta oblicza token uwierzytelniania w odniesieniu do identyfikatora efemerycznego punktu publicznego VU: $T_{PICC} = \text{CMAC}(K_{MAC}, VU.PK_{eph})$. Punkt publiczny musi być w formacie używanym przez VU (zob. ppkt 2 powyżej). Karta wysyła N_{PICC} i T_{PICC} do przyrządu rejestrującego.”;

r) w pkt 10.5.2 pozycja CSM_191 otrzymuje brzmienie:

„CSM_191 Każdy obiekt danych wymagający zaszyfrowania wypełnia się zgodnie z [ISO 7816-4] przy użyciu wskaźnika treści wypełnienia »01«. Na potrzeby obliczenia MAC obiekty danych w APDU wypełnia się również zgodnie z [ISO 7816-4].

Uwaga: wypełnianie na potrzeby bezpiecznej wymiany komunikatów zawsze przeprowadza się za pomocą warstwy bezpiecznej wymiany komunikatów, a nie algorytmów CMAC czy CBC.

Podsumowanie i przykłady

Polecenie APDU z zastosowaniem bezpiecznej wymiany komunikatów będzie miało następującą strukturę w zależności od przypadku odpowiadającego mu niezabezpieczonego polecenia (»DO« oznacza obiekt danych):

Przypadek 1: CLA INS P1 P2 || Lc' || DO »8E« || Le

Przypadek 2: CLA INS P1 P2 || Lc' || DO »97« || DO »8E« || Le

Przypadek 3 (parzysty bajt INS): CLA INS P1 P2 || Lc' || DO »81« || DO »8E« || Le

Przypadek 3 (nieparzysty bajt INS): CLA INS P1 P2 || Lc' || DO »B3« || DO »8E« || Le

Przypadek 4 (parzysty bajt INS): CLA INS P1 P2 || Lc' || DO »81« || DO »97« || DO »8E« || Le

Przypadek 4 (nieparzysty bajt INS): CLA INS P1 P2 || Lc' || DO »B3« || DO »97« || DO »8E« || Le

gdzie Le = »00« albo »00 00« w zależności od tego, czy stosuje się krótkie długości pól czy rozszerzone długości pól; zob. [ISO 7816-4].

Odpowiedź APDU z zastosowaniem bezpiecznej wymiany komunikatów będzie miała następującą strukturę w zależności od przypadku odpowiadającej mu niezabezpieczonej odpowiedzi:

Przypadek 1 lub 3: DO »99« || DO »8E« || SW1SW2

Przypadek 2 lub 4 (parzysty bajt INS) bez szyfrowania: DO »81« || DO »99« || DO »8E« || SW1SW2

Przypadek 2 lub 4 (parzysty bajt INS) z szyfrowaniem: DO »87« || DO »99« || DO »8E« || SW1SW2

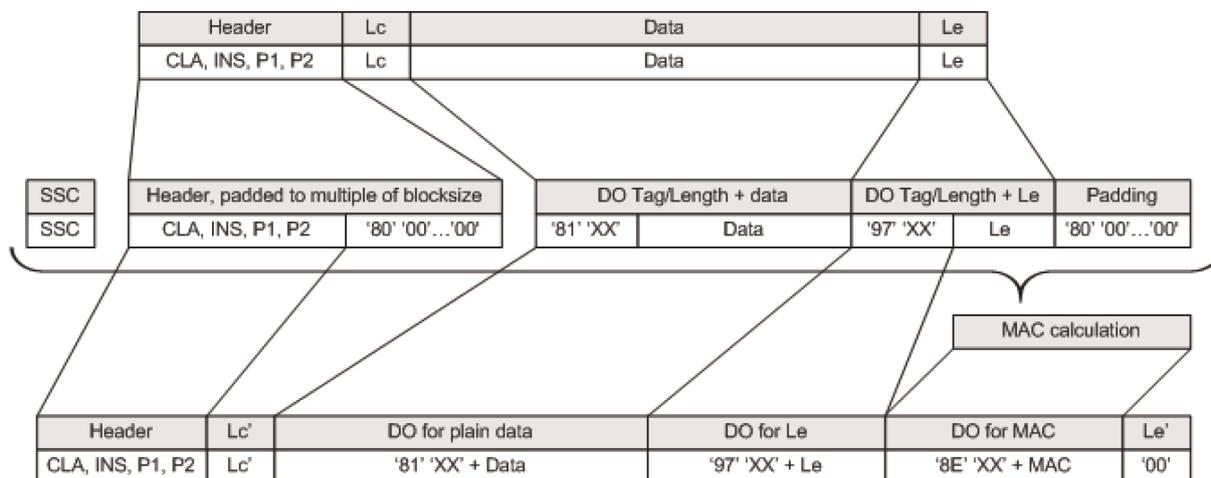
Przypadek 2 lub 4 (nieparzysty bajt INS) bez szyfrowania: DO »B3« || DO »99« || DO »8E« || SW1SW

Uwaga: przypadków 2 lub 4 (nieparzysty bajt INS) z szyfrowaniem nigdy nie stosuje się w łączności między VU a kartą.

Poniżej przedstawiono trzy przykłady przekształceń APDU w odniesieniu do poleceń z parzystym kodem INS. Rys. 8 przedstawia uwierzytelnione polecenie APDU określone w przypadku 4, rys. 9 przedstawia uwierzytelnioną odpowiedź APDU określoną w przypadku 1 / przypadku 3, a rys. 10 przedstawia zaszyfrowaną i uwierzytelnioną odpowiedź APDU określoną w przypadku 2/4.

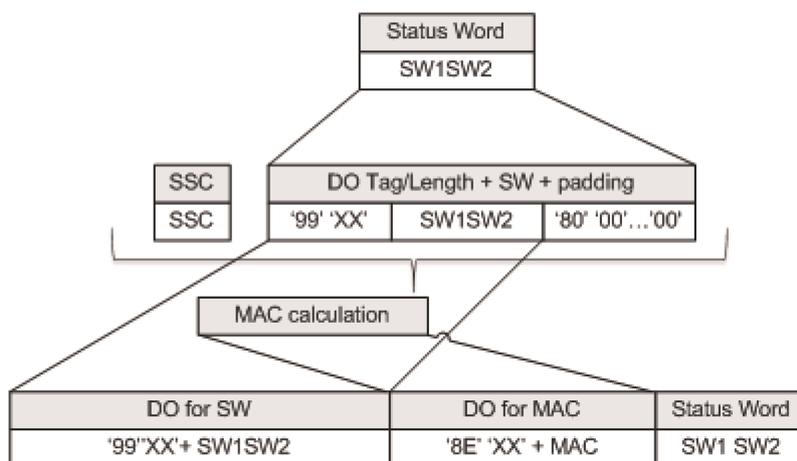
Rysunek 8

Przekształcenie uwierzytelnionego polecenia APDU określonego w przypadku 4



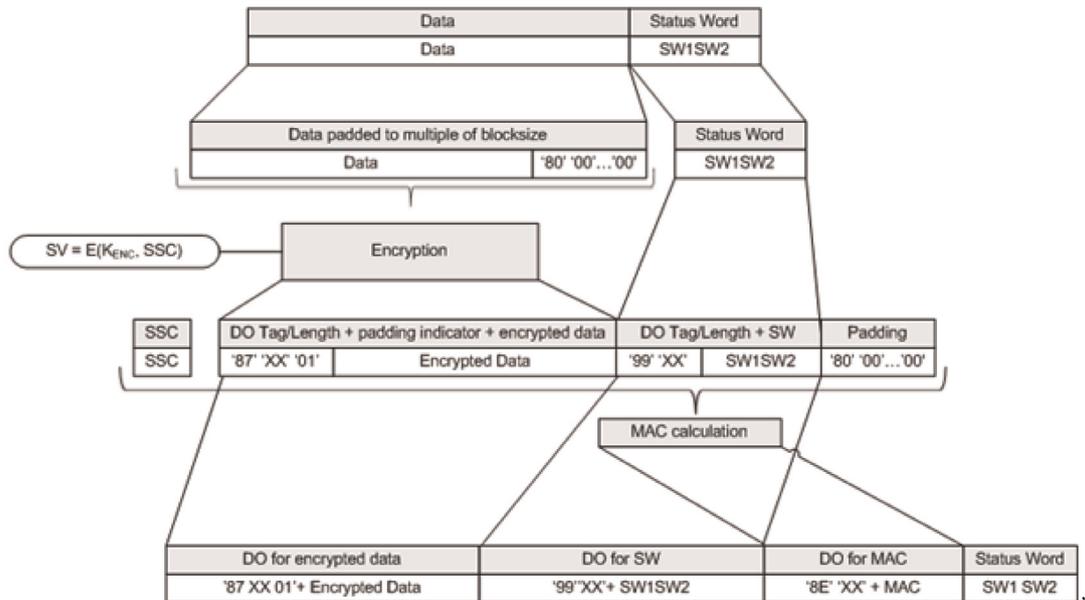
Rysunek 9

Przekształcenie uwierzytelnionej odpowiedzi APDU określonej w przypadku 1/ przypadku 3



Rysunek 10

Przekształcenie zaszyfrowanej i uwierzytelnionej odpowiedzi APDU określonej w przypadku 2/ przypadku 4



s) w pkt 10.5.3 pozycja CSM_193 otrzymuje brzmienie:

„CSM_193 Karta do tachografu przerywa trwającą sesję bezpiecznej wymiany komunikatów tylko i wyłącznie wówczas, gdy zaistnieje jeden z poniższych warunków:

- karta otrzyma odkryte polecenie APDU,
- karta wykryje błąd bezpiecznej wymiany komunikatów w poleceniu APDU:
 - brak oczekiwanego obiektu danych bezpiecznej wymiany komunikatów, nieprawidłową kolejność obiektów danych lub uwzględnienie nieznanego obiektu danych,
 - nieprawidłowy obiekt danych bezpiecznej wymiany komunikatów, np. nieprawidłowa wartość MAC lub nieprawidłowa struktura TLV;
- karta straci zasilanie lub zostanie zresetowana;
- VU rozpocznie proces uwierzytelniania VU;
- osiągnięty zostanie limit dotyczący liczby poleceń i powiązanych odpowiedzi w ramach bieżącej sesji. W odniesieniu do danej karty limit ten określa producent, uwzględniając wymogi bezpieczeństwa dotyczące używanego sprzętu, przy czym maksymalna liczba poleceń i powiązanych odpowiedzi w ramach bezpiecznej wymiany komunikatów wynosi 240 w każdej sesji.”;

t) w pkt 11.3.2 wprowadza się następujące zmiany:

(i) pozycja CSM_208 akapit pierwszy otrzymuje brzmienie:

„Podczas ustanawiania powiązania z VU urządzenie zewnętrzne GNSS używa protokołu przedstawionego na rys. 5 (sekcja 10.2.2) w celu weryfikacji łańcucha certyfikatów VU.”;

(ii) pozycja CSM_210 otrzymuje brzmienie:

„CSM_210 Po zweryfikowaniu certyfikatu VU_MA urządzenie zewnętrzne GNSS przechowuje ten certyfikat do wykorzystania w czasie normalnej pracy; zob. sekcja 11.3.3.”;

u) pkt 11.3.3 pozycja CSM_211 akapit pierwszy otrzymuje brzmienie:

„W czasie normalnej pracy przyrząd rejestrujący i EGF używają protokołu wskazanego na rys. 11 w celu weryfikacji czasowej ważności przechowywanych certyfikatu EGF_MA oraz do celów ustalenia klucza publicznego VU_MA na potrzeby późniejszego uwierzytelnienia VU. W czasie normalnej pracy nie odbywa się dalsza wzajemna weryfikacja łańcuchów certyfikatów.”;

v) tabela 6 w pkt 12.3 otrzymuje brzmienie:

„Tabela 6

Liczba bajtów danych zwykłego tekstu i danych zaszyfrowanych zgodnie z instrukcją określoną w [ISO 16844-3]

Instrukcja	Żądanie / odpowiedź	Opis danych	Liczba bajtów danych zwykłego tekstu zgodnie z [ISO 16844-3]	Liczba bajtów danych zwykłego tekstu przy użyciu kluczy AES	Liczba bajtów zaszyfrowanych danych przy użyciu kluczy AES o długości w bitach		
					128	192	256
10	żądanie	Dane uwierzytelnienia + numer pliku	8	8	16	16	16
11	odpowiedź	Dane uwierzytelnienia + zawartość pliku	16 lub 32 w zależności od pliku	16 lub 32 w zależności od pliku	32 / 48	32 / 48	32 / 48
41	żądanie	Numer seryjny czujnika ruchu	8	8	16	16	16
41	odpowiedź	Klucz parowania	16	16 / 24 / 32	16	32	32
42	żądanie	Klucz sesji	16	16 / 24 / 32	16	32	32
43	żądanie	Informacje o parowaniu	24	24	32	32	32
50	odpowiedź	Informacje o parowaniu	24	24	32	32	32
70	żądanie	Dane uwierzytelnienia	8	8	16	16	16
80	odpowiedź	Wartość licznika czujnika ruchu + dane uwierzytelnienia	8	8	16	16	16”

w) w pkt 13.1 wymóg dotyczący numeru seryjnego VU w pozycji CSM_224 otrzymuje brzmienie:

„numeru seryjnego VU

tj. numeru seryjnego VU lub identyfikatora wniosku o certyfikat (typ danych VuSerialNumber lub CertificateRequestID) – zob. CSM_123”;

x) w pkt 13.3 pozycja CSM_228 ppkt 2 otrzymuje brzmienie:

„2. karta kontrolna stosuje wskazany klucz główny DSRC w połączeniu z numerem seryjnym VU lub identyfikatorem wniosku o certyfikat zawartym w danych zabezpieczających DSRC w celu wyprowadzenia specyficznych dla VU kluczy DSRC $K_{VU_{DSRC_ENC}}$ i $K_{VU_{DSRC_MAC}}$, jak określono w CSM_124;”;

y) w pkt 14.3 wprowadza się następujące zmiany:

(i) w pozycji CSM_234 tekst przed uwagami do rys. 13 otrzymuje brzmienie:

„IDE może samodzielnie przeprowadzać weryfikację podpisu złożonego w odniesieniu do pobranych danych lub może do tego celu używać karty kontrolnej. W przypadku używania karty kontrolnej weryfikacja podpisów odbywa się zgodnie ze schematem przedstawionym na rysunku 13. W celu zweryfikowania czasowej ważności certyfikatu przedstawionego przez IDE karta kontrolna używa swojego wewnętrznego czasu bieżącego, jak określono w pozycji CSM_167. Karta kontrolna aktualizuje swój czas bieżący, jeżeli data wejścia w życie autentycznego certyfikatu będącego »wiarygodnym źródłem czasu« jest późniejsza niż czas bieżący określony na karcie. Za wiarygodne źródło czasu karta uznaje wyłącznie następujące certyfikaty:

- certyfikaty łączące ERCA drugiej generacji,
- certyfikaty MSCA drugiej generacji,
- certyfikaty VU_Sign lub Card_Sign drugiej generacji wydane przez to samo państwo, które wydało certyfikat własny karty kontrolnej.

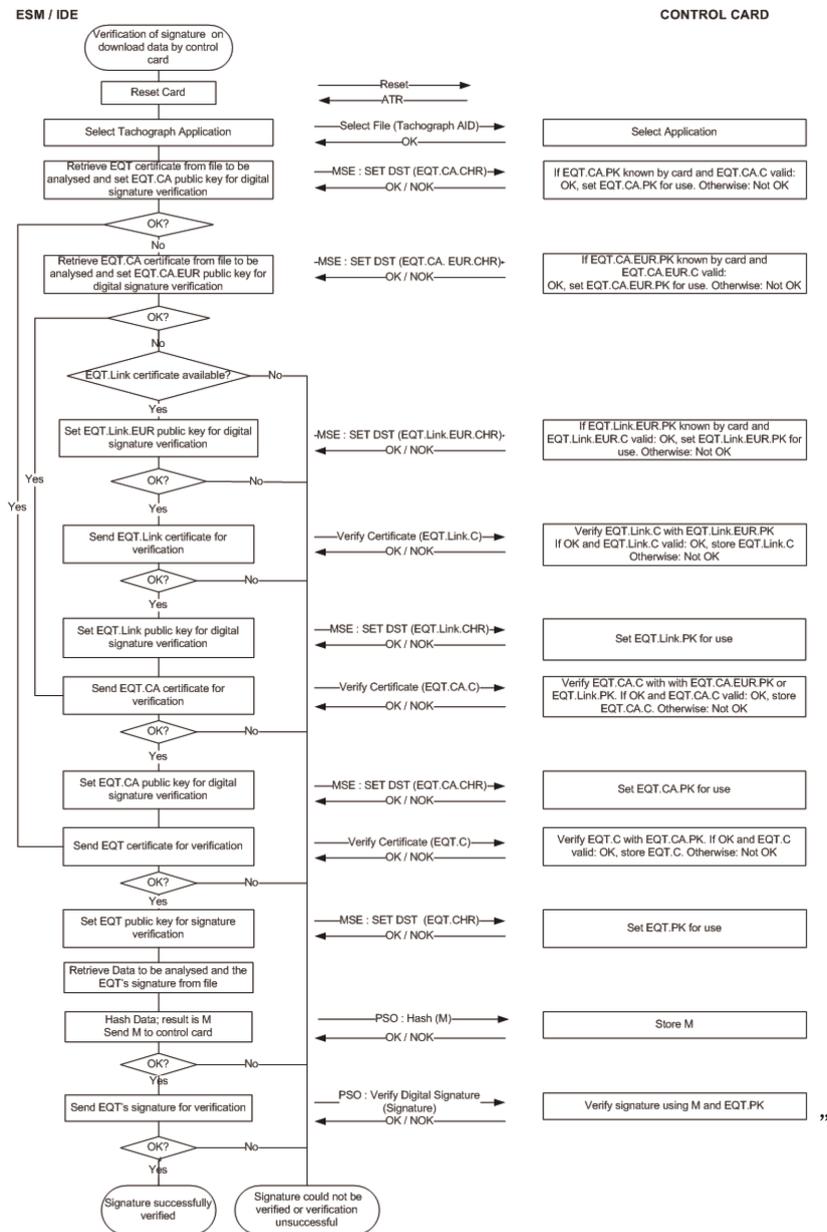
W przypadku gdy urządzenie samodzielnie przeprowadza weryfikację podpisy, IDE weryfikuje autentyczność i ważność wszystkich certyfikatów w łańcuchu certyfikatów w pliku danych oraz weryfikuje podpis złożony w stosunku do danych według schematu podpisu określonego w [DSS]. W obu przypadkach dla każdego certyfikatu odczytywanego z pliku danych konieczne jest sprawdzenie prawidłowości pola Upoważnienie Posiadacza Certyfikatu (CHA):

- Pole CHA certyfikatu EQT wskazuje certyfikat VU lub karty (odpowiednio do przypadku) na potrzeby podpisu (zob. dodatek 1, typ danych EquipmentType).
- CHA certyfikatu EQT.CA musi wskazywać MSCA.
- CHA certyfikatu EQT.Link musi wskazywać ERCA.”;

(ii) rys. 13 zastępuje się następującym rysunkiem:

„Rysunek 13

Protokół weryfikacji podpisu złożonego w odniesieniu do pobranego pliku danych



37) w dodatku 12 wprowadza się następujące zmiany:

a) w pkt 3 wprowadza się następujące zmiany:

(i) w pozycji GNS_4 akapit drugi po rys. 2 otrzymuje brzmienie:

„Dokładność położenia opiera się na formacie komunikatu RMC opisanym powyżej. Pierwszą część pól 3 i 5 wykorzystuje się do określenia stopni. Pozostałe określają minuty kątowne z dokładnością do trzech miejsc po przecinku. Zatem dokładność wynosi 1/1 000 minuty kątownej lub 1/60 000 stopnia (ponieważ jedna minuta to 1/60 stopnia).”;

(ii) punkt GNS_5 otrzymuje brzmienie:

„GNS_5 Przyrząd rejestrujący przechowuje w bazie danych VU informacje o położeniu dotyczące szerokości i długości geograficznej z dokładnością 1/10 minuty kątownej lub 1/600 stopnia, jak określono w dodatku 1 w odniesieniu do współrzędnych geograficznych »GeoCoordinates«.

VU może wykorzystać polecenie GSA (dotyczące rozmycia dokładności GPS i aktywnych satelitów) w celu ustalenia i zarejestrowania gotowości i dokładności sygnału. W szczególności HDOP stosuje się w celu wskazania poziomu dokładności zarejestrowanych danych dotyczących lokalizacji (zob. pkt 4.2.2). VU będzie przechowywał wartość poziomu rozmycia dokładności (HDOP) obliczaną jako minimum wartości HDOP zgromadzonych w dostępnych systemach GNSS.

Identyfikator GNSS wskazuje odpowiedni identyfikator NMEA dla każdej konstelacji GNSS i systemu wspomagającego opartego na wyposażeniu satelitarnym SBAS.

Rysunek 3

Struktura komunikatu GSA

1 2 3 4
1 4 1 5 1 6 1 7 1 8

↓ ↓ ↓ ↓
↓ ↓ ↓ ↓ ↓ ↓

\$<GNSS Id.>GSA,a,a,x,x,x,x,x,x,x,x,x,x,x,x,x,x,x,x*x*hh

- 1) Tryb wyboru
- 2) Tryb
- 3) ID pierwszego satelity użytego do ustalenia położenia
- 4) ID drugiego satelity użytego do ustalenia położenia
- ...
- 14) ID dwunastego satelity użytego do ustalenia położenia
- 15) PDOP
- 16) HDOP
- 17) VDOP
- 18) Suma kontrolna "

(iii) pozycja GNS_6 otrzymuje brzmienie:

„GNS_6 Komunikat GSA przechowuje się z numerem rekordu »02«-»06«.”;

b) w pkt 4.2.1 wprowadza się następujące zmiany:

(i) pozycja GNS_16 otrzymuje brzmienie:

„GNS_16 W protokole łączności nie są obsługiwane pola o rozszerzonej długości.”;

(ii) pozycja GNS_18 otrzymuje brzmienie:

„GNS_18 Jeżeli chodzi o funkcje: 1) gromadzenia i rozpowszechniania danych GNSS; 2) gromadzenia danych dotyczących konfiguracji urządzenia zewnętrznego GNSS; oraz 3) protokołu zarządzania, bezpieczny nadajnik-odbiornik GNSS symuluje inteligentną kartę za pomocą architektury systemu plików składającej się z pliku głównego (MF), pliku dedykowanego (DF) z identyfikatorem aplikacji określonym w dodatku 1 rozdział 6.2 (»FF 44 54 45 47 4D«) i z trzema plikami elementarnymi (EF) zawierającymi certyfikaty oraz jednego pojedynczego pliku elementarnego (EF.EGF) z identyfikatorem pliku równym »2F2F«, jak opisano w tabeli 1.”;

(iii) pozycja GNS_20 otrzymuje brzmienie:

„GNS_20 Bezpieczny nadajnik-odbiornik GNSS używa pamięci do przechowywania danych i jest w stanie przeprowadzić co najmniej 20 milionów cykli zapisu/odczytu. Poza tym aspektem o konstrukcji wewnętrznej i wdrażaniu bezpiecznego nadajnika-odbiornika GNSS decydują producenci.

Mapowanie numerów rekordów i danych przedstawiono w tabeli 1. Należy zauważyć, że istnieje pięć komunikatów GSA dotyczących konstelacji GNSS i systemu wspomagającego opartego na wyposażeniu satelitarnym SBAS.”;

c) w pkt 4.2.2 pozycja GNS_23 ppkt 5 otrzymuje brzmienie:

„5. Procesor VU sprawdza otrzymane dane, wyodrębniając informacje (np. o długości geograficznej, szerokości geograficznej, czasie) z komunikatu NMEA RMC. Komunikat RMC NMEA zawiera informację o tym, czy położenie jest prawidłowe. Jeżeli położenie nie jest prawidłowe, dane dotyczące lokalizacji nie są jeszcze dostępne i nie można ich wykorzystać w celu zarejestrowania położenia pojazdu. Jeżeli położenie jest prawidłowe, procesor VU wyodrębnia również wartości HDOP z komunikatów NMEA GSA i oblicza minimalną wartość w stosunku do dostępnych systemów satelitarnych (tj. jeżeli ustalenie położenia jest możliwe).”;

d) w pkt 4.4.1 pozycja GNS_28 otrzymuje brzmienie:

„GNS_28 Jeżeli VU nie uda się nawiązać połączenia z powiązaniem z urządzeniem zewnętrznym GNSS przez dłużej niż 20 minut ciągłej pracy, przyrząd ten generuje i rejestruje zdarzenie typu »EventFaultType« z wartością enum »0E«H Błąd komunikacji z urządzeniem zewnętrznym GNSS oraz ze znacznikiem czasu ustawionym na bieżącą godzinę. Zdarzenie zostanie wygenerowane, wyłącznie jeżeli spełnione będą następujące dwa warunki: a) tachograf inteligentny nie znajduje się w trybie kalibracyjnym; oraz b) pojazd jest w ruchu. W tym kontekście występuje błąd połączenia, gdy bezpieczny nadajnik-odbiornik VU nie otrzyma komunikatu odpowiedzi po wysłaniu komunikatu żądania, jak opisano w pkt 4.2.”;

e) w pkt 4.4.2 pozycja GNS_29 otrzymuje brzmienie:

„GNS_29 W przypadku naruszenia integralności fizycznej urządzenia zewnętrznego GNSS bezpieczny nadajnik-odbiornik GNSS kasuje całą swoją pamięć, w tym materiał kryptograficzny. Jak opisano w GNS_25 i GNS_26, VU wykrywa manipulowanie, jeżeli odpowiedź ma status »6690«. Następnie VU generuje zdarzenie typu »EventFaultType« z wartością enum »19«H Wykrywanie manipulowania GNSS. Urządzenie zewnętrzne GNSS nie może już również odpowiadać na żadne żądania zewnętrzne.”;

f) w pkt 4.4.3 pozycja GNS_30 otrzymuje brzmienie:

„GNS_30 Jeżeli bezpieczny nadajnik-odbiornik GNSS nie otrzymuje danych z odbiornika GNSS przez dłużej niż 3 godziny ciągłej pracy, urządzenie to generuje komunikat odpowiedzi na polecenie READ RECORD z numerem rekordu »01« i polem danych o rozmiarze 12 bajtów, wszystkich ustawionych na 0xFF. Po otrzymaniu komunikatu odpowiedzi z określoną wartością pola danych VU generuje i rejestruje zdarzenie typu »EventFaultType« z wartością enum »0D«H Brak informacji o pozycji z odbiornika GNSS ze znacznikiem czasu o bieżącej wartości czasu, wyłącznie jeżeli spełnione będą następujące dwa warunki: a) tachograf inteligentny nie znajduje się w trybie kalibracyjnym; oraz b) pojazd jest w ruchu.”;

g) w pkt 4.4.4 tekst w pozycji GNS_31 aż do rys. 4 otrzymuje brzmienie:

„Jeżeli VU wykryje, że certyfikat EGF wykorzystywany do celów wzajemnego uwierzytelniania stracił ważność, przyrząd rejestrujący generuje i rejestruje zdarzenie przyrządu rejestrującego typu »EventFaultType« z wartością enum »IB«H Wygaśnięcie certyfikatu urzędnika zewnętrznego GNSS ze znacznikiem czasu o bieżącej wartości czasu. VU nadal wykorzystuje otrzymane dane GNSS o położeniu.”;

h) w pkt 5.2.1 pozycja GNS_34 otrzymuje brzmienie:

»GNS_34 Jeżeli VU nie otrzymuje danych z odbiornika GNSS przez dłuższą niż 3 godziny ciągłej pracy, przyrząd ten generuje i rejestruje zdarzenie typu »EventFaultType« z wartością enum »OD«H Brak informacji o pozycji z odbiornika GNSS ze znacznikiem czasu o bieżącej wartości czasu, wyłącznie jeżeli spełnione będą następujące dwa warunki: a) tachograf inteligentny nie znajduje się w trybie kalibracyjnym; oraz b) pojazd jest w ruchu.«;

i) pkt 6 otrzymuje brzmienie:

„6. KONFLIKT CZASOWY GNSS

Jeżeli VU wykryje rozbieżność wynoszącą ponad 1 minutę między czasem funkcji pomiaru czasu przyrządu rejestrującego a czasem z odbiornika GNSS, przyrząd rejestrujący zarejestruje zdarzenie typu „EventFaultType” z wartością enum »OB«H Konflikt czasowy (między GNSS a wewnętrznym zegarem VU). Po wywołaniu zdarzenia dotyczącego konfliktu czasowego VU nie weryfikuje rozbieżności czasu przez następne 12 godzin. Wydarzenie to nie uruchamia się, jeżeli odbiornik GNSS nie wykrywał prawidłowego sygnału GNSS w ciągu ostatnich 30 dni.”;

38) w dodatku 13 wprowadza się następujące zmiany:

a) w pkt 2 akapit czwarty otrzymuje brzmienie:

„W tym miejscu należy wyjaśnić, że w niniejszym dodatku nie określa się:

- operacji gromadzenia *danych* i zarządzania tym procesem w ramach VU (co jest określone w innym miejscu w rozporządzeniu lub w przeciwnym razie stanowi funkcję projektu produktu);
- formy przedstawienia zgromadzonych danych w aplikacji zainstalowanej na urządzeniu zewnętrznym;
- przepisów dotyczących bezpieczeństwa danych wykraczających poza zabezpieczenia zapewniane przez Bluetooth® (takie jak szyfrowanie) w odniesieniu do treści *danych* (które zostaną określone w innym miejscu w rozporządzeniu [dodatek 11 »Wspólne mechanizmy zabezpieczenia«]);
- protokołów Bluetooth® wykorzystywanych przez interfejs ITS.”;

b) w pkt 4.2 akapit trzeci otrzymuje brzmienie:

„W momencie gdy urządzenie zewnętrzne pojawi się po raz pierwszy w zakresie działania VU, można rozpocząć proces parowania Bluetooth® (zob. również załącznik 2). Urządzenia wymieniają adresy, nazwy, profile i wspólny klucz tajny, co pozwala im się łączyć, ilekroć znajdą się w pobliżu siebie w przyszłości. Po zakończeniu tego etapu urządzenie zewnętrzne uzyskuje status urządzenia zaufanego i jest w stanie inicjować żądania pobrania danych z tachografu. Nie przewiduje się możliwości dodawania mechanizmów szyfrowania poza mechanizmami zapewnianymi przez Bluetooth®. Jeżeli jednak dodatkowe mechanizmy zabezpieczeń są konieczne, zostaną one dodane zgodnie z dodatkiem 11 »Wspólne mechanizmy zabezpieczenia«.”;

c) w pkt 4.3 wprowadza się następujące zmiany:

(i) akapit pierwszy otrzymuje brzmienie:

„Ze względów bezpieczeństwa VU będzie wymagał systemu autoryzacji za pomocą kodu PIN działającego oddzielnie od systemu parowania Bluetooth. Każdy VU musi być w stanie generować kody PIN służące do uwierzytelniania, składające się z co najmniej 4 cyfr. Za każdym razem gdy urządzenie zewnętrzne paruje się z VU, musi wprowadzić poprawny kod PIN, zanim otrzyma jakiegokolwiek dane.”;

(ii) akapit trzeci po tabeli 1 otrzymuje brzmienie:

„Podczas gdy producent może zapewnić możliwość zmiany kodu PIN bezpośrednio przez VU, kodu PUC nie można zmienić. Zmiana kodu PIN, o ile jest możliwa, wymaga wprowadzenia obecnego kodu PIN bezpośrednio w VU.”;

d) w pkt 4.4 akapit drugi po nagłówku »Pole danych« otrzymuje brzmienie:

„Jeżeli dane, które mają być obsługiwane, są większe niż miejsce dostępne w jednym komunikacie, zostaną podzielone na kilka podkomunikatów. Każdy podkomunikat ma taki sam nagłówek i SID, ale zawiera dwubajtowy licznik, bieżący licznik (Counter Current, CC) i maksymalny licznik (Counter Max, CM), w celu wskazania numeru podkomunikatu. Aby umożliwić kontrolę błędów i przerwanie przesyłania, urządzenie przyjmujące zatwierdza każdy podkomunikat. Urządzenie przyjmujące może przyjąć podkomunikat, zażądać ponownego przesłania podkomunikatu, zażądać od urządzenia wysyłającego ponownego rozpoczęcia transmisji lub jej przerwania.”;

e) w załączniku 1 wprowadza się następujące zmiany:

(i) tytuł otrzymuje brzmienie:

„1) WYKAZ DANYCH DOSTĘPNYCH ZA POŚREDNICTWEM INTERFEJSU ITS”;

(ii) w tabeli w pkt 3 po pozycji „Brak informacji o położeniu z odbiornika GNSS” dodaje się pozycję w brzmieniu:

„Błąd połączenia z urządzeniem zewnętrznym GNSS	— najdłuższe zdarzenie w każdym z ostatnich 10 dni ich występowania, — 5 najdłuższych zdarzeń w ciągu ostatnich 365 dni.	— data i godzina początku zdarzenia, — data i godzina końca zdarzenia, — typ karty, numer, państwo członkowskie wydające kartę i generacja dla każdej karty wprowadzonej na początku lub pod koniec zdarzenia, — liczba podobnych zdarzeń w tym dniu.”
---	---	---

(iii) w pkt 5 dodaje się tiret w brzmieniu:

„— usterka interfejsu ITS (w stosownych przypadkach).”;

f) w specyfikacjach ASN.1 w załączniku 3 wprowadza się następujące zmiany:

(i) po wierszu 206 dodaje się wiersze 206a–206e w brzmieniu:

```

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

```

(ii) wiersze 262–264 otrzymują brzmienie:

```

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

```

(iii) wiersz 275 otrzymuje brzmienie:

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

(iv) wiersze 288–310 otrzymują brzmienie:

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

(v) wiersze 362 i 363 otrzymują brzmienie:

```
„362     driver1MaximumDailyDrivingTime BIT STRING (SIZE(4)),
363     driver2MaximumDailyDrivingTime BIT STRING (SIZE(4)),;”
```

(vi) po wierszu 410 dodaje się wiersze 410a i 410b w brzmieniu:

```
„410a     comErrorWithExternalGNSSFacility
410b     CommunicationErrorWithTheExternalGNSSFacility,;”
```

(vii) po wierszu 539 dodaje się wiersze 539a–539j w brzmieniu:

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

39) w dodatku 14 wprowadza się następujące zmiany:

a) pkt 5.5 w spisie treści otrzymuje brzmienie:

„5.5 Wsparcie wdrażania dyrektywy (UE) 2015/719 490”;

b) w pkt 2 akapit trzeci otrzymuje brzmienie:

„W takim przypadku czas dostępny na nawiązanie łączności jest ograniczony, ponieważ łączność ma ukierunkowany charakter i cechuje się krótkim zasięgiem. Ponadto właściwe organy kontrolne mogą korzystać ze środków łączności wykorzystywanych do celów zdalnego monitorowania tachografu również do innych celów (np. do przekazywania informacji dotyczących maksymalnych obciążeń i wymiarów pojazdów ciężarowych określonych w dyrektywie (UE) 2015/719), przy czym działania w tym zakresie mogą być podejmowane oddzielnie lub sekwencyjnie według uznania właściwych organów kontrolnych.”;

c) w pkt 5.1 wprowadza się następujące zmiany:

(i) pozycja DSC_19 tiret dwunaste otrzymuje brzmienie:

„— antenę DSRC-VU umieszcza się w miejscu, w którym zapewnia optymalną łączność DSRC między pojazdem a anteną drogową czytnika, w przypadku gdy czytnik został zainstalowany w odległości 15 m z przodu pojazdu i na wysokości 2 m, możliwie blisko środkowej części szyby w poziomie i w pionie. W przypadku pojazdów lekkich odpowiednie jest zainstalowanie anteny w górnej części szyby przedniej. W przypadku pozostałych pojazdów antenę DSRC należy zamontować w pobliżu dolnej albo górnej części szyby przedniej.”;

(ii) pozycja DSC_22 akapit pierwszy otrzymuje brzmienie:

„Współczynnik kształtu anteny nie został zdefiniowany i stanowi przedmiot decyzji handlowej, dopóki wbudowany DSRC-VU spełnia wymagania zgodności określone w sekcji 5 poniżej. Antena jest umieszczona w miejscu określonym w DSC_19 i skutecznie wspomaga przypadki wykorzystania opisane w pkt 4.1.2 i 4.1.3.”;

d) w pkt 5.4.3 sekwencja 7 otrzymuje brzmienie:

„7 REDCR > DSRC-VU Wysła GET.request w odniesieniu do danych innego Atrybutu (w razie potrzeby)”;

e) w pkt 5.4.4 w definicji modułu ASN.1 w pozycji DCS_40 wprowadza się następujące zmiany:

(i) wiersz pierwszy sekwencji dla TachographPayload otrzymuje brzmienie:

„tp15638VehicleRegistrationPlate LPN - Vehicle Registration Plate as per EN 15509¹”

(ii) dodaje się przypis ¹ w brzmieniu:

„1. Jeżeli LPN zawiera AlphabetIndicator LatinAlphabetNo2 lub latinCyrillicAlphabet, znaki specjalne są ponownie mapowane w urządzeniu interrogatora drogowego przy zastosowaniu specjalnych przepisów zgodnie z załącznikiem E do normy ISO/DIS 14 906,2.”;

(iii) usuwa się cyfrę 2 w górnym indeksie z wiersza, w którym zdefiniowano znacznik czasu bieżącego rekordu (Timestamp of current record);

(iv) definicja modułu ASN.1 dla RtmTransferAck otrzymuje brzmienie:

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

f) w pkt 5.4.5 pozycja RTM12 w tabeli 14.3 otrzymuje brzmienie:

<p>„RTM12 Usterka czujnika</p>	<p>VU generuje wartość w postaci liczby całkowitej w odniesieniu do elementu danych RTM12.</p> <p>VU przypisuje zmiennej sensorFault wartość:</p> <ul style="list-style-type: none"> — 1 w przypadku zarejestrowania w ciągu ostatnich 10 dni zdarzenia typu »35H« związanego z usterką czujnika, — 2 w przypadku zarejestrowania w ciągu ostatnich 10 dni typu zdarzenia związanego z usterką odbiornika GNSS (wewnętrznego albo zewnętrznego, o wartości enum»36«H lub »37« H); — 3 w przypadku zarejestrowania w ciągu ostatnich 10 dni zdarzenia typu »0E«H związanego z błędem łączności z urządzeniem zewnętrznym GNSS; — 4 w przypadku zarejestrowania w ciągu ostatnich 10 dni zarówno usterki czujnika, jak i usterki odbiornika GNSS; — 5 w przypadku zarejestrowania w ciągu ostatnich 10 dni zarówno zdarzenia typu usterka czujnika, jak i błąd łączności z urządzeniem zewnętrznym GNSS; — 6 w przypadku zarejestrowania w ciągu ostatnich 10 dni zarówno zdarzenia typu usterka odbiornika GNSS, jaki i błąd łączności z urządzeniem zewnętrznym GNSS; — 7 w przypadku zarejestrowania w ciągu ostatnich 10 dni występowania wszystkich trzech usterek czujnika, W PRZECIWNYM WYPADKU przypisuje wartość 0, jeżeli w ciągu ostatnich 10 dni nie zarejestrowano żadnych zdarzeń. 	<p>— usterka czujnika jeden oktet zgodnie ze słownikiem danych</p>	<p>sensorFault INTEGER (0..255);</p>
--	---	--	--

g) pkt 5.4.6 pozycja DSC_43 otrzymuje brzmienie:

„DSC_43 Wszystkie dane wymieniane w ramach DSRC koduje się przy użyciu reguł PER (Packed Encoding Rules) UNALIGNED, z wyjątkiem TachographPayload oraz OwsPayload, które koduje się przy użyciu reguł OER (Octet Encoding Rules) zdefiniowanych w normie ISO/IEC 8825-7, Rec. ITU-T X.696.”;

h) w pkt 5.4.7 w kolumnie czwartej w tabeli 14.9 tekst w rubryce opisującej Rtm-ContextMark; otrzymuje brzmienie:

„Identyfikator obiektu obsługiwanej normy, części i wersji. Przykład: ISO (1) norma (0) TARV (15638) część 9 (9) wersja 1 (1).

Wartość pierwszego oktetu to 06H i stanowi identyfikator obiektu. Wartość drugiego oktetu to 06H i stanowi jego długość. Kolejne 6 oktetów koduje przykładowy identyfikator obiektu.”;

i) pkt 5.5 i 5.5.1 otrzymują brzmienie:

„5.5. Wsparcie wdrażania dyrektywy (UE) 2015/719

5.5.1. Przegląd

DSC_59 W celu wsparcia wdrażania dyrektywy (UE) 2015/719 w sprawie maksymalnych obciążeń i wymiarów pojazdów ciężarowych protokół transakcji służący do pobierania danych OWS za pośrednictwem połączenia interfejsu DSRC działającego na częstotliwości 5,8 GHz będzie taki sam jak protokół używany do przekazywania danych dotyczących zdalnego monitorowania tachografu (zob. 5.4.1) – jedyna różnica polega na tym, że identyfikator obiektu odnoszący się do normy TARV będzie odnosił się do części 20 normy ISO 15638 (TARV) dotyczącej systemów ważenia w pojeździe.”;

j) pkt 5.6.1 pozycja DSC_68 lit. a) otrzymuje brzmienie:

„a) aby można było zawierać umowy z różnymi dostawcami na dostawę VU i DSRC-VU oraz w praktyce różnych serii DSRC-VU, połączenie między VU a DSRC-VU niebędącym elementem wewnętrznym VU musi być otwartym połączeniem standardowym. VU musi być połączony z DSRC-VU za pomocą:”;

k) pkt 5.7.1 pozycja DSC_77 otrzymuje brzmienie:

„DSC_77 Już zabezpieczone dane są przekazywane DSRC-VU za pomocą funkcji VUSM. VUSM sprawdza, czy dane zarejestrowane w DSRC-VU zostały poprawnie zarejestrowane. Rejestrowanie i zgłaszanie wszelkich błędów, jakie wystąpiły podczas przesyłania danych z VU do pamięci DSRC-VU, odbywa się przy użyciu zdarzenia typu EventFaultType z wartością enum ustawioną na »0C«H Błąd łączności z urządzeniem do łączności na odległość wraz ze znacznikiem czasu.”;

40) w dodatku 15 wprowadza się następujące zmiany:

a) pkt 2.2 akapit pierwszy otrzymuje brzmienie:

„Przyjmuje się, że karty do tachografu pierwszej generacji są interoperacyjne z przyrządami rejestrującymi pierwszej generacji zgodnie z załącznikiem IB do rozporządzenia (EWG) nr 3821/85, natomiast karty do tachografu drugiej generacji są interoperacyjne z przyrządami rejestrującymi drugiej generacji zgodnie z załącznikiem IC do niniejszego rozporządzenia. Ponadto zastosowanie mają przedstawione poniżej wymogi.”;

b) w pkt 2.4.1 pozycja MIG_011 wprowadza się następujące zmiany:

(i) tiret pierwsze otrzymuje brzmienie:

„— niepodpisane pliki elementarne IC i ICC (fakultatywnie),”;

(ii) tiret trzecie otrzymuje brzmienie:

„— pliki elementarne zawierające inne dane aplikacyjne (w pliku DF Tachograph) żądane przez protokół pobierania danych z kart pierwszej generacji. Informacje takie są zabezpieczone podpisem cyfrowym zgodnie z mechanizmami zabezpieczenia pierwszej generacji.

Tego rodzaju pobieranie nie może obejmować plików elementarnych zawierających dane aplikacyjne istniejących wyłącznie w kartach kierowców (i kartach warsztatowych) drugiej generacji (pliki elementarne zawierające dane aplikacyjne w pliku DF Tachograph_G2).”;

c) w pkt 2.4.3 pozycje MIG_014 i MIG_015 otrzymują brzmienie:

„MIG_014 Poza ramami kontroli kierowców przez organ kontrolny spoza UE dane z przyrządów rejestrujących drugiej generacji są pobierane z zastosowaniem mechanizmów zabezpieczenia drugiej generacji i protokołu pobierania danych określonego w dodatku 7 do niniejszego załącznika.

MIG_015 Aby organy kontrolne spoza UE mogły kontrolować kierowców, opcjonalnie można również umożliwić pobieranie danych z przyrządów rejestrujących drugiej generacji z zastosowaniem mechanizmów zabezpieczenia pierwszej generacji. Pobierane dane mają wtedy taki sam format jak dane pobierane z przyrządu rejestrującego pierwszej generacji. Funkcję tę można wybrać za pomocą poleceń w menu.”.

ZAŁĄCZNIK II

W załączniku II do rozporządzenia (UE) 2016/799 wprowadza się następujące zmiany:

1) w rozdziale I pkt 1 lit. b) otrzymuje brzmienie:

„b) numeru homologacji odpowiadającego numerowi świadectwa homologacji wydanego dla prototypu urządzenia rejestrującego lub wykresówki, bądź karty do tachografu, umieszczonemu bezpośrednio obok tego prostokąta.”;

2) w rozdziale III pkt 5 otrzymuje brzmienie:

„5. Zgłoszono do homologacji w dniu:”;

3) w rozdziale IV pkt 5 otrzymuje brzmienie:

„5. Zgłoszono do homologacji w dniu:”.
