INTERNATIONAL STANDARD

ISO 15638-9

First edition
2020-08

Intelligent transport systems — Framework for cooperative telematics applications for regulated commercial freight vehicles (TARV) —

Part 9: Remote digital tachograph monitoring

Systèmes intelligents de transport — Cadre pour applications télématiques coopératives pour véhicules de fret commercial réglementé (TARV) —

Partie 9: Monitorage du tachygraphe électronique à distance (RTM)

Reference number
ISO 15638-9:2020(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems*.

This first edition of ISO 15638-9 cancels and replaces ISO/TS 15638-9:2013, which has been technically revised. The main changes compared to the previous edition are as follows:

— Inclusion of remote inspection using short-range wireless interrogator for enforcement inspection purposes.

A list of all parts in the ISO 15638 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Many ITS technologies have been embraced by commercial transport operators and freight owners in the areas of fleet management, safety and security. On-board applications have also been developed for governmental use. Such regulatory services in use or being considered vary from jurisdiction to jurisdiction, but include electronic on-board recorders, digital tachograph, on-board mass monitoring, 'mass' data for regulatory control and management, weigh-in-motion, vehicle access methods, hazardous goods tracking and eCall. Additional applications with a regulatory impact being developed include fatigue management, speed monitoring and vehicle penalties imposed based on location, distance and time.

In such an emerging environment of regulatory and commercial applications, it is timely to consider an overall architecture (business and functional) that could support these functions from a single platform within a commercial freight vehicle that operates within such regulations. International Standards will allow for a speedy development and specification of new applications that build upon the functionality of a generic specification platform. A series of standards deliverables is required to describe and define the framework and requirements so that the on-board equipment and back office systems can be commercially designed in an open market to meet common requirements of jurisdictions.

The ISO 15638 TARV series addresses and defines the framework for a range of cooperative telematics applications for regulated vehicles (e.g. access methods, driver fatigue management, speed monitoring, on-board mass monitoring, Remote Tachograph Monitoring, ADR management). The overall scope includes the concept of operation, legal and regulatory issues, and the generic cooperative provision of services to regulated vehicles, using an on-board ITS platform. The framework is based on a (multiple) service provider-oriented approach with provisions for the approval and auditing of service providers.

The ISO 15638 series provides both the means to achieve current requirements for telematics applications for regulated vehicles and the basis for future development of cooperative telematics applications for regulated vehicles.

The ISO 15638 series is timely, as many governments (Europe, North America, Asia and Australia/New Zealand) are considering the use of telematics for a range of regulatory purposes.

This document provides specifications for weigh-in-motion and on-board weighing monitoring and supports several defined communication profiles in which this function may be performed.

NOTE 1 The definition of what comprises a 'regulated' vehicle is regarded as an issue for national decision and can vary from jurisdiction to jurisdiction. This series does not impose any requirements on nations in respect of how they define a regulated vehicle.

NOTE 2 The definition of what comprises a 'regulated' service is regarded as an issue for national decision and can vary from jurisdiction to jurisdiction. This series does not impose any requirements on nations in respect of which services for regulated vehicles jurisdictions they will require, or support as an option, but will provide standardized sets of requirements descriptions for identified services to enable consistent and cost-efficient implementations where implemented.

Intelligent transport systems — Framework for cooperative telematics applications for regulated commercial freight vehicles (TARV) —

Part 9:
Remote digital tachograph monitoring

1 Scope

This document addresses the provision of 'Remote Digital Tachograph Monitoring' and specifies the form and content of the transmission of such data required to support such systems, and access methods to that data.

This document provides specifications for common communications and data exchange aspects of the application service remote digital tachograph monitoring that a jurisdiction regulator can elect to require or support as an option, including:

a) High level definition of the service that a service provider provides. The service definition describes common service elements but does not define the detail of how such an application service is instantiated, nor the acceptable value ranges of the data concepts defined.

b) Means to realize the service.

c) Application data naming, content and quality that an IVS delivers, including a number of profiles for data (noting that requirements and constraints of what can/cannot be transmitted over the air can vary between jurisdictions).

d) Support for a number of defined communication profiles to enable remote inspection.

This document is not applicable for analogue tachograph equipment/systems.

This document provides specifications for the following communication profiles:

— **Communication Profile C1: Roadside inspection using a short-range wireless communication interrogator instigating a physical roadside inspection (master<>slave)**

  Profile C1a: via a hand aimed or temporary roadside mounted and aimed interrogator

  Profile C1b: via a vehicle mounted and directed interrogator

  Profile C1c: via a permanent or semi-permanent roadside or overhead gantry

— **Communication Profile C2: Roadside inspection using a short-range wireless communication interrogator instigating a download of data to an application service provider via an ITS-station communication (master<>slave + peer<>peer)**

  Profile C2a: via a hand aimed or temporary roadside mounted and aimed interrogator

  Profile C2b: via a vehicle mounted and directed interrogator

  Profile C2c: via a permanent or semi-permanent roadside or overhead gantry

— **Communication Profile C3: Remote inspection addressed via an ITS-station instigating a download of data to an application service provider via a wireless communications interface** (as defined in ISO 15638-2).

It is possible that subsequent versions of this document will support additional communication profiles.

NOTE 1 The definition of what comprises a 'regulated' service is regarded as an issue for national decision and can vary from jurisdiction to jurisdiction. This document does not impose any requirements on nations in respect of which services for regulated vehicles jurisdictions will require, or support as an option, but provides standardized sets of requirements descriptions for identified services to enable consistent and cost-efficient implementations where instantiated.

NOTE 2 The ISO 15638 series has been developed for use in the context of regulated commercial freight vehicles (hereinafter referred to as 'regulated vehicles'). However, there is nothing to prevent a jurisdiction from extending or adapting the scope to include other types of regulated vehicles, as it deems appropriate.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 14906, *Electronic fee collection — Application interface definition for dedicated short-range communication*

ISO 15638-1, *Intelligent transport systems — Framework for collaborative Telematics Applications for Regulated commercial freight Vehicles (TARV) — Part 1: Framework and architecture*

ISO 15638-2, *Intelligent transport systems — Framework for collaborative Telematics Applications for Regulated commercial freight Vehicles (TARV) — Part 2: Common platform parameters using CALM*

ISO 15638-3, *Intelligent transport systems — Framework for collaborative Telematics Applications for Regulated commercial freight Vehicles (TARV) — Part 3: Operating requirements, 'Approval Authority' procedures, and enforcement provisions for the providers of regulated services*

ISO/TS 15638-4, *Intelligent transport systems — Framework for cooperative telematics applications for regulated commercial freight vehicles (TARV) — Part 4: System security requirements*

ISO 15638-5:2013, *Intelligent transport systems — Framework for collaborative Telematics Applications for Regulated commercial freight Vehicles (TARV) — Part 5: Generic vehicle information*

ISO 15638-6:2014, *Intelligent transport systems — Framework for collaborative Telematics Applications for Regulated commercial freight Vehicles (TARV) — Part 6: Regulated applications*

ERC 70-03, *ERC RECOMMENDATION 70-03 Relating To The Use Of Short Range Devices (Srd)*

ETSI EN 300-674-1, V1.2.1:2004-08, *Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band; Part 1: General characteristics and test methods for Road Side Units (Interrogator) and On-Board Units (OBU)*

ETSI ES 200-674-1, V2.2.1:2011-02, *Intelligent Transport Systems (ITS); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communication (DSRC); Part 1: Technical characteristics and test methods for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band*

ETSI TS 102-792, V1.2.1:2015-06, *Intelligent Transport Systems (ITS); Mitigation techniques to avoid interference between European CEN Dedicated Short Rang Communication (CEN DSRC) equipment and Inteligent Transport Systems (ITS) operating in the 5 GHz frequency range*

EN 12253, *Road transport and traffic telematics — Dedicated short-range communication — Physical layer using microwave at 5,8 GHz*

EN 12795, *Road transport and traffic telematics — Dedicated Short Range Communication (DSRC) — DSRC data link layer: medium access and logical link control*

EN 12834, *Road transport and traffic telematics — Dedicated Short Range Communication (DSRC) — DSRC application layer*

EN 13372, *Road transport and traffic telematics (RTTT) — Dedicated short-range communication — Profiles for RTTT applications*

ARIB STD-T75, *Dedicated Short-Range Communication*

TTAS KO-06.0025, Standard of *DSRC* Radio Communication between Road-side Equipment and On-board Equipment in 5,8GHz band

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 15638-1 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
app
small (usually) *Java™*[1)] (3.21) applets, organized as software bundles, that support *application services* (3.2) by keeping the *data pantry* (3.14) provisioned with up to date data

3.2
application service
service provided by a *service provider* (3.32) enabled by accessing data from the *IVS* (3.18) of a *regulated vehicle* (3.30) via a wireless communications network

3.3
application service provider
ASP
party that provides an *application service* (3.2)

3.4
app library
separately secure area of memory in *IVS* (3.18) where apps are stored with different access controls to *data pantry* (3.14)

3.5
approval
formal affirmation that an applicant has satisfied all the requirements for appointment as an *application service provider* (3.3) or that an application service delivers the required service levels

3.6
approval agreement
written agreement made between an *approval authority (regulatory)* (3.7) and a *service provider* (3.32)

Note 1 to entry: An *approval authority (regulatory)* (3.7) approval agreement recognizes the fact that a *service provider* (3.32), having satisfied the *approval authority's* requirements for appointment as a *service provider,* is appointed in that capacity, and sets out the legal obligations of the parties with respect to the on-going role of the *service provider*.

1) Java™ is an example of a suitable product available commercially. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of this product.

3.7
approval authority
<regulatory> organization (usually independent) which conducts *approval* (3.5) and ongoing *audit* (3.9) for *service providers* (3.32) on behalf of a *jurisdiction* (3.22)

3.8
architecture
formalized description of the design of the structure of TARV and its *framework* (3.17)

3.9
audit/auditing
review of a party's capacity to meet, or continue to meet, the initial and ongoing *approval agreements* (3.6) as a *service provider* (3.32)

3.10
basic vehicle data
data that shall be maintained/provided by all *IVS* (3.18) regardless of *jurisdiction* (3.22)

3.11
communications access for land mobiles
CALM
layered solution that enables continuous or quasi continuous communications between vehicles and the infrastructure, or between vehicles, using such (multiple) wireless telecommunications media that are available in any particular location, and which have the ability to migrate to a different available media where required and where media selection is at the discretion of *user* (3.37) determined parameters by using a suite of standards based on ISO 21217 (*CALM* architecture) and ISO 21210 (*CALM* networking)

3.12
commercial application(s)
ITS applications in *regulated vehicles* (3.30) for commercial (non-regulated) purposes

EXAMPLE Asset tracking, vehicle and engine monitoring, cargo security, driver management.

3.13
core data
basic vehicle data (3.10) plus any additional data required to provide an implemented *regulated application service* (3.29)

3.14
data pantry
secure area of memory in *IVS* (3.18) where data values are stored with different access controls to *app library* (3.4)

3.15
driver
person driving the *regulated vehicle* (3.30) at any specific point in time

3.16
facilities
layer that sits on top of the communication stack and helps to provide data interoperability and reuse, and to manage applications and enable dynamic real time loading of new applications

3.17
framework
particular set of beliefs or ideas referred to in order to describe a scenario or solve a problem

3.18
in-vehicle system
IVS
ITS-station (3.19) and connected (TARV/RTM) equipment on board a vehicle known in EFC specific equipment as OBE (on-board equipment) or OBU (on-board unit)

Note 1 to entry: Often known in tachograph specific regulations as VU (vehicle unit).

3.19
interrogator
off-board device which can establish a wireless communications session with the IVS and request the provision of tachograph data which is often a mobile device under the control of an agent of the jurisdiction

3.20
ITS-station
ITS-s
entity in a communication network, comprised of application, *facilities* (3.16), networking and access layer components specified that operate within a bounded secure management domain

Note 1 to entry: For details, see ISO 21217.

3.21
Java™
object oriented open source operating language developed by SUN systems

3.22
jurisdiction
government, road or traffic authority which owns the *regulatory applications* (3.28)

EXAMPLE Country, state, city council, road authority, government department (customs, treasury, transport).

3.23
jurisdiction regulator
agent of the *jurisdiction* (3.22) appointed to regulate and manage TARV within the domain of the *jurisdiction* which may or may not be the *approval authority (regulatory)* (3.7)

3.24
operator
fleet manager of a *regulated vehicle* (3.30)

3.25
physical roadside inspection
physical inspection of the tachograph data of a stopped vehicle by agents of the application service provider (usually police or inspectors appointed by the jurisdiction)

3.26
prime service provider
service provider (3.32) who is the first contractor to provide *regulated application services* (3.29) to the *regulated vehicle* (3.30), or a nominated successor on termination of that initial contract and who is also responsible for maintaining the installed *IVS* (3.18)

Note 1 to entry: If the *IVS* was not installed during the manufacture of the vehicle, the *prime service provider* is also responsible for installing and commissioning the *IVS* (3.18).

3.27
profile
common and consistent elaboration of content and sequence of a set of chosen classes, conforming subsets, options, parameters, and/or data concepts to accomplish a particular function/specification

3.28
regulated application
regulatory application
application arrangement using TARV utilized by *jurisdictions* (3.22) for granting certain categories of commercial vehicles rights to operate in regulated circumstances subject to certain conditions, or indeed to permit a vehicle to operate within the *jurisdiction* and which may be mandatory or voluntary at the discretion of the *jurisdiction*

3.29
regulated application service
TARV *application service* (3.2) to meet the requirements of a regulated application that is mandated by a regulation imposed by a *jurisdiction* (3.22), or is an option supported by a *jurisdiction*

3.30
regulated vehicle
vehicle that is subject to regulations determined by the *jurisdiction* (3.22) as to its use on the road system of the *jurisdiction* in regulated circumstances, subject to certain conditions, and in compliance with specific regulations for that class of regulated vehicle and which at the option of *jurisdictions* may require the provision of information via *TARV* or provide the option to do so

3.31
remote tachograph monitoring
RTM
collection, collation, and transfer of data from an on-board electronic *tachograph* (3.35) system to an *application service provider* (3.3)

3.32
service provider
party which is certified by an approval *authority (regulatory)* (3.7) as suitable to provide regulated or commercial ITS *application services* (3.2)

3.33
session
wireless communication exchange between the *ITS-station* (3.19) of an *IVS* (3.18) and the *ITS-station* of its *application service provider* (3.3) to achieve data update, data provision, upload apps, or otherwise manage the provision of the *application service* (3.2), or a wireless communication provision of data to the *ITS-station* of an *IVS* (3.18) from any other *ITS-station*

3.34
specification
explicit and detailed description of the nature and functional requirements and minimum performance of equipment, service or a combination of both

3.35
tachograph
sender unit usually mounted to a vehicle gearbox, a tachograph head and a digital driver card, which records the *regulated vehicle* (3.30) speed and the times at which it was driven and aspects of the *driver's* (3.15) activity selected from a choice of modes

3.36
telematics
use of wireless media to obtain and transmit (data) from a distant source

3.37
user
individual or party that enrols in and operates within a regulated or *commercial application* (3.12) *service* (3.2)

EXAMPLE *Driver* (3.15), transport *operator* (3.24), freight owner.

4 Symbols and abbreviated terms

ADU	Application Data Unit
APDU	application protocol data unit
App	applet (JAVA™ application or similar)
ASN.1	Abstract Syntax Notation One
ASP	application service provider
BER	Bit Error Rate
BLE	Bluetooth Low Energy
BST	Beacon Service Table
CALM	communications access for land mobiles
CAN	controller area network
CRC	cyclic redundancy check
DSRC	Dedicated Short-Range Communication
EID	Element Identifier
EFC	Electronic Fee Collection
EN	European Norm (Standard)
GNSS	Global Navigation Satellite System
ID	Identity
ITS-s	ITS station
IVS	In-vehicle system
L7	Layer 7 of DSRC (Application Layer Core of DSRC)
LID	logical link control identifier
LLC	logical link control
LPDU	link layer protocol data unit
MAC	Media Access Control (Media Access Layer Core of DSRC)
MA-DATA	MAC sublayer primitive to the LLC sublayer
OBE	On-board equipment (EFC term for IVS)
OBU	On-board unit (EFC term for IV unit)
PrWA	private uplink window allocation
PuWA	public uplink window allocation
RR	response request

RSU	Road-side unit (EFC term for roadside interrogator)
RTM	remote tachograph monitoring
SAP	Service access point
SE	service element
T-APDU	Transfer-Application Protocol Data Unit
TARV	telematics applications for regulated vehicles
VST	vehicle service table
VU	vehicle unit (EU regulatory term for tachograph IVS)
WGS84	World Geodetic System 1984
Ms	Microsecond

5 Conformance

Requirements to demonstrate conformance to any of the general provisions or specific application services described in this document shall take into consideration the data requirements imposed by the jurisdiction where they are instantiated.

Systems claiming conformance with this document may support one or more of Communication Profiles C1, C2 and C3 as defined in Clause 1, but shall support at least one of these options.

Systems that wish to claim conformance with TARV ITS-station<>ITS station communications, shall support at least communication profile C3, together with conformance to ISO 15638 Parts 1 to 6.

Jurisdictions requiring and regulating the use of remotely monitored tachographs are recommended to specifically regulate in the case of the use of Profile C1 and/or Profile C2. It is further recommended (but not required) that jurisdictions whose data requirements require support of Profile C1 for regulatory enforcement purposes also at least encourage the ability to technically support Profiles C2 and C3 in addition (for later potential migration purposes).

6 General overview and framework requirements

6.1 General

This document addresses the provision of 'Remote Digital Tachograph Monitoring' and specifies the form and content of the transmission of such data required to support such systems, and access methods to that data.

This document is appropriate for digital tachograph systems. It is not appropriate for analogue tachograph systems.

ISO 15638-1 provides a framework and architecture for TARV. It provides a general description of the roles of the actors in TARV and their relationships.

For a clear understanding of the TARV framework, architecture and detail and specification of the roles of the actors involved, the reader is referred to ISO 15638-1.

ISO 15638-6 provides the core requirements for all regulated applications. For a clear explanation of the general context into which the provision of this application service is provided, the reader is referred to ISO 15638-6.

The present version of this document provides specifications for the following Communication Profiles:

— **Communication Profile C1: Roadside inspection using a short-range wireless communication interrogator instigating a physical roadside inspection (master<>slave)**

  Profile C1a: via a hand aimed or temporary roadside mounted and aimed interrogator;

  Profile C1b: via a vehicle mounted and directed interrogator;

  Profile C1c: via a permanent or semi-permanent roadside or overhead gantry.

  See 6.2 for overview.

— **Communication Profile C2: Roadside inspection using a short-range wireless communication interrogator, instigating a download of data to an application service provider (master<>slave + peer<>peer)**

  Profile C2a: via a hand aimed or temporary roadside mounted and aimed interrogator;

  Profile C2b: via a vehicle mounted and directed interrogator;

  Profile C2c: via a permanent or semi-permanent roadside or overhead gantry.

  See 6.3 for overview.

— **Communication Profile C3: Remote inspection addressed via an ITS-station instigating a download of data to an application service provider via a wireless communications interface (peer<>peer)** (as defined in ISO 15638-2)

  See 6.4 for overview.

NOTE Within the Member States of the European Union, remote tachograph monitoring is controlled by Regulation 2016/799/EC and its Appendix 14, which was published on 2016-05-26 and entered into force from 2016-06-15. This constrains remote tachograph monitoring in the European Union to the transaction defined in Annex B using 5,8 GHz DSRC. Annex B is consistent with this Regulation. For European regulatory requirements regarding the short-range communications interface see 2016/799/EC Appendix 14.

6.2 Overview of Communication Profile C1 — Remote roadside inspection using a short-range wireless communication interrogator instigating a physical roadside inspection

6.2.1 General overview of Communication Profile C1

This profile covers the use case where an agent of the jurisdiction:

a) Uses a short-range communication interrogator to remotely identify a vehicle which is potentially in violation of the tachograph regulations of the jurisdiction.

b) Once identified, the agent of the jurisdiction controlling the interrogation decides whether the vehicle should be stopped, and if so, instructs colleagues downstream to stop the vehicle and effect a physical download of data from the vehicle, or may pass the data directly to them to enable them to make such decisions.

This scenario is appropriate (but not limited to) situations where local data requirements require the physical 'arrest' of a vehicle potentially in violation of regulations and/or where the regulations require a physical download of data made by an agent of the jurisdiction, directly from the 'arrested' vehicle in order to support a prosecution, and/or situations where data concerning the driver is prohibited from being sent via wireless communications.

There are three subset profiles of this remote inspection:

6.2.1.1 Profile C1a — Via a hand aimed or temporary roadside mounted and aimed interrogator

In this use case the agent of the jurisdiction is situated at the roadside, and aims a hand held, tripod mounted, or similar portable interrogator from the roadside towards the centre of the windshield of the targeted vehicle. The interrogation (transaction profiles defined in Annex A, and data profiles defined in Annex C) is made via short range communication such as 5,8 GHz DSRC (defined in Annex B), taking into consideration the data requirements of the jurisdiction. See Figure 1.

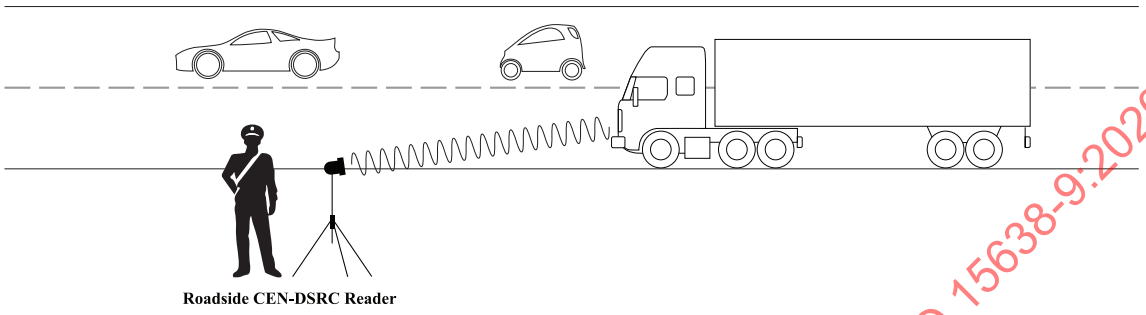


Figure 1 — Use case 1: Roadside interrogation using short range communication

6.2.1.2 Profile C1b — Via a vehicle mounted and directed interrogator

In this use case the agent of the jurisdiction is situated within a moving vehicle, and either aims a hand held, portable interrogator from the vehicle towards the centre of the windshield of the targeted vehicle, or the interrogator is mounted within the vehicle so as to point towards the centre of the windshield of the targeted vehicle when the interrogator's vehicle is in a particular position relevant to the targeted vehicle (for example directly ahead in a stream of traffic). The interrogation (transaction profiles defined in Annex A, and data profiles defined in Annex C) is made via short range communication such as 5,8 GHz DSRC (defined in Annex B), taking into consideration the data requirements of the jurisdiction. See Figure 2.

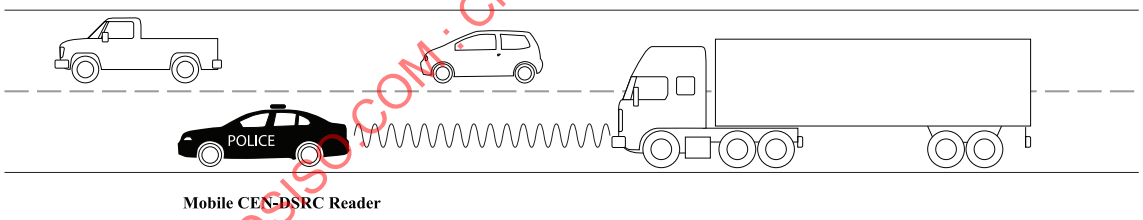


Figure 2 — Use case 2: Vehicle based interrogation using short range communication

6.2.1.3 Profile C1c — Via a permanent or semi-permanent roadside or overhead gantry

In this use case a permanent or semi-permanent gantry or roadside interrogation equipment is activated remotely to the instruction of the agent of the jurisdiction so as to point towards the centre of the windshield of the targeted vehicle when the vehicle passes under or by the interrogator. The interrogation (transaction profiles defined in Annex A, and data profiles defined in Annex C) is made via short range communication such as 5,8 GHz DSRC (as defined in Annex B), taking into consideration the data requirements of the jurisdiction. See Figure 3.

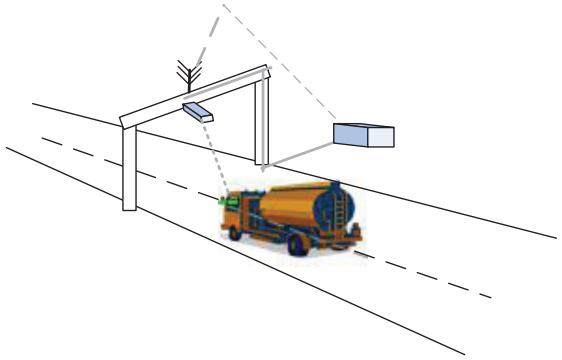


Figure 3 — Gantry mounted interrogator using short range communication

6.3 Overview of Communication Profile C2 — Roadside inspection using a short-range wireless communication interrogator, instigating a download of data to an application service provider

6.3.1 General overview of Communication Profile C2

This use case covers the scenario where an agent of the jurisdiction:

a) Uses a short range communication interrogator to remotely identify a vehicle which is potentially in violation of the tachograph regulations of the jurisdiction.

b) Once so identified, the interrogator provides the vehicle IVS with a case reference code and a destination IP address via the short range communication, and instructs the vehicle IVS to provide the tachograph data required by the tachograph regulation of the jurisdiction.

c) The vehicle IVS then sends the data (probably via its ITS-station) together with the requested destination IP address and case reference to a previously supplied address of the application service provider.

NOTE Consistent with other TARV standards, as part of security measures, except for remote interrogation using short range wireless equipment, it does not send data directly to the requested destination address.

The application service provider is then responsible for validating the requested destination IP address, and if valid, forwards the case reference code and tachograph data to the requested IP address (but these stages of the process are outside the scope of this document. Regulations are given in the data requirements of the jurisdiction).

In this use case, the application service provider may be an agent of/appointed by the jurisdiction or may be a commercial application service provider who is under legal obligation to provide tachograph data to the jurisdiction on request from the jurisdiction. In the case in a jurisdiction where the ASP for this use case is to be an agent of the jurisdiction, then the valid IP address of the ASP shall have been programmed into the memory of the tachograph/ITS-station of all affected vehicles.

There are three subset profiles of this remote inspection:

— Profile C2a: via a hand aimed or temporary roadside mounted and aimed interrogator;

— Profile C2b: via a vehicle mounted and directed interrogator;

— Profile C2c: via a permanent or semi-permanent roadside or overhead gantry.

The interrogation variants are as shown in Figures 1 to 3 above. The overall interrogation scenario is as shown in Figure 4. Transaction profiles are defined in Annex A, data profiles are defined in Annex C, and a wireless transaction is defined in Annex B.

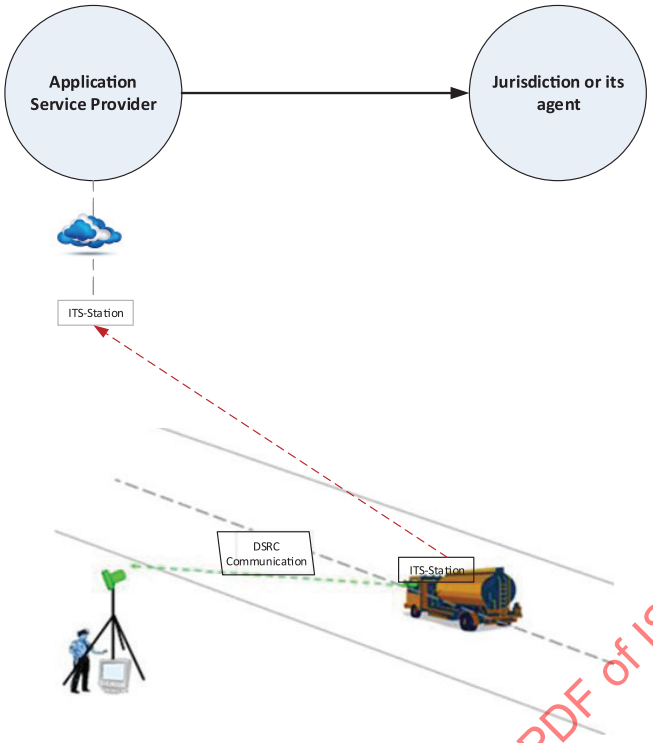


Figure 4 — Communication Profile C2

6.4 Overview of Communication Profile C3 — Remote inspection addressed via an ITS-station instigating a download of data to an application service provider via a wireless communications interface (as defined in ISO 15638-2)

6.4.1 General overview of Communication Profile C3

This profile covers the scenario where an agent of the jurisdiction either:

a) Directly uses an ITS-station to interrogate the target vehicle via the ITS-station of the target vehicle (probably because of its location in a target zone), or

b) Remotely (from any internet connected location) addresses the vehicle via the IP address of the target vehicle to remotely identify a vehicle which is potentially in violation of the tachograph regulations of the jurisdiction.

c) Once so identified, the agent of the jurisdiction via the ITS-station<>ITS-station communication provides the vehicle IVS with a case reference code and a destination IP address, and instructs the vehicle IVS to provide the tachograph data required by the tachograph regulation of the jurisdiction.

d) The vehicle IVS then sends the data via its ITS-station, together with the requested destination IP address and case reference, to a previously supplied address of the application service provider. Consistent with other TARV standards, as part of security measures, it never sends data directly to the requested destination address.

The application service provider is then responsible for validating the requested destination IP address, and if valid, forward the case reference code and tachograph data to the requested IP address (but these stages of the process are outside the scope of this document. Regulations are given in the data requirements of the jurisdiction).). Transaction profiles are defined in Annex A, and data profiles are defined in Annex C.

In this use case, the application service provider may be an agent of/appointed by the jurisdiction or may be a commercial application service provider who is under legal obligation to provide tachograph

data to the jurisdiction on request from the jurisdiction, or may simply be a legitimate application service provider seeking data from the vehicle (for example for the vehicle operator). In the case of a jurisdiction where the ASP for this use case is to be an agent of the jurisdiction, then the valid IP address of the ASP shall have been programmed into the memory of the tachograph/ITS-station of all affected vehicles.

See Figure 5 for a pictorial example.

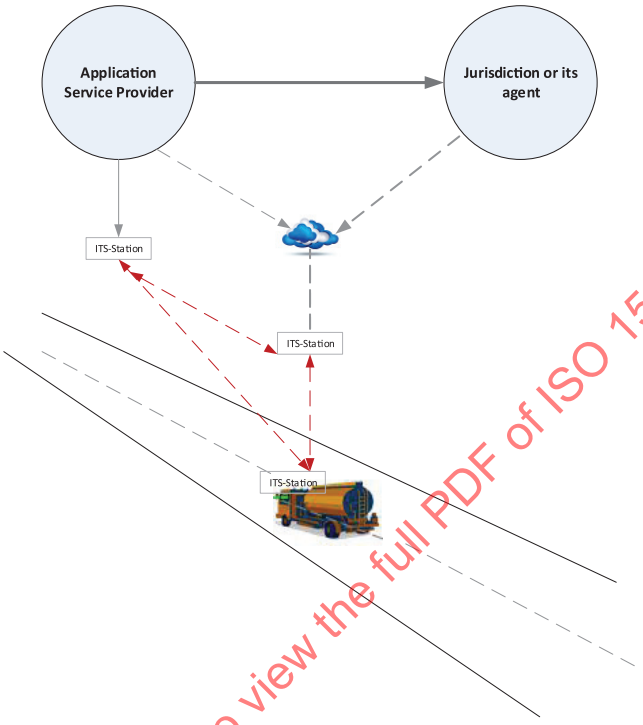


Figure 5 — Communication Profile C3

6.5 Communications requirements

6.5.1 General communications requirements

6.5.1.1 In order to be conformant with this document, the communications employed shall conform with a communications option specified in ISO 15638-2.

6.5.1.2 The ISO 15638 series has been developed for use in the context of regulated commercial freight vehicles. There is nothing, however, to prevent a jurisdiction extending or adapting the scope to include other types of regulated vehicles, as it deems appropriate.

6.5.2 Communications profile C1 requirements

6.5.2.1 Communication may be made via any short-range communications medium supported by ISO 15638-2, operating within the appropriate regional regulatory framework, such as:

a) ERC RECOMMENDATION 70-03 (Tromsø 1997 and subsequent amendments) Relating To The Use of Short Range Devices (SRD);

b) ARIB STD-T75; Dedicated Short-Range Communication (Japan);

c) TTAS.KO-06.0025; Standard of *DSRC* Radio Communication between Road-side Equipment and On-board Equipment in 5,8 GHz band (Korea);

but it shall be specified which of these options is supported, taking into consideration the tachograph regulations of the jurisdiction in which the vehicle is registered.

Transaction profiles are defined in Annex A, data profiles are defined in Annex C and the short-range transaction is defined in Annex B.

6.5.2.2 These are controlled circumstances where the initial communication is made directly between the vehicle and equipment operated by the agent of the jurisdiction acting as an 'inspector' or a mobile inspection point of the jurisdiction (an 'interrogator').

6.5.2.3 The transaction and its security provisions shall be effected in accordance with the relevant normative annexes of this document (and within the context of TARV, the interrogator of the jurisdiction shall be considered in this case to be a special case of an 'application service provider').

6.5.2.4 The inspector of the jurisdiction shall comply to the security provisions specified in the annexes to this document and be aware of any local data requirements imposed by the jurisdiction.

6.5.2.5 Specific aspects of tachograph data shall be as determined in the Annexes to this document, or given in the data requirements of the jurisdiction.

6.5.3 Communications profile C2 requirements

6.5.3.1 The short-range interrogation shall conform to the requirements of 6.5.2.1.

6.5.3.2 The provision of data to the application service provider shall conform to the requirements of 6.5.4.1.

6.5.3.3 Transaction profiles are defined in Annex A, data profiles are defined in Annex C, and the DSRC transaction is defined in Annex B.

6.5.4 Communications profile C3 requirements

6.5.4.1 Communications may be any communications medium supported in ISO 15638-2.

a) The overall architecture employed shall comply to ISO 15638-1 to ISO 15638-6.

b) The security employed shall comply to ISO 15638-4.

c) The 'basic vehicle data' shall comply to ISO 15638-5.

d) The generic conditions for this application service shall comply to ISO 15638-6.

Transaction profiles are defined in Annex A and data profiles are defined in Annex C.

7 Requirements for services using generic vehicle data

The means by which the access commands for generic vehicle information specified in ISO 15638-5 can be used to provide all or part of the data required in order to support a regulated application service shall be as defined in ISO 15638-6 or as specified in the annexes supporting this document.

8 Application services that require data in addition to basic vehicle data

8.1 General

Shall be conducted as defined in ISO 15638-6 or as specified in the Annexes of this document.

8.2 Quality of service requirements

This document contains no general requirements concerning quality of service. Such aspects shall be determined by a jurisdiction as part of its data requirements for any particular regulated application service. However, where a specified regulated application service has specific quality of service requirements essential to maintain interoperability, these aspects shall be as specified in Clause 10 or as specified in annexes of this document.

8.3 Test requirements

This document contains no general requirements concerning test requirements. Such aspects shall be determined by a jurisdiction as part of its data requirements for any particular regulated application service, and issued as a formal test requirements specification document. However, where a specified regulated application service has specific test requirements essential to maintaining interoperability, these aspects shall be as specified in Clause 10, relating to this regulated application service, or in a separate standards document referenced within that Clause, or specified in the annexes of this document, and where multiple jurisdictions recognize a benefit to common test procedures for a specific regulated application service, this shall be the subject of a separate standards document, or be as specified within data requirements with common requirements issued by or on behalf of those jurisdictions.

8.4 Marking, labelling and packaging

This document has no specific requirements for marking labelling or packaging. The marking and labelling requirements for any in-vehicle equipment shall be specified in standards pertaining to that physical equipment or be specified within a data requirement issued by the jurisdiction.

However, where the privacy of an individual may be potentially or actually compromised by any instantiation based on the ISO 15638 series of standards, the contracting parties shall make such risk explicitly known to the implementing jurisdiction and shall be aware of the privacy laws and data requirements of the implementing jurisdiction and shall mark up or label any contracts specifically and explicitly drawing attention to any loss of privacy and precautions taken to protect privacy. Attention is drawn to ISO/TR 12859 in this respect.

9 Common features of regulated TARV application services

9.1 General

The details of particular instantiations of regulated application service are as designed by the application service system to meet the requirements of a particular jurisdiction and are not specified herein, save as described below. ISO 15638-6 specifies the generic roles and responsibilities of actors in the systems, and instantiations that claim conformance with this document shall also be conformant with the general requirements of ISO 15638-6.

Annexes to this document provide a number of transaction profiles (Annex A) and data concept profiles (Annex C), which may be selected and mandated for use by a jurisdiction or group of jurisdictions.

The services included in this document include both communications using ITS-station transactions consistent with other TARV applications and also the special case of roadside inspection using 5,8 GHz DSRC interrogation.

9.1.1 Communication Profiles C1 and C2

9.1.1.1 This document provides profiles for a direct communication between an 'inspector' or 'mobile inspection point' of the jurisdiction (an 'interrogator'), that does not involve any other application service provider. Communication Profiles C1 and C2 use specific short-range communications means specified in Annexes of this document. See 10.1.2 and Annex B.

9.1.1.2 In the case of the specific instance of a short range communication between an inspector of the jurisdiction and a vehicle using specific means specified in annexes of this document, the inspector, acting as an "interrogator" may be considered as special instantiation of an Application Service Provider, and any on-board file content deletion shall take into consideration the data requirements of the jurisdiction.

9.1.1.3 See Figure 6.

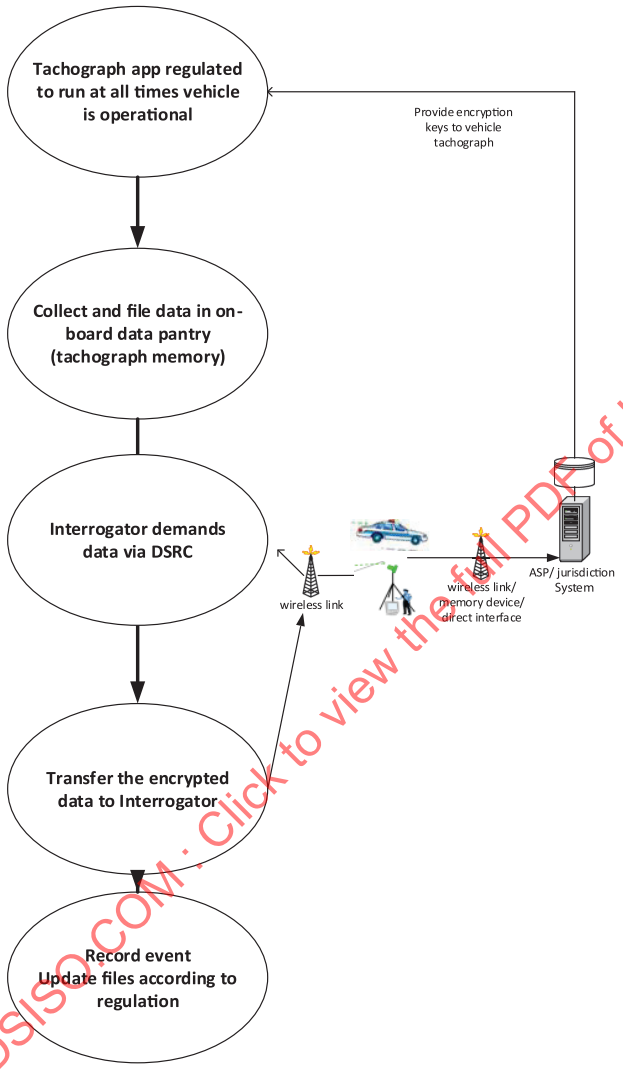


Figure 6 — Short-range interrogation (Communication Profiles C1 and C2)

9.1.1.4 For clarity: The difference between communication profile C1 and C2 is that while both interrogations are made by an inspector using a short-range interrogator, profile C1 returns the data in a secured form directly to the inspector's interrogator, while profile C2 acknowledges the request directly, but sends the data via an ITS-station to the application service provider (via communications profile C3). The application service provider verifies that the enquirer is genuine, and if so, forwards the data to the inspector.

9.1.2 Communication Profile C3

9.1.2.1 The means by which data is provisioned into the data pantry and the means to obtain the TARV LDT and core data, where required, are described in ISO 15638-6:2014, Clause 8.

9.1.2.2 In order to minimize demand on the IVS (which it is assumed may be performing multiple application services simultaneously, as well as supporting general safety related cooperative vehicle systems), and because national requirements and system offerings will differ, a 'cloud' approach has been taken in defining TARV regulated application services.

9.1.2.3 The TARV approach is for the on-board app supporting the application service to collect and collate the relevant data, and at intervals determined by the app, or on demand from the application service provider (ASP), pass that data to the ASP. All of the actual application service processing shall occur in the mainframe system of the ASP (in the 'cloud'). For further information, see ISO 15638-6:2014, Clause 9.

9.1.2.4 At a conceptual level, the TARV system is therefore essentially simple, as shown in Figure 7. The process is similar to that for CoreData, but data is supplied to a different on-board file in the data pantry.

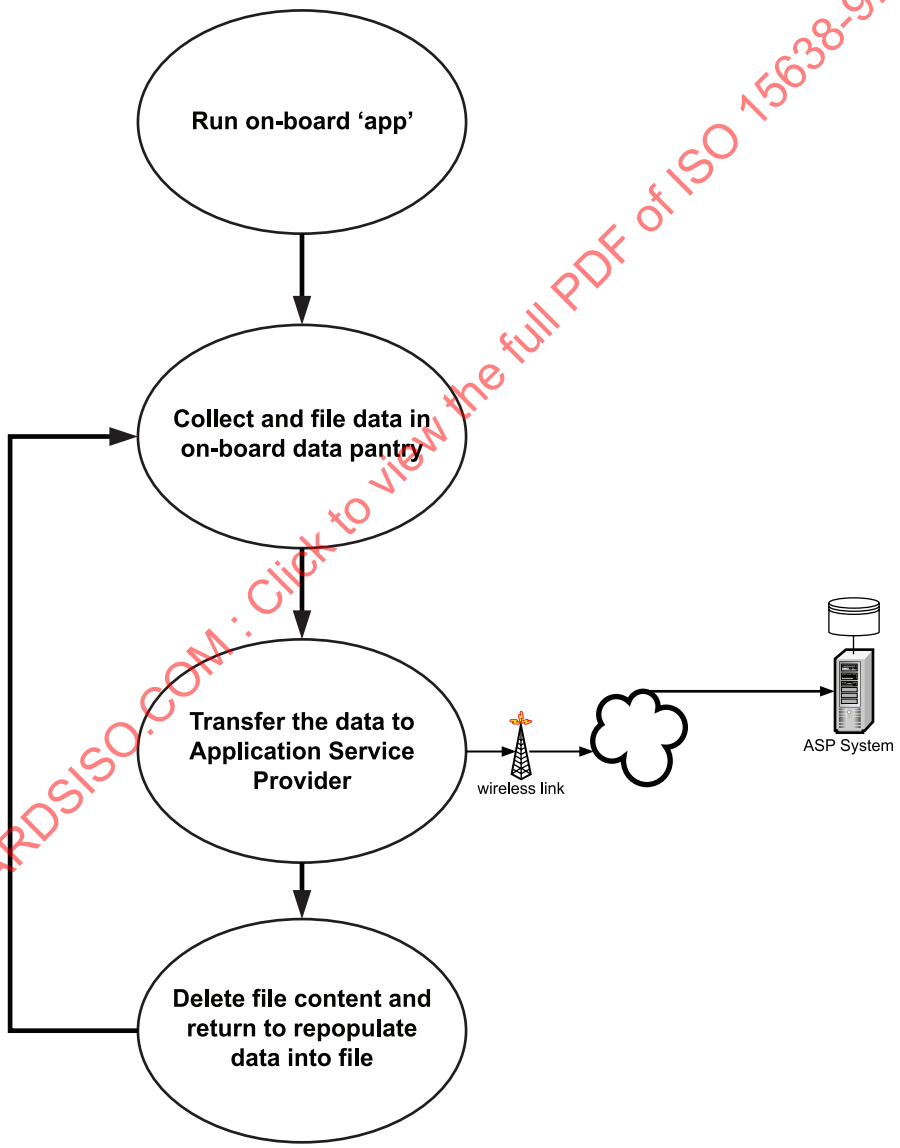


Figure 7 — TARV regulated application service on-board procedure (Communication Profile C3)

At a common generic functional level for this application service, the process may be seen as shown in Figure 8 below, however the connected equipment may/may not be required in all cases.

9.2 Common role of the jurisdiction, approval authority, service provider and user

In the case of Communication Profiles C1 and C2, the common role of the jurisdiction, approval authority, application service provider and user is given in a data requirement of the jurisdiction in which the vehicle is operating.

In the case of Communication Profile C3, the common role of the jurisdiction, approval authority, application service provider and user shall be as defined in ISO 15638-6 and is given in a data requirement of the jurisdiction in which the vehicle is operating.

9.3 Common characteristics for instantiations of regulated application services

In the case of Communication Profiles C1 and C2, the common characteristics for instantiations of regulated application services are given in a data requirement of the jurisdiction in which the vehicle is operating.

In the case of Communication Profile C3, the common characteristics for instantiations of regulated application services shall be as defined in ISO 15638-6.

9.4 Common sequence of operations for regulated application services

9.4.1 General

In the case of Communication Profiles C1 and C2, the common sequence of operations for the remote tachograph operation is given in a data requirement of the jurisdiction in which the vehicle is operating.

In the case of Communication Profile C3, the common sequence of operations for regulated application services shall be as defined in ISO 15638-6.

9.4.2 Quality of service

Generic quality of service provisions for application services shall be as defined in ISO 15638-6 or, at the discretion of the jurisdiction, given in a data requirement of the jurisdiction in which the vehicle is operating.

9.5 Information security

It is assumed that data will normally be encrypted before it is sent across the wireless medium.

It is also assumed that encryption techniques will change over time.

Each packet of RTM data shall therefore comprise five elements. See Table 1.

Table 1 — Structure of RTM data

A	B	C	D	E
No of octets of payload data	No of octets of security data	Payload data	Security data	10101010 end of field identifier octet
2 octets	2 octets	(A) Octets of payload data	(B) Octets of security data	1 octet
Example: 3	2	111111110000000011111111	0000000011111111	10101010

Payload data shall comprise the information content to be transferred across the air interface. Other than the overall field size constraint of A (65535 octets), the number of octets of payload data is not limited per se by the standard, but may be limited by the physical and practical constraints of the

communication medium (for example when using Communications Profile C1) or by a data requirement of the jurisdiction.

Security data shall comprise the security 'keys' or links to keys or other security mechanisms provided to enable the payload data to be decrypted. Other than the overall field size constraint of B (65 535 octets), the number of octets of security data is not limited per se by the standard, but may be limited by the physical and practical constraints of the communication medium.

In the case of Communication Profile C1, the data is to be transferred in 'frames' of a maximum of 128 octets, of which 18 octets are used by header and control data, leaving 110 octets, of which 50 octets are reserved for security data, and 10 octets for internal categorization management, leaving up to 50 octets of payload data per frame as defined elsewhere within the normative Annexes to this document.

In the case of Communication Profile C3, information security shall be as defined in ISO/TS 15638-4. In the case of Communication Profile C1, security provisions are as defined in Annex B. In the case of Communication Profile C2, security provisions for the information request functions shall be as determined in Annex B, and the security provisions for information provision shall be as determined in ISO/TS 15638-4.

9.6 Data naming content and quality

In the case of Communication Profile C3, data naming shall be as defined in ISO 15638-5:2013, 8.2, 8.3 and 8.4, or shall be as defined in Annex C of this document.

In the case of Communication Profiles C1 and C2, data naming shall be as defined in Annex C of this document.

Variations specific to the remote tachograph monitoring application service shall be as defined below.

9.7 Software engineering quality systems

In the case of Communication Profile C3, software engineering quality systems shall be as defined in ISO 15638-6, or, at the discretion of the jurisdiction, given in a data requirement of the jurisdiction in which the vehicle is operating.

9.8 Quality monitoring station

The availability of quality monitoring stations shall be as defined in ISO 15638-6, or, at the discretion of the jurisdiction, given in a data requirement of the jurisdiction, in which the vehicle is operating.

9.9 Audits

In the case of Communication Profile C3, audits shall be as defined in ISO 15638-6.

In the case of Communication Profiles C1 and C2, audits shall take into consideration the data requirements of the jurisdiction in which the vehicle is operating.

9.10 Data access control policy

In the case of Communication Profile C3, to protect the data and information held by the application service provider, each provider shall adopt a risk-based data access control policy for employees of the provider.

In the case of Communication Profiles C1 and C2, audits shall take into consideration the data requirements of the jurisdiction in which the vehicle is operating.

9.11 Approval of IVSs and service providers

In the case of Communication Profile C3, generic provisions for the approval of IVSs and service providers shall be as specified in ISO 15638-3. Detailed provisions for specific regulated applications are given by the regime of the jurisdiction.

In the case of communication profiles C1 and C2, generic provisions for the approval of IVSs and service providers are given in a data requirement of the jurisdiction in which the vehicle is operating.

10 Remote tachograph monitoring (RTM)

10.1 TARV RTM service description and scope

10.1.1 Generic TARV RTM use case via the application service provider

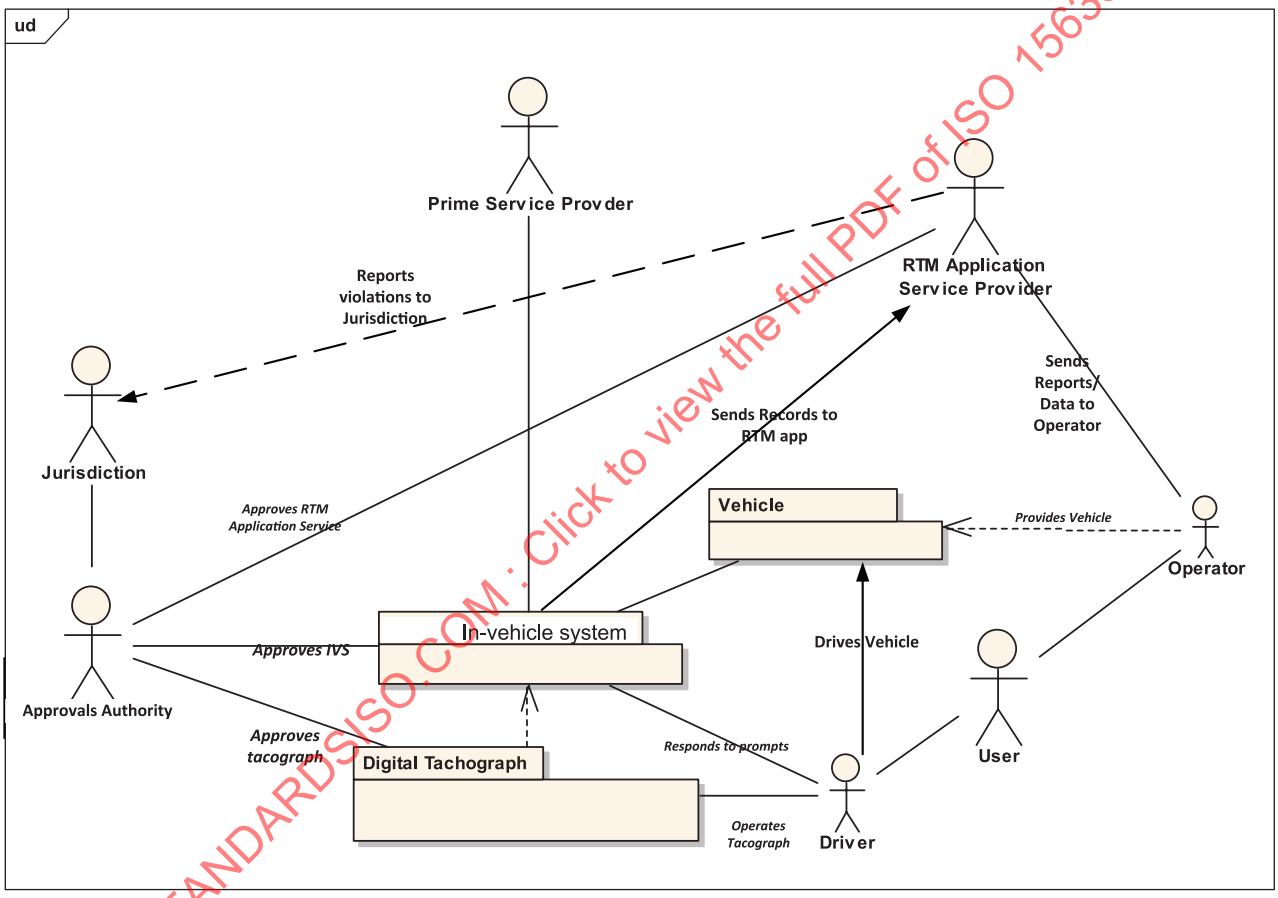


Figure 8 — Remote tachograph monitoring use case

Figure 8 provides an illustration of a TARV remote tachograph (RTM) monitoring system. Communication Profiles C1 and C2 of this application service are defined in 10.1.2. Communication Profile C3 of this application service is described in 10.1.3 and 10.1.4.

NOTE In the case of Communication Profiles C1 and C2, the RTM Application Service Provider is an 'inspector' of the jurisdiction using a short-range wireless interrogator.

This use case applies where tachograph data is obtained in scenarios such as:

a) Communication profile C1: Interrogation of the tachograph by an inspector of the jurisdiction using a short-range wireless interrogator in accordance with procedures defined in the Annexes of this document. (See 10.1.2).

b) Communication profile C2: Interrogation of the tachograph by an inspector of the jurisdiction using a short-range wireless interrogator with a response via the ITS-station of the vehicle to a predetermined IP address and validation of the requested final destination for the data made by the application service provider.

c) Communication profile C3: Requests for tachograph data broadcast to vehicles within range of a fixed or mobile interrogation point using any wireless access medium that can communicate with the ITS-station of the vehicle/tachograph or requests for tachograph data by a legitimate source such as the operator of the vehicle or the jurisdiction by addressing the IPv6/IPv4 address of the vehicle ITS-station or its tachograph with validation of the requested destination for the data provided by the application service provider.

10.1.2 Specific use case of tachograph inspection by an inspector of the jurisdiction using short range equipment (Communication profiles C1 and C2)

In the situation of the inspection of a specific vehicle tachograph by an authorized agent of the jurisdiction using a short range mobile means of wireless interrogation in the circumstance where there is no opportunity to validate the destination of the inspector's address via a remote application service provider, validation of the inspector's interrogator shall be made using the processes defined in the Annexes of this document, and shall use communication profiles defined in Annex B of this document, and transaction profiles specified in Annex A of this document and data concept profiles specified in Annex C of this document, or as specified in the data requirements of the jurisdiction.

This application service is described in 10.1.3, 10.1.4 and 10.2.

10.1.3 Description of TARV RTM regulated application service

TARV RTM is a means to deliver data concepts containing digital tachograph data to an application service provider using the TARV IVS and a wireless communication interface between the IVS and the application service provider central system.

The objective of Communication Profile C1 is to provide data to determine whether a vehicle's progress should be 'arrested' in order to fully check the tachograph data (full tachograph data is not transferred). The objectives of Communication Profiles C2 and C3, is, in situations where it is allowed, to automatically provide the relevant tachograph data to the jurisdiction via an application service provider. What comprises "relevant" tachograph data in these instantiations may vary between jurisdictions, so this document provides the means to transfer this data, but the specification of the exact data concept transferred shall be at the determination of the jurisdiction. Some optional data profiles that a jurisdiction may select are provided in Annex C, but jurisdictions are not bound to use one of these optional profiles in order to claim compliance with this document.

Communication Profiles as defined in Annex A and B of this document are therefore a generic means of transferring data which is specified by the local data requirements of the jurisdiction and these profiles do NOT specify any of the precise content of the tachograph data concept transferred (which shall be at the determination of the jurisdiction).

However, whilst the objective of Communications Profiles C2 and C3 are to provide all of the tachograph data required for the interrogation by wireless means, the objective in Communication Profile C1 is simply to provide relevant data via the wireless communication in order to determine, or assist to determine, whether the vehicle should be stopped in order to extract data from its tachograph. The amount of data that can be transferred within Communication Profile C1 is limited (to 50 octets payload), because of the nature and limitations of the communication transaction.

International, regional and national data requirements shall determine the content of electronic tachograph data. However, Annex C provides some data concept profiles that jurisdictions may elect to use, specify, or specify by reference to a particular profile specified in this document.

EXAMPLE In Europe, EU regulation 1360/2002 (Recording equipment in road transport) and latterly, EU regulation EU 165-2014 (tachographs in road transport) provide the requirements in countries of the European Union for digital tachograph equipment, and combined with Regulation 561/2006/EC of the European Union (driving and rest times of professional drivers), provides the regime for driver monitoring in Nation states within its jurisdiction. Tachograph data profiles adopted by the EC, and therefore widely in use in at least 28 countries, are provided as optional data concept profiles in Annex C.

NOTE Annex A provides specifications for Communication transaction profiles; Annex B outlines a wireless communication to access this data (including security provisions); subclause 9.6 provides specifications for security and is complemented in Annex B with direct security measures for a wireless solution (B.1.6.5); and Annex C provides specifications for data.

The exact nature and form of the requirements and reports will vary from jurisdiction to jurisdiction, and such detail is not standardized in this document. This document specifies the basic architecture and basic information needed to support this type of application service using TARV, so that the in-vehicle system can satisfy the requirements of any likely instantiation by a different jurisdiction/application service provider, or so that the regulated vehicle and equipment can support the different requirements of different jurisdictions when the regulated vehicle and driver are operating within their domain. However, Annexes A and C also provide profiles of tachograph data access transactions and data concepts which regulators may elect to adopt as the norm within their jurisdiction.

The nature and form of the tachograph device/function within a vehicle is not specified in this document, but may be expected to be standardized and/or regulated elsewhere by jurisdictions. Although tachograph regulations differ around the world, in order for TARV RTM to operate, it is a requirement that at least the following features be present in the digital tachograph:

a) The digital tachograph shall be able to output the following data using an appropriate dedicated serial link independent from an optional CAN bus connection (ISO 11898 series), to allow their processing by other electronic units installed in the regulated vehicle.

b) When the ignition of the regulated vehicle is ON, key tachograph data (as determined by the digital tachograph system design) is permanently broadcast to the IVS.

c) When the ignition of the regulated vehicle is OFF, at least any change of driver or co-driver activity and/or any insertion or withdrawal of a tachograph card shall generate a corresponding data output. In the event that data output has been withheld whilst the ignition of the regulated vehicle is OFF, that data shall be made available once the ignition of the vehicle is ON again.

d) Data stored into the data memory shall not be affected by an external power supply cut-off of less than twelve months in type approval conditions.

e) Notwithstanding that the data to be transferred shall be a function of system design and regulatory requirements and is not determined in this document, the recording equipment of the tachograph shall be able to store in its data memory the following vehicle unit identification data:

   — name of the manufacturer,

   — address of the manufacturer (or a reference to a data registry where such data is available. A reference to a publicly available International register of manufacturers may optionally be stored as a ManufacturerID and URL of the register.),

   — part number,

   — serial number,

   — software version number,

   — software version installation date,

— year of equipment manufacture,

— approval number,

— length, in bytes (octets) of 'RTMdata' file,

and, shall be able to store in its data memory the data required by the jurisdiction requiring the tachograph.

f) The data stored in its data memory shall be made accessible to the IVS and the TARV RTM app in a standard and declared format.

Figure 8 provides an illustration of a TARV remote digital tachograph monitoring system. This application service is described in 10.1.4 and 10.2.

10.1.4 Description of TARV RTM application service

The TARV remote tachograph monitoring (RTM) application service may exhibit itself in a number of different forms in different jurisdictions. In each case the use case shown in Figure 8 may vary slightly and is therefore an example, not a requirement. It is likely to be named differently according to its origin and the regulatory environment in which it is instantiated.

The exact nature and form of the requirements and reports will vary from jurisdiction to jurisdiction, and such detail is not standardized in this document. This document specifies the basic architecture and information needed to support this type of application service using TARV, so that the in-vehicle system can satisfy the requirements of any likely instantiation by a different jurisdiction/application service provider, or so that the regulated vehicle and equipment can support the different requirements of different jurisdictions when the regulated vehicle and driver are operating within their domain. Annex A provides details of communication transactions for each communication profile and Annex C provide profiles of tachograph data concepts which regulators may elect to adopt as the norm within their jurisdiction, and Annex B outlines a wireless communication transaction. Later editions of this document may specify additional communication transactions.

Figure 8 shows an appropriate example use case where reports are required by the jurisdiction and where compliance is also monitored such that transgression may result in an offense/prosecution, which is perhaps the most comprehensive example of the TARV RTM application service.

10.2 Concept of operations for TARV RTM

10.2.1 General

TARV remote tachograph monitoring (RTM) is an application service that transfers digital tachograph data from a vehicle to an application service provider (who may be a commercial service provider or may be an inspector of the jurisdiction), using a TARV IVS and a wireless communication interface (Communication Profile C3), or in the case of a direct short range communication, between the inspector ('interrogator') and the vehicle using a short range wireless communication (such as Communication Profiles C1 and C2). Requirements for remote tachograph monitoring may vary from one jurisdiction to another. Therefore, this document neither specifies nor requires the use of particular specific data concepts, nor controls the content of the tachograph data, but a number of example data concept profiles, and transactions, are provided in Annex C of this document, which may be suitable to be specified in the data requirements of jurisdictions using this document.

10.2.2 Statement of the goals and objectives of the TARV RTM system

The objective is to provide data from an on-board digital tachograph to an application service provider, or the agent of the application service provider.

The service is achieved by an app in the IVS requesting tachograph data from the digital tachograph, storing the data in a uniquely identified file, and sending the data as determined in the app (at

defined intervals or on demand from the application service provider system). Principal provision of the application service is provided by the landside application system, or a mobile inspection point ('interrogator'), and the on-board application is a means of feeding data to that landside system, or interrogator, and may on occasions receive data from the landside-based application service system.

10.2.3 Strategies, tactics, policies, and constraints affecting the TARV RTM system

The principle issues affecting the system are those of collecting data from an unspecified device.

This application service restricts itself to providing a medium to transfer (unspecified) data from an on-board device to the application service provider using the TARV IVS. It does not design the application service. That is left to the jurisdiction, the application service provider, and approval authority (regulatory).

The IVS is a device of limited capability and will be expected to be multi-tasking with other TARV 'apps' and also conducting non-TARV cooperative vehicle system apps at the same time. It is therefore important that the IVS is not overloaded by a complicated TARV RTM app.

In many jurisdictions, there may be a requirement to provide data to a mobile roadside inspection point or a vehicle mounted device ('interrogator') operated by an inspector/agent of the jurisdiction (Communication Profiles C1 and C2). These requirements may vary from one jurisdiction to another and may indeed vary for different instantiations within a jurisdiction.

This document therefore supports:

a) Obtaining tachograph data by interrogating via a short range ('interrogator') that is wirelessly connected in accordance with short-range communication such as that defined in Annex B, or infra-red, communication provisions as specified in ISO 15638-2 (Communication Profiles C1 and C2).

b) Obtaining tachograph data by interrogating via a mobile interrogator that is wirelessly connected in accordance with one or more of the other wireless media specified in ISO 15638-2 (Communication Profile C3).

c) Obtaining tachograph data by interrogating via a fixed gantry or roadside beacon that is wirelessly connected in accordance with one or more of the other wireless media specified in ISO 15638-2 (Communication Profile C1, C2, or C3).

d) Obtaining tachograph data by remotely addressing the IPv6/IPv4 address of a vehicle ITS-station or its tachograph that is wirelessly connected in accordance with one or more of the wireless media specified in ISO 15638-2 (Communication Profile C3).

In the case of an instantiation of a) (Communication Profile C1), the data may be sent directly to the interrogating inspector using the transaction and security provisions of Annexes A, B and C of this document or may (Communication Profiles C2 and C3) be provided only to a predetermined address of an application service provider and forwarded by the ASP to the interrogating inspector.

In the case of instantiations of c) and d), part of the security provisions are that data shall be supplied only to a predetermined address of an application service provider.

10.2.4 Organizations, activities, and interactions among participants and stakeholders of TARV RTM

It should be noted that an entity may perform multiple roles and in doing so takes on the responsibility to perform the functions described under those roles.

In the case of RTM, the application service provider may be a commercial service contracted to provide the operator who has instructed the application service provider to meet the demands of the jurisdiction on behalf of the operator, or the RTM application service provider may be an agent or department of the jurisdiction.

10.2.5 Clear statement of responsibilities and authorities delegated for TARV RTM

Table 2 provides a list of the actors involved, their activities and interactions.

Table 2 — TARV RTM actors involved, their activities and interactions

ACTOR	ROLE	ACTIVITIES	INTERACTIONS
Jurisdiction (J)	Sets requirements for mandatory and supported TARV RTM	Publishes specifications	ALL
		Obtains regulations	ALL: Establish regime and regulations PSP: Register ASP: Register, receive reports Op: Vehicle Registration Dr: Licence, issue Tachograph
		May provide tachographs	
		Appoints approval authority	CA: Contract. Instruct. Receive reports
		Monitors reports	AJ: Employ, process enforcement
		Instigates enforcement	
Approval authority (CA)	Implements jurisdiction policy at equipment and service approval level	Certifies IVS, tachograph, application service instantiations	PSP: Certify IVS ASP: Certify application service Op: Certify tachograph
		Conducts Q of S maintenance to instruction of jurisdiction	
Agent of jurisdiction (AJ)	Inspection and enforcement	Inspects tachographs	Dr: Inspections
		Instigates enforcement actions	Dr: Enforcement Op: Enforcement
Prime service provider (PSP)	Responsibility for IVS	Installs and/or commissions IVS	CA: May apply to certify IVS Op: Installation
		Maintains IVS	Op: Maintain IVS
		May provide tachographs	
Application service provider (ASP)	Provides TARV RTM application services	Develops instantiation of TARV RTM application service	CA: Applies for approval of service
		Contracts with users	Op: Contracts

Table 2 *(continued)*

ACTOR	ROLE	ACTIVITIES	INTERACTIONS
		Provides TARV RTM application service to users and jurisdiction	Op: Provides service Dr: May provide service J: Provides service/reports AJ: reinforcement
Operator (Op)	Provides regulated vehicle	'Employs'/contracts drivers	Dr: Employs/contracts
	Uses regulated vehicle for commerce and logistics	Operates regulated vehicle	J: Registers regulated vehicle PSP: Contracts, receives service (install/maintain) ASP: Contracts, receives service
		Receives reports from ASP	
Driver (Dr)	Drives regulated vehicle to instruction of operator		Op: To instruction
		Signs into TARV RTM system	IVS: Signs driver into system
		Drives regulated vehicle	
		Interfaces with AJ	AJ: Provides Access to Tachograph

10.2.5.1 The jurisdiction is responsible for the regime and data requirements.

10.2.5.2 The jurisdiction employs an approval authority (regulatory) or otherwise provides its function.

10.2.5.3 The jurisdiction provides means for enforcement (where required) to meet the requirements of the regime of the jurisdiction.

10.2.5.4 The prime service provider shall install/commission IVS and maintain the IVS.

10.2.5.5 The prime service provider shall install/commission tachograph and maintain the tachograph.

10.2.5.6 The application service provider (ASP) shall develop the TARV RTM application service or use a TARV RTM application service provided by the jurisdiction. In the case of RTM, the application service provider may be a commercial service contracted to provide the operator who has instructed the application service provider to meet the demands of the jurisdiction on behalf of the operator (Communication Profile C3), or the RTM application service provider may be an agent or department of the jurisdiction, for example using an 'interrogator' in an enforcement scenario (Communication Profiles C1 and C2).

10.2.5.7 The application service provider shall obtain any required approval of its TARV RTM service from the approval authority (regulatory).

10.2.5.8 The application service provider shall contract with the user (normally operator but in some instantiations also with the driver).

10.2.5.9 The application service provider shall be responsible for providing the application service to the jurisdiction, operator and driver as specified in its service offering. In the case of RTM, the contract may be explicit and commercial, or may be an implicit condition of the data requirements of the jurisdiction that allows the use of the vehicle and/or driver on the highways of the jurisdiction.

10.2.5.10 The operator shall be responsible for providing the regulated vehicle.

10.2.5.11 The operator shall be responsible for being aware of requirements of the jurisdiction regarding TARV RTM.

10.2.5.12 The operator shall be responsible for paying levies required by the jurisdiction, prime service provider and application service provider.

10.2.5.13 The driver shall be responsible for following instructions, including use of digital tachograph.

10.2.6 Equipment required for TARV RTM

10.2.6.1 TARV IVS

10.2.6.1.1 The system shall be designed to work using TARV IVS as defined in the ISO 15638 series of standards (Communication Profile C3), or via an 'interrogator' using a short-range wireless communication link as determined in annexes to this document (Communication Profiles C1 and C2).

10.2.6.1.2 Communication Profile C3: The IVS shall be provided with an interface capable of receiving data from the installed tachograph, and the tachograph shall have the means to provide data to the IVS for transfer to the application service provider. That transfer may be 'pushed' by the digital tachograph or 'pulled' from the digital tachograph according to the design of the digital tachograph and the TARV RTM app in the IVS, and is a function of the application service design, and not the specifications of this document.

Communication Profiles C1 and C2: If required by the jurisdiction of the country of registration of the vehicle, or the jurisdiction within which the vehicle is being operated, the IVS shall be capable of being interrogated using a short-range wireless communication link as determined in Annex B to this document, taking into consideration the data requirements of the jurisdiction.

10.2.6.1.3 The form and function of the electronic tachograph equipment is deliberately not defined in this document and is considered to be at the discretion of the jurisdiction or the marketplace.

10.2.6.1.4 The prime service provider/application service provider shall provide to the approval authority (regulatory), evidence of compliance from an appropriate body to demonstrate the suitability for use in vehicles for the IVS, tachograph and all associated components.

10.2.6.1.5 It shall not be possible for collected or stored remote tachograph data to be accessible or capable of being manipulated by any person, device or system, other than that authorized by the application service provider.

10.2.6.2 TARV RTM 'app'

10.2.6.2.1 The digital tachograph shall supply data to the IVS. This may be 'pushed' at the instigation of the digital tachograph, or 'pulled' at the instigation of the TARV RTM app according to the design of the equipment and app software and is a matter for commercial design decision or the requirements of the regime of the jurisdiction.

10.2.6.2.2 TARV RTM data shall be presented in accordance with a transaction profile as specified in Annex A of this document. The transaction profiles determined in this document do not prescribe the detailed data content, which is dependent on the jurisdiction. Optional Data concepts are provided in Annex C.

10.2.6.2.3 The TARV RTM app running on the IVS records the received tachograph data in the form specified by the jurisdiction and makes transactions to provide the data as specified in Annex A.

10.2.6.2.4 At intervals determined by the certified application service system specification, or on receipt of an instruction to provide the requested data, the TARV RTM app shall send the TARV RTM data held in the file, 'RTMdata' held in the data pantry of the IVS to the TARV RTM system of the application service provider via its most appropriate wireless communications interface.

10.2.6.2.5 Once the TARV RTM system of the application service provider has acknowledged successful receipt of the data, the data shall be deleted from the memory of the RTM IVS unless the jurisdiction, user or application service provider requires it for other purposes, and a new file shall be created for future use.

Deletion from the RTM IVS does not imply deletion from the memory of the tachograph (of which storage and deletion shall take into consideration the design and function of the tachograph and the data requirements of the jurisdiction). Deletion in this subclause simply means deletion from any temporary files created to collate data from the tachograph in order to make the required transmission of data.

10.2.6.2.6 It shall not be possible for collected or stored tachograph data in any software or non-volatile memory within the RTM IVS to be accessible or capable of being manipulated by any person, device or system (including via any self-declaration device), other than that authorized by the jurisdiction or application service provider.

10.2.6.3 Tachograph

The design and operation of the tachograph is not specified in this document. These should take into consideration any statutory and regulators requirements.

10.2.7 Operational processes for the TARV RTM system

Shall be as defined in 9.2.

For detail of the operational processes see 10.3 (sequence of operations for remote digital tachograph (monitoring) and Figure 9.

10.2.8 Role of the jurisdiction for TARV RTM

Shall be as defined in 9.3.

10.2.9 Role of the TARV RTM prime service provider

Shall be as defined in 9.4.

10.2.10 Role of the TARV RTM application service provider

Shall be as defined in 9.5.

10.2.11 Role of the TARV RTM user

Shall be as defined in 9.6.

10.2.12 Generic characteristics for all instantiations of the TARV remote tachograph monitoring (RTM) application service

10.2.12.1 A remote tachograph monitoring application service is approved. It utilizes a TARV RTM IVS which communicates to the prime service provider/application service provider and has the ability to obtain data from the regulated vehicle digital tachograph.

10.2.12.2 The application service provider shall load a TARV RTM App into the IVS of the operator's vehicles.

10.2.12.3 The TARV RTM App shall run whenever the regulated vehicle is operating.

10.2.12.4 The TARV RTM App shall record the data specified in its app in the RTM IVS.

10.2.12.5 The application service provider shall design/install/operate its remote tachograph monitoring system as approved by the approval authority (regulatory).

10.2.12.6 Unless otherwise instructed by the data requirements of the jurisdiction, the IVS shall provide its TARV RTM data to the application service provider using the TARV IVS wireless link at least once every 24 hours (Communication Profile C3). Every transfer shall include framing data that identifies its sequential order, IVS ID, version number of IVS and version number of the TARV RTM app or (Communication Profiles C1 and C2) where providing data in accordance with Annex B using a short-range wireless communication.

The system shall acknowledge receipt of the data via the TARV IVS wireless link. Once the data has been acknowledged it shall be deleted from the RTM IVS memory unless the operator or ASP chooses to retain it in the IVS memory for other openly declared purposes with the assent of the user.

Deletion from the RTM IVS does not imply deletion from the memory of the tachograph (of which storage and deletion shall be in accordance with the design and function of the tachograph and take into consideration the data requirements of the jurisdiction). Deletion in this subclause simply means deletion from any files created to collate data from the tachograph in order to make the required transmission of data.

10.2.12.7 The application service system shall retain and back up the TARV RTM data to the data requirements of the jurisdiction.

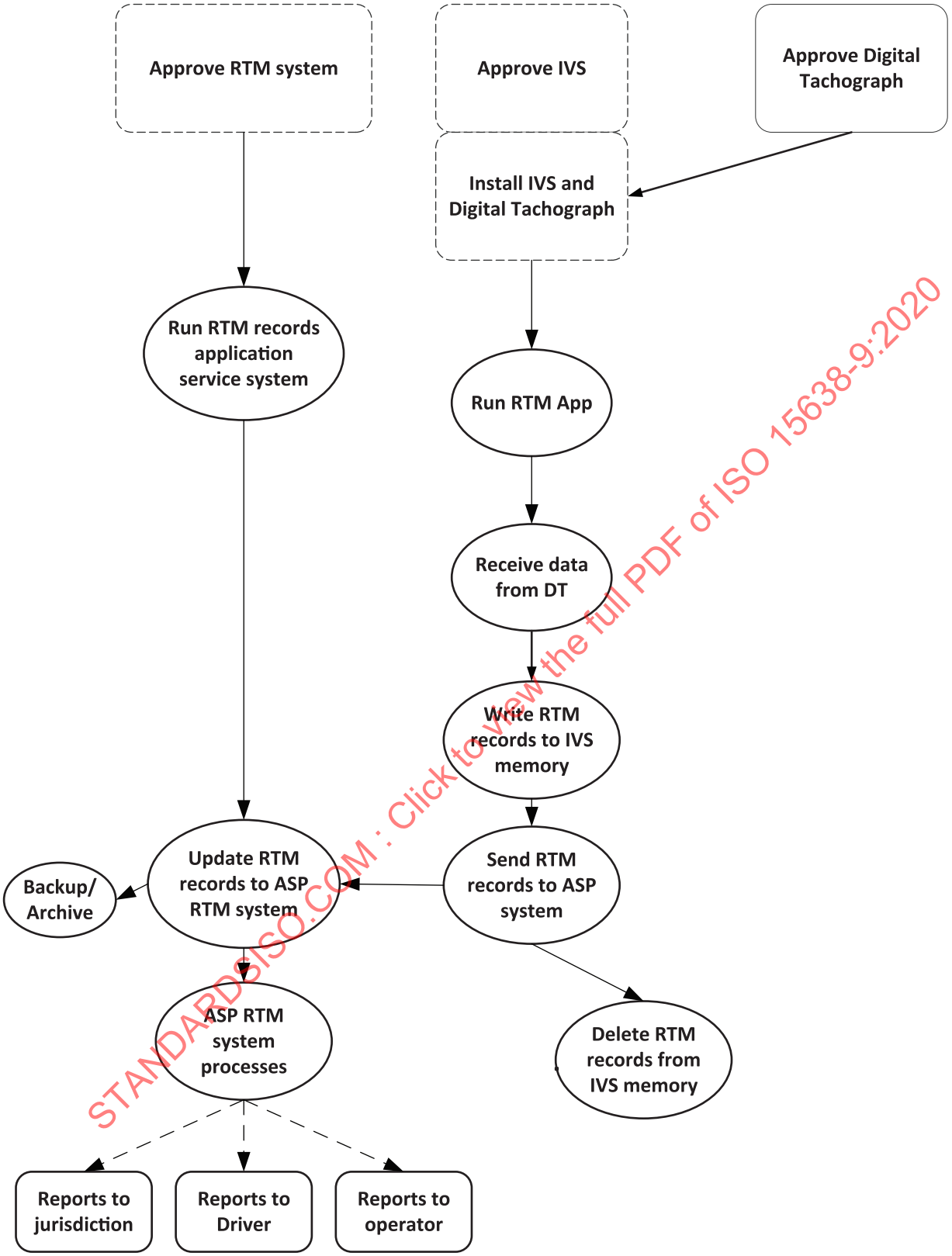
10.2.12.8 The application service provider shall provide reports to the jurisdiction or its agents, taking into consideration the requirements of the jurisdiction when approving the product.

10.2.12.9 TARV RTM records received by the IVS and stored in the 'RTMdata' file held in the data pantry of the IVS are sent to the application service provider. The application service provider is responsible for providing the service to the regulated vehicle operator, and in the event of contravention, to the jurisdiction.

10.3 Sequence of operations for TARV RTM

10.3.1 General

The business process and sequence of operations is shown in Figure 9.



Key

ASP application service provider

DT digital tachograph

IVS in-vehicle system

RTMremote tachograph monitoring

Figure 9 — TARV RTM business process and procedure

10.4 TARV RTM service elements

10.4.1 TARV RTM service element (SE) 1 — Establish 'Remote tachograph monitoring' regulations, requirements, and approval arrangements

The jurisdiction is responsible for defining its requirements for its variant of the remote tachograph monitoring application service, including data security provisions (within the security frameworks supported/enabled by this document), obtaining any legislation and/or regulations, and defining the procedure for an application service provider to gain approval for its instantiation of the TARV RTM application service.

10.4.2 TARV RTM SE2 — Request system approval

The application service provider shall seek approval for its instantiation of the remote tachograph monitoring application service from the approval authority (regulatory) taking into consideration the regime established by the jurisdiction.

10.4.3 TARV RTM SE3 — User (operator) contracts with prime service provider

It shall be a prerequisite requirement for any potential vehicle operator opting or being required to sign up for the TARV RTM application service that its regulated vehicles be TARV equipped with a TARV compliant IVS at point of manufacture or installed by a prime service provider, and that there be a maintenance contract with a prime service provider for that equipment. (See ISO 15638-1).

That equipment may be (Communication Profile C3) an ITS-station supporting wireless transactions via one or more of the wireless media supported in ISO 15638-2, or (Communication Profiles C1 and C2) via a specific short-range communication device as specified in Annexes A and B of this document.

10.4.4 TARV RTM SE4 — User (operator) equips vehicle with a digital tachograph

It shall be a prerequisite for any potential vehicle operator opting or being required to sign up for the TARV RTM application service that its regulated vehicles be TARV equipped with a digital tachograph at point of manufacture or installed by a prime service provider, and that there be a maintenance contract with a prime service provider for that equipment.

10.4.5 TARV RTM SE5 — User contracts with application service provider

The user (operator) shall contract with an application service provider who offers an approved TARV RTM application service to provide the TARV RTM application service to nominated vehicles.

In the case of RTM, the application service provider may be an agent appointed by the jurisdiction or a department of the jurisdiction, in which case there will be no specific contract, but in this use case it shall be a general condition of use of the vehicle on the roadways/highways of the jurisdiction.

10.4.6 TARV RTM SE6 — Application service provider uploads software into the TARV equipped vehicles of the operator

The service provider shall upload and commission the on-board TARV RTM app software into the TARV equipped vehicles of the operator.

10.4.7 TARV RTM SE7 — Create data

When the ignition of the regulated vehicle is turned on, the TARV RTM app in the data library of the IVS shall be instigated.

The app shall collate data taking into consideration the requirements of the jurisdiction.

There is no mandatory data required for conformance with this document, but any of the data profiles provided in Annex C may be mandated for use by the data requirements of a jurisdiction, or the jurisdiction may determine and require its own mandatory data, in which case it is responsible for ensuring that those within its control are adequately informed concerning its requirements.

10.4.8 TARV RTM SE8 — Recording of digital tachograph data

Shall be in accordance with one of the options in Annex C of this document or take into consideration the data requirements of the jurisdiction.

10.4.9 TARV RTM SE10 — 'Interrogated' request for tachograph data

10.4.9.1 Communication Profile C1 (Via Short range mobile interrogator)

10.4.9.1.1 Obtaining tachograph data by interrogating via a short range mobile interrogator that is wirelessly connected in accordance with the short range communication specified in Annex B and operating within EN 12253, EN 12795, EN 13372, EN 12834 and ISO 15638-2 (Communication Profiles C1 and C2 as defined in EN 13372).(Selected parameters tested in accordance with appropriate tests in EN 300 674-1.)

10.4.9.1.2 The interrogator shall establish a communication in accordance with Annex B of this document.

10.4.9.1.3 The interrogator shall ensure security in accordance with 9.4.1 and B.1.6.5 of this document.

10.4.9.1.4 The interrogator shall then transfer one of the data concepts defined in Annex C of this document, via one of the Communication Profile C1 transactions defined in Annex A of this document.

10.4.9.1.5 The interrogator shall confirm receipt of the data as specified in Annexes A and B of this document.

10.4.9.1.6 The session shall be closed as specified in Annex B of this document.

10.4.9.2 Communication Profile C2 (Via Short range mobile interrogator/ISO 15638-2 provision of data)

10.4.9.2.1 Obtaining tachograph data by interrogating via a short-range mobile interrogator that is wirelessly connected in accordance with the short range communication specified in Annex B operating within ERC 70-03 and ISO 15638-2 (Communication Profiles C1 and C2) and providing the data via an ITS-station to an application service provider.

10.4.9.2.2 The interrogator shall establish a communication in accordance with Annex B of this document.

10.4.9.2.3 The interrogator shall ensure security in accordance with 9.6, and in the case of EN 5,8 GHz DSRC, B.1.6.5 of this document.

10.4.9.2.4 An interrogating ITS-station shall request specific data given by the data requirements of the jurisdiction or as determined in ISO 15638-6:2014, 7.1 and 8.1.2.

10.4.9.2.5 The interrogator shall also provide at the time of the request, a unique 8 octet reference number (URef), and a destination IPv6 address (ReqDest) where it requests the data to be sent.

10.4.9.2.6 On receipt of the request to its IPv6/IPv4 address, the RTM IVS shall acknowledge the request with the appropriate ACKnowledgement defined in ISO 15638-6:2014, 8.3.5, <T>, which acknowledges that a request for RTM data has been received.

10.4.9.2.7 The IVS shall then close the communication session.

10.4.9.2.8 The IVS shall then open a new communication session using an available and appropriate CALM wireless medium.

10.4.9.2.9 The IVS shall then send the RTM datafile to a predetermined destination IPv6 (internet) address that has previously been stored in the memory of the data pantry by its ASP, together with the URef and ReqDest provided by the interrogator.

10.4.9.2.10 On successful receipt of the data, the recipient at the predetermined destination IPv6 address shall send an acknowledgement <RTX> to the IVS.

10.4.9.2.11 On receipt of the acknowledgement <RTX> the IVS shall close its communication session.

10.4.9.2.12 The ASP shall be responsible for verifying that the interrogation is legitimate, appropriate and from an accepted source, and having verified this, shall be responsible for sending the data to the interrogator requested IPv6 address. The means and detail of how this is achieved are outside the scope of this document.

10.4.9.3 Communication Profile C3 (via ISO 15638-2 ITS-station provision of data)

10.4.9.3.1 Obtaining tachograph data by interrogating via a fixed gantry or roadside beacon wirelessly connected in accordance with one or more of the wireless media specified in ISO 15638-2, or

10.4.9.3.2 Obtaining tachograph data by interrogating via a mobile interrogator that is wirelessly connected in accordance with one or more of the wireless media specified in ISO 15638-2, or

10.4.9.3.3 Receiving a request to provide tachograph data via the IP address of the tachograph or ITS-station.

10.4.9.3.4 In the event that the IVS of a vehicle receives a wireless interrogation requesting the RTM data, the requestor shall also provide at the time of the request, a unique 8 octet reference number (URef), and a destination IPv6 address (ReqDest) where it requests the data to be sent.

10.4.9.3.5 On receipt of the wireless request to the ITS-station of the RTM IVS, the ITS-station of the RTM IVS shall acknowledge, to the interrogating source address, the request with the appropriate ACKnowledgement defined in ISO 15638-6:2014, 8.3.5 <T>, which acknowledges that a request for RTM data has been received.

10.4.9.3.6 The IVS shall then close the communication session.

10.4.9.3.7 The IVS shall then open a new communication session using an available and appropriate CALM wireless medium.

10.4.9.3.8 The IVS shall then send the RTM datafile to a predetermined destination IP (internet) address that has previously been stored in the memory of the data pantry by its ASP, together with the URef and ReqDest provided by the interrogator.

10.4.9.3.9 On successful receipt of the data, the recipient at the predetermined destination IPv6 address shall send an acknowledgement <RTX> to the IVS.

10.4.9.3.10 On receipt of the acknowledgement <RTX> the IVS shall close its communication session.

10.4.9.3.11 The ASP shall be responsible for verifying that the interrogation is legitimate, appropriate and from an accepted source, and having verified this, shall be responsible for sending the data to the interrogator requested IPv6 address. The means and detail of how this is achieved is outside the scope of this document.

10.4.10 TARV RTM SE9 — Pre-programmed interval sending digital tachograph data to application service provider (Communication profile C3)

10.4.10.1 Where required by the jurisdiction, or by the operator, at time intervals determined by the on-board TARV RTM app, taking into consideration the data requirements of the jurisdiction or the operator, the RTM IVS shall send the 'RTMdata' file to the TARV RTM application service provider system via a wireless communication supported by the IVS and application service provider system as:

<START><LENGTH>< RTMdata file><RTMdata><END>

10.4.10.2 The content of the RTMdata file shall be a data concept profile as specified in Annex A of this document.

10.4.10.3 On successful receipt of the TARV RTM file the application service provider system shall send an acknowledgement <RTX> to the IVS. On receipt of the ACKnowledgement <RTX> the IVS shall clear the data held within the 'RTMdata' file and start to repopulate the 'RTMdata' file with data as defined by the TARV RTM app.

10.4.10.4 If an ACKnowledgement is not received within 60 seconds of sending the data, the TARV RTM app shall attempt to resend the data and shall continue to do so at intervals determined by the specification of the TARV RTM application service approved by the approval authority (regulatory) until the data has been successfully sent and ACKnowledged.

10.4.10.5 Whenever the regulated vehicle ignition is switched to OFF, the on-board TARV RTM app shall append a record <Time><'OFF'> to the 'RTMdata' file and the IVS shall send the file to the TARV RTM application service provider system via a wireless communication supported by the IVS and application service provider system.

10.4.10.6 On successful receipt of the TARV RTM file containing the end data (<Time><'OFF'>) the application service provider system shall send an ACKnowledgement <RXX> to the IVS, and unless otherwise instructed by the specification of the application service approved by the approval authority (regulatory), on receipt of the ACKnowledgement <RXX> the IVS shall delete the 'RTMdata' file from its memory, and the TARV RTM app shall terminate.

10.4.10.7 Because of the titling regime defined above, each TARV RTM file is uniquely identifiable by the host TARV RTM application service when it is received.

10.4.10.8 The manner in which the application service uses the information captured and forwarded to it by the IVS ('RTMdata' files) to perform the application service, and the method of reporting to the jurisdiction and operator is outside of the scope of this document and shall be the subject of definition by the jurisdiction and the application service provider.

10.4.11 TARV RTM SE11: End of session

If required by the data requirements of the jurisdiction, at the end of the driving session when the driver turns the digital tachograph off, or the ignition of the regulated vehicle is switched to OFF, on receipt of this information the IVS shall ensure whenever possible that the application service provider system is updated via a wireless connection from the IVS (see 10.4.8). If it is not possible for the IVS to update the application service provider system at this point in time, the IVS shall update the application service provider system at the earliest opportunity (for example when the regulated vehicle ignition is next switched on).

Otherwise, 'end of session' occurs when the interrogator closes the session, or when the wireless communication link to/from the interrogator is lost, or the session has been closed in accordance with the provisions of 10.4.10.

10.5 Generic TARV RTM data naming, content and quality

Communication Profile C3: The data content of the tachograph data shall be as defined by the application service/tachograph design.

In the case of fixed or mobile interrogation, except in the case of interrogation using 5,8 GHz DSRC as specified in the annexes to this document, the 'RTMdata' file shall be titled as shown in Table 3.

Table 3 — Formal title of a TARV RTM record

FILE TYPE		Format of file name	Notes/Source
RTM	**Mandatory**	<YYMMDD><hhmmss><vehicle registration number><' RTMdata'> Example 110316 070603 GB 1 KV76WRR RTMdata As: 110316070603KV76WRRRTMdata	Subclause 10.4.7 ([RTMdata file])

10.6 RTM data content

Communication Profile C3: The content of the RTMdata file shall be one or more of the data concept profiles specified in Annex C of this document.

Communication Profiles C1 and C2: The content of data provided for mobile inspections using short range communications shall be one or more of the data concept profiles specified in Annex C of this document, or the jurisdiction may determine and require its own mandatory data, in which case it is responsible for ensuring that those within its control are adequately informed concerning its requirements.

10.7 TARV RTM application service specific provisions for quality of service

The integrity of the data is important, and other sensors as well as parameters may then be required based on the approaches and techniques used to provide assurance of the quality of the data. The generic quality of service provisions for the service elements specified in 10.4 are defined in ISO 15638-6 and ISO 15638-5.

Instantiation specific requirements shall be part of the data requirements of the jurisdiction. However, in defining such requirements jurisdictions shall wherever possible, use performance based or functional specifications in order to avoid locking requirements into technologies that will become obsolete.

NOTE Having prescribed integrity and its parameters into an operational system, it is harder to move to other integrity indicators when new technologies emerge.

See also Clause 9 for general quality of service requirements.

10.8 TARV RTM application service specific provisions for test requirements

There are no specific provisions for test requirements specified in this document, except as specified for a short-range communication with a mobile interrogator (Communication Profiles C1 and C2), which shall be tested to meet the requirements of EN 300 674-1 appropriate to the parameter defined in this document.

NOTE The parameters used are specified in B.1.5 and are a combination of parameters taken from EN 12253 and profile definition tables from EN 13372.

10.9 TARV RTM application specific rules for the approval of IVSs and 'Service Providers'

Shall be as specified in ISO 15638-6:2014, 9.12 or given by a data requirement of the jurisdiction.

Annex A
(informative)

RTM Communication and Transaction profiles

A.0 Communication profiles

This version of this document supports and defines three types of communication profiles:

— **Communication Profile C1: Roadside inspection using a short-range wireless communication interrogator instigating a physical roadside inspection, (master <> slave)**

  Profile C1a: via a hand aimed or temporary roadside mounted and aimed interrogator

  Profile C1b: via a vehicle mounted and directed interrogator

  Profile C1c: via a permanent or semi-permanent roadside or overhead gantry

— **Communication Profile C2: Roadside inspection using a short-range wireless communication interrogator, instigating a download of data to an application service provider via an ITS-station communication (master <> slave + peer <> peer)**

  Profile C2a: via a hand aimed or temporary roadside mounted and aimed interrogator

  Profile C2b: via a vehicle mounted and directed interrogator

  Profile C2c: via a permanent or semi-permanent roadside or overhead gantry

— **Communication Profile C3: Remote inspection addressed via an ITS-station instigating a download of data to an application service provider via a wireless communications interface (as defined in ISO 15638-2) (peer <> peer)**

  Profile C3a: via an interrogation from an ITS-station

  Profile C3b: via a remote interrogation directed to the IP address of a specific vehicle

The Communication profiles are described and defined in 6.1 to 6.5.

This annex provides the definition for the RTM transactions for each of these communication profile options.

A.1 Communication Profile C1 — Interrogated request for tachograph data using short range 5,8 GHz DSRC communication

A.1.1 This is a master<>slave communication where an interrogator requests and an IVS supplies RTM data (for an inspector to evaluate whether or not to stop a vehicle).

A.1.2 The interrogator shall establish a communication in accordance with Annex B of this document.

A.1.3 The interrogator shall then request data and the IVS shall transfer data concepts as defined in Annex C of this document in accordance with the transaction defined in Annex B of this document.

NOTE An example ASN.1 module for the RtmData transaction is provided in B.1.5.2.

A.1.4 The interrogator shall confirm receipt of the data as specified in Annex B of this document by issuing a RELEASE defined in accordance with the transaction defined in Annex B of this document.

A.1.5 The session shall be closed as specified in Annex B of this document.

A.1.6 From the perspective of the command and response sequence, the transaction is described as follows:

Sequence	Sender		Receiver	Description	Action
1	Interrogator	>	IVS	Initialisation of the communication link – Request	Interrogator broadcasts BST
2	IVS	>	Interrogator	Initialisation of the communication link – Response	If BST supports AID=2 then IVS Requests a private window
3	Interrogator	>	IVS	Grants a private window	Sends Frame containing private window allocation
4	IVS	>	Interrogator	Sends VST	Sends Frame comprising VST
5	Interrogator	>	IVS	Requests LPDU for specific EID	
6	IVS	>	Interrogator	Sends LPDU for specific EID	Sends frame of data containing the LPDU for specific EID
7	Interrogator	>	IVS	Requests LPDU for next specified EID (if appropriate)	
8	IVS	>	Interrogator	Sends LPDU for specific EID	Sends frame of data containing the LPDU for specific EID
9	Interrogator	>	IVS	Acknowledges successful receipt of data	Sends RELEASE command which closes transaction
10	IVS			Closes transaction	

A.2 Communication Profile C2 — Roadside inspection using a short-range wireless communication interrogator, instigating a download of data to an application service provider via an ITS-station

A.2.1 This is a combination of master<>slave communication where an interrogator requests RTM data, which is subsequently supplied to a remote application service provider in a peer<>peer communication via its ITS-station.

NOTE While in Communication Profile C1, the data transferred is expected to only be enough data to evaluate whether to stop the vehicle and then download data by direct physical connection to the digital tachograph (from which decisions of whether to enforce/prosecute will be made by inspectors at the scene). In Communication Profile C2 the 5,8 GHz DSRC equipment is used to trigger the supply of a larger set of data directly to an application service provider via an ITS-station.

A.2.2 A TARV RTM app running on the IVS records the received tachograph data in a file, 'RTMdata' held in the data pantry of the IVS, taking into consideration the data requirements of the jurisdiction. The means by which this process occurs is outside the specifications of this document and shall be to the data requirements of the jurisdiction.

A.2.3 The interrogator shall establish a communication in accordance with Annex B of this document, the IVS responding to the BST with a request for a private window. Once the private window is granted and the response to BST (VST is received):

A.2.4 The interrogator shall send an ACTION command instructing the IVS to deliver data to a specified service provider.

A.2.5 The IVS shall record the data and acknowledge the request.

A.2.6 The IVS shall record the SET_DEST-REF data in an area allocated for this data in its data pantry. The organization of the memory of the IVS is not defined in this document and shall be a matter of product design and in accordance with the requirements of ISO 15638-1, ISO 15638-3, and ISO 15638-5.

A.2.7 The interrogator shall close the communication by issuing a RELEASE as specified in Annex B of this document.

A.2.8 The 5,8 GHz DSRC communication session shall be closed as specified in Annex B of this document.

A.2.9 The IVS shall then transfer the data to a predetermined address by its application service provider in accordance with the procedures described in A.3.1.7.

A.3 Communication Profile C3 — Remote inspection addressed via an ITS-station instigating a download of data to an application service provider via a wireless communications interface

A.3.1 Interrogated request for tachograph data via ITS-station

A.3.1.1 As specified in 10.4.7 (TARV RTM SE7), when the ignition of the regulated vehicle is turned on, the TARV RTM app in the data library of the IVS shall be instigated.

The app shall first create a RTMdata file and shall name the file

<YYMMDD><hhmmss><vehicle registration number><' RTMdata'>

and shall record the IVS ID, as specified in ISO 15638-5, as the first data element in the file, followed by a comma as

<IVS Unique identity><,>

A.3.1.2 As specified in 10.4.8, TARV RTM SE8, where required by the data requirements of the jurisdiction, at intervals determined by the application service app, the app shall obtain a stream of data from the digital tachograph ('pull') or the tachograph shall send a stream of data ('push') to the RTM IVS.

The IVS shall update the 'RTMdata' file adding the new data to the end of the file, in the format

<'start'><tachographdata><'END'>

The length of the data file 'RTMdata' shall be recorded as a numeric value representing a number of octets (octets).

A.3.1.3 The TARV RTM app running on the IVS, records the received tachograph data in a file, 'RTMdata' held in the data pantry of the IVS.

A.3.1.4 On receiving an interrogation request from an ITS-station <> ITS-station communication, requesting the RTM data, the interrogator shall also provide at the time of the request, a unique 8 octet reference number (URef) and a destination IPv6 address (ReqDest) where it requests the data to be sent.

A.3.1.5 The RTM IVS shall acknowledge the request with the appropriate ACKnowledgement defined in ISO 15638-6:2014, 8.3.5 <T>, which acknowledges that a request for RTM data has been received.

A.3.1.6 The IVS shall then close the communication session.

A.3.1.7 The TARV RTM app shall then send the TARV RTM data held in the file, 'RTMdata' held in the data pantry of the IVS to a predetermined IP address of the application service provider via its most appropriate wireless communications interface, together with the requested destination address and interrogators reference code.

A.3.1.8 Once the TARV RTM system of the application service provider has acknowledged successful receipt of the data, the 'RTMdata' file shall be deleted from the memory of the IVS unless the user, jurisdiction or application service provider requires it for other purposes, and a new file shall be created for future use.

This subclause concerns only transient data files created in order to effect the transfer of RTM data. It does not concern data stored in the digital tachograph, which shall not be deleted and shall be retained taking into consideration data requirements of the jurisdiction.

A.3.1.9 On successful receipt of the data, the recipient at the predetermined destination IPv6 address shall send an acknowledgement <RTX> to the IVS.

A.3.1.10 On receipt of the acknowledgement <RTX> the IVS shall close its communication session.

A.3.1.11 The ASP shall be responsible for verifying that the interrogation is legitimate, appropriate and from an accepted source, and having verified this, shall be responsible for sending the data to the interrogator requested IPv6 address. The means and detail of how this is achieved is outside the scope of this document.

A.3.1.12 It shall not be possible for collected or stored tachograph data in any software or non-volatile memory within the IVS or digital tachograph to be accessible or capable of being manipulated by any person, device or system (including via any self-declaration device), other than that authorised by the application service provider.

A.3.1.13 In Europe, 5,9 GHz C-ITS ITS-stations shall be required to have a means to detect 5,8 GHz CEN DSRC transmissions, and while in the presence of such signals, shall reduce the power of its emitted 5,9 GHz signals in accordance with ETSI/TS 102-792:2015, 5.4 in order to mitigate possible interference on 5,8 GHz CEN DSRC sessions.

A.3.2 Obtaining tachograph data by remotely addressing the IPv6/IPv4 address of a vehicle ITS-station or its tachograph that is wirelessly connected in accordance with one or more of the wireless media specified in ISO 15638-2

A.3.2.1 In the event that the ITS-station of the IVS of a vehicle receives a wireless interrogation, addressed to its IP address, requesting the RTM data, that communication shall also provide, at the time of the request, a unique 8 octet reference number (URef), and a destination IPv6 address (ReqDest) where it requests the data to be sent.

A.3.2.2 On receipt of the request to its IPv6/IPv4 address the RTM IVS shall acknowledge the request with the appropriate acknowledgement defined in ISO 15638-6:2014, 8.3.5, <T>, which acknowledges that a request for RTM data has been received.

A.3.2.3 The IVS shall then close the communication session.

A.3.2.4 The IVS shall then open a new communication session using an available and appropriate CALM wireless medium.

A.3.2.5 The IVS shall then send the RTM datafile to a predetermined destination IPv6 (internet) address that has previously been stored in the memory of the data pantry by its ASP, together with the URef and ReqDest provided by the interrogator.

A.3.2.6 On successful receipt of the data, the recipient at the predetermined destination IPv6 address shall send an acknowledgement <RTX> to the IVS.

A.3.2.7 On receipt of the acknowledgement <RTX> the IVS shall close its communication session.

A.3.2.8 The ASP shall be responsible for verifying that the interrogation is legitimate, appropriate and from an accepted source, and having verified this, shall be responsible for sending the data to the interrogator requested IPv6 address. The means and detail of how this is achieved are outside the scope of this document.

A.3.3 Obtaining tachograph data by interrogating via a fixed gantry or roadside beacon is wirelessly connected in accordance with one or more of the wireless media specified in ISO 15638-2

A.3.3.1 In the event that the IVS of a vehicle receives a wireless interrogation requesting the RTM data, the interrogator shall also provide, at the time of the request, a unique 8 octet reference number (URef), and a destination IPv6 address (ReqDest) where it requests the data to be sent.

A.3.3.2 On receipt of the wireless request to the ITS-station of the RTM IVS, the ITS-station of the RTM IVS shall acknowledge, to the interrogating source address, the request with the appropriate ACKnowledgement defined in ISO 15638-6:2014, 8.3.5 <T>, which acknowledges that a request for RTM data has been received.

A.3.3.3 The IVS shall then close the communication session.

A.3.3.4 The IVS shall then open a new communication session using an available and appropriate CALM wireless medium.

A.3.3.5 The IVS shall then send the RTM datafile to a predetermined destination IPv6 (internet) address that has previously been stored in the memory of the data pantry by its ASP, together with the URef and ReqDest provided by the interrogator.

A.3.3.6 On successful receipt of the data, the recipient at the predetermined destination IPv6 address shall send an acknowledgement <RTX> to the IVS.

A.3.3.7 On receipt of the acknowledgement <RTX> the IVS shall close its communication session.

A.3.3.8 The ASP shall be responsible for verifying that the interrogation is legitimate, appropriate and from an accepted source, and having verified this, shall be responsible for sending the data to the interrogator requested IPv6 address. The means and detail of how this is achieved are outside the scope of this document.

A.3.4 Obtaining tachograph data by interrogating via a mobile interrogator that is wirelessly connected in accordance with one or more of the wireless media specified in ISO 15638-2 (Communication profile C3)

A.3.4.1 In the event that the IVS of a vehicle receives a wireless interrogation requesting the RTM data, the interrogator shall also provide, at the time of the request, a unique 8 octet reference number (URef), and a destination IPv6 address (ReqDest) where it requests the data to be sent.

A.3.4.2 On receipt of the wireless request to the ITS-station of the RTM IVS, the ITS-station of the RTM IVS shall acknowledge, to the interrogating source address, the request with the appropriate ACKnowledgement defined in ISO 15638-6:2014, 8.3.5 <T>, which acknowledges that a request for RTM data has been received.

A.3.4.3 The IVS shall then close the communication session.

A.3.4.4 The IVS shall then open a new communication session using an available and appropriate CALM wireless medium.

A.3.4.5 The IVS shall then send the RTM datafile to a predetermined destination IPv6 (internet) address that has previously been stored in the memory of the data pantry by its ASP, together with the URef and ReqDest provided by the interrogator.

A.3.4.6 On successful receipt of the data, the recipient at the predetermined destination IPv6 address shall send an acknowledgement <RTX> to the IVS.

A.3.4.7 On receipt of the acknowledgement <RTX> the IVS shall close its communication session.

A.3.4.8 The ASP shall be responsible for verifying that the interrogation is legitimate, appropriate and from an accepted source, and having verified this, shall be responsible for sending the data to the interrogator requested IPv6 address. The means and detail of how this is achieved is outside the scope of this document.

A.3.4.9 The session shall be closed as specified in A.5.

A.4 Pre-programmed downloads of tachograph data (Communication profile C3)

A.4.1 Pre-programmed interval sending digital tachograph data to application service provider

A.4.1.1 Where required by the data requirements of the jurisdiction, or by the operator, at time intervals determined by the on-board TARV RTM app, taking into consideration the requirements of the jurisdiction or the operator, the RTM IVS shall send the 'RTMdata' file to the TARV RTM application service provider system via a wireless communication supported by the IVS and application service provider system as:

<START><LENGTH>< RTMdata file><RTMdata><END>

A.4.1.2 The content of the RTMdata file shall be a data concept profile as specified in Annex C of this document.

A.4.1.3 On successful receipt of the TARV RTM file the application service provider system shall send an ACKnowledgement <RTX> to the IVS. On receipt of the acknowledgement <RTX> the IVS shall clear the data held within the 'RTMdata' file and start to repopulate the 'RTMdata' file with data as defined by the TARV RTM app.

A.4.1.4 If an ACKnowledgement is not received within 60 seconds of sending the data, the TARV RTM app shall attempt to resend the data and shall continue to do so at intervals determined by the specification of the TARV RTM application service approved by the approval authority (regulatory) until the data has been successfully sent and ACKnowledged.

A.4.1.5 Whenever the regulated vehicle ignition is switched to OFF, the on-board TARV RTM app shall append a record <Time><'OFF'> to the 'RTMdata' file and the IVS shall send the file to the TARV RTM application service provider system via a wireless communication supported by the IVS and application service provider system.

A.4.1.6 On successful receipt of the TARV RTM file containing the end data (<Time><'OFF'>) the application service provider system shall send an ACKnowledgement <RXX> to the IVS, and unless

otherwise instructed by the specification of the application service approved by the approval authority (regulatory), on receipt of the ACKnowledgement <RXX> the IVS shall delete the 'RTMdata' file from its memory and the TARV RTM app shall terminate.

A.4.1.7 Because of the titling regime defined above, each TARV RTM file is uniquely identifiable by the host TARV RTM application service when it is received.

A.4.1.8 The manner in which the application service uses the information captured and forwarded to it by the IVS ('RTMdata' files) to perform the application service, and the method of reporting to the jurisdiction and operator is outside of the scope of this document and shall be the subject of definition by the jurisdiction and the application service provider.

A.4.1.9 The session shall be closed as specified in A.5.

A.5 End of session

Except in the aspects of A.1 and A.2 (Communication Profiles C1 and C2: interrogation via DSRC communication), where end of transaction procedures are defined in Annex B, and there are no end of driving session procedures, at the end of the driving session when the driver turns the digital tachograph off, or the ignition of the regulated vehicle is switched to OFF, on receipt of this information the IVS shall ensure whenever possible that the application service provider system is updated via a wireless connection from the IVS using an appropriate wireless communication medium supported by ISO 15638-2.

If it is not possible for the IVS to update the application service provider system at this point in time, the IVS shall update the application service provider system at the earliest opportunity (for example when the regulated vehicle ignition is next switched on).

Annex B
(informative)

Communication Profile for EN 5,8 GHz DSRC communications

B.1 Overview and context

B.1.1 Overview

Annex B is consistent with European Regulation 2016/799/EC and its Appendix 14, which was published on 2016-05-26 and entered into force from 2016-06-15. Any revision of that Regulation can require an update/amendment to this document.

The scope for this annex is limited to:

— physical systems: Communication between ITS-stations of the interrogator/roadside and the vehicle using a 5,8 GHz DSRC interface between them (all functions and information flows related to these parts);

— DSRC-link requirements;

— Tachograph data request and supply transactions over the DSRC interface.

Data elements to be used are provided in Annex C.

Security provisions are provided in 9.6 and B.1.6.5.

Mechanisms for IVS and interrogator used in these DSRC transactions are specified below.

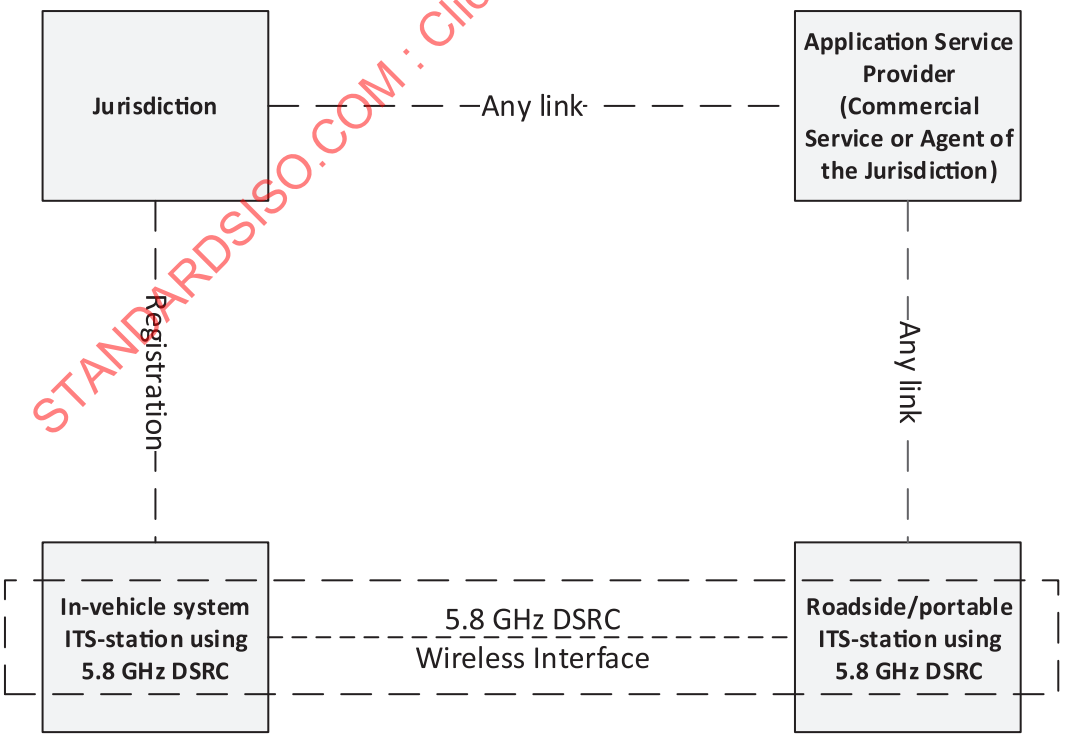


Figure B.1 — Scope for this use case (within the box delimited with a dotted line)

Figure B.2 shows the scope of this use case from a DSRC-stack perspective.

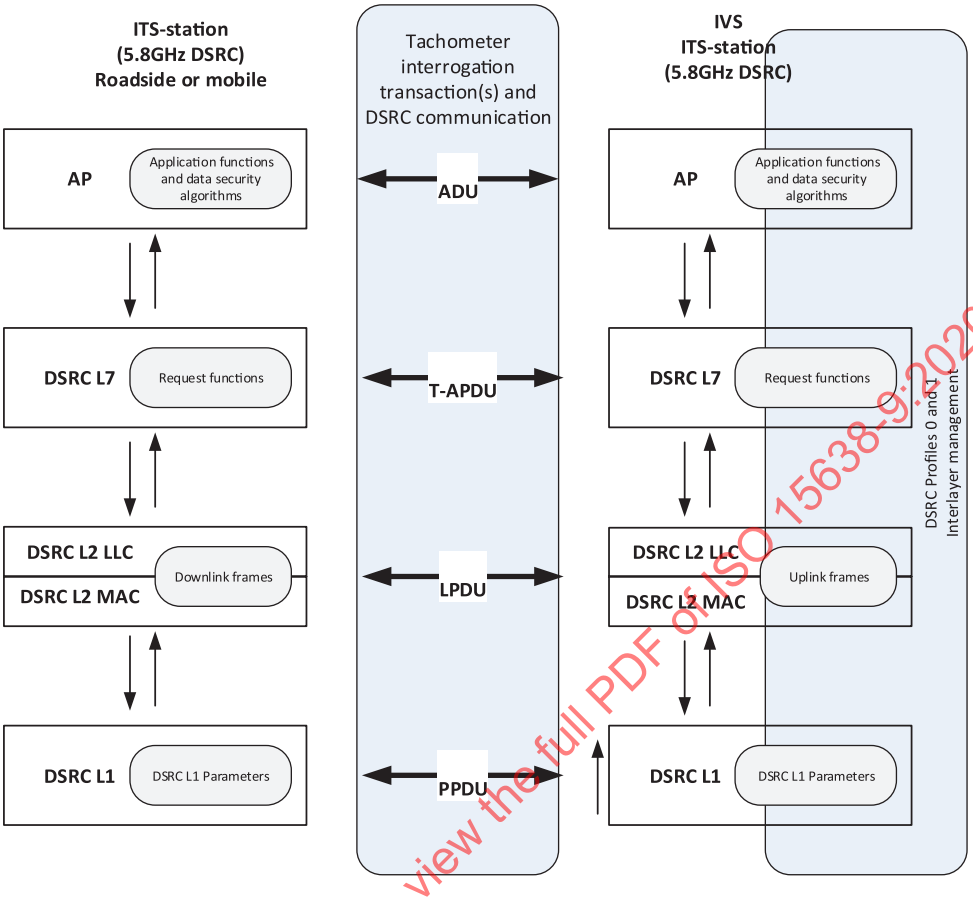


Figure B.2 — Relations between 5,8 GHz DSRC communications stack elements

This annex specifies a communication profile use case for short range transactions between an interrogator and the vehicle to obtain data from a tachograph on-board the vehicle, using 5,8 GHz DSRC. The base standards that this use case are based upon are shown in Figure B.3. However, it should be clearly noted that there are four regional variations. It is necessary for jurisdictions to determine and declare with which of these base standards tachograph equipment/IVS used within their jurisdiction shall need to conform.

Figure B.3 shows the relationship between the ISO 15638 series TARV standards, ISO CALM standards (including via 5,8 GHz DSRC for RTM), and 5,8 GHz DSRC EFC standards.

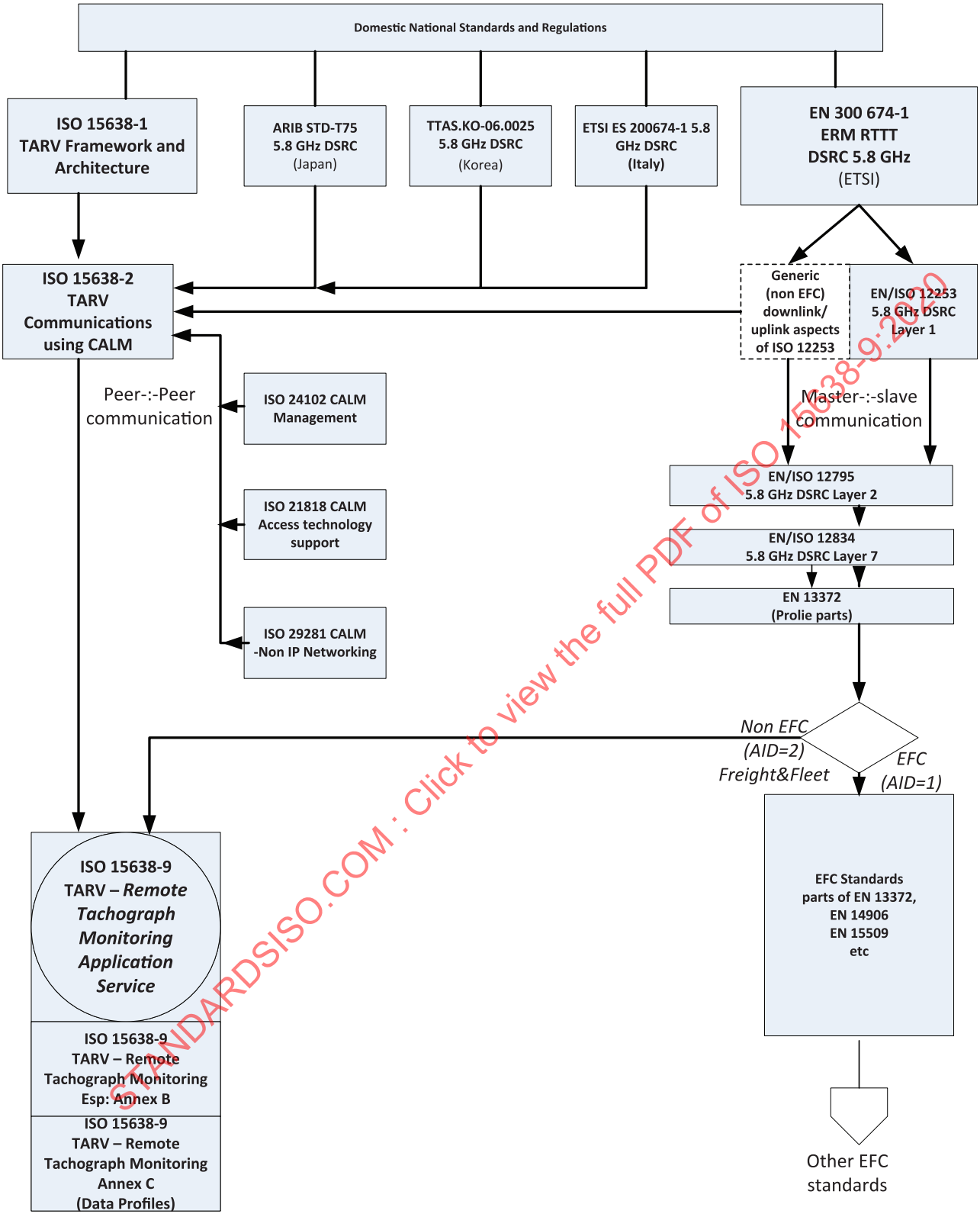


Figure B.3 — Relation and references between ISO 15638-9 (this document), CALM Communications and 5,8 GHz DSRC base standards

B.1.2 Use cases

The use cases where a 5,8 GHz DSRC communication may be used are described in 6.2 (Communication Profile C1) and 6.3 (Communication Profile C2.).

B.1.3 Physical layer

The system shall operate in accordance with one of the four base 5,8 GHz DSRC standards:

— ETSI EN 300-674-1(Europe, Australia, parts of the Americas, and other regions),

— ARIB T-75 (Japan),

— TTAS.KO-06.0025 (Korea),

— ETSI .TS 200-674-1 (Italy).

This annex concerns only 5,8 GHz DSRC communications, in a master/slave communication.

In Europe, 5,9 GHz C-ITS ITS-stations are required to have a means to detect 5,8 GHz CEN DSRC transmissions, and to reduce the power of emitted 5,9 GHz signals in accordance with ETSI/TS 102-792:2015, 5.4, in order to mitigate possible interference on 5,8 GHz CEN DSRC sessions.

B.1.4 Profile C1 transactions

Transactions operating within ERC 70-03 and EU Regulation (EU) No 165/2014 are defined in B.1.5 and subsequent clauses.

Other ISO 15638-2 communication means (including the 5,9 GHz so called 'DSRC'), based on peer-to-peer communications, are not the subject of this normative annex.

For Profile C2 communications, see A.2.

Transactions using:

— ARIB T-75 (Japan),

— TTAS.KO-06.0025 (Korea),

— ETSI .TS 200-674-1 (Italy)

may use national standards specifications to transfer 5,8 GHz data.

B.1.5 Communications Profile C1 transactions operating within EN 12253, 5,8 GHz DSRC and the profile definitions of EN 12834

Where the system is operating within the regulatory parameters of ERC 70-03, it shall further conform to the following uplink and downlink parameters from EN 12253, EN 12275, EN 12834 and profile parameters as defined in EN 13372. If profile 0 is supported by the RSU then the value of data element Profile in BST shall be 0. If Profile C1 is supported by the RSU then the value of data element Profile in BST shall be 1.

In order to optimize the mobile read situation, some of the parameter values differ from those in EN 12253. This is made explicitly clear in the tables below. Only those parameters that are consistent with requirements in EN 12253 or EN 13372 can be tested using appropriate tests for that parameter from EN 300 674-1.

B.1.5.1 5,8 GHz European DSRC downlink and uplink parameters

Table B.1 — Downlink parameters

Item No.	Parameter	Value(s)	Remarks
D1	Downlink Carrier Frequencies	There are four alternatives which may be used by an interrogator: 5,797 5 GHz 5,802 5 GHz 5,807 5 GHz 5,812 5 GHz	Within ERC 70-03. Carrier Frequencies may be selected by the implementer of the roadside system and need not be known in the IVS (Consistent with EN 12253, EN 13372)
D1a [a]	Tolerance of Carrier Frequencies	within ±5 ppm	**(**Consistent with EN 12253**)**
D2	Interrogator Transmitter Spectrum Mask	Within ERC 70-03. Interrogator shall be according to Class B, C as defined in EN 12253 . No other specific requirement within this document	Parameter used for controlling interference between interrogators in proximity (as defined in EN 12253 and EN 13372). Not a relevant parameter for this document
D3	IVS Minimum Frequency Range	5,795 – 5,815 GHz	(Consistent with EN 12253)
D4 [a]	Maximum E.I.R.P.	Within ERC 70-03 (unlicensed) Maximum +33 dBm	(Consistent with EN 12253)
D4a	Angular E.I.R.P. mask	According to declared and published specification of interrogator designer	
D5 [a]	Polarization	Left hand circular	**(**Consistent with EN 12253**)**
D5a [a]	Cross-Polarization	XPD: In bore sight: (Interrogator) RSU t ≥ 15 dB (IVS) OBU r ≥ 10 dB At -3 dB area: (Interrogator) RSU t ≥ 10 dB (IVS) OBU r ≥ 6 dB	**(**Consistent with EN 12253**)**
D6 [a]	Modulation	Two level amplitude modulation	**(**Consistent with EN 12253**)**
D6a [a]	Modulation index	0,5 ... 0,9	**(**Consistent with EN 12253**)**
D6b [a]	Eye pattern	≥90 % (time) / ≥85 % (amplitude)	**(**Consistent with EN 12253**)**
D7 [a]	Data coding	FM0 "1" bit has transitions only at the beginning and end of the bit interval. "0" bit has an additional transition in the middle of the bit interval compared to the "1" bit.	**(**Consistent with EN 12253**)**
D8 [a]	Bit rate	500 kBit/s	**(**Consistent with EN 12253**)**
D8a	Tolerance of Bit Clock	better than ±100 ppm	**(**Consistent with EN 12253**)**
D9	Bit Error Rate (B.E.R.) for communication	≤10 – 6 when incident power at OBU (IVS) is in the range given by [D11a to D11b]	**(**Consistent with EN 12253**)**

[a] Downlink parameters subject to conformance testing in accordance with relevant parameter test from EN 300 674-1.

Table B.1 *(continued)*

Item No.	Parameter	Value(s)	Remarks
D10	Wake-up trigger for IVS	IVS shall wake up on receiving any frame with 11 or more octets (including preamble)	No special wake-up pattern is necessary. IVS may wake up on receiving a frame with less than 11 octets (Consistent with EN 12253)
D10a	Maximum start time	≤5 ms	**(**Consistent with EN 12253**)**
D11	Communication zone	Spatial region within which a B.E.R. according to D9a is achieved	**(**Consistent with EN 12253**)**
D11a [a]	Power limit for communication (upper)	–24dBm	
D11b [a]	Power Limit for communication (lower)	Incident power: –43 dBm (boresight) –41 dBm (within ±45° corresponding to the plane parallel to the road surface when the IVS later is installed in the vehicle (Azimuth))	**(**Consistent with EN 12253**)**
D12	Cut-off power level of IVS	–60 dBm	(Consistent with EN 12253)
D13	Preamble	Preamble is mandatory	**(**Consistent with EN 12253**)**
D13a	Preamble length and pattern	16 bits ±1 bit of FM0 coded “1” bits	**(**Consistent with EN 12253**)**
D13b	Preamble wave form	An alternating sequence of low level and high level with pulse duration of 2 µs. The tolerance is given by D8a	**(**Consistent with EN 12253**)**
D13c	Trailing Bits	The interrogator is permitted to transmit a maximum of 8 bits after the end flag. An IVS is not required to take these additional bits into account	**(**Consistent with EN 12253**)**
[a] Downlink parameters subject to conformance testing in accordance with relevant parameter test from EN 300 674-1.			

Table B.2 — Uplink parameters

Item No.	Parameter	Value(s)	Remark
U1 [a]	Sub-carrier Frequencies	An IVS shall support 1,5 MHz and 2,0 MHz An interrogator shall support 1,5 MHz or 2,0 MHz or both. U1-0: 1,5 MHz U1-1: 2,0 MHz	Selection of sub-carrier frequency (1,5 MHz or 2,0 MHz) depends on the EN 13372 profile selected.
U1a	Tolerance of sub-carrier frequencies	within ±0,1 %	(Consistent with EN 12253)
U1b	Use of side bands	Same data on both sides	(Consistent with EN 12253)
[a] Uplink parameters subject to conformance testing in accordance with relevant parameter test from EN 300 674-1.			

Table B.2 *(continued)*

Item No.	Parameter	Value(s)	Remark
U2	IVS transmitter spectrum mask	According to EN 12253 1) Out band power: see ETSI EN 300 674-1 2) In band power: ≤[U4a] dBm in 500 kHz 3) Emission in any other uplink channel: U2(3)-1 = −35 dBm in 500 kHz	(Consistent with EN 12253)
U4 [a]	Maximum E.I.R.P.	Within ERC 70-03 (unlicensed)	
U4a [a]	Maximum Single Side Band E.I.R.P. (boresight)	Two options: — U4a-0: −14 dBm — U4a-1: −21 dBm	According to declared and published specification of equipment designer
U4b [a]	Maximum Single Side Band E.I.R.P. (35^0)	Two options: — Not applicable — −17 dBm	According to declared and published specification of equipment designer
U5 [a]	Polarization	Left hand circular	(Consistent with EN 12253)
U5	Cross polarization	XPD: In bore sight: (Interrogator) RSU r ≥15 dB (IVS) OBU t ≥10 dB At −3 dB: (Interrogator) RSU r ≥10 dB (IVS) OBU t ≥6 dB	(Consistent with EN 12253)
U6	Sub-carrier modulation	2-PSK Encoded data synchronized with sub-carrier: Transitions of encoded data coincide with transitions of sub- carrier	(Consistent with EN 12253)
U6b	Duty cycle	Duty cycle: 50 % ±α, α ≤5 %	
U6c	Modulation on carrier	Multiplication of modulated sub-carrier with carrier	(Consistent with EN 12253)
U7 [a]	Data coding	NRZI (No transition at beginning of "1" bit, transition at beginning of "0" bit, no transition within bit)	(Consistent with EN 12253)
U8 [a]	Bit rate	250 kbit/s	(Consistent with EN 12253)
U8a	Tolerance of Bit clock	Within ±1 000 ppm	(Consistent with EN 12253)
U9a	B.E.R.	$\leq 10^{-6}$	(Consistent with EN 12253)
U10		Response to downlink	Does not affect uplink
U11	Communication zone	The spatial region within which the IVS is situated such that its transmissions are received by the interrogator with a B.E.R. of less than that given by U9a	(Consistent with EN 12253)
U12a	Conversion gain (lower limit)	1 dB for each side band Range of angle: Circularly symmetric between bore sight and ±45°	Greater than the specified value range for each side band within a circular cone around boresight of ±45° opening angle

[a] Uplink parameters subject to conformance testing in accordance with relevant parameter test from EN 300 674-1.

Table B.2 *(continued)*

Item No.	Parameter	Value(s)	Remark
U12b	Conversion gain (upper limit)	10 dB for each side band	Less than the specified value range for each side band within a circular cone around boresight of ±45° opening angle
U13	Preamble	Preamble is mandatory.	(Consistent with EN 12253)
U13a	Preamble length and pattern	32 to 36 µs modulated with sub-carrier only, then 8 bits of NRZI coded "0" bits.	(Consistent with EN 12253)
U13b	Trailing bits	The IVS is permitted to transmit a maximum of 8 bits after the end flag. An interrogator is not required to take these additional bits into account.	(Consistent with EN 12253)
[a] Uplink parameters subject to conformance testing in accordance with relevant parameter test from EN 300 674-1.			

B.1.5.2 ASN.1 module for the RtmData transaction

The ASN.1 module definition for the DSRC data within the RTM application is using the ASN.1 technique in accordance with ISO/IEC 8824-1. The packed encoding rules given in ISO/IEC 8825-2 with the restrictions defined in ISO 15628:2013, 6.2.7 apply. The ASN.1 module follows:

```
TarvRtm {iso(1) standard(0) 15638 part9(9) version1(1)} DEFINITIONS AUTOMATIC TAGS
::= BEGIN
IMPORTS
-- Imports data attributes and elements from EFC which are used for RTM
LPN
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports function parameters from the EFC Application Interface Definition
SetMMIRq
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports the L7 DSRCData module data from the EFC Application Interface Definition
Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList, AttributeList,
Attributes,
BeaconID, BST, Dsrc-EID, DSRCApplicationEntityID, Event-Report-Request, Event-Report-Response,
EventType, Get-Request, Get-Response, Initialisation-Request, Initialisation-Response,
ObeConfiguration, Profile, ReturnStatus, Time, T-APDUs, VST
FROM EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)};
```

```
-- Definitions of the RTM functions:


RTM-InitialiseComm-Request ::= BST
RTM-InitialiseComm-Response::= VST
RTM-DataRetrieval-Request::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid, attrIdList,
accessCredentials ABSENT,iid ABSENT})
RTM-DataRetrieval-Response::= Get-Response {RtmContainer} (WITH COMPONENTS {..., eid, iid ABSENT})
RTM-TerminateComm::= Event-Report-Request {RtmContainer}(WITH COMPONENTS {mode (FALSE), eid (0),
eventType (0)})
RTM-DeliverData-Request ::= Action-Request {RtmContainer} (WITH COMPONENTS {..., actionType
(8), accessCredentials ABSENT, iid ABSENT}
RTM-DeliverData-Response ::= Action-Response {RtmContainer} (WITH COMPONENTS {..., iid ABSENT})
RTM-TestComm-Request::= Action-Request {RtmContainer} (WITH COMPONENTS {..., eid (0), actionType
(15), accessCredentials ABSENT, iid ABSENT})

RTM-TestComm-Response::= Action-Response {RtmContainer} (WITH COMPONENTS {..., fill (SIZE(1)), eid
(0), iid ABSENT})



-- Definitions of the RTM attributes:
RtmData ::= SEQUENCE {
    encryptedTachographPayload OCTET STRING (SIZE(67)) (CONSTRAINED BY { -- calculated encrypting
TachographPayload}),
    dSRCSecurityData OCTET STRING
    }
TachographPayload ::= SEQUENCE {
                    tp15638VehicleRegistrationPlate   LPN -- Vehicle Registration Plate as per EN
15509.
                    tp15638SpeedingEvent              BOOLEAN, -- 1= Irregularities in speed (see
Annex 1C)
                    tp15638DrivingWithoutValidCard    BOOLEAN, -- 1= Invalid card usage (see Annex 1C)
                    tp15638DriverCard                 BOOLEAN,-- 0= Indicates a valid driver card (see
Annex 1C)
                    tp15638CardInsertion              BOOLEAN, -- 1= Card insertion while driving (see
Annex 1C)
                    tp15638MotionDataError            BOOLEAN, -- 1= Motion data error (see Annex 1C)
                    tp15638VehicleMotionConflict      BOOLEAN, -- 1= Motion conflict (see Annex 1C)
                    tp156382ndDriverCard              BOOLEAN, -- 1= Second driver card inserted (see
Annex 1C)
                    tp15638CurrentActivityDriving     BOOLEAN, -- 1= other activity selected;
                                                          -- 0= driving selected
                    tp15638LastSessionClosed          BOOLEAN, -- 1= improperly, 0= properly,
closed
                    tp15638PowerSupplyInterruption    INTEGER (0..127), -- Supply interrupts in the
last 10 days
                    tp15638SensorFault                INTEGER (0..255),-- eventFaultType as per data
dictionary
```

```
-- All subsequent time related types as defined in Annex 1C.
                    tp15638TimeAdjustment         INTEGER(0..4294967295), -- Time of the last time
adjustment
                    tp15638LatestBreachAttempt    INTEGER(0..4294967295), -- Time of last breach
attempt
                    tp15638LastCalibrationData    INTEGER(0..4294967295), -- Time of last calibration
data
                    tp15638PrevCalibrationData    INTEGER(0..4294967295), -- Time of previous
calibration data
                    tp15638DateTachoConnected     INTEGER(0..4294967295), -- Date tachograph connected
                    tp15638CurrentSpeed           INTEGER (0..255), -- Last current recorded speed
                    tp15638Timestamp              INTEGER(0..4294967295) -- Timestamp of current
record
                    }

RtmDestRef::=SEQUENCE{
  dest   IA5String (SIZE(80)) -- requested destination IP address url for the data
  ref    IA5String (SIZE(0..20))   -- reference of unique significance for the inspector
  }

RtmActionParameter ::= SEQUENCE {
  destRef RtmDestRef,
  attributeList SEQUENCE OF {AttributeId}
  }
Rtm-ContextMark ::= SEQUENCE {
  standardIdentifier            StandardIdentifier, -- identifier of the TARV part and its version
  rtmCommProfile                INTEGER {
                                          c1 (1),
                                          c2 (2),
                                          c3 (3)
                                      } (0..255) DEFAULT 1
    }
RtmTransferAck ::= INTEGER {
              ok (1),
              noK (2)
              } (1..255)
StandardIdentifier ::= OBJECT IDENTIFIER
RtmContainer ::= CHOICE {
          integer          [0]  INTEGER,
          bitstring        [1]  BIT STRING,
          octetstring      [2]  OCTET STRING (SIZE (0..127, ...)),
          universalString  [3]  UniversalString,
          beaconId         [4]  BeaconID,
          t-apdu           [5]  T-APDUs,
          dsrcApplicationEntityId  [6]  DSRCApplicationEntityID,
          dsrc-Ase-Id      [7]  Dsrc-EID,
          attrIdList       [8]  AttributeIdList,
```

```
            attrList            [9]  AttributeList{RtmContainer},
            rtmData            [10]  RtmData,
            rtmContextmark     [11]  Rtm-ContextMark,
            reserved12         [12]  NULL,
            reserved13         [13]  NULL,
            reserved14         [14]  NULL,
            time               [15]  Time,
      -- values from 16 to 255 reserved for ISO/CEN usage
            }
ManufacturerID ::= INTEGER(0..65535)

END
```

B.1.6 Operating context

B.1.6.1 Prerequisites

This annex has been prepared considering the prerequisites listed below in a) to c).

a) The data acquired shall be read only, since the operator of the interrogator shall not interfere with the working of the IVS.

b) All attributes shall be present in the IVS such that an operator of an interrogator can read the same data from all IVS/tachographs independent of type and make. In case an attribute does not make sense in a certain IVS implementation, a value assignment for “not applicable” or “not defined” is provided in each case.

c) The interrogator shall be able to receive the same information irrespective of IVS/tachograph implementation decisions.

B.1.6.2 Location constraints

The remote interrogation of vehicles using a 5,8 GHz DSRC interface shall not be used within 200 metres of an operational 5,8 GHz DSRC Electronic Fee Collection gantry.

NOTE This is to avoid any possible interference with electronic fee collection communications.

B.1.6.3 Frames

The communication between interrogator and IVS is a master<>slave transaction controlled by the interrogator and based on the exchange of ‘frames’ of data exchange as defined in EN 12795.

NOTE The frames have the format shown in Table B.3 and are described in the following paragraphs. There is also a special case of a ‘frame’ without the LPDU (Link layer Protocol Data Unit) field, which is used in some specific situations.

The above note is informative, and in the event of any doubt, the specifications in EN 12795 apply.

The size of the whole ‘frame’ varies from 9 octets up to 128 octets, and this size variation is associated with the LPDU field, which carries the payload data (up to a maximum payload of 110 octets).

A one octet ‘frame’ delimiter is placed at the beginning and at the end of each frame (value 01111110 [base 2]). This is followed by the ‘Link Address Field’ which has 5 octets and contains the LID (Link Identifier), which is used to keep the communication private between different users. Next is the ‘MAC’ field which is a single octet (see Table B.4) and it is used to:

— indicate if the frame contains an LPDU,

— specify the transmission direction,

— allocate public/private windows, and

— also request private windows.

Table B.3 — Frame format

Flag	Link Address Field	MAC Control Field	LPDU	Frame Check Sequence	Flag
1 octet	5 octets	1 octet	Up to 110 octets	2 octets	1 octet

The MAC control field is as shown in Table B.4.

Table B.4 — MAC control field format

L	D(b)	A or R	C/R	S	X	X	X	X
Where:								
L		indicates the existence or absence of the LPDU in the frame: 'L' equals '1', LPDU exists, otherwise value 0						
D(b)		indicates the link direction: '0' indicates 'downlink' and '1' indicates uplink.						
A		indicates window allocation (only used in downlinks); R: indicates window request (only used in uplinks).						
C/R		identifies the LPDU as a command or a response: 0 = command, 1 = response.						
S		distinguishes the first allocation of a private uplink and is not relevant on downlink.						
		The other three bits are presented but not used.						

B.1.6.4 Information security

Security of the payload data shall be as defined in 9.6. RTM data shall always be encrypted before being made available by the VU to the DSRC communication function.

Within this communication using 5,8 GHz DSRC, provision is made for up to 50 octets of security data (keys, and other security mechanisms/techniques), and the encrypted data (including security data) is then sent 'en clair' transmission. The provision for security data is that of a 'black box' allocation. Specific security techniques are not specified in this document (and are expected to change over time). Specific security provisions are to be at the discretion and determination of the jurisdiction, which is responsible for ensuring that all communicating parties have access to instruction on how to use their security provisions.

B.1.6.5 RTM LPDU

The data for the RTM LDPU shall be of up to 110 octets comprised as shown in Table B.5.

Table B.5 — Payload — Information and security data

No of octets of payload data	No of octets of security data	Payload data	Security data	10101010 end of field identifier octet
2 octets	2 octets	(A) Octets of payload data	(B) Octets of security data	1 octet
Example: 3	 2	 111111110000000011111111	 0000000011111111	 10101010

Subclause 9.6 determines that security data shall comprise the security 'keys' or links to keys or other security mechanisms provided to enable the payload data to be decrypted. While 9.6 effectively does not limit the number of octets of security data, within the 5,8 GHz DSRC use case that is the subject of this annex, up to a maximum of 50 octets may be used for security.

While 9.6 effectively does not limit the number of octets of payload data, within the 5,8 GHz DSRC use case that is the subject of this annex, up to a maximum of 54 octets may be used for payload data. Four octets of payload data are used for payload categorization. Net payload data shall therefore be up to a maximum of 50 octets. The payload data shall be structured as shown in Tables B.6 and B.7.

Table B.6 — Payload data

AID	TARV ID	TARV App ID	Payload data
1 octet	1 octet	2 octets	Up to 50 octets
Always=2	Always=1	Assigned application value. Normally equivalent to relevant TARV standard EG: RTM = 9 WIM = 20	Data to a scheme standardized in Annex C or issued and required by a jurisdiction

Table B.7 — Payload — Information and security data (detail)

No. of octets of payload data	No. of octets of security data	AID	Freight&Fleet ID = TARV	TARV App ID	Payload data	Security data	10101010 end of field identifier octet
2 octets	2 octets	1 octet	1 octet	2 octets	Up to 50 octets	Up to 50 Octets of security data	1 octet
Example: 3	2	Always = 2	Always = 1	EG: RTM = 9 WIM = 20	11111111 00000000 11111111	00000000 11111111	10101010

The total LPDU is therefore of the construct shown in Table B.8.

Table B.8 — Construct of RTM LPDU

Flag	Link Address Field	MAC Control Field									Frame check sequence	Flag
1 octet	5 octets	1 octet	**LPDU**								2 octets	1 octet
			No. of octets of payload data	**No. of octets of security data**	**AID**	**TARV ID**	**TARV App ID**	**Payload data**	**Security data**	**10101010 end of field identifier octet**		
Example:			2 octets	2 octets	1 octet	1 octet	2 octets	Up to 54 octets	Up to 50 octets of security data	1 octet		

Table B.8 *(continued)*

Flag	Link Address Field	MAC Control Field									Frame check sequence	Flag
0111 1110	00000000 11111111 00000000 11111111 00000000	00000000	00000000 00000011	00000000 00000010	00000010	00000001	00000000 00001001	11111111 00000000 …… 11111111	00000000 …… 11111111	10101010	00000000 11111111	01111110

B.1.6.6 Equipment design

Equipment design shall largely be at the discretion of the market place or to requirements specified by a jurisdiction, and operating within ERC 70-03 and B.1.5, and tested against the appropriate parameters of EN 300 674-1.

However, certain positioning specifications are required to enable the targeting of antennae.

B.1.6.7 Interrogator form factor

The design and form factor of the interrogator shall be a function of commercial design, operating within the limitations defined in ERC 70-03, and the design and performance specifications defined in this annex, thus providing the marketplace maximum flexibility to design and provide equipment to meet the particular needs of any particular jurisdiction to meet their particular interrogation scenarios.

B.1.6.8 IVS form factor

The design and form factor of the IVS and its positioning within or without other in-vehicle equipment (such as the tachograph) shall be a function of commercial design, operating within ERC 70-03, and the design and performance specifications defined in this annex or taking into consideration the data requirements of the jurisdiction, and tested against the appropriate parameters of EN 300 674-1.

The communication between the tachograph and the DSRC function may be a wired communication or a Bluetooth Low Energy (BLE) communication, and the physical location of the IVS DSRC function may be integral with the antenna on the windshield of the vehicle, internal to the tachograph, or located somewhere between.

In order that different suppliers may be contracted to supply the tachograph/vehicle unit and the IVS DSRC function, and indeed different batches of DSRC equipment, the connection between the tachograph vehicle unit and the IVS DSRC function shall be an open standard connection. The tachograph vehicle unit shall connect with the IVS DSRC function using fixed cable of 2 m, using a Straight DIN 41612 H11 Connector – 11 pin approved male connector from the IVS DSRC function to match a similar DIN/ISO approved female connector from the tachograph vehicle unit, or shall connect with the IVS DSRC function using Bluetooth Low Energy (BLE). The IVS DSRC function shall be reasonably capable to accept data concept values from other intelligent vehicle equipment by means of an open industry standard connection and protocols.

B.1.6.9 Interrogator antenna form factor

The design of the interrogator antenna shall be a function of commercial design, operating within ERC 70-03, and tested against the appropriate parameters of EN 300 674-1, adapted to optimize the reading performance of the IVS for the specific purpose and read circumstances in which the interrogator has been designed to operate. Specifically, the interrogator antenna shall be bound by the constraints of B.1.5.

B.1.6.10 IVS antenna form factor

The design of the IVS DSRC antenna shall be a function of commercial design, operating within ERC 70-03, and tested against the appropriate parameters of EN 300 674-1. Specifically, the IVS antenna shall be bound by the constraints of B.1.5.

The instantiation of the VU antenna and its fitment in the vehicle shall reasonably protect the IVS DSRC antenna from wilful or accidental damage or disconnection from the VU.

In a test environment in a workshop, an IVS antenna, affixed behind a standard clear front windshield, should successfully connect with a standard test communication and successfully provide an RTM LPDU transaction as defined within this annex, at a distance of 10 m, better than 99 % of the time, averaged over 1 000 read interrogations.

B.1.6.11 IVS antenna position

The IVS antenna shall be positioned in the lower part of the centre of the vehicle windshield in the area identified in Figure B.4. Specifically, it shall be positioned:

— Between the centreline of the vehicle and the centre of the steering wheel,

— at a height of approximately 1,5 m to 2,2 m from the road surface,

— at least 10 cm away from the windshield wiper at rest, and

— less than 50 cm away from the windshield wiper at rest.

— The windscreen area in front of the antenna shall not be metalized.

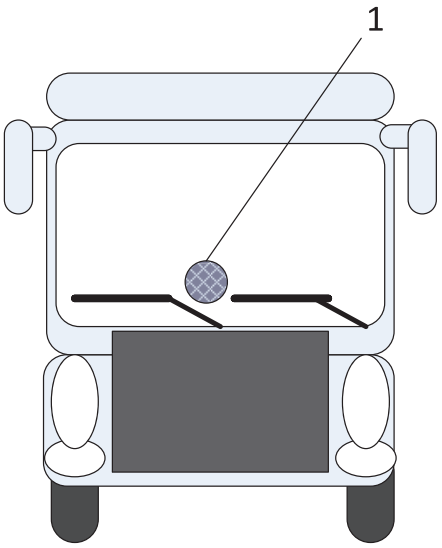
— There shall be no objects (e.g. name badges, stickers, foil anti reflection (tinting) strips, sun visors) within a radius of 10 cm from where the antenna is mounted.

— The antenna shall be mounted so that its boresight is approximately 90° to the surface of the road (i.e. vertical orientation).

— Similar technology devices used for tolling shall not be positioned within 10 cm of the VU.

The DSRC antenna shall be securely connected to the DSRC function either directly within the module mounted to the windshield, or through a dedicated cable constructed in a manner to make illegal disconnection difficult.

It is recommended that disconnection of or interference with the functioning of IVS antenna, and deliberate masking of or otherwise detrimentally affecting the operational performance of the antenna be made a violation of the data requirements of the jurisdiction.



Key

1 DSRC antenna location

Figure B.4 — Positioning of the 5,8 GHz DSRC antenna in the windshield of regulated vehicles

A later amendment to this document may impose minimum reading performance requirements.

In a test environment, an IVS antenna, affixed behind a standard clear front windshield, should successfully connect with a standard test communication and successfully provide an RTM LPDU transaction as defined within this document, at a distance of 2 . . 10 metres, better than 99 % of the time, averaged over 1 000 read interrogations.

B.1.7 Data download protocol

B.1.7.1 Overview

NOTE The purpose of the initialisation phase (Step 1) is to set up the communication between the interrogator and IVSs that have entered the 5,8 GHz DSRC (master/slave) transaction zone but have not yet established communication with the interrogator, and to notify the application processes.

The transaction phase can only be reached after completion of the initialisation phase.

Step 1 Initialisation. The interrogator sends a frame containing a 'beacon service table' (BST) that includes the application identifiers (AIDs) in the service list that it supports. In the RTM application this will simply be the service with the AID value = 2 (Freight&Fleet). The IVS DSRC function evaluates the received BST and shall respond (see below) with the list of the supported applications within the Freight&Fleet domain, or shall not respond if none are supported. If the interrogator does not offer AID = 2, the IVS DSRC function shall terminate the transaction with the interrogator.

Step 2 The IVS DSRC function sends a frame containing a request for a private window allocation.

Step 3 The interrogator sends a frame containing a private window allocation.

Step 4

The IVS DSRC function uses the allocated private window to send a frame containing its vehicle service table (VST). This VST includes a list of all the different application instantiations that this IVS DSRC function supports in the framework of AID = 2. The different instantiations shall be identified by means of uniquely generated EIDs, each associated with a parameter value indicating the standard supported. In the case of RTM, the parameter value shall be an Object Identifier related to ISO 15638-9 (TARV) (this document). Associated to this Object Identifier, an optional indicator identifies the RTM Communication Profile. If this indicator is omitted, Communication Profile C1 is implicitly selected.

Step 5

Next the interrogator analyses the offered VST, and either terminates the connection (RELEASE) since it is not interested in anything the VST has to offer (i.e. it is receiving a VST from an IVS DSRC function that is not supporting the RTM transaction), or, if it receives an appropriate VST it starts an app instantiation.

Step 6

To bring this about, the interrogator shall send a frame containing a command to retrieve the RTM data and, possibly, according to the selected C1 or C2 Communication Profile by identifying the location where data has to be sent, and the attribute to get to the specific IVS DSRC function and allocates a private window.

Step *7*

The IVS DSRC function uses the newly allocated private window to send a frame that contains either:

1. the attribute RtmData (payload element + security element) as specified in C.1, in case of Communication Profile C1
2. an explicit acknowledgement, in case of Communication Profile C2.

Step 8	If there are multiple services requested, the value 'n' is changed to the next service reference number and the process repeated.
Step 9	The interrogator confirms receipt of the data by sending a frame containing a RELEASE command to the IVS DSRC function to terminate the session and stop the IVS DSRC function from creating a new session OR if it has failed to validate a successful receipt of the LDPU, goes back to step 6.

See Figure B.5.

B.1.7.2 Automatically repeating interrogations

A single interrogation starts with its instigation by the interrogator and the cycle terminates with the 'End of interrogation' as shown in Figure B.5.

However, there are some circumstances, for example a mobile interrogator mounted in a vehicle travelling in a lane adjacent to the target vehicles, or where a 'train' of vehicles is passing a roadside interrogator, where it is desirable to undertake continuous or repeating interrogations. In this scenario by setting the value of *s* to 1, instead of terminating its action at the end of an interrogation cycle, the interrogator then proceeds to issue another BST and repeat the transaction cycle.

The exact detail of how such a read cycle is instantiated in the interrogator is a function of interrogator design and is outside the scope of this document.

B.1.7.3 RTM operating in a multi-service environment

While Figure B.5 shows the process flow purely from the context of RTM, the architecture is designed to also support multiple service provision, via the serial reading of data for multiple applications [for example RTM and Weigh in Motion (WIM)] in a sequence.

Figure B.6 shows a similar process flow, but operating within a repeating loop, V.

In this sequence the interrogator may read one application, followed by the next and the next, until the sequence is completed or the VU moves out of range.

The exact detail of how such a loop is instantiated in the interrogator is a function of interrogator design and is outside the scope of this document.

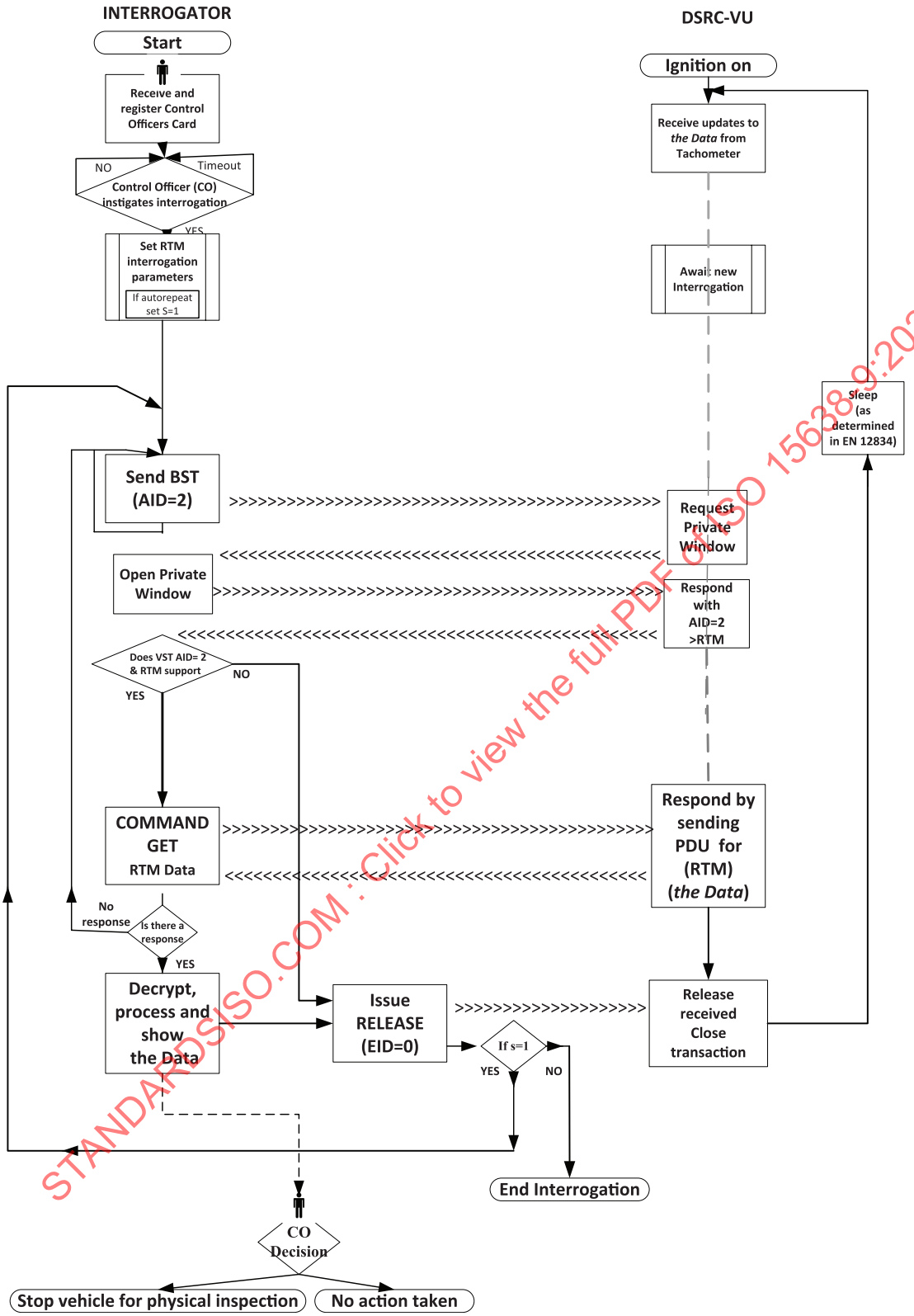
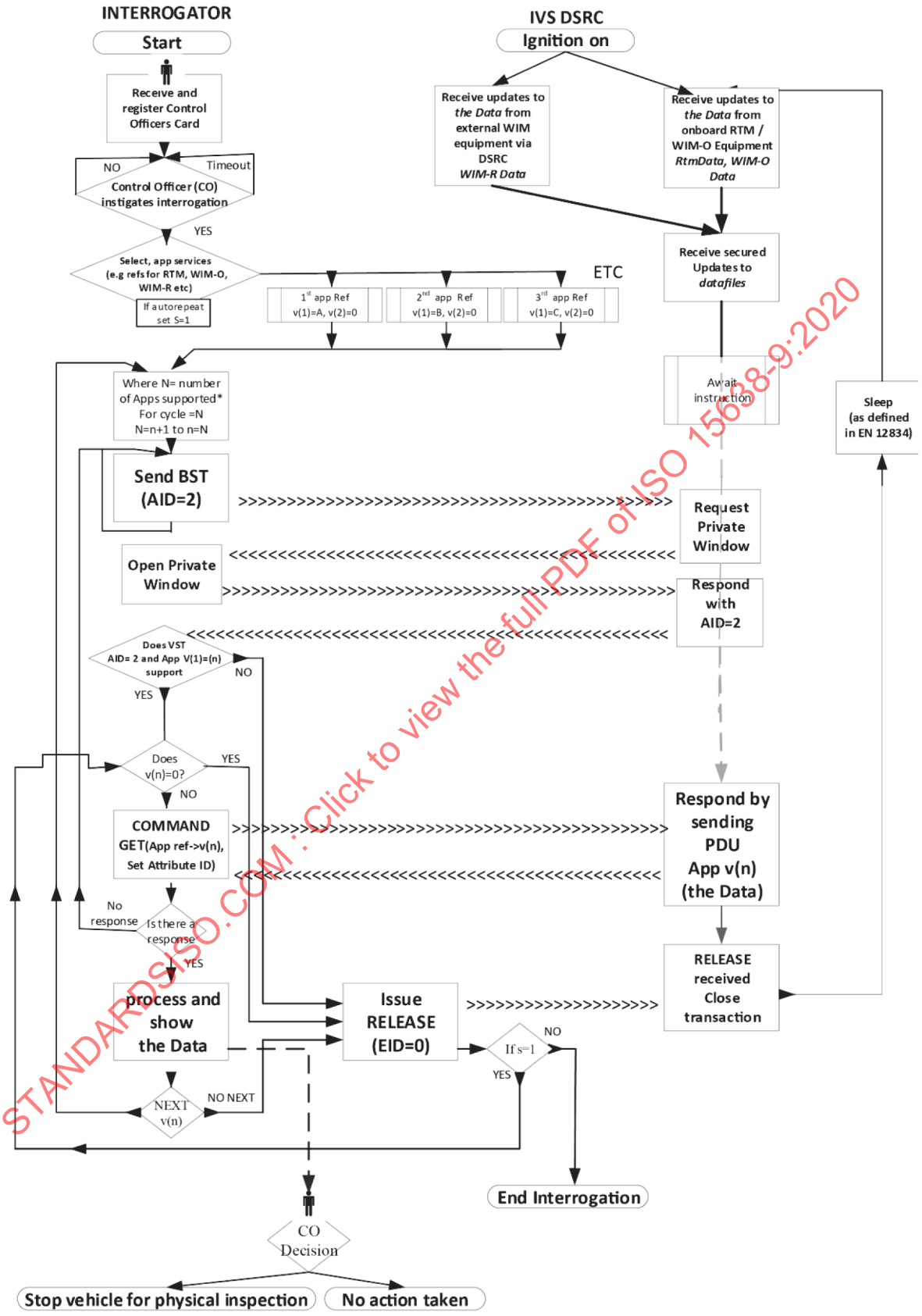


Figure B.5 — RTM over 5,8 GHz DSRC process flow



Key

N the number of applications in the sequence

N a specific application reference code (e.g. 9 = RTM, 20 = WIM etc)

Figure B.6 — Multiple application interrogation over 5,8 GHz DSRC process flow

Figures B.5 and B.6, describe the situations for Communication Profile C1.

For Communication Profile C2, while the start of the interrogation is the same sequence, the response to the “request" is simply an acknowledgement. The data is then sent by other means to the enquirer (via the application service provider, as defined in Communication Profile C3.).

B.1.7.4 Commands

The following commands are the only functions used in an RTM transaction phase

RTM-InitialiseComm-Request	A command, issued from the interrogator in the form of a broadcast with definition of applications that the interrogator supports.
InitialiseComm-Response	An answer from the IVS-DSRC confirming the connection and containing a list of supported application instances with characteristics and information how to address them (EID).
RTM-DataRetrieval-Request	A command, issued from the interrogator to the DSRC-VU, that specifies the application instantiation to be addressed by means of a defined EID, as received in the VST, instructing the IVS-DSRC to send the selected attribute(s) with the data. The objective of the RTM-DataRetrieval-Request is for the interrogator to obtain the data from the DSRC-VU.
DataRetrieval-Response	An answer from the IVS-DSRC that contains the data requested.
RTM-DeliverData-Request	A command, issued from the interrogator to the DSRC-VU, that specifies the application instantiation to be addressed by means of a defined EID, as received in the VST, instructing the IVS-DSRC to retrieve the selected attribute(s) with the Data and transfer it to the Service Provider identified by a specific URL. The objective of the RTM-DeliverData-Request command is for the interrogator to make the DSRC-VU deliver the data to a Service Provider.
RTM-DeliverData-Response	An answer from the DSRC VU on the RTM-DeliverData-Response command.
RTM-TestComm-Request	A command, instructing the IVS-DSRC to send back data from the IVS-DSRC to the interrogator. The objective of the RTM-DeliverData-Request command is to enable workshops or test facilities to test that the DSRC link is working without needing access to security credentials.
RTM-TestComm-Response	An answer from the DSRC VU on the RTM-TestComm-Request command.

RTM-TerminateComm	A command, instructing the IVS-DSRC that the transaction is ended. The objective of this command is to end the session with the DSRC-VU. On receipt of this command the IVS-DSRC shall not respond to any further interrogations under the current connection. Note that according to EN 12834 an IVS-DSRC will not connect twice to the same interrogator unless it has been out of the communication zone for 255 seconds or if the Beacon ID of the interrogator is changed. The objective of this command is to end the session with the IVS. On receipt of the this command the IVS shall not respond to any further interrogations for a period of approximately 60 seconds, after which it shall return to its normal functionality. NOTE This is to prevent the IVS DSRC repetitively responding to interrogation while still within the zone of short-range communication with the interrogator, thus blocking the communication channel.
NOTE The CEN DSRC standards include other commands, but they are not used in, and inappropriate for, the RTM application.	

B.1.8 Data structures

The semantic structure of the data when passed across the DSRC shall be as defined in B.1.6 and B.2.1.5. The way these data are technically structured is specified in this clause.

The payload data shall be received, encrypted, by the IVS DSRC, and shall be passed, as already encrypted, as the LPDU 'payload data' concept across the DSRC to the DSRC-interrogator.

The 'payload' element of the LPDU shall conform to a data concept defined in Annex C or take into consideration the data requirements of a jurisdiction.

B.1.9 Interaction process

B.1.9.1 Window management

B.1.9.1.1 General

The following subclauses provide an explanation of the window management interaction process that is defined in EN 12795.

As defined in EN 12795, public and private downlink/uplink windows are distinguished by their 'logical link control identifier' LID, whether a broadcast LID or a private LID is present.

Besides these situations, there is a third, the minimum time gap between an uplink followed by a downlink (T1). This corresponds to 32 µs.

B.1.9.1.2 Example of frame exchange

Figure B.7 (for information) describes an example of the ideal exchange of frames between the fixed and the mobile equipment and also the communication primitives within the logical link control (LLC).

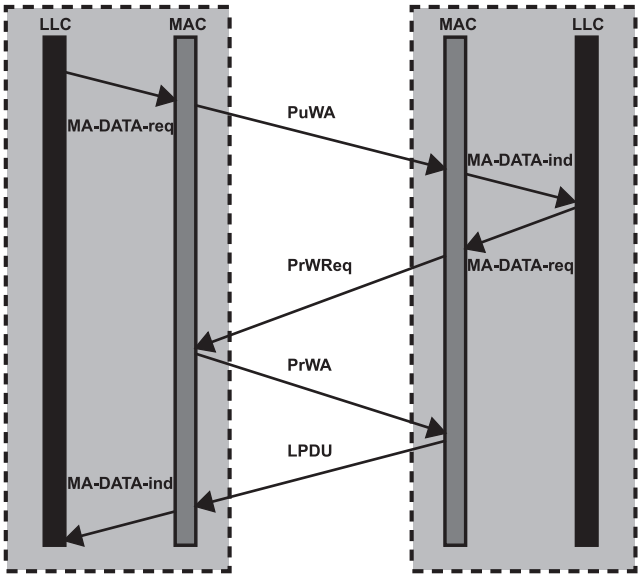


Figure B.7 — Communication example between interrogator and IVS

B.1.9.1.3 State machine

B.1.9.1.3.1 MA-DATA.request

The primitive is passed from the LLC sublayer to the MAC sublayer to request that an LPDU is transmitted in the first available downlink window (EN 12795).

For the RTM application, this equates to the GET_RTM_LPDU command. In 5,8 GHz DSRC standards, at the first level of the interrogation transaction it is known as the MA-DATA.request.

The primitive provides the following parameters:

MA-DATA.request(LID, LPDU, RR)

The link identifier (LID) is the LID of the service access point (SAP) for which the frame is intended. It may be a private LID, the broadcast LID or a multicast LID.

The LPDU may be null (in this case no LPDU is included in the frame transmitted).

The response request (RR) indicates whether or not the fixed equipment allocates an uplink window in immediate connection to the downlink frame transmitted.

In the public window, only the request for a private window is made and no LPDU is transferred. Once the private window is granted, the MA-DATA.request is made (GET_RTM_LPDU [Value for RTM = 9]) and the frame of RTM data will be provided by the IVS to the interrogator.

B.1.9.1.3.2 MA-DATA.indication

The primitive is passed from the MAC sublayer to the LLC sublayer to indicate the successful reception of a valid frame from a mobile SAP.

The primitive provides the following parameters

MA-DATA.indication (LID, LPDU)

The LID is the content of the link address field of the frame received.

B.1.9.2 Behaviour of the IVS

The behaviour of the IVS, when it is within the range of the interrogator can be described in the state machine, shown (for information) in Figure B.8.

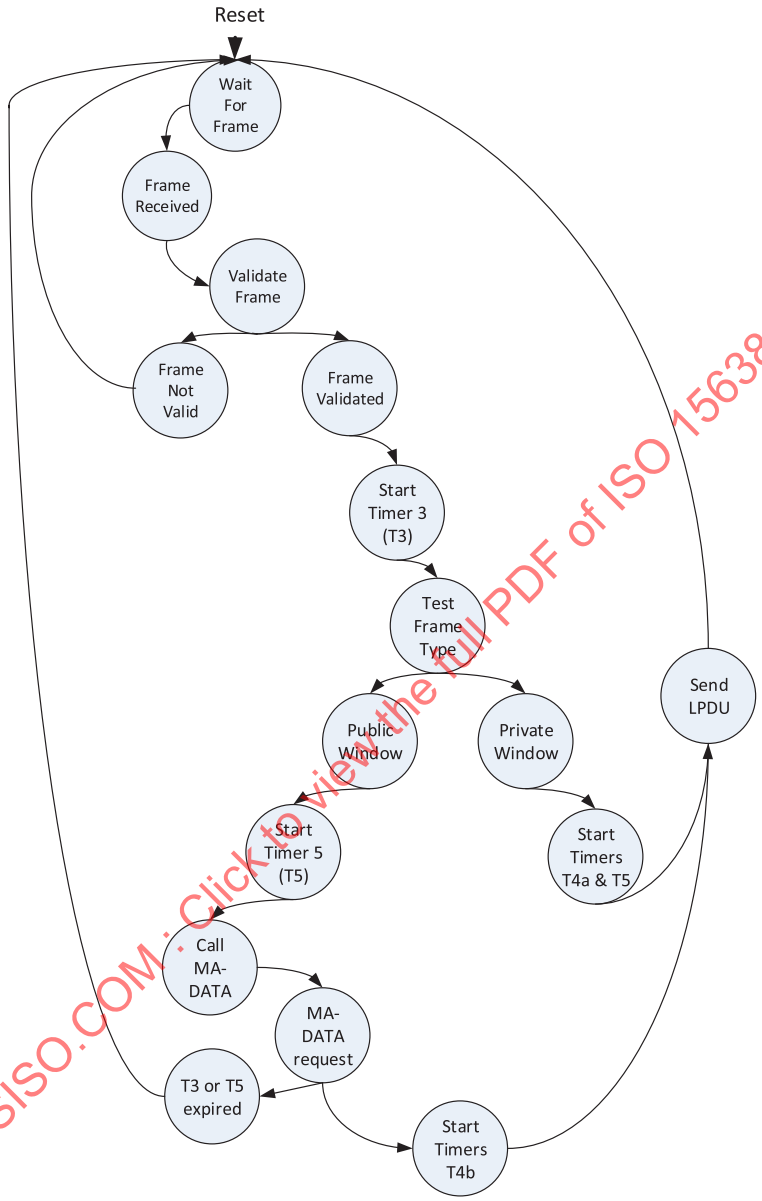


Figure B.8 — State machine describing the MAC layer behaviour of the IVS

B.1.9.3 State transitions

B.1.9.3.1 The following paragraphs explain the process, state by state, and the corresponding transition conditions are indicated. The discussion is separated between 'public' and 'private' allocation, beginning in the point where the state machine finishes the common steps.

B.1.9.3.2 'Wait for frame'

In this state, the IVS is waiting for a new input proceeding from the interrogator, whether it is the first or any other frame, during the communication.

— Transition condition: the reception of a new frame.

B.1.9.3.3 'Validate Frame/ Start Timer3 (T3)'

In this state, the frame is validated by comparison with the pre-defined format, particularly the Cyclic Redundancy Check (CRC). Timer3 (T3) is enabled. This timer is used to control both situations (Public or a Private Uplink Window).

— Transition conditions: If an error occurs during the validation, the process returns to 'Wait for frame'. If not, it advances to the following state.

B.1.9.3.4 'Test frame type' state

Here the distinction is made between a PuWA (Public Window Allocation) and PrWA (Private Window Allocation).

— Transition conditions: If the frame received is a PuWA, advances to 'Start Timer5 (T5)/ Call the MA-DATA-ind' state. If it is a PrWA, advances to 'Start Timers4a, 5 (T4a, T5)'.

For information, Figure B.9 shows the state machine concerning only the Public Uplink.

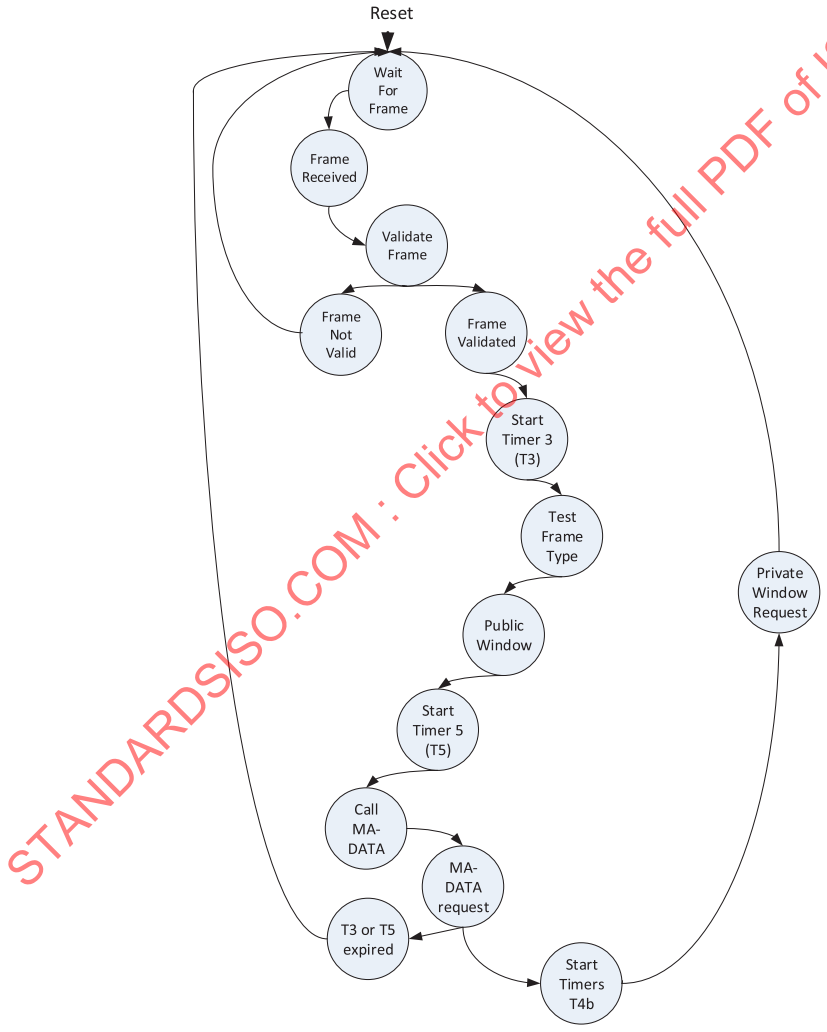


Figure B.9 — State machine concerning only the Public Uplink

B.1.9.3.5 'Start Timer 5 (T5)/ Call the MA-DATA-ind'

The Timer 5 (T5) is enabled. This timer controls the time duration of the uplink window. Function MA-DATA-ind is called. This is the pre-defined MAC service primitive to communicate into the logical link control.

— Transition conditions: If T3 or T5 expires, the process will end and return to the initial state 'Wait for frame'. If the response is a request, through MA-DATA_req, the state will change to the 'Start Timer4b (T4b) state'.

B.1.9.3.6 'Start Timer4b (T4b)'

This is quite a simple state that just starts the Timer4b (T4b), to control the correct time to send the information. PrWReq is sent and the process returns to the 'Wait for frame' state.

— Transition condition: PrWReq is sent.

B.1.9.3.7 Private window allocation

Figure B.10 illustrates the state machine concerning only the Private Uplink.

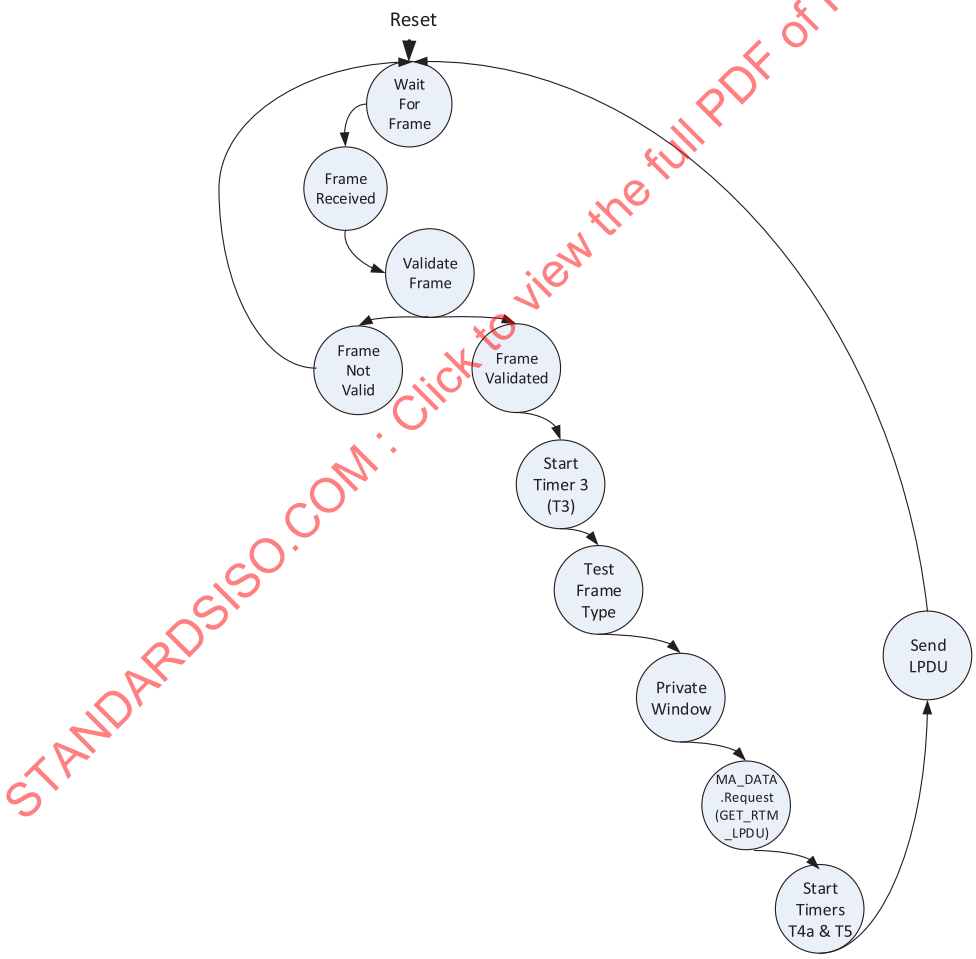


Figure B.10 — State machine concerning only the Private Uplink branch

The transactions/sequence shall be as defined in EN 12795.

If in the 'Test frame type' state a PrWA is detected, the following state will be 'Start Timers4a, 5 (T4a, T5)'.

B.1.9.3.8 'Start Timers4a, 5 (T4a, T5)

Both Timer4a (T4a) and Timer5 (T5) are enabled, to proceed with information sent.

— Transition condition: The pending LPDU is sent.

B.1.9.3.9 Context marks

Context marks are not used in the RTM applications.

B.2 5,8 GHz DSRC Functions for RTM

B.2.1 Functions in detail

B.2.1.1 General

Subclauses B.2.1.2 to B.2.1.6 define the functions for EN 5,8 GHz DSRC only. For other supported media, consult the referenced standard.

B.2.1.2 Security and encryption

The detail of security and encryption measures regarding data made available and supplied across the 5,8 GHz DSRC link is no included in the provisions of this document. This document assumes that data is provided to the DSRC as a data concept for transfer already encrypted, together with a security data concept for encryption data (keys etc.) and shall be structured as defined in 9.6 and B.1.6.5.

B.2.1.3 Creating and maintaining data

The means by which the IVS obtains and updates the data pantry of the IVS is outside the scope of this document, though may be determined in accordance with the data requirements of the jurisdiction, may be in accordance with other international, regional or national standards, or may be a combination of two or more of these.

This document assumes that RTM data is made available to the data pantry of the IVS, already encrypted, and including security data, as a combined data concept value, such that it can be provided to/accessed upon receipt of a command for data from the interrogator, via the 5,8 GHz DSRC.

B.2.1.4 Initialise communication

Initialisation of the communication shall be induced by the interrogator. The invocation of an initialisation request by the interrogator attempts to initialise communication between interrogator and IVS. After successful initialisation, the function "Initialise communication" shall notify the applications on the interrogator and IVS sides.

Initialisation shall be carried out in accordance with EN 12795 and B.1.

B.2.1.5 Data transfer mechanism

Payload data defined previously are requested by the interrogator after initialisation phase, and consequently transmitted by the IVS in the allocated window. The command GET is used by the interrogator to retrieve data.

For all DSRC exchanges, data shall be encoded using PER (Packed Encoding Rules).

B.2.1.6 Detailed DSRC transaction description

As described in B.1.

The following tables give a practical example of an interrogation session.

In the Initialisation phase, the interrogator starts sending a BST. See Table B.9.

Table B.9 — Initialisation — BST frame settings

Field	Settings
Link Identifier	Broadcast address
BeaconId	As per EN 12834
Time	As per EN 12834
Profile	No extension
MandApplications	No extension, EID not present, Parameter not present, AID = 2 Freight&Fleet
NonMandApplications	Not present
ProfileList	No extension, number of profiles in list = 0
Fragmentation header	No fragmentation
Layer 2 settings	Command PDU, UI command

A practical example of the settings specified in Table B.9, with an indication of bit encodings, is given in the following Table B.10.

Table B.10 — Initialisation — BST frame contents example

Octet #	Attribute field	bits in octet	Description
1	FLAG	0111 1110	Start flag
2	Broadcast ID	1111 1111	Broadcast address
3	MAC Control Field	1010 s000	Command PDU
4	LLC Control field	0000 0011	UI command
5	Fragmentation header	1xxx x001	No fragmentation
6	BST	1000	Initialisation request
	SEQUENCE {		
	OPTION	0	NonMand applications not present
	indicator BeaconID SEQUENCE {		
	ManufacturerId	Xxx	Manufacturer Identifier
	(INTEGER(0..65535)		
7		xxxx xxxx	
8		xxxx x	
	IndividualID (0..134217727)	Xxx	27 bit ID available for manufacturer
9		xxxx xxxx	
10		xxxx xxxx	
11		xxxx xxxx	
	}		
12	Time INTEGER(0..4294967295)	xxxx xxxx	32 bit UNIX real time
13		xxxx xxxx	
14		xxxx xxxx	
15		xxxx xxxx	
16	Profile INTEGER (0..127,...)	0000 0000	No extension. Example profile 0
17	MandApplications SEQUENCE (SIZE(0..127,...)) OF {	0000 0001	No extension, Number ofmandApplications = 1

Table B.10 *(continued)*

Octet #	Attribute field	bits in octet	Description
18	SEQUENCE { OPTION indicator	0	EID not present
	OPTION indicator	0	Parameter not present
	AID DSRCApplicationEntityID } }	00 0010	No extension. AID = 2 Freight&Fleet
19	ProfileList SEQUENCE (0..127,...) OF Profile }	0000 0000	No extension, number of profiles in list = 0
20	FCS	xxxx xxxx	Frame check sequence
21		xxxx xxxx	
22	Flag	0111 1110	End Flag

An IVS-DSRC, when receiving a BST, requires the allocation of a private window, as specified by EN 12795 and EN 13372, 7.1.1, with no specific RTM settings. Table B.11 provides an example of bit encoding.

Table B.11 — Initialisation — Private window allocation request frame contents

Octet #	Attribute field	bits in octet	Description
1	FLAG	0111 1110	Start flag
2	Private LID	xxxx xxxx	Link address of specific IVS DSRC
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	0110 0000	Private window request
7	FCS	xxxx xxxx	Frame check sequence
8		xxxx xxxx	
9	Flag	0111 1110	End Flag

The interrogator then answers by allocating a private window, as specified by EN 12795 and EN 13372, 7.1.1 with no specific RTM settings.

Table B.12 provides an example of bit encoding.

Table B.12 — Initialisation — Private window allocation frame contents

Octet #	Attribute field	bits in octet	Description
1	FLAG	0111 1110	Start flag
2	Private LID	xxxx xxxx	Link address of the specific IVS DSC
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	0010 s000	Private window allocation
7	FCS	xxxx xxxx	Frame check sequence
8		xxxx xxxx	
9	Flag	0111 1110	End Flag

The IVS DSRC, when receiving the private window allocation, sends its VST (Vehicle Service Table) as defined in EN 12834 and EN 13372, 6.3.2, 7.1.1, and 7.1.3 with settings as specified Table B.13, using the allocated transmission window.

Table B.13 — Initialisation — VST frame settings

Field	Settings
Private LID	As per EN 12834
VST parameters	Fill = 0, then for each supported application: EID present, parameter present, AID = 2, EID as generated by the OBU
Parameter	No extension, Container choice 11, followed by RTM Context Mark
ObeConfiguration	The optional ObeStatus field shall not be used
Fragmentation header	No fragmentation
Layer 2 settings	Command PDU, UI command

The IVS-DSRC shall support the "Freight and Fleet" application, identified by the Application Identifier '2'. Other Application Identifiers may be supported, but shall not be present in this VST, as the BST only requires AID = 2. The "Applications" field contains a list of the supported application instances in the IVS-DSRC. For each supported application instantiation, a reference to the appropriate standard is given, made of an Rtm Context mark, which is composed of an OBJECT IDENTIFIER representing the related standard, its part (9 for RTM) and possibly its version, and possibly an identifier of the Communication Profile, plus an EID that is generated by the IVS-DSRC, and associated to that application instance.

A practical example of the settings specified in Table B.13, with an indication of bit encodings, is given in Table B.14, where the IVS-DSRC only supports Communication Profile C1.

Table B.14 — Initialisation — VST frame contents example with only C1 support

Octet #	Attribute field	bits in octet	Description
1	FLAG	0111 1110	Start flag
2	Private LID	xxxx xxxx	Link address of the specific IVS DSRC
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1100 0000	Command PDU
7	LLC Control field	0000 0011	UI command
8	Fragmentation header	1xxx x001	No fragmentation
9	VST SEQUENCE { Fill	1001	Initialisation response
		0000	Unused and set to 0
10	Profile INTEGER (0..127,...) Applications SEQUENCE OF {	0000 0000	No extension. Example profile 0 No extension, 1 application
11		0000 0001	
12	SEQUENCE { OPTION indicator OPTION indicator AID DSRCApplicationEntityID	1	EID present
		1	Parameter present
		00 0010	No extension. AID = 2 Freight&Fleet

Table B.14 *(continued)*

Octet #	Attribute field	bits in octet	Description
13	EID Dsrc-EID	xxxx xxxx	Generated by the IVS DSRC function and identifying the application instance.
14	Parameter Container	0000 0010	No extension, Container Choice = 0210, Rtm Context Mark, Octet string
15		0000 1000	No extension, Rtm Context Mark length = 810
16	Rtm-ContextMark ::= SEQUENCE { StandardIdentifier, }	0000 0101	Object Identifier of the supported standard, part, and version. Example: ISO (1) Standard (0) TARV (15638) part9(9) Version1 (1).
17		0010 1000	
18		1111 1010	
19		0001 0110	
20		0000 1001	
21		0000 0001	
22	ObeConfiguration Sequence { OPTION indicator EquipmentClass INTEGER (0..32767)	0	ObeStatus not present
		xxx xxxx	
23		xxxx xxxx	
24	ManufacturerId INTEGER (0..65535) }	xxxx xxxx	Manufacturer identifier for the DS-RC-VU. See ISO 14816 Register.
25		xxxx xxxx	
26	FCS	xxxx xxxx	Frame check sequence
27		xxxx xxxx	
28	Flag	0111 1110	End Flag

Table B.15 shows an example of VST generated by an IVS-DSRC that supports Communication Profile C1 and Communication Profile C2.

Table B.15 — Initialisation (RTM-InitialiseComm-Request) — VST frame contents example with C1 and C2 support

Octet #	Attribute field	bits in octet	Description
1	FLAG	0111 1110	Start flag
2	Private LID	xxxx xxxx	Link address of the specific VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1100 0000	Command PDU
7	LLC Control field	0000 0011	UI command
8	Fragmentation header	1xxx x001	No fragmentation

Table B.15 *(continued)*

Octet #	Attribute field	bits in octet	Description
9	VST SEQUENCE {	1001	Initialisation response
	Fill	0000	Unused and set to 0
10	Profile INTEGER (0..127,...)	0000 0000	No extension. Example profile 0
11	Applications SEQUENCE OF {	0000 0010	No extension, 2 applications
12	SEQUENCE {	1	EID present
	OPTION indicator	1	Parameter present
	OPTION indicator AID DSRCApplicationEntityID	00 0010	No extension. AID = 2 Freight&Fleet
13	EID Dsrc-EID	xxxx xxxx	Generated by the OBU and identifying the application instance.
14	Parameter Container {	0000 0010	No extension, Container Choice = 02_{10}, Rtm Context Mark, Octet string
15		0000 1001	No extension, Rtm Context Mark length = 9_{10}
16	Rtm-ContextMark ::= SEQUENCE {	0000 0101	Object Identifier of the supported standard, part, and version. Example: ISO (1) Standard (0) TARV (15638) part9(9) Version1 (1)
17		0010 1000	
18	standardIdentifier, rtmCommProfile }	1111 1010	
19		0001 0110	
20		0000 1001	
21		0000 0001	
23		0000 0001	Communication Profile C1
24	SEQUENCE {	1	EID present
	OPTION indicator	1	Parameter present
	OPTION indicator AID DSRCApplicationEntityID	00 0010	No extension. AID = 2 Freight&Fleet
25	EID Dsrc-EID	xxxx xxxx	Generated by the OBU and identifying the application instance.
26	Parameter Container {	0000 0010	No extension, Container Choice = 02_{10}, Rtm Context Mark, Octet string
27		0000 1001	No extension, Rtm Context Mark length = 9_{10}
28	Rtm-ContextMark ::= SEQUENCE {	0000 0101	Object Identifier of the supported standard, part, and version. Example: ISO (1) Standard (0) TARV (15638) part9(9) Version1 (1).
29		0010 1000	
30	standardIdentifier, rtmCommProfile }	1111 1010	
31		0001 0110	
32		0000 1001	
33		0000 0001	
34		0000 0010	Communication Profile C2

Table B.15 *(continued)*

Octet #	Attribute field	bits in octet	Description
35	ObeConfiguration Sequence {		
	OPTION indicator	0	ObeStatus not present
	EquipmentClass INTEGER (0..32767)	xxx xxxx	
36		xxxx xxxx	
38	ManufacturerId INTEGER (0..65535) }	xxxx xxxx	Manufacturer identifier for the DSRC-VU. See ISO 14816 Register.
39	FCS	xxxx xxxx	Frame check sequence
40		xxxx xxxx	
41	Flag	0111 1110	End Flag

In the case of Communication Profile C1, the interrogator then reads the data by issuing a GET command, conforming to the GET command defined in EN 12834, with settings as specified in Table B.16.

Table B.16 — Presentation — GET request (RTM-DataRetrieval-Request) frame settings

Field	Settings
Invoker Identifier (IID)	Not present
Link Identifier (LID)	Link address of the specific IVS DSRC
Chaining	No
Element Identifier (EID)	As specified in the VST. No extension
Access Credentials	No
AttributeIdList	No extension, 1 attribute, AttributeID = 1 (RtmData)
Fragmentation	No
Layer2 settings	Command PDU, Polled ACn command

Table B.17 shows an example of reading the RTM data that belong to the TARV suite of standards.

Table B.17 — Presentation — Get Request (RTM-DataRetrieval-Request) frame example

Octet #	Attribute field	bits in octet	Description
1	FLAG	0111 1110	Start flag
2	Private LID	xxxx xxxx	Link address of the specific IVS DSRC
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1010 s000	Command PDU
7	LLC Control field	n111 0111	Polled ACn command, n bit
8	Fragmentation header	1xxx x001	No fragmentation

Table B.17 *(continued)*

Octet #	Attribute field	bits in octet	Description
9	RTM-DataRetrieval-Request	0110	Get request
	SEQUENCE {	0	Access Credentials not present
	Option	0	IID not present
	Option	1	Attribute List present
	Option	0	Set to 0.
	Fill BIT STRING(SIZE(1)) }		
10	EID (INTEGER(0..127)	xxxx xxxx	The EID of the RTM application instance, as specified in the VST. No extension
11	AttributeIdList SEQUENCE OF { AttributeId }	0000 0001	No extension, number of attributes = 1
12		0000 0001	AttributeId = 1, RtmData. No extension
13	FCS	xxxx xxxx	Frame check sequence
14		xxxx xxxx	
15	Flag	0111 1110	End Flag

In the Communication Profile C1, the IVS-DSRC, when receiving the RTM-DataRetrieval-Request, sends a DataRetrieval-Response with the requested data conforming to the GET response defined in EN 12834, with settings as specified in Table B.18.

Table B.18 — Presentation — GET response (DataRetrieval-Response) frame settings

Field	Settings
Invoker Identifier (IID)	Not present
Link Identifier (LID)	As per EN 12834
Chaining	No
Element Identifier (EID)	As specified in the VST.
Access Credentials	No
Fragmentation	No
Layer2 settings	Response PDU, Response available and command accepted, ACn command

Table B.19 shows an example of reading the RTM data that belong to the TARV series of standards.

Table B.19 — Presentation — Response frame contents example

Octet #	Attribute field	bits in octet	Description
1	FLAG	0111 1110	Start flag
2	Private LID	xxxx xxxx	Link address of the specific IVS DSRC
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1101 0000	Response PDU
7	LLC Control field	n111 0111	Response available, ACn command n bit
8	LLC Status field	0000 0000	Response available and command accepted
9	Fragmentation header	1xxx x001	No fragmentation