INTERNATIONAL STANDARD

ISO 15638-20

First edition
2020-07

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

Part 20: Weigh-in-motion monitoring

Reference number
ISO 15638-20:2020(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*.

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.

The ISO 15638 series of standards defines and addresses 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 of standards 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 of standards 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.

Consistent with other parts of the ISO 15638 series of standards, this document does not prescribe nor proscribe particular modes of operation. Rather, it provides a number of defined communication and data profiles within which jurisdictions may achieve their objectives for remote weigh-in-motion monitoring within the objectives and constraints of their regulations. This document recognizes that those requirements and constraints will differ between jurisdictions.

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

Part 20: Weigh-in-motion monitoring

1 Scope

This document addresses the provision of 'weigh-in-motion 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 both on-board weighing (WIM-O) systems and in-road "weigh-in-motion" (WIM-R) systems, and provides a profile where the vehicle weight measured is recorded on-board using equipment already installed for "Remote Tachograph Monitoring".

This document provides specifications for common communications and data exchange aspects of the application service weigh-in-motion monitoring (WIM-O and WIM-R) 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 has to provide (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 has to deliver, 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.

The present version of this document provides specifications for the following application profiles:

— **Application Profile A1: Vehicle weight measurement from "On-Board Weighing" systems (WIM-O);**

— **Application Profile A2: Vehicle weight measurement from in-road 'weigh-in-motion' systems where data is transferred to the IVS (WIM-R).**

NOTE 1 Vehicle weight measurement from in-road 'weigh-in-motion' systems where data is linked to a specific vehicle by ANPR or other techniques and sent via landline or cellular communications to a processing centre is also a viable and alternate option, but as it does not include carrying data on-board the vehicle is not a TARV use case.

The present version of this document provides specifications for the following communication profiles:

— **Communication Profile 1: 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 2: 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 3: 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).

Subsequent versions of this document can support additional communication profiles.

NOTE 2 The ISO 15638 series of standards has been developed for use in the context of regulated commercial freight vehicles (hereinafter referred to as 'regulated vehicles'). There is nothing, however, 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 11898-1, *Road vehicles — Controller area network (CAN) — Part 1: Data link layer and physical signalling*

ISO 15638-1, *Intelligent transport systems — Framework for cooperative telematics applications for regulated vehicles (TARV) — Part 1: Framework and architecture*

ISO 15638-2, *Intelligent transport systems — Framework for cooperative telematics applications for regulated 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*

ISO 15638-9, *Intelligent transport systems — Framework for cooperative telematics applications for regulated commercial freight vehicles (TARV) — Part 9: Remote digital tachograph monitoring*

EN ETSI 300 674-1, *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)*

ARIB STD-T75, *Dedicated Short-Range Communication (Japan)*

TTAS KO-06.0025, Standard of *DSRC* Radio Communication between Road-side Equipment and On-board Equipment in 5.8 GHz band (Korea)

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 12834:2003, *Road transport and traffic telematics — Dedicated Short Range Communication (DSRC) — DSRC application layer*

EN 13372:2012, *Road transport and traffic telematics — Dedicated Short Range Communication (DSRC) — Profiles for RTTT applications*

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™* (3.23) applets, organized as software bundles, that support *application services* (3.3) by keeping the *data pantry* (3.16) provisioned with up to date data

3.2
application profile
characteristics and specification of the information and transaction detail required to meet a set of *user* (3.49) needs which within the common high-level *framework* (3.19) of this document, allows different *jurisdictions* (3.24) to receive different detail of transaction or to specify a particular communications means

3.3
application service
service provided by a *service provider* (3.44) enabled by accessing data from the *IVS* (3.19) of a *regulated vehicle* (3.43) via a wireless communications network

3.4
application service provider
ASP
party that provides an *application service* (3.3)

3.5
app library
separately secure area of memory in *IVS* (3.19) where apps are stored [with different access controls to *data pantry* (3.16)]

3.6
approval
formal affirmation that an applicant has satisfied all of the requirements for appointment as an *application service provider* (3.4) or that an *application service* (3.3) delivers the required service levels

3.7
approval agreement
written agreement made between an *approval authority (regulatory)* (3.8) and a *service provider* (3.44)

Note 1 to entry: An *approval authority (regulatory)* (3.8) *approval agreement* recognizes the fact that a *service provider* (3.44), 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.*

3.8
approval authority
<regulatory> organization (usually independent) which conducts *approval* (3.6) and ongoing *audit* (3.10) for *service providers* (3.44) on behalf of a *jurisdiction* (3.24)

3.9
architecture
formalized description of the design of the structure of *TARV* and its *framework* (3.19)

3.10
audit
auditing
review of a party's capacity to meet, or continue to meet, the initial and ongoing *approval agreements* (3.7) as a *service provider* (3.44)

3.11
basic vehicle data
data maintained/provided by all *IVS* (3.19) [regardless of *jurisdiction* (3.24)]

3.12
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* (3.49) determined parameters by using a suite of standards based on ISO 21217 [*CALM* (3.12) architecture] and ISO 21210 (*CALM* networking) that provide a common platform for a number of standardized media using *ITS-stations* (3.22) to provide wireless support for applications, such that the application is independent of any particular wireless medium

3.13
commercial application(s)
ITS applications in *regulated vehicles* (3.43) for commercial (non-regulated) purposes

EXAMPLE Asset tracking, vehicle and engine monitoring, cargo security, *driver* (3.17) management.

3.14
communications profile
characteristics and specification of the communication detail required to meet a set of *user* (3.49) needs using a selected wireless medium

3.15
core data
basic vehicle data (3.11) plus any additional data required to provide an implemented *regulated application service* (3.42)

3.16
data pantry
secure area of memory in *IVS* (3.19) where data values are stored [with different access controls to *app library* (3.5)]

3.17
driver
person driving the *regulated vehicle* (3.43) at any specific point in time

3.18
facilities layer
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

3.19
framework
particular set of beliefs or ideas referred to in order to describe a scenario or solve a problem

3.20
in-vehicle system
IVS
ITS-station (3.22) and connected (TARV/*WIM*) equipment on board a vehicle

Note 1 to entry: Known in EFC specific equipment as OBE (on-board equipment) or OBU (on-board unit).

Note 2 to entry: Often known in weigh-in-motion and *tachograph* (3.47) specific regulations as VU (vehicle unit).

3.21
interrogator
off-board device which can establish a wireless communications session with the IVS (including 5,8 GHz DSRC) and request the provision of weigh-in-motion data, often a mobile device under the control of an agent of the *jurisdiction* (3.24)

3.22
ITS-station
ITS-s
entity in a communication network, comprised of application, *facilities layer* (3.18), networking and access layer components specified in ISO 21217 that operate within a bounded secure management domain

3.23
Java™[1)]
object oriented open source operating language developed by SUN systems

3.24
jurisdiction
government, road or traffic authority which owns the r*egulatory applications* (3.41)

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

3.25
jurisdiction regulator
agent of the *jurisdiction* (3.24) appointed to regulate and manage *TARV* within the domain of the *jurisdiction* which may or may not be the *approval authority (regulatory)* (3.8)

3.26
on-board weighing system
generation of vehicle weight data from equipment on-board the vehicle

Note 1 to entry: The technical means of generating such data is not specified in this document, only the resultant data.

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.

3.27
operator
operator of interrogation equipment

3.28
physical roadside inspection
physical inspection of the weigh-in-motion data of a stopped vehicle by agents of the *application service provider* (3.4) [most usually police or inspectors appointed by the *jurisdiction* (3.24)]

3.29
prime service provider
service provider (3.44) who is the first contractor to provide *regulated application services* (3.42) to the *regulated vehicle* (3.43), or a nominated successor on termination of that initial contract, responsible to maintain the installed *IVS* (3.19) and to install and commission new *IVS* (3.19)

3.40
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

3.41
regulated application
regulatory application
application arrangement using TARV utilized by *jurisdictions* (3.24) 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*

Note 1 to entry: May be mandatory or voluntary at the discretion of the *jurisdiction.*

3.42
regulated application service
TARV application service (3.3) to meet the requirements of a regulated application (3.41) that is mandated by a regulation imposed by a *jurisdiction* (3.24), or is an option supported by a *jurisdiction*

3.43
regulated vehicle
vehicle that is subject to regulations determined by the *jurisdiction* (3.24) 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*

Note 1 to entry: At the option of *jurisdictions,* this may require the provision of information via *TARV* or provide the option to do so.

3.44
service provider
party which is certified by an *approval authority (regulatory)* (3.8) as suitable to provide regulated or commercial ITS *application services* (3.3)

3.45
session
wireless communication exchange between the *ITS-station* (3.22) of an *IVS* (3.19) and the *ITS-station* of its *application service provider* (3.4) to achieve data update, data provision, upload apps, or otherwise manage the provision of the *application service* (3.3), or a wireless communication provision of data to the *ITS-station* of an *IVS* (3.19) from any other *ITS-station*

3.46
specification
explicit and detailed description of the nature and functional requirements and minimum performance of equipment, service or a combination of both

3.47
tachograph
sender unit usually mounted to a vehicle gearbox, a tachograph head and a digital *driver* (3.17) card, which records the *regulated vehicle* (3.43) speed and the times at which it was driven and aspects of the *driver's* (3.17) activity selected from a choice of modes

3.48
telematics
use of wireless media to obtain and transmit (data) from a distant source

3.49
user
individual or party that enrols in and operates within a regulated or *commercial application* (3.13) *service* (3.2)

EXAMPLE *Driver* (3.17), fleet manager, freight owner.

3.50
weigh-in-motion
weigh-in-motion system
generation of vehicle weight data from equipment either onboard (WIM-O) or embedded in the road pavement (WIM-R) and transferred to the *IVS* (3.20) of the vehicle ready for subsequent inspection

Note 1 to entry: The technical means of generating such data is not specified in this document, only the resultant data.

3.51
weigh-in-motion system-onboard
WIM-O
generation of vehicle weight data from equipment within the vehicle

Note 1 to entry: The technical means of generating such data is not specified in this document, only the resultant data.

3.52
weigh-in-motion system-roadway
WIM-R
generation of vehicle weight data from equipment embedded in the road pavement and transferred to the *IVS* (3.20) of the vehicle ready for subsequent inspection

Note 1 to entry: The technical means of generating such data is not specified in this document, only the resultant data.

4 Symbols and abbreviated terms

ADU	Application Data Unit
APDU	application protocol data unit
ANPR	Automatic number plate recognition
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)
LDT	Local data tree
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)
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 weigh-in-motion IVS)
WIM	Weigh-in-Motion
WIM-O	Weigh-in-Motion from onboard equipment
WIM-R	Weigh-in-Motion from in-road equipment
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 applications (Application Profiles 1 and/or 2) as defined in Clause 1, but shall support at least one of these options.

Systems claiming conformance with this document may support one or more of Communication Profiles 1, 2 and 3 as defined in Clause 1, but shall support at least one of these options.

6 General overview and framework requirements

6.1 General

This document addresses the provision of 'weigh-in-motion monitoring' and specifies the form and content of the transmission of such data required to support such systems and access methods to that data. The data may be transferred by a variety of means (as ITS-station -:- ITS-station data transfers in a C-ITS environment using 5,9 GHz, 3G, 4G, LTE or similar) transfers using interrogations from short range dedicated communication systems (such as 5,8 GHz) or other agency approved methods.

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 understanding 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 Application Profiles:

— **Application Profile A1: The generation of vehicle weight data from equipment on-board the vehicle (WIM-O)**

  The technical means of generating such data is not specified in this document, only the resultant data.

— **Application Profile A2: The generation of vehicle weight data from equipment embedded in the road pavement and transferred to memory on-board (WIM-R)**

  The technical means of generating such data is not specified in this document, only the resultant data.

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).

Jurisdictions requiring and regulating the use of remotely monitored WIM-O/WIM-R systems are recommended to specifically regulate in the case of the use of Communication Profile 1 and/or Communication Profile 2, and for each Application Profile. It is further recommended (but not required) that jurisdictions whose data requirements require support of Profile 1 for regulatory enforcement purposes also at least encourage the ability to technically support Profiles 2 and 3 in addition (for later potential migration purposes).

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 (e.g. 5,8 GHz DSRC) to remotely identify a vehicle which is potentially in violation of the vehicle weight regulations of the jurisdiction;

b) Once identified, the agent of the jurisdiction controlling the interrogation may use the data in accordance with the enforcement data requirements of the jurisdiction. or decide whether the vehicle should be stopped, and if so, instruct colleagues downstream to stop the vehicle.

This last 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 Communication 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 is made via short range communication such as 5,8 GHz DSRC, taking into consideration the data requirements of the jurisdiction. See Figure 1.

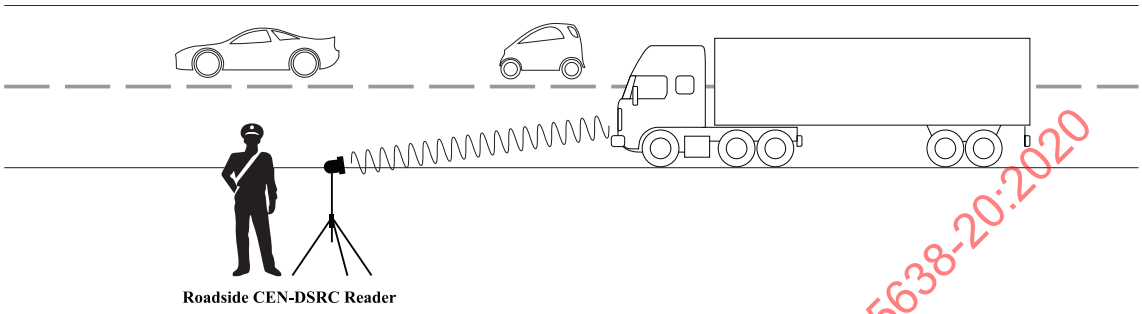


Figure 1 — Use case 1: C1a-roadside interrogation using short range communication

6.2.1.2 Communication 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 is made via short range communication such as 5,8 GHz DSRC), taking into consideration the data requirements of the jurisdiction. See Figure 2.

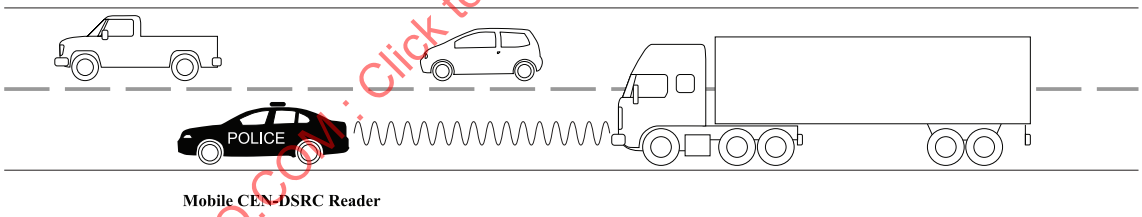


Figure 2 — Use case 2: C1b-vehicle based interrogation using short range communication

6.2.1.3 Communication 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 is made via short range communication such as 5,8 GHz DSRC), taking into consideration the data requirements of the jurisdiction. See Figure 3.

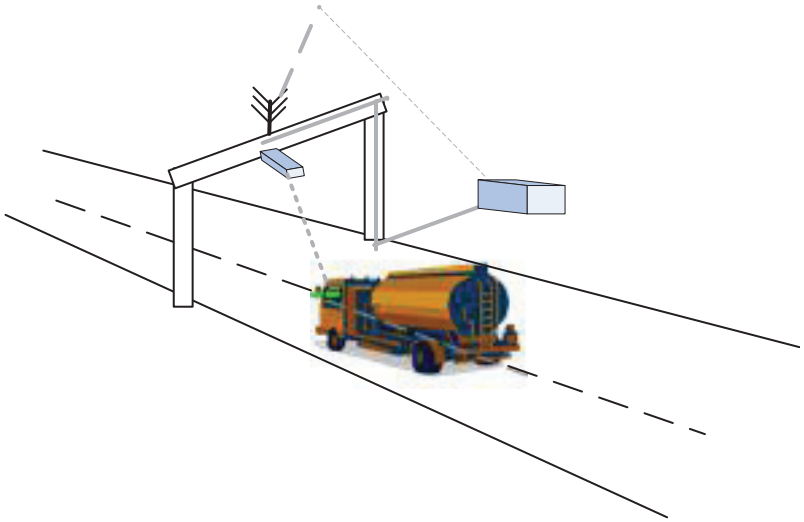


Figure 3 — Gantry mounted interrogator using short range communication

6.3 Overview of Communication Profile 2 — 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 2

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

a) Uses a short range communication interrogator (e.g. 5,8 GHz DSRC) to remotely identify a vehicle which is potentially in violation of the vehicle weight 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 DSRC communication, and instructs the vehicle IVS to provide the weigh-in-motion data required by the weigh-in-motion regulation of the jurisdiction.

c) 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.

NOTE Consistent with other TARV standards, as part of security measures, except for remote interrogation using secured 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 weigh-in-motion 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 weigh-in-motion data to the jurisdiction on request from the jurisdiction. 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 weigh-in-motion/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.

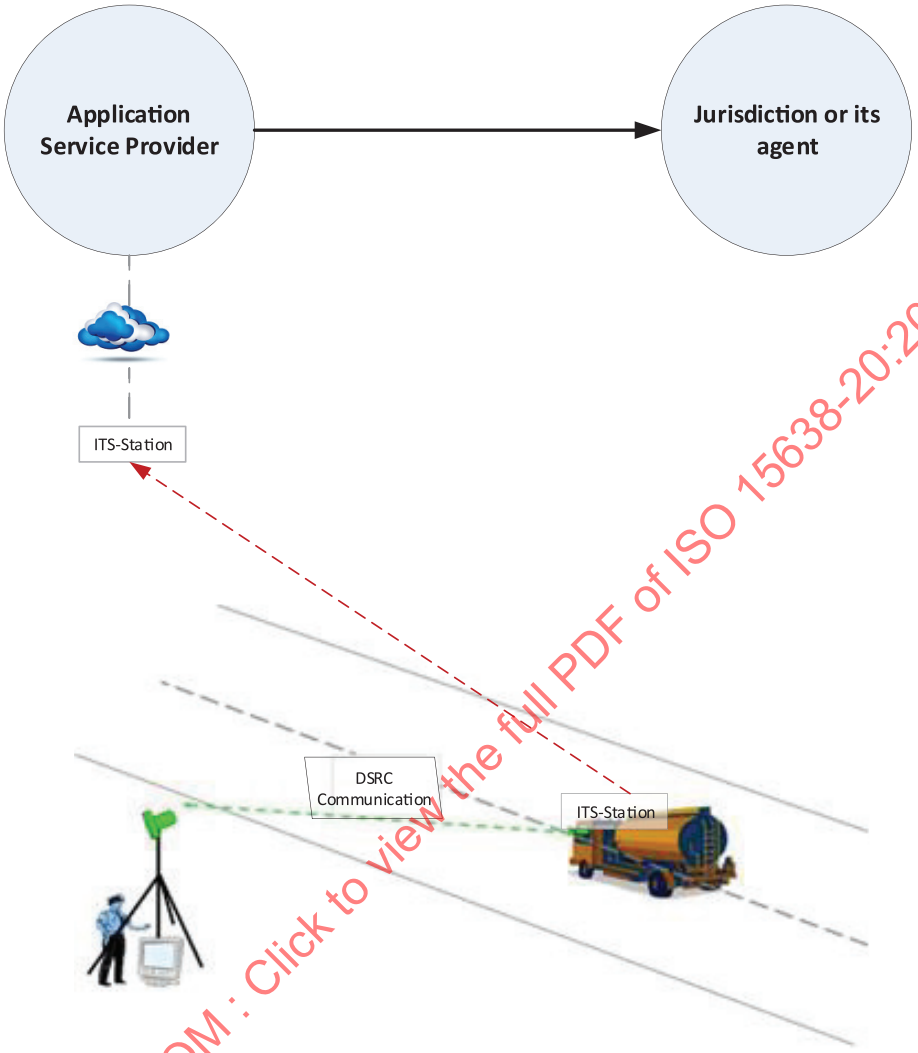


Figure 4 — Communication Profile C2

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:

a) An agent of the jurisdiction either 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 a systematic or random remote vehicle check), or 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 vehicle weight regulations of the jurisdiction.

b) 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 weigh-in-motion data required by the weigh-in-motion regulation of the jurisdiction.

c) 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, in this communication profile 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, forwards the case reference code and weigh-in-motion 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 weigh-in-motion 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 fleet manager). 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 weigh-in-motion/ITS-station of all affected vehicles.

See Figure 5 for a pictorial example.

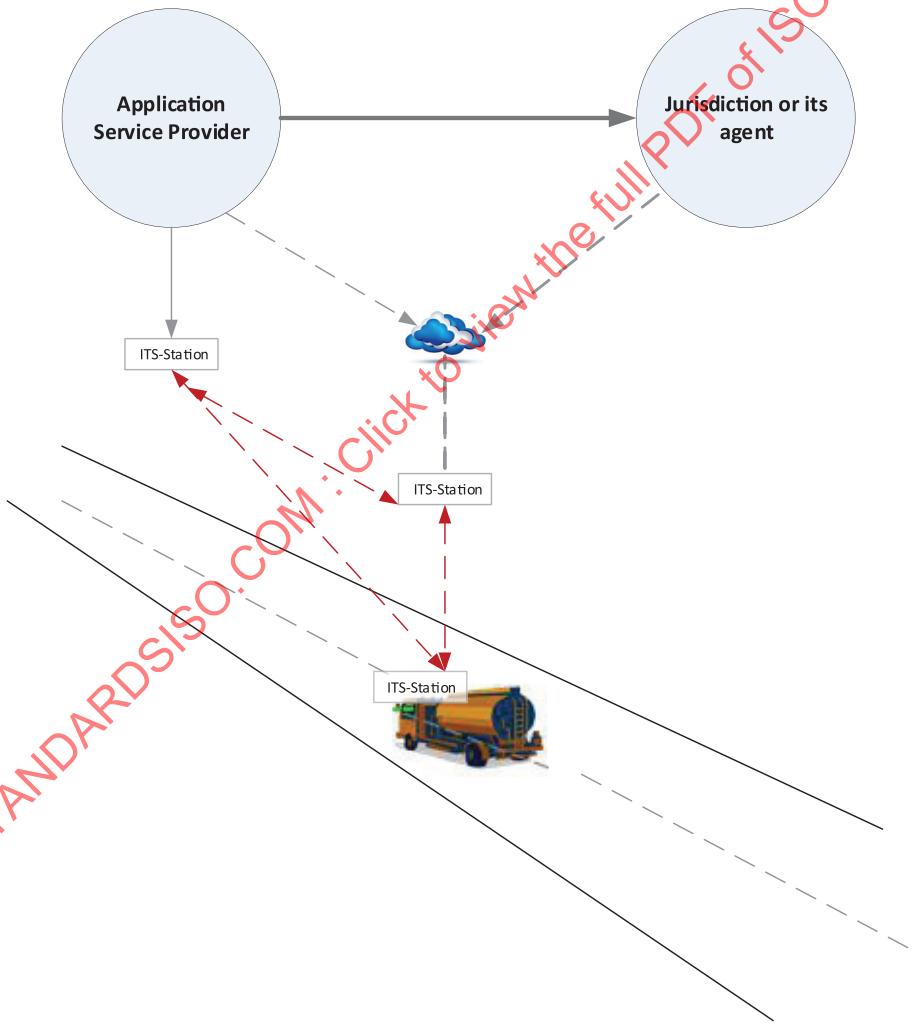


Figure 5 — Communication Profile C3

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 comply 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 from extending or adapting the scope to include other types of regulated vehicles, as it deems appropriate.

6.5.2 Communications profile C1 requirements

Communication may be made via any short-range communications medium supported by ISO 15638-2, specifically:

a) EN ETSI EN 300 674-1 V1.2.1 (2004-08),

b) ARIB STD-T75,

c) TTAS.KO-06.0025,

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

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 annexes to this document.

6.5.2.5 Specific aspects of weigh-in-motion data shall be as determined in 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.

6.5.4 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 and to ISO 15638-6.

b) The security employed shall comply to ISO/TS 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.

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 maintain 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 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 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 communication 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 secured short-range communication (e.g. 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.

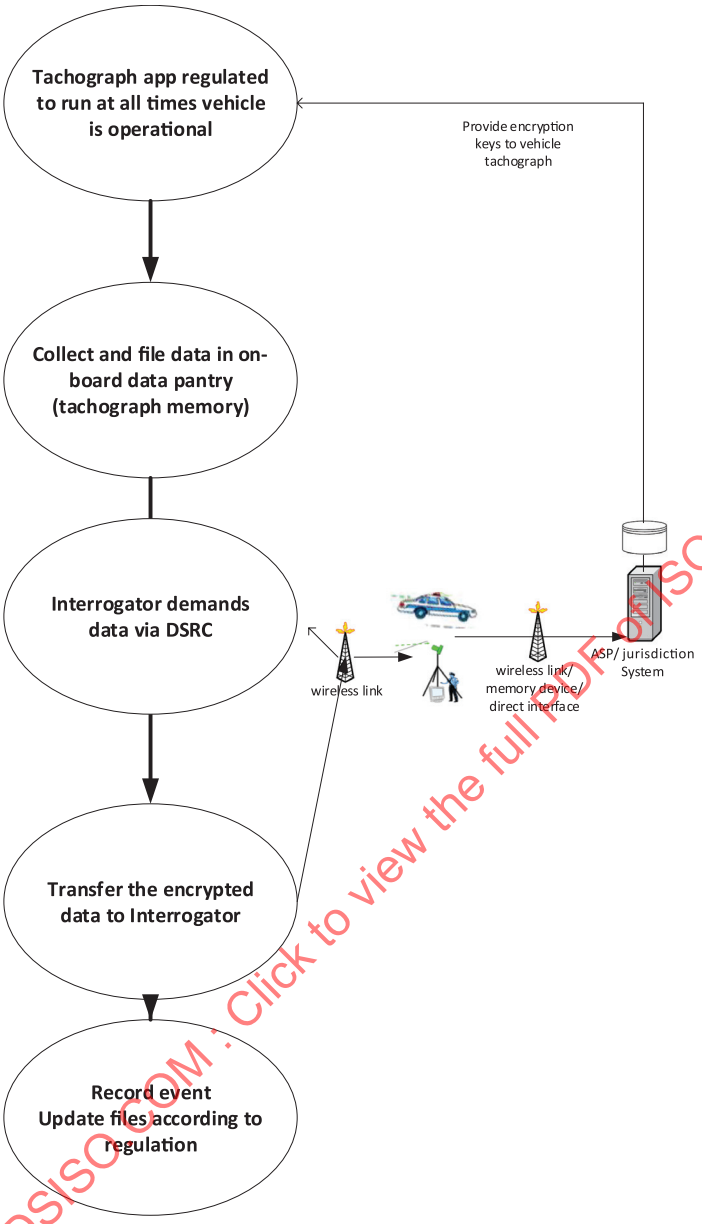


Figure 6 — Short Range Interrogation (Communication Profiles C1 and C2)

9.1.2 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 local data tree (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 15638-6:2013, 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.

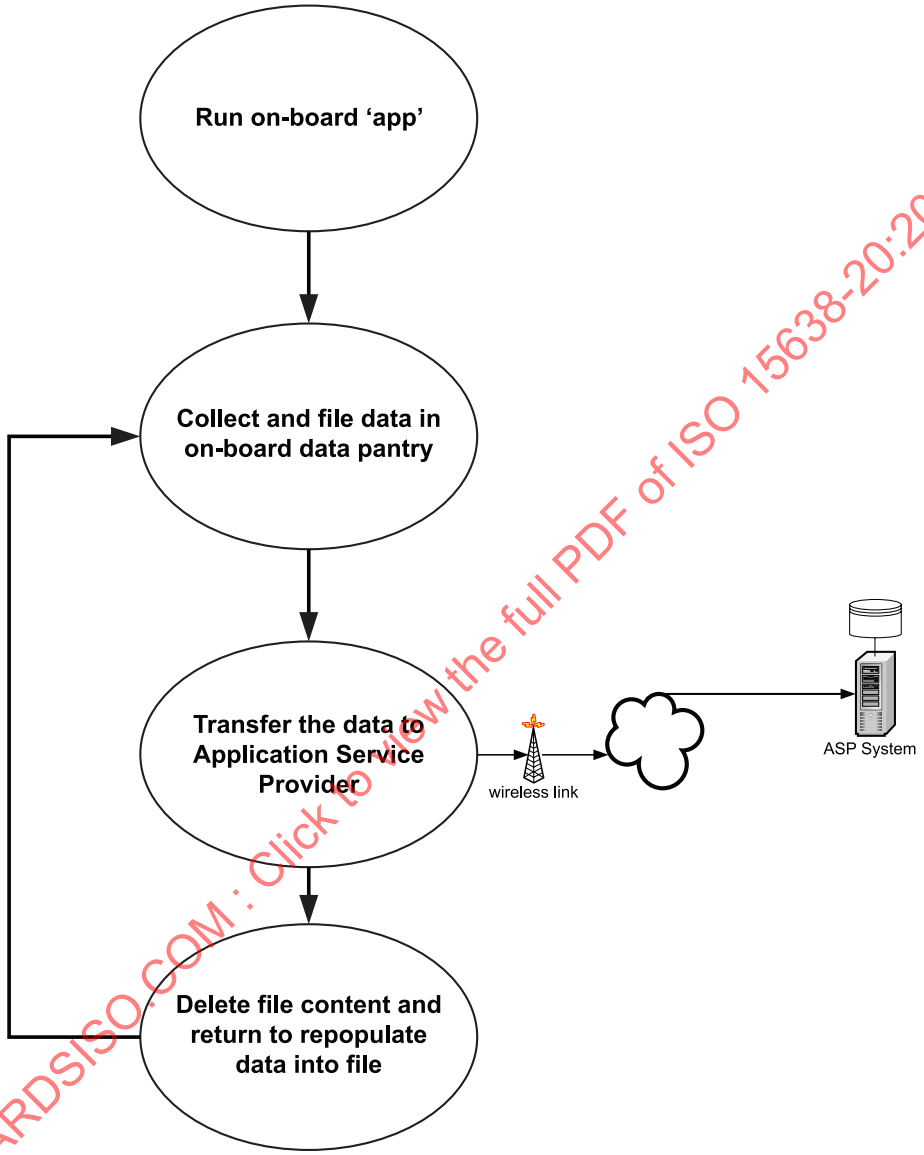


Figure 7 — TARV Regulated application service on-board procedure (Communication Profile C3)

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 or 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

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

In the case of Communication Profile 3, the common sequence of operations for regulated application services shall be as defined in ISO 15638-6.

9.5 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.

9.6 Information security

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

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

Each packet of WIM data shall therefore comprise 5 elements. See Table 1.

Table 1 — Structure of WIM 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 (65 535 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 1) 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 1, 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 normative annexes to this document.

In the case of Communication Profile 3, information security shall be as defined in ISO/TS 15638-4, and there are no practical length restrictions. In the case of Communication Profiles 1, security provisions are as defined in Annex B. In the case of Communication Profile 2, 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.

9.7 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 weigh-in-motion application service shall be as defined below.

9.8 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.

9.9 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.

9.10 Audits

In the case of Communication Profile 3, audits shall be as defined in ISO 15638-6.

In the case of Communication Profiles 1 and 2, audits shall take into consideration the data requirements of the jurisdiction in which the vehicle is operating.

9.11 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 1 and 2, audits shall take into consideration the data requirement of the jurisdiction in which the vehicle is operating.

9.12 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 Weigh-in-motion (WIM)

10.1 TARV WIM service description and scope

10.1.1 Generic TARV WIM use case via the application service provider

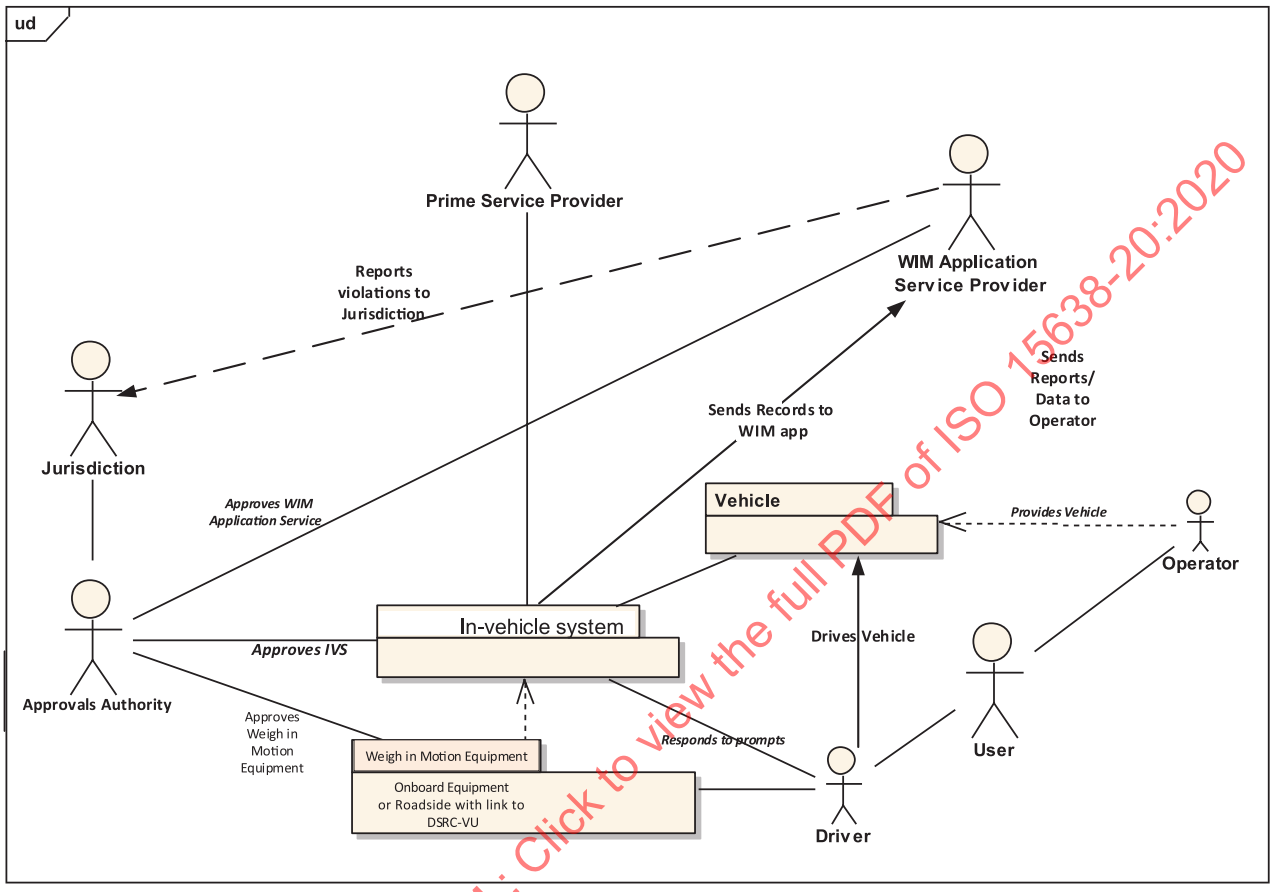


Figure 8 — Weigh-in-motion use case

Figure 8 provides an illustration of a TARV remote weigh-in-motion (WIM) 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 1 and 2, the WIM 'Application Service Provider' is an 'inspector' of the jurisdiction using a short-range wireless interrogator.

10.1.2 Types of weigh-in-motion

The architectural objective of weigh-in-motion is to provide an application service provider with the weight of a vehicle, measured while the vehicle is in motion. For the purposes of this document, the agent of a jurisdiction who is regulating vehicles through WIM using secured DSRC communications is deemed to be the ASP.

Vehicle weight can be obtained in two ways:

a) Using weigh equipment on-board the vehicle (WIM-O).

b) Using weigh equipment embedded in the road pavement, (WIM-R), with data transferred to the vehicle by wireless means.

10.1.3 WIM-O (weigh-in-motion system Onboard)

The generation of vehicle weight data from equipment within the vehicle; the technical means of generating such data is not specified in this document, only the resultant data.

10.1.4 WIM-R (weigh-in-motion system Roadway)

The generation of vehicle weight data from equipment embedded in the road pavement and transferred to the IVS of the vehicle ready for subsequent inspection by wireless means. The technical means of generating such data is not specified in this document, only the resultant data.

NOTE 1 Vehicle weight measurement from in-road 'weigh-in-motion' systems where data is linked to a specific vehicle by ANPR or other techniques and sent via landline or cellular communications to a processing centre is also a viable and alternate option, but as it does not include carrying data on-board the vehicle is not a TARV use case.

Once the roadside equipment has the vehicle weight value(s) established and identified the affected vehicle, it uses wireless means to transfer the WIM-R data to the IVS of the vehicle. This can be achieved using a C-ITS ITS-station - : - ITS-station Communication Profile C3), or, and more likely, by means of short range communications such as 5,8 GHz DSRC. Communication Profile C1 (see also Annex B).

NOTE 2 The advantage of using short range DSRC is that it is easier to localize, identify and transfer the data to the vehicle using such technologies.

In any event, this data transfer requires that the identification of the vehicle (for example ANPR, or a Communication Profile C1 exchange) is made and that identification data accompanies the vehicle weight data to provide a validation that the recorded vehicle weight is that of the vehicle into whose memory it is recorded.

10.1.5 Storage of the WIM data on-board the vehicle

The WIM data (WIM-O and/or WIM-R data) is stored in the IVS.

In a Communication Profile C2/C3 scenario, this will most likely be in the data pantry of the IVS.

In a Communication Profile C1 scenario, this is most likely to be within the IVS-DSRC (See Annex B). This document does not specify how the IVS is organized, but it is recommended that where WIM is used as part of regulatory control, that the jurisdiction specify in their data requirements the exact availability conditions for this data.

10.1.6 WIM inspection and Communication Profiles

This use case applies where weigh-in-motion data is obtained by a jurisdiction in scenarios such as:

a) Communication Profile 1: Interrogation of the weigh-in-motion system data by an inspector of the jurisdiction using a short-range wireless interrogator in accordance with procedures defined in annexes of this document. (See 10.1.2).

b) Communication Profile 2: Interrogation of the weigh-in-motion 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 3: Requests for weigh-in-motion 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 or requests for weigh-in-motion data by a legitimate source such as the driver of the vehicle or the jurisdiction by addressing the IPv6/IPv4 address of the vehicle ITS-station or its weigh-in-motion system with validation of the requested destination for the data provided by the application service provider.

10.1.7 Specific use case of weigh-in-motion inspection by an inspector of the jurisdiction using short range equipment (Communication profiles 1 and 2)

In the situation of the inspection of a specific vehicle weigh-in-motion system by an authorized agent of the jurisdiction using a short range mobile means of wireless interrogation (e.g. 5,8 GHz DSRC) in the circumstance where there is no opportunity to validate the destination of the inspectors address via a remote application service provider, validation of the inspectors interrogator shall be made using the processes defined in annexes of this document, and shall use communication profiles and security 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 below.

10.1.8 Description of TARV WIM regulated application service

TARV WIM is a means to deliver data concepts containing weigh-in-motion 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, or to provide the data via a short-range wireless communication to an agent of the jurisdiction acting as an ASP for the jurisdiction.

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 weigh-in-motion data. The objectives of Communications profiles C2 and C3, is, in situations where it is allowed, to automatically provide the relevant weigh-in-motion data to the jurisdiction via an application service provider. What comprises "relevant" weigh-in-motion 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. Vehicles may however be bound by the data requirements of the jurisdiction in which the vehicle is operating, to measure and/or retain specific WIM data. Where consensus can be achieved, later versions of this document may add further Profiles for additional communications and/or data concepts.

Communication Profiles as defined in Annexes 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 weigh-in-motion data concept transferred (which shall be at the determination of the jurisdiction).

However, whilst the objective of Communications Profiles C2 and C3 is to provide all of the weigh-in-motion 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 any regulatory action or whether to stop the vehicle for further inspection. 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 determine the content of electronic weigh-in-motion data. However, Annex C provides for information some data concept profiles that support this document.

EXAMPLE In Europe, DIRECTIVE (EU) 2015/719, and *Regulation (EU) 165/2014,* provide the overall requirements in countries of the European Union for weigh-in-motion, and combined with current European driving regulations provide the regime for driver monitoring in Nation states within its jurisdiction .Weigh-in-motion 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 provides 'specifications for 5,8 GHz DSRC communications to access this data (including security provisions); 9.6 provides specifications for security and is complemented in Annex B with direct security measures for 5,8 GHz DSRC (B.1.6.5); and Annex C provides specifications for data profiles.

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.

The nature and form of the weigh-in-motion 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 weigh-in-motion regulations differ around the world, in order for TARV WIM to operate it is a requirement that at least the following features are present in the weigh-in-motion:

a) Any WIM-O (on-board) weigh-in-motion system shall be able to output the following data using an appropriate dedicated serial link independent from an optional CAN bus connection (ISO 11898-1), to allow their processing by other electronic units installed in the regulated vehicle.

b) When the ignition of a WIM-O equipped vehicle is ON, key weigh-in-motion data (as determined by the weigh-in-motion system design) is permanently broadcast to the IVS.

c) 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.

d) 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 a WIM-O equipped vehicle 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 '*WIM-O data*' file;

   and shall be able to store in its data memory the data required by the jurisdiction requiring the weigh-in-motion data.

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

Figure 8 provided an illustration of a TARV weigh-in-motion monitoring system. This application service is described in 10.1.4 and 10.2.

10.1.9 Description of TARV WIM application service

The TARV 'weigh-in-motion' (WIM) 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 provides example profiles of weigh-in-motion application data concepts which regulators may elect to adopt as the norm within their jurisdiction, and Annex B provides the specification of a 5,8 GHz DSRC communication transaction.

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

10.2 Concept of operations for TARV WIM

10.2.1 General

The TARV 'weigh-in-motion' (WIM) is an application service that transfers weigh-in-motion application data (generated by an on-board WIM-O system or transferred to on-board memory from a roadside WIM-R system) 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 3), or in the case of a direct short range communication, between the inspector ('interrogator') and the vehicle using a short range wireless communication (Communication Profiles C1 and C2). Requirements for weigh-in-motion may vary from one jurisdiction to another. Therefore, this document does not specify nor require the use of particular specific data concepts, nor control the content of the weigh-in-motion data, but a number of example data concept profiles, and transactions, are provided in Annex C of 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 WIM system

The objective is to provide WIM (WIM-O and/or WIM-R) data from a vehicle to an application service provider, or the agent of the application service provider.

The service is achieved by an app in the IVS requesting weigh-in-motion data from the weigh-in-motion system, 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 service provider 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 WIM 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) application service.

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 WIM 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 weigh-in-motion data from the vehicle by interrogating via a short range ('interrogator') that is wirelessly connected in accordance with 5,8 GHz DSRC, or infra-red, communication provisions as specified in ISO 15638-2 (Communication Profiles C1 and C2).

b) Obtaining weigh-in-motion 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 3).

c) Obtaining weigh-in-motion data by interrogating via a fixed gantry or roadside beacon 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 weigh-in-motion data by remotely addressing the IPv6/IPv4 address of a vehicle ITS-station or its weigh-in-motion that is wirelessly connected in accordance with one or more of the wireless media specified in ISO 15638-2 (Communication Profile 3).

In the case of an instantiation of a) (Communication Profile 1), 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 to 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 WIM

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 WIM, 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 WIM application service provider may be an agent or department of the jurisdiction.

10.2.5 Clear statement of responsibilities and authorities delegated for TARV WIM

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

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

Actor	Role	Activities	Interactions
Jurisdiction (J)	Sets requirements for mandatory and supported TARV WIM	Publishes specifications	ALL
		Obtains regulations	ALL: Establish regime and regulations PSP:Register ASP Register, receive reports Op: Vehicle Registration Dr: Licence, issue Weigh-in-motion

Table 2 *(continued)*

Actor	Role	Activities	Interactions
		May provide Weigh-in-motion systems	
		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, Weigh-in-motion, Application Service instantiations	PSP: Certify IVS ASP: Certify Application Service Op: Certify Weigh-in-motion system
		Conducts Q of S maintenance to instruction of jurisdiction	
Agent of jurisdiction **(AJ)**	Inspection and Enforcement	Inspects Weigh-in-motion systems	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 Weigh-in-motion systems	
Application service provider **(ASP)**	Provides TARV WIM application services	Develops instantiation of TARV WIM application service	CA: Applies for approval of Service
		Contracts with *users*	Op: Contracts
		Provides TARV WIM application service to users and jurisdiction	Op: Provides service Dr: May provide service J: Provides service/reports AJ: re enforcement
Owner **(Ow)**	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

Table 2 *(continued)*

Actor	Role	Activities	Interactions
		Receives reports from ASP	
Driver (Dr)	Drives regulated vehicle to instruction of owner		Op: to instructions
		Sings into TARV WIM system	IVS: signs driver into system
		Drives regulated vehicle	
		Interfaces with AJ	AJ: Provides Access to Weigh-in-motion system

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 provide 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 weigh-in-motion system and maintain the system.

10.2.5.6 The application service provider (ASP) shall develop the TARV WIM application service or use a TARV WIM application service provided by jurisdiction. In the case of WIM, 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 WIM 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 WIM service from the approval authority (regulatory).

10.2.5.8 The application service provider shall contract with the user (normally fleet manager 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 jurisdiction, operator and driver as specified in its service offering. In the case of WIM, 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 fleet manager 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 WIM.

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

10.2.5.13 The driver shall be responsible for following instructions, including use of weigh-in-motion system.

10.2.6 Equipment required for TARV WIM

10.2.6.1 TARV IVS WIM-0

The on-board weigh-in-motion system (WIM-O) shall have the means to provide data to the IVS for transfer to the application service provider. The weigh-in-motion system shall supply data to the IVS. This may be 'pushed' at the instigation of the weigh-in-motion system, or 'pulled' at the instigation of the TARV WIM 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. The weigh-in-motion system shall be to a design approved by the jurisdiction. The operation of the weigh-in-motion system is out of the scope of this document.

The specification, form and function of the electronic weigh-in-motion equipment is deliberately not defined in this document and is considered to be at the determination of the jurisdiction or the marketplace, (at the discretion of the jurisdiction).

Communication Profile C3: The IVS shall be provided with an interface capable of receiving data from the installed weigh-in-motion system, and that transfer may be 'pushed' by the weigh-in-motion system or 'pulled' from the weigh-in-motion system according to the design of the weigh-in-motion system and the TARV WIM app in the IVS, and is a function of the application service design, and not the specifications of this document.

10.2.6.2 TARV IVS WIM-R

An equipped vehicle shall have the means to record data in the IVS and/or the IVS-DSRC in accordance with the data requirements of the jurisdiction.

EXAMPLE In the European Union, the IVS-DSRC equipment used for remote tachograph monitoring is used to collect, hold and transfer WIM-R and/or WIM-O data.

10.2.6.3 TARV IVS WIM-O and WIM-R

10.2.6.3.1 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).

10.2.6.3.2 Communication Profiles 1 and 2: 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.

10.2.6.3.3 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, weigh-in-motion system and all associated components.

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

10.2.6.4 TARV WIM 'app'

10.2.6.4.1 TARV WIM 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 shall be at the discretion of the jurisdiction. Optional/Example Application Data profiles are provided in Annex C.

10.2.6.4.2 The TARV WIM app running on the IVS records the received weigh-in-motion data (WIM-O and/or WIM-R) in the form specified by the jurisdiction, and makes transactions to provide the data as specified in Annex A.

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

10.2.6.4.4 Once the TARV WIM system of the application service provider has acknowledged successful receipt of the data, the data shall be deleted from the memory of the WIM IVS unless the jurisdiction, user or application service provider requires it for other purposes, and a new file shall be created for future use. For clarity, deletion from the WIM IVS does not imply deletion from the memory of the weigh-in-motion system (storage and deletion of which shall take into consideration the design and function of the weigh-in-motion system and the data requirements of the jurisdiction). Deletion in this clause simply means deletion from any temporary files created to collate data from the system in order to make the required transmission of data.

10.2.6.4.5 It shall not be possible for collected or stored weigh-in-motion data in any software or non-volatile memory within the WIM 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 within the regulatory provisions of the jurisdiction.

10.2.7 Operational processes for the TARV WIM system

Shall be as defined in 9.2.

For detail of the operational processes see 10.3 (sequence of operations for weigh-in-motion monitoring).

10.2.8 Role of the jurisdiction for TARV WIM

Shall be as defined in 9.3.

10.2.9 Role of the TARV WIM prime service provider

Shall be as defined in 9.4.

10.2.10 Role of the TARV WIM application service provider

Shall be as defined in 9.5.

10.2.11 Role of the TARV WIM user

Shall be as defined in 9.6.

10.2.12 Generic characteristics for all instantiations of the TARV weigh-in-motion (WIM) application service

10.2.12.1 A remote weigh-in-motion monitoring application service is approved; it utilizes a TARV WIM IVS which communicates to the prime service provider / application service provider and has the ability to obtain data from the regulated vehicle weigh-in-motion system.

10.2.12.2 The application service provider shall load a TARV WIM App into the IVS of the fleet manager's vehicles.

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

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

10.2.12.5 The application service provider shall design/install/operate its weigh-in-motion 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 WIM data to the application service provider using the TARV IVS wireless link at least once every 24 hours (Communication Profile 3). Every transfer shall include framing data that identifies its sequential order, IVS ID, version number of IVS and version number of the TARV WIM app; or (Communication Profiles 1 and 2) where providing data in accordance with Annex B using a short-range wireless communication under the control of an agent of the jurisdiction.

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

10.2.12.7 The application service system shall retain and back up the TARV WIM data taking into consideration the 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 specification and requirements of the jurisdiction when approving the product.

10.2.12.9 TARV WIM records received by the IVS and stored in the `'WIMdata'` 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 driver or fleet manager, and in the event of contravention, to the jurisdiction, in accordance with the regime of the jurisdiction.

10.3 Sequence of operations for TARV WIM

10.3.1 General

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

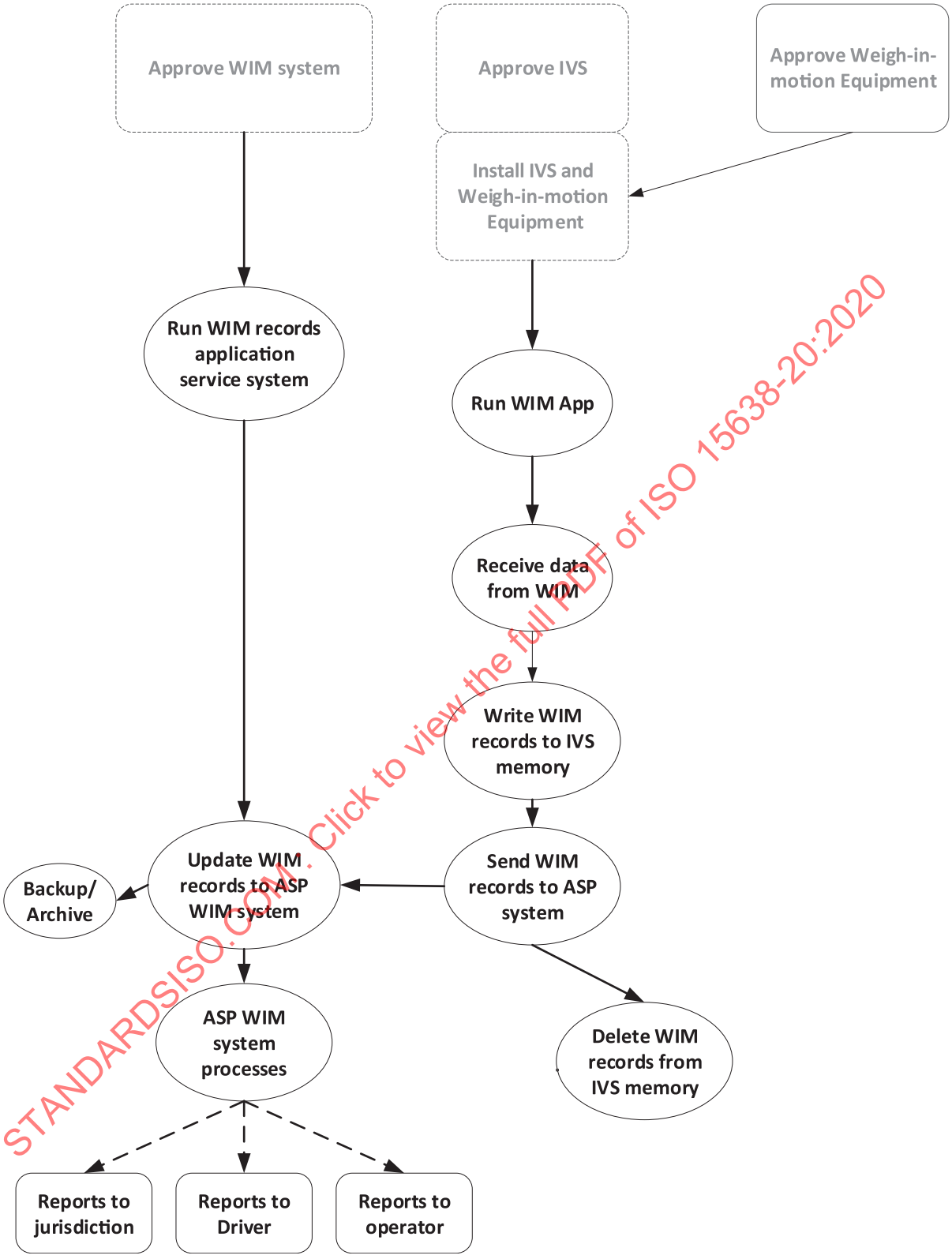


Figure 9 — TARV WIM Business process and procedure

10.4 TARV WIM service elements

10.4.1 TARV WIM service element (SE) 1 — Establish 'weigh-in-motion' regulations, requirements, and approval arrangements

The jurisdiction is responsible for defining its requirements for its variant of the weigh-in-motion application service, including data security provisions (within the security frameworks supported/enabled by this document), obtain any data requirements, and define the procedure for an application service provider to gain approval for its instantiation of the TARV WIM application service.

10.4.2 TARV WIM SE2 — Request system approval

The application service provider shall seek approval for its instantiation of the weigh-in-motion application service from the approval authority (regulatory) taking into consideration the regime established by the jurisdiction.

10.4.3 TARV WIM SE3 — User (fleet owner) contracts with prime service provider

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

That equipment may be (Communication Profile 3) an ITS-station supporting wireless transactions via one or more of the wireless media supported in ISO 15638-2, or (Communication Profiles 1 and 2) may be via a specific short range communication device as specified in Annexes A and B of this document.

10.4.4 TARV WIM SE4 — User (fleet owner) equips vehicle with a weigh-in-motion system

It shall be a prerequisite for any potential vehicle fleet owner opting or being required to sign up for the TARV WIM application service that its regulated vehicles are TARV equipped with a weigh-in-motion system at point of manufacture or installed by a prime service provider, and that there is a maintenance contract with a prime service provider for that equipment.

10.4.5 TARV WIM SE5 — User contracts with application service provider

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

In the case of WIM 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 shall be a general condition of use of the vehicle on the roadways/highways of the jurisdiction.

10.4.6 TARV WIM SE6 — Application service provider uploads software into the TARV equipped vehicles of the fleet owner

The service provider shall upload and commission the on-board TARV WIM app software into the TARV equipped vehicles of the fleet owner.

10.4.7 TARV WIM SE7 — Create Data

When the ignition of the regulated vehicle is turned on, the TARV WIM 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 compliance 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 shall be responsible to ensure that those within its control are adequately informed concerning its requirements.

10.4.8 TARV WIM SE8 — Recording of weigh-in-motion 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 WIM SE10 — 'Interrogated' request for weigh-in-motion data

10.4.9.1 Communication Profile 1 (via short range mobile interrogator)

10.4.9.1.1 Obtaining weigh-in-motion data by interrogating via a short-range mobile interrogator that is wirelessly connected in accordance with so called European 5,8 GHz DSRC as specified in EN ETSI 300 674-1 and ISO 15638-2 (Communication Profiles 1 and 2).

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 9.6 and Annex B (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 1 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 2 (Via Short range mobile interrogator/ISO 15638-2 provision of data)

10.4.9.2.1 Obtaining weigh-in-motion data by interrogating via a short-range mobile interrogator that is wirelessly connected in accordance with so called European 5,8 GHz DSRC as specified in EN ETSI 300 674-1 and ISO 15638-2 (Communication Profiles 1 and 2) 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 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.

10.4.9.2.3 On receipt of the request to its IPv6/IPv4 address, the WIM 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 WIM data has been received.

10.4.9.2.4 The IVS shall then close the communication session.

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

10.4.9.2.6 The IVS shall then send the WIM 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.

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

10.4.9.2.8 On receipt of the acknowledgement <WMX> the IVS shall close its communication session.

10.4.9.2.9 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 to send the data to the interrogator requested IPv6 address. The means and detail of how this is achieved is outside the scope of this document.

10.4.9.3 Communication Profile 3 (Via ISO 15638-2 ITS-station provision of data)

10.4.9.3.1 Obtaining weigh-in-motion 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 weigh-in-motion 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 weigh-in-motion data via the IP address of the weigh-in-motion system or ITS-station.

10.4.9.3.4 In the event that the IVS of a vehicle receives a wireless interrogation requesting the WIM 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 WIM IVS, the ITS-station of the WIM 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 WIM 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 WIM 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 <WMX> to the IVS.

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

10.4.9.3.11 The ASP shall be responsible to verify that the interrogation is legitimate, appropriate and from an accepted source, and having verified this, shall be responsible to send 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 WIM SE9 — Pre-programmed interval sending weigh-in-motion data to application service provider (Communication Profile 3)

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

<START><LENGTH>< WIMdata file><WIMdata><END>

10.4.10.2 The content of the WIM data 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 WIM file the application service provider system shall send an ACKnowledgement <WMX> to the IVS. On receipt of the ACKnowledgement <WMX> the IVS shall clear the data held within the 'WIMdata' file and start to repopulate the 'WIMdata' file with data as defined by the TARV WIM app.

10.4.10.4 If an ACKnowledgement is not received within 60 seconds of sending the data the TARV WIM app shall attempt to resend the data and shall continue to do so at intervals determined by the specification of the TARV WIM 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 WIM app shall append a record <Time><'OFF'> to the 'WIMdata' file and the IVS shall send the file to the TARV WIM 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 WIM 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 'WIMdata' file from its memory and the TARV WIM app shall terminate.

10.4.10.7 Because of the titling regime defined above, each TARV WIM file is uniquely identifiable by the host TARV WIM 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 ('WIMdata' files) to perform the application service, and the method of reporting to the jurisdiction and operator is outside of the scope of this document shall be the subject of definition by the jurisdiction and the application service provider.

10.4.11 TARV WIM 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 weigh-in-motion system 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 10.4.9 above). 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 10.4.11.

10.5 Generic TARV WIM data naming, content and quality

Communication Profile 3: The data content of the weigh-in-motion data shall be as defined by the application service/weigh-in-motion system design.

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

Table 3 — Formal title of a TARV WIM record

File type		Format of file name	Notes/Source
WIM	**Mandatory**	<YYMMDD><hhmmss><vehicle registration number><'*WIMdata*'> Example 110316 070603 GB 1 KV76WRR *WIMdata* As: 110316070603KV76WRR*WIMdata*	Subclause 10.4.8 ([*WIMdata* file])

10.6 WIM data content

Communication Profile 3: The content of the *WIMdata* file shall be one or more of the data concept profiles specified in Annex C of this document.

Communication Profiles 1 and 2: 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 shall be responsible to ensure that those within its control are adequately informed concerning its requirements.

10.7 TARV WIM 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

functionally 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 come along.

See also Clause 9 above for general quality of service requirements.

10.8 TARV WIM application service specific provisions for test requirements

There are no specific provisions for test requirements specified in this version of this document, except as specified for a short-range communication with a mobile interrogator (Communication Profiles 1 and 2), which shall be tested to meet the requirements of EN 300 674-1.

10.9 TARV WIM 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)

WIM communication and transaction profiles

A.1 Communication Profiles

This issue of this document supports and defines three types of communication profile:

- **Communication Profile 1: Roadside inspection using a short range wireless communication interrogator instigating a physical roadside inspection, (master -:- slave)**
  - Profile 1a: via a hand aimed or temporary roadside mounted and aimed interrogator
  - Profile 1b: via a vehicle mounted and directed interrogator
  - Profile 1c: via a permanent or semi-permanent roadside or overhead gantry
- **Communication Profile 2: 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 2a: via a hand aimed or temporary roadside mounted and aimed interrogator
  - Profile 2b: via a vehicle mounted and directed interrogator
  - Profile 2c: via a permanent or semi-permanent roadside or overhead gantry
- **Communication Profile 3: 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 3a: via an interrogation from an ITS-station
  - Profile 3b: 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 WIM transactions for each of these communication profile options.

A.2 Communication Profile 1 — Interrogated request for weigh-in-motion data using short range 5,8 GHz DSRC communication

A.2.1 This is a master-:-slave communication where an interrogator requests and an IVS supplies WIM data (for an inspector to evaluate whether or not to stop a vehicle).

A.2.2 The interrogator shall establish a communication in accordance with Annex B of this document.

A.2.3 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.

A.2.4 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.2.5 The session shall be closed as specified in Annex B of this document.

A.3 Communication Profile 2 — Roadside inspection using a short-range wireless communication interrogator, instigating a download of data to an application service provider via an ITS-station

A.3.1 This is a combination of master-:-slave communication where an interrogator requests WIM data, which is subsequently supplied to a remote application service provider in a peer-:-peer communication via its ITS-station.

A.3.2 A TARV WIM app running on the IVS records the received weigh-in-motion data in a file, 'WIMdata' held in the data pantry of the IVS taking into consideration with the data requirements of the jurisdiction. The means by which this process occurs is out of the specifications of this document and shall be to the requirements of the data requirements of the jurisdiction.

A.3.3 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.

This is achieved via the ACTION.request TRANSFER defined in B.1.7.4. This transaction sends the IP address requested by the equipment of the inspector (as the final destination where the inspector wishes to see the interrogated data, usually the IP address of the inspector).

A.3.4 The IVS shall record the data in its data pantry memory and respond with the ACKnowledgement <T>

as

Set-Response BIT STRING ::= '01010100'B

}

A.3.5 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.3.6 The interrogator shall confirm receipt of the data, by issuing a RELEASE as specified in Annex B of this document.

A.3.7 The 5,8 GHz DSRC communication session shall be closed as specified in Annex B of this document.

A.3.8 The IVS shall then transfer the data to a predetermined address its application service provider in accordance with the procedures described in A.4.1.7 et sequitur below.

A.4 Communication Profile 3 — Remote inspection addressed via an ITS-station instigating a download of data to an application service provider via a wireless communications interface

A.4.1 Interrogated request for weigh-in-motion data via ITS-station.

A.4.1.1 As specified in 10.4.8 (TARV WIM SE7), when the ignition of the regulated vehicle is turned on, the TARV WIM app in the data library of the IVS shall be instigated.

The app shall first create a `WIMdata` file and shall name the file

<YYMMDD><hhmmss><vehicle registration number><' *WIMdata*'>

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.4.1.2 As specified in 10.4.9 -TARV WIM 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 weigh-in-motion system ('pull') or the weigh-in-motion system shall send a stream of data ('push') to the WIM IVS.

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

<'start'><weigh-in-motiondata><'END'>

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

A.4.1.3 The TARV WIM app running on the IVS records the received weigh-in-motion data in a file, '*WIMdata*' held in the data pantry of the IVS.

A.4.1.4 On receiving an interrogation request from an ITS-station -:- ITS-station communication, requesting the WIM 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.4.1.5 The WIM IVS shall acknowledge the request with the appropriate ACKnowledgement defined in of ISO 15638-6:2014, 8.3.5, <T>, which acknowledges that a request for WIM data has been received.

A.4.1.6 The IVS shall then close the communication session.

A.4.1.7 The TARV WIM app shall then send the TARV WIM data held in the file, '*WIMdata*' 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.4.1.8 Once the TARV WIM system of the application service provider has acknowledged successful receipt of the data, the '*WIMdata*' 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.

A.4.1.9 On successful receipt of the data, the recipient at the predetermined destination IPv6 address shall send an acknowledgement <WMX> to the IVS.

A.4.1.10 On receipt of the acknowledgement <WMX> the IVS shall close its communication session.

A.4.1.11 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 to send 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.4.1.12 It shall not be possible for collected or stored weigh-in-motion data in any software or non-volatile memory within the IVS or weigh-in-motion system 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 application service provider.

A.4.2 Obtaining weigh-in-motion data by remotely addressing the IPv6/IPv4 address of a vehicle ITS-station or its weigh-in-motion system that is wirelessly connected in accordance with one or more of the wireless media specified in ISO 15638-2.

A.4.2.1 In the event that ITS-station of the IVS of a vehicle receives a wireless interrogation, addressed to its IP address, requesting the WIM 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.4.2.2 On receipt of the request to its IPv6/IPv4 address the WIM 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 WIM data has been received.

A.4.2.3 The IVS shall then close the communication session.

A.4.2.4 The IVS shall then open a new communication session using an available and appropriate CALM wireless medium.

A.4.2.5 The IVS shall then send the WIM 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.4.2.6 On successful receipt of the data, the recipient at the predetermined destination IPv6 address shall send an acknowledgement <WMX> to the IVS.

A.4.2.7 On receipt of the acknowledgement <WMX> the IVS shall close its communication session.

A.4.2.8 The ASP shall be responsible to verify that the interrogation is legitimate, appropriate and from an accepted source, and having verified this, shall be responsible to send 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.4.3 Obtaining weigh-in-motion 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.4.3.1 In the event that the IVS of a vehicle receives a wireless interrogation requesting the WIM 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.4.3.2 On receipt of the wireless request to the ITS-station of the WIM IVS, the ITS-station of the WIM 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 WIM data has been received.

A.4.3.3 The IVS shall then close the communication session.

A.4.3.4 The IVS shall then open a new communication session using an available and appropriate CALM wireless medium.

A.4.3.5 The IVS shall then send the WIM 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.4.3.6 On successful receipt of the data, the recipient at the predetermined destination IPv6 address shall send an acknowledgement <WMX> to the IVS.

A.4.3.7 On receipt of the acknowledgement <WMX> the IVS shall close its communication session.

A.4.3.8 The ASP shall be responsible to verify that the interrogation is legitimate, appropriate and from an accepted source, and having verified this, shall be responsible to send 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.4.4 Obtaining weigh-in-motion 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 3).

A.4.4.1 In the event that the IVS of a vehicle receives a wireless interrogation requesting the WIM 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.4.4.2 On receipt of the wireless request to the ITS-station of the WIM IVS, the ITS-station of the WIM 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 WIM data has been received.

A.4.4.3 The IVS shall then close the communication session.

A.4.4.4 The IVS shall then open a new communication session using an available and appropriate CALM (3.12) wireless medium.

A.4.4.5 The IVS shall then send the WIM 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.4.4.6 On successful receipt of the data, the recipient at the predetermined destination IPv6 address shall send an acknowledgement <WMX> to the IVS.

A.4.4.7 On receipt of the acknowledgement <WMX> the IVS shall close its communication session.

A.4.4.8 The ASP shall be responsible to verify that the interrogation is legitimate, appropriate and from an accepted source, and having verified this, shall be responsible to send 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.4.4.9 The session shall be closed as specified in A.6 below.

A.5 Pre-programmed downloads of weigh-in-motion data (Communication Profile 3)

A.5.1 Pre-programmed interval sending weigh-in-motion data to application service provider.

A.5.1.1 Where required by the data requirements of the jurisdiction, or by the operator, at time intervals determined by the on-board TARV WIM app, taking into consideration the requirements of the jurisdiction or the operator, the WIM IVS shall send the '*WIMdata*' file to the TARV WIM application service provider system via a wireless communication supported by the IVS and application service provider system as:

<START><LENGTH>< WIMdata file>< WIMdata><END>

A.5.1.2 The content of the WIMdata file shall be a data concept profile as specified in Annex C of this document.

A.5.1.3 On successful receipt of the TARV WIM file the application service provider system shall send an ACKnowledgement <WMX> to the IVS. On receipt of the ACKnowledgement <WMX> the IVS shall clear the data held within the '*WIMdata*' file and start to repopulate the '*WIMdata*' file with data as defined by the TARV WIM app.

A.5.1.4 If an ACKnowledgement is not received within 60 seconds of sending the data the TARV WIM app shall attempt to resend the data and shall continue to do so at intervals determined by the specification of the TARV WIM application service approved by the approval authority (regulatory) until the data has been successfully sent and ACKnowledged.

A.5.1.5 Whenever the regulated vehicle ignition is switched to OFF, the on-board TARV WIM app shall append a record <Time><'OFF'> to the '*WIMdata*' file and the IVS shall send the file to the TARV WIM application service provider system via a wireless communication supported by the IVS and application service provider system.

A.5.1.6 On successful receipt of the TARV WIM 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 '*WIMdata*' file from its memory and the TARV WIM app shall terminate.

A.5.1.7 Because of the titling regime defined above, each TARV WIM file is uniquely identifiable by the host TARV WIM application service when it is received.

A.5.1.8 The manner in which the application service provider uses the information captured and forwarded to it by the IVS ('*WIMdata*' files) to perform the application service, and the method of reporting to the jurisdiction and operator is outside of the scope of this document shall be the subject of definition by the jurisdiction and the application service provider.

A.5.1.9 The session shall be closed as specified in A.6.

A.6 End of session

Except in the aspects of clauses A.1 and A.2 above (Communication Profiles 1 and 2: 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 weigh-in-motion system 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
(normative)

Communication Profile for 5,8 GHz DSRC communications

B.1 Overview and context

B.1.1 Overview

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;

— Weigh-in-motion 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 above and B.1.6.5 below.

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

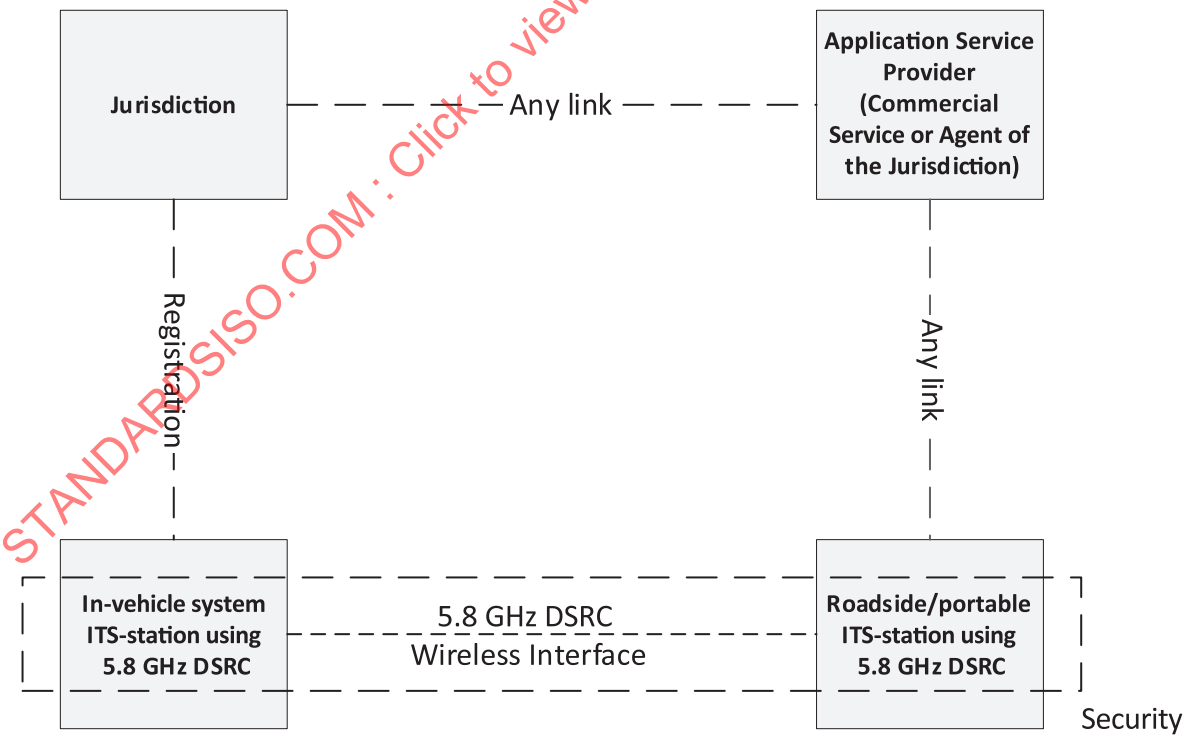


Figure B.1 — Scope for this use case (within the box delimited with a dotted line)

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

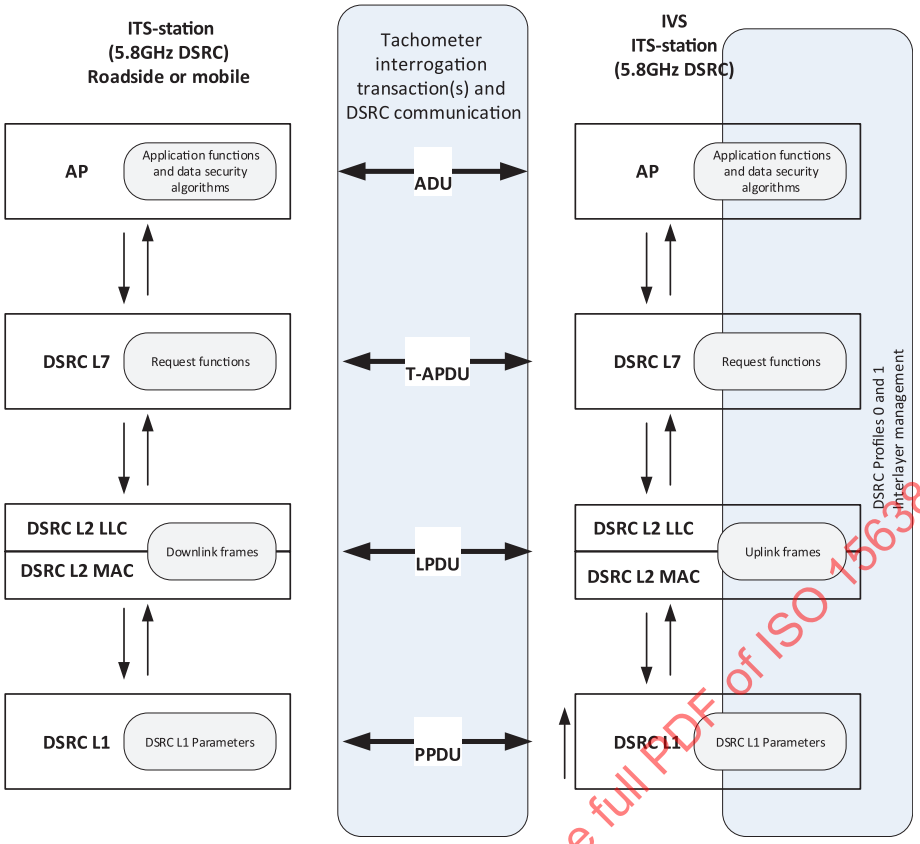


Figure B.2 — Relations between 5,8 GHz DSRC communications stack elements

This annex specifies a communication profile use case for short range transactions between an interrogator and the vehicle to obtain data from a weigh-in-motion system 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. Jurisdictions will need to determine and declare with which of these base standards weigh-in-motion equipment/IVS used within their jurisdiction shall need to comply.

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

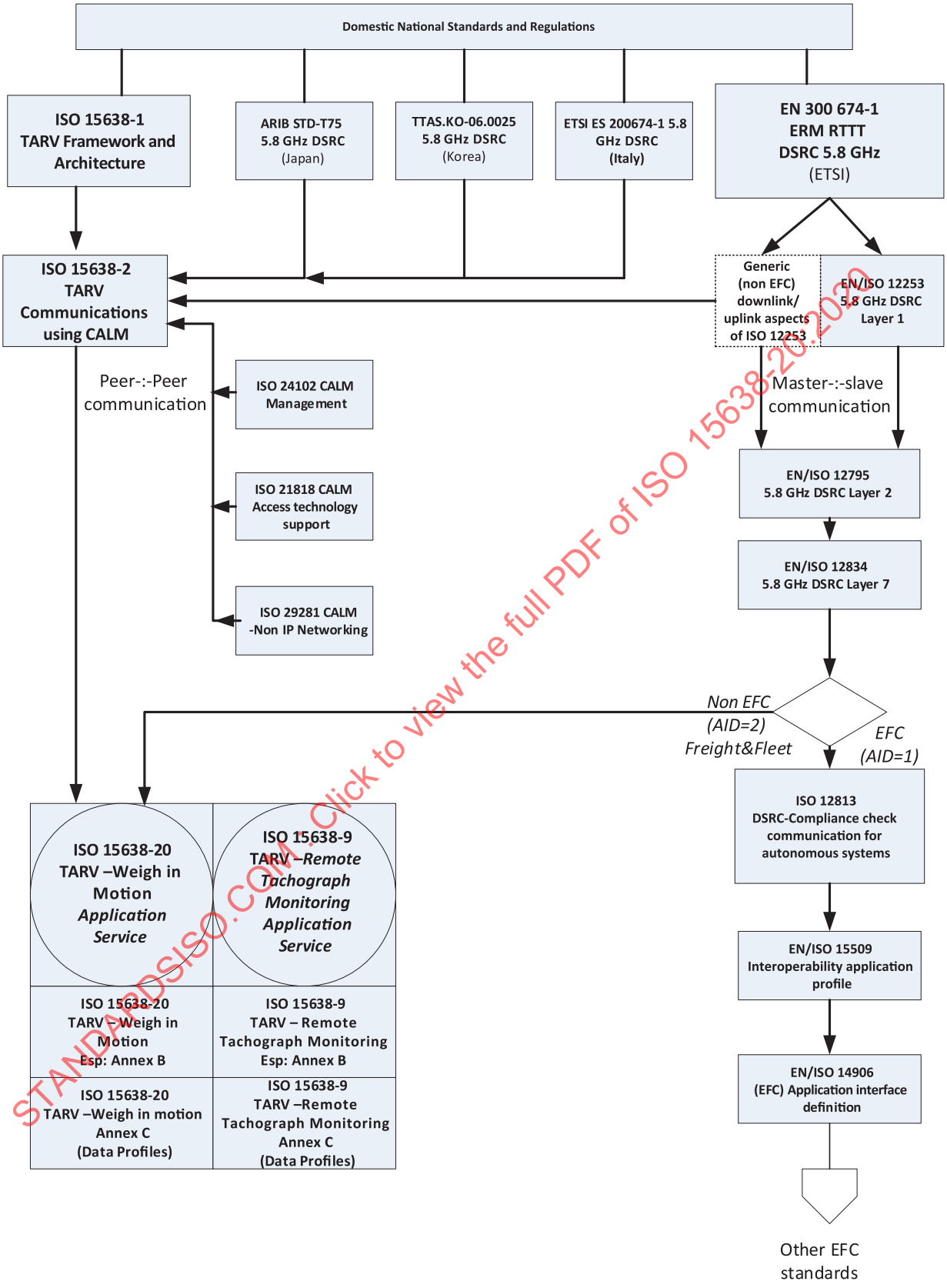


Figure B.3 — Relation and references between ISO 15638-20, CALM Communications and 5,8 GHz DSRC base standards

B.1.2 Use cases

The use cases where a 5,8 GHz DSRC communication may be used are described in 6.2 (Profile 1) and 6.3 (Profile 2.).

B.1.3 Physical layer

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

ETSI EN 600 374-1 (Europe, Australia, parts of the Americas, and other regions);

ARIB STD-T75 (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.

B.1.4 Profile 1 transactions

Transactions operating within EN 300 674-1 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 2 communications, see A.2.

Transactions using:

ARIB STD-T75 (Japan);

TTAS.KO-06.0025 (Korea);

ETSI .TS 200 674-1 (Italy);

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

B.1.5 Profile 1 transactions operating within EN 600 374-1, 5,8 GHz DSRC

Where the system is operating in accordance with EN 600 374-1, it shall further conform to the following uplink and downlink parameters from EN 12253. All physical layer parameters other than those given in Tables B.1 and B.2 shall operate within the limits defined in EN 300 674-1:

Table B.1 — Downlink parameters

Item No.	Parameter	Value(s)	Remarks
D6 (*)	Modulation	Two level amplitude modulation.	
D6a (*)	Modulation Index	0.5 ... 0.9	
D6b (*)	Eye Pattern	≤90 % (time) / ≤85 % (amplitude)	
D7 (*)	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.	
D8 (*)	Bit rate	500 kBit/s	
D8a	Tolerance of Bit Clock	better than ±100 ppm	

Table B.1 *(continued)*

Item No.	Parameter	Value(s)	Remarks
D9a	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].	
D10	Wake-up trigger for OBU	OBU (IVS) shall wake up on receiving any frame with 11 or more octets (including preamble)	No special wake-up pattern is necessary. OBU (IVS) may wake up on receiving a frame with less than 11 octets
D10a	Maximum Start Time	≤5 ms	
D11	Communication zone	Spatial region within which a B.E.R. according to D9a is achieved	
D13	Preamble	Preamble is mandatory.	
D13a	Preamble Length and Pattern	16 bits ± 1 bit of FM0 coded “1” bits	
D13b	Preamble Wave form	An alternating sequence of low level and high level with pulse duration of 2 µs. The tolerance is given by D8, D8a and D6b.	
D13c	Trailing Bits	The RSU (interrogator) is permitted to transmit a maximum of 8 bits after the end flag. An OBU (IVS) is not required to take these additional bits into account.	

Table B.2 — Uplink parameters

Item No.	Parameter	Value(s)	Remark
U6	Sub-Carrier Modulation	2-PSK Encoded data synchronized with sub-carrier: Transitions of encoded data coincide with transitions of sub- carrier.	
U6b	Eye Pattern/Duty Cycle	Eye pattern: ≤90 % / ≤90 %; or Duty Cycle: 50 % ± ±, ± ≤5 %	
U6c	Modulation on Carrier	Multiplication of modulated sub-carrier with carrier.	
U7 (*)	Data Coding	NRZI (No transition at beginning of "1" bit, transition at beginning of "0" bit, no transition within bit)	
U8 (*)	Bit Rate	250 kbit/s	
U8a	Tolerance of Bit Clock	Within ±1 000 ppm	
U9a	B.E.R.	≤10^{-6}	

Table B.2 *(continued)*

Item No.	Parameter	Value(s)	Remark
U11	Communication Zone	The spatial region within which the OBU (IVS) is situated such that its transmissions are received by the RSU (interrogator) with a B.E.R. of less than that given by U9a.	
U13	Preamble	Preamble is mandatory.	
U13a	Preamble Length and Pattern	32 to 36 µs modulated with sub-carrier only, then 8 bits of NRZI coded "0" bits.	
U13b	Trailing Bits	The OBU (IVS) is permitted to transmit a maximum of 8 bits after the end flag. An RSU is not required to take these additional bits into account.	

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 must be present in the IVS such that an operator of an interrogator can read the same data from all IVS/weigh-in-motion systems 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 must be able to receive the same information irrespective of IVS/weigh-in-motion system 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 100 metres of an operational 5,8 GHz DSRC EFC 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 are 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 as 'frame', without the LPDU (Link layer Protocol Data Unit) field, which is used in some specific situations.

This 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 is a single octet (please 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

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. WIM 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 in clear 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 who shall have the responsibility to ensure that all communicating parties have access to, instruction how to use their security provisions.

B.1.6.5 WIM LPDU

The data for the WIM 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 below 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: *WIM* = 20 (RTM = 9)	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: *WIM* = 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 WIM 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		
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 or to requirements specified by a jurisdiction, and operating within the parameters of EN 300 674-1 and B.1.5 above.

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

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 EN 300 674-1, 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 weigh-in-motion system) shall be a function of commercial design, operating within the limitations defined in EN 300 674-1, and the design and performance specifications defined in this annex or taking into consideration the data requirements of the jurisdiction.

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

The vehicle unit VU shall connect with the IVS-DSRC using fixed cable of 2 m, using a Straight DIN 41612 H11 Connector – 11 pin approved male connector to match a similar DIN/ISO approved Straight DIN 41612 H11 Connector female connector on the VU manufacturer device) or shall connect with the IVS-DSRC using Bluetooth Low Energy (BLE).

The IVS 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 the limitations defined in 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 not be bound by the constraints of EN 12253 except for the parameters defined in B.1.5, thus providing greater flexibility for equipment design and instantiation in this reading environment.

B.1.6.10 IVS antenna form factor

The design of the IVS-DSRC antenna shall be a function of commercial design, operating within the limitations defined in EN 300 674-1. Specifically, the IVS antenna design shall not be bound by the constraints of EN 12253 except for the parameters defined in B.1.5, thus providing greater flexibility for equipment design and instantiation in this reading environment.

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 a WIM LPDU transaction as defined within this Annex, at a distance of 2 m to 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;

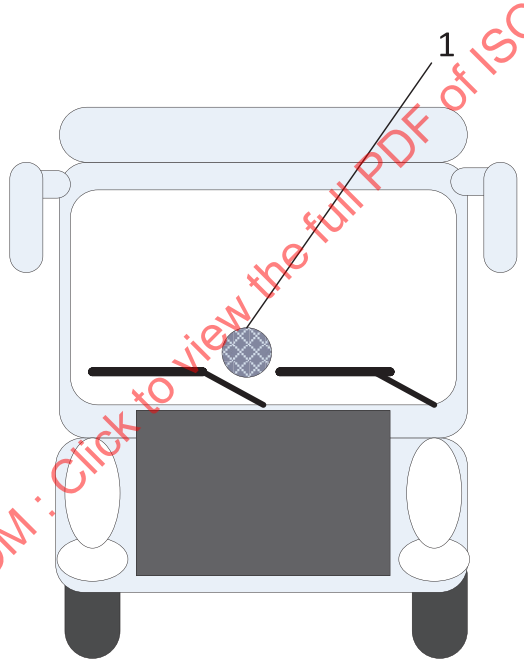
— at least 10 cm above the windshield wiper at rest;

— less than 50 cm above the windshield wiper at rest.

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 it faces at approximately 90° to the surface of the road (i.e. vertical orientation).

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



Key

1 DSRC antenna location

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

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 a WIM LPDU transaction as defined within this document, at a distance of 2 m to 10 m, better than 99 % of the time, averaged over 1 000 read interrogations.

B.1.7 Data retrieval 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 WIM application this will simply be the service with the AID value = 2 (Freight&Fleet). The IVS 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 the WIM application, the IVS-DSRC shall shut down its transaction with the interrogator.

— Step 2 The IVS 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 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 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 WIM, the parameter value shall be 20.

— 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 that is not supporting the WIM standard), 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:

  a) the attribute RtmData (payload element + security element) as specified in B.2.1.6, in case of Communication Profile C1;

  b) 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 to terminate the session and stop the IVS 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 below.

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 WIM operating in a multi-service environment

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

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

where:

— N is the number of applications in the sequence;

— n is a specific application reference code (e.g. 20 = WIM, 9 = RTM).

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.

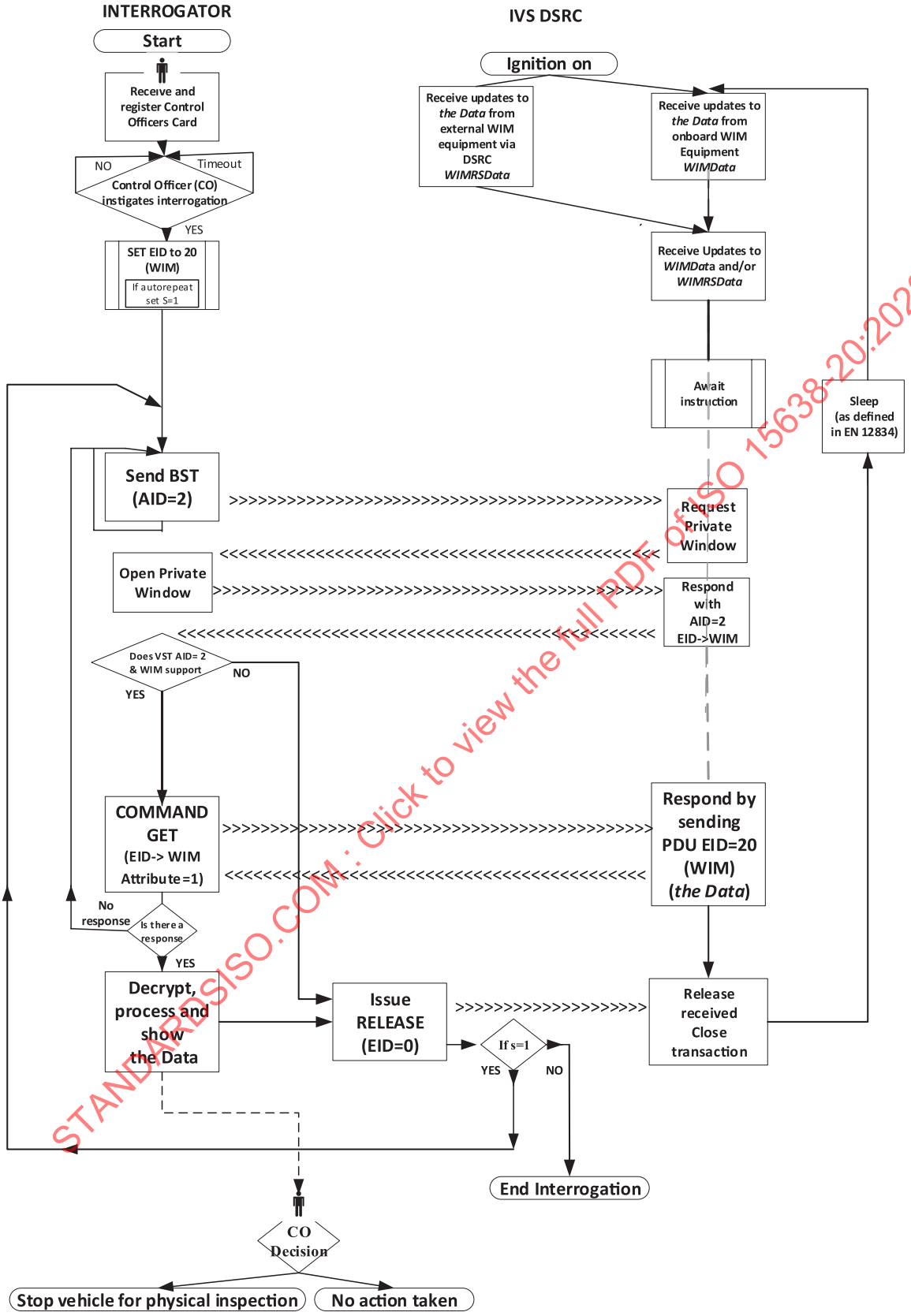


Figure B.5 — WIM over 5,8 GHz DSRC process flow

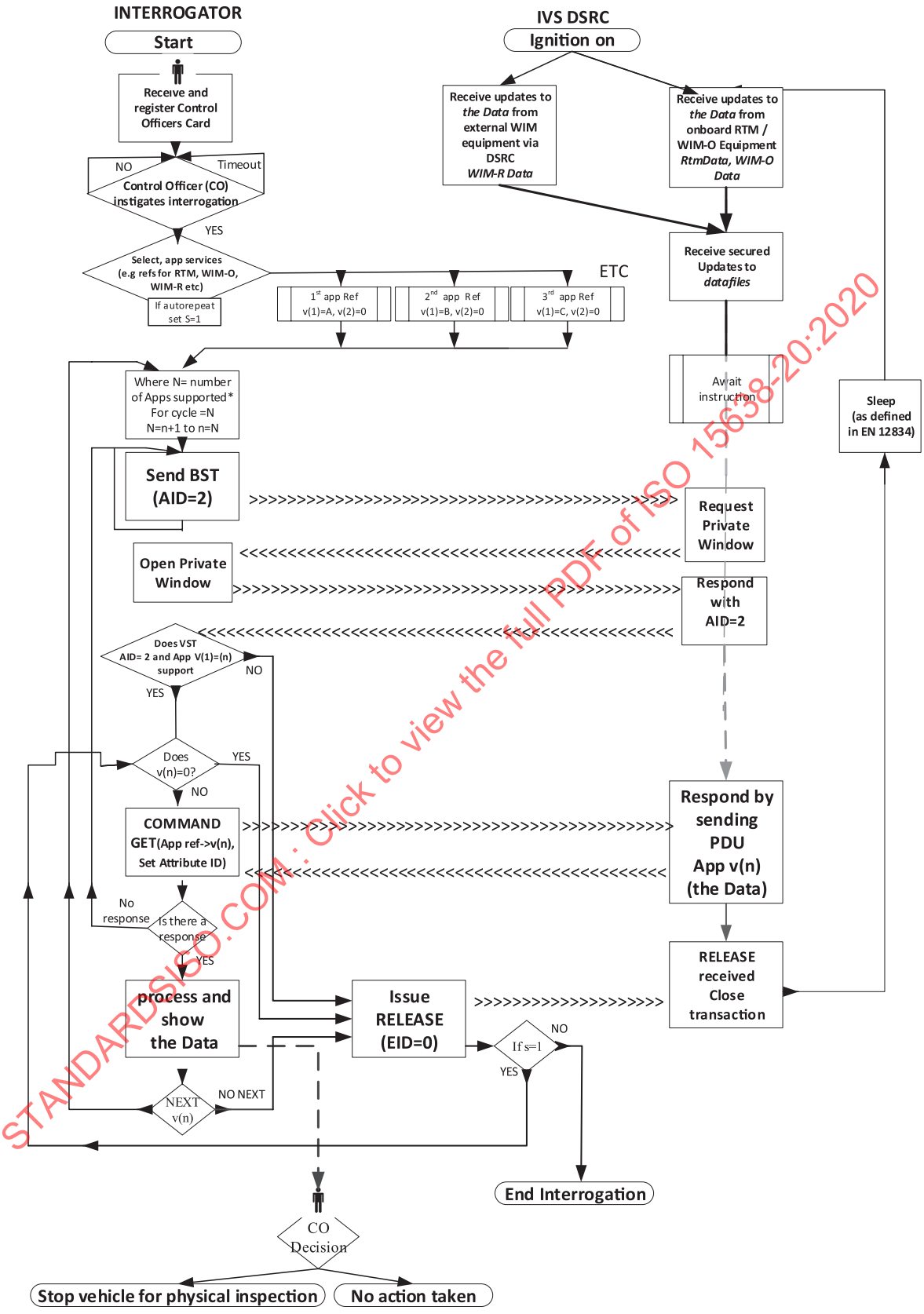


Figure B.6 — Multiple application interrogation over 5,8 GHz DSRC process flow

B.1.7.4 Commands

The following commands are the only functions used in a WIM-0/WIM-R transaction phase.

B.1.7.4.1 INITIALISATION.request: A command, issued from the interrogator in the form of a broadcast with definition of applications that the interrogator supports.

B.1.7.4.2 INITIALISATION.response: An answer from the IVS-DSRC confirming the connection and containing a list of supported application instances with characteristics and information on how to address them (EID).

B.1.7.4.4 Data-Retrieval.request: A command, issued from the interrogator to the IVS-DSRC, 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 Data-Retrieval command is for the interrogator to obtain the Data from the IVS-DSRC.

B.1.7.4.5 Data-Retrieval.response: An answer from the IVS-DSRC that contains the Data requested.

B.1.7.4.6 Upload.Request: A command, issued from the interrogator to the IVS-DSRC, 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 upload it to the 'Service Provider ' identified by the specific URL.

NOTE The objective of the Upload.Request is for the interrogator to make the IVS-DSRC deliver the Data to a Service provider.

B.1.7.4.7 Upload.Response: An answer from the IVS-DSRC on the UPLOAD command.

B.1.7.4.8 DataTx.request: A command, issued from the interrogator to the IVS-DSRC, that specifies the application instantiation to be addressed by means of a defined EID, as received in the VST, instructing the IVS-DSRC to receive the selected attribute(s) with the Data. The objective of the DataTx command is for the interrogator to deliver the Data to the IVS-DSRC.

B.1.7.4.9 DataTx.response: An answer from the IVS-DSRC that acknowledges the reception of the data transferred by a DataTx.request.

B.1.7.4.10 TestComm.request: A command, instructing the IVS-DSRC to send back data from the IVS-DSRC to the interrogator. The objective of the TestComm command is to enable workshops or type approval test facilities to test that the DSRC link is working without needing access to WIM data.

B.1.7.4.10 TestComm.response: An answer from the DSRC VU on the TestComm request.

B.1.7.4.11 Terminate.request (RELEASE): A command, instructing the IVS-DSRC that the transaction is ended. The objective of the Terminate command is to end the session with the IVS-DSRC. On receipt of the Terminate 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.

B.1.7.5 Interrogation command sequence

From the perspective of the command and response sequence, the transaction is described in the following Tables B.9 and B.10

Table B.9 — Commands and responses sequence in a WIM GET transaction

Sequence	Sender	Receiver	Description	Action
1	interrogator	IVS-DSRC	Initialisation of the communication link – Request	interrogator broadcasts BST
2	IVS-DSRC	interrogator	Initialisation of the communication link – Response	If BST supports AID = 2 then DSRC-VU Requests a private window
3	interrogator	IVS-DSRC	Grants a private window	Sends Frame containing private window allocation
4	IVS-DSRC	interrogator	Sends VST	Sends Frame comprising VST
5	interrogator	IVS-DSRC	Sends GET.request for data in Attribute for specific EID	
6	IVS-DSRC	interrogator	Sends GET.response with requested Attribute for specific EID	Sends Attribute (WIMData.) with data for specific EID
7	interrogator	IVS-DSRC	Sends RELEASE command which closes transaction	Acknowledges positive result by closing transaction

Table B.10 — Commands and responses sequence in a WIM SET transaction

Sequence	Sender	Receiver	Description	Action
1	interrogator	IVS-DSRC	Initialisation of the communication link – Request	interrogator broadcasts BST
2	IVS-DSRC	interrogator	Initialisation of the communication link – Response	If BST supports AID = 2 then IVS-DSRC requests a private window
3	interrogator	IVS-DSRC	Grants a private window	Sends Frame containing private window allocation
4	IVS-DSRC	interrogator	Sends VST	Sends Frame comprising VST
5	interrogator	IVS-DSRC	Sends SET.request with data in Attribute for specific EID	
6	IVS-DSRC	interrogator	Sends SET.response with ack Attribute for specific EID	
7	interrogator	IVS-DSRC	Sends RELEASE command which closes transaction	Acknowledges positive result by closing transaction

The two basic operations (SET and GET) may be intermixed inside a single transaction, provided the execution time does not exceed the time in which the vehicle remains in the DSRC communication zone.

An example of the transaction sequence and contents of the exchanged frames is in B.2.1.6.

B.1.8 Data structures

The payload (WIM-0/WIM-R data) consists of the concatenation of:

1. EncryptedWIMPayload data, which is the encryption of the WIMPayload defined in ASN.1 in C.3.2. The method of encryption is described in Tachograph Regulations Appendix 11;

2. DSRCSecurityData, specified in Tachograph Regulations Appendix 11.

The WIM-0/WIM-R data are being addressed as WIM Attributes and are transferred in the WIM container = 10.

The Attribute identifiers are assigned as specified in Table B.11.

Table B.11 — WIM attribute identifiers

Identifier	Attribute
1	WIM-R
2	WIM-O

B.1.9 ASN.1 module for the WIM DSRC transaction

The ASN.1 module definition for the DSRC data within the WIM application is defined in Annex C.

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

B.1.9.1 Window management

B.1.9.1.1 General

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).

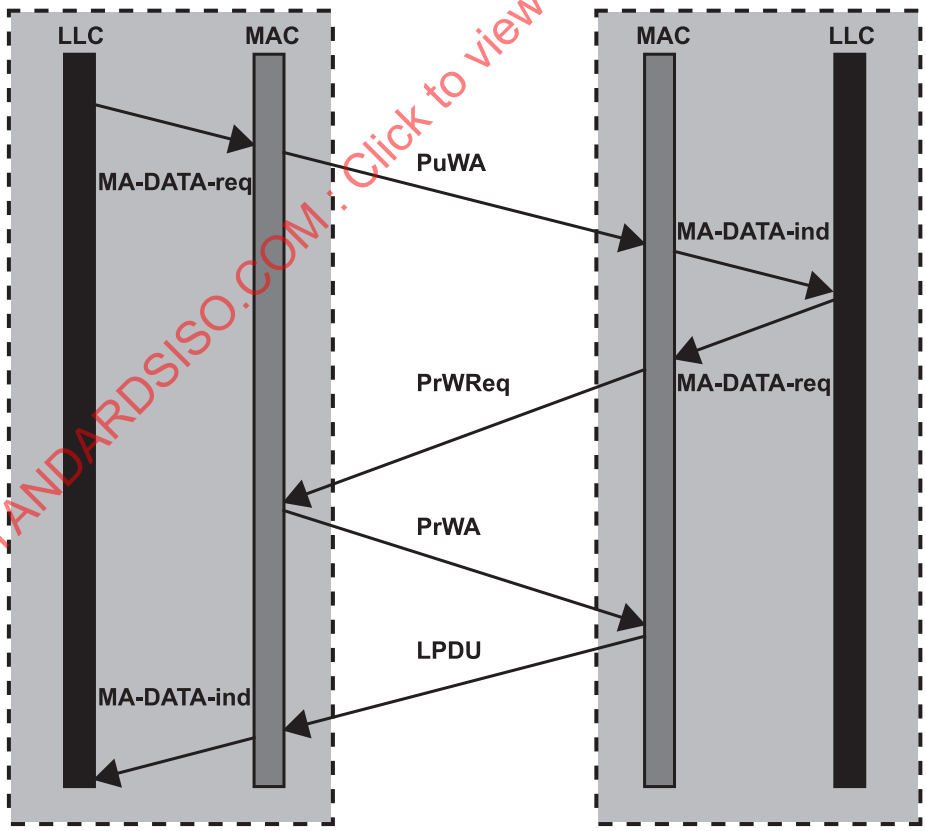


Figure B.7 — Communication example between interrogator and IVS

B.1.9.1.3 State machine

B.1.9.1.3.1 MA-DATA.request

The primitive shall be 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 WIM application, this equates to the GET_WIM_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 shall provide the following parameters:

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

The link identifier (LID) shall be 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 shall be included in the frame transmitted).

The response request (RR) shall indicate whether or not the fixed equipment shall allocate 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_WIM_LPDU [Value for WIM = 20]) and the frame of WIM data will be provided by the IVS to the interrogator.

B.1.9.1.3.2 MA-DATA.indication

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

The primitive shall provide the following parameters

MA-DATA.indication(LID, LPDU)

The LID shall be 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.

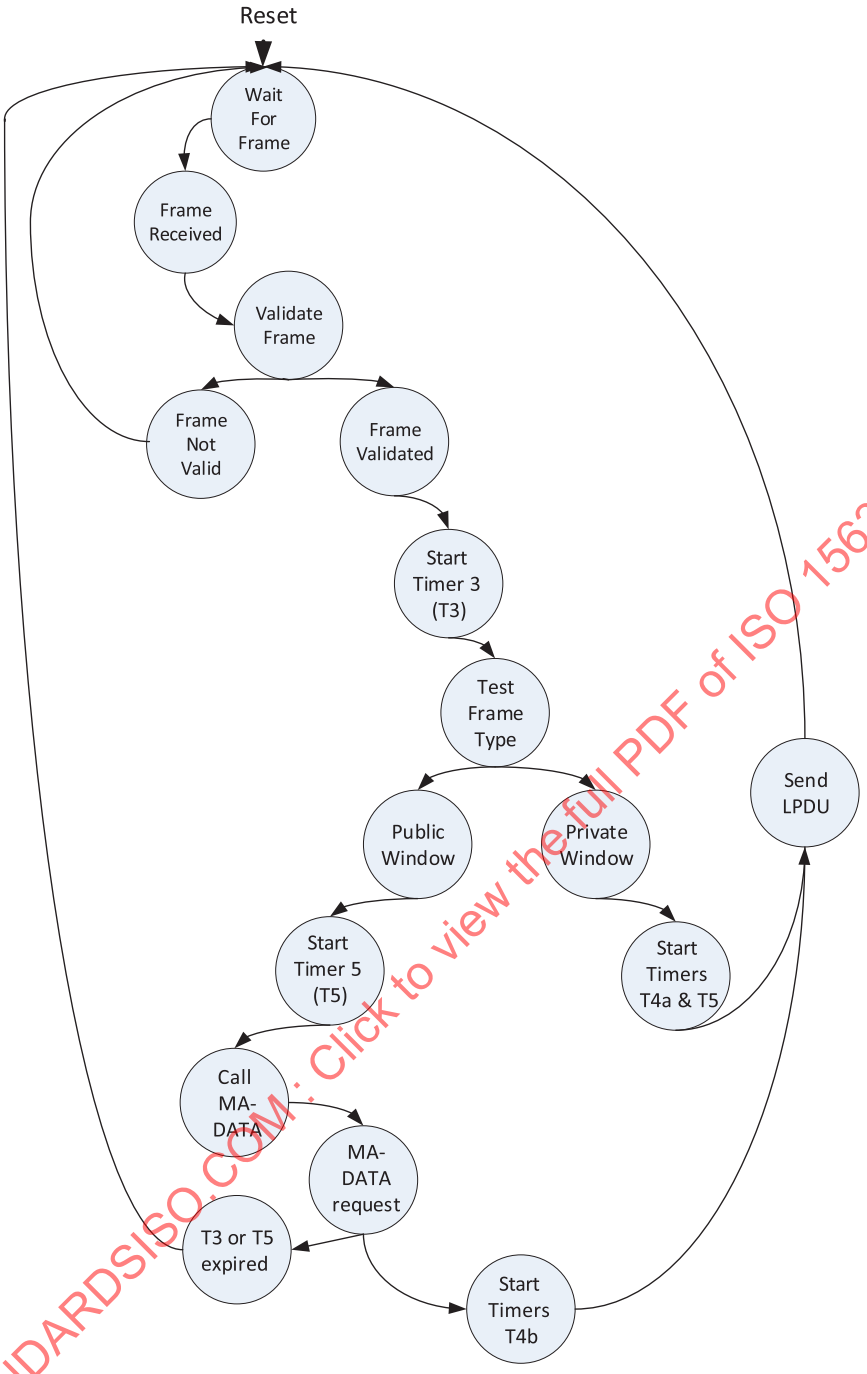


Figure B.8 — State machine describing the MAC layer behaviour of the IVS

B.1.9.3 State transitions

B.1.9.3.1 General

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 at 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

In this state, 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.

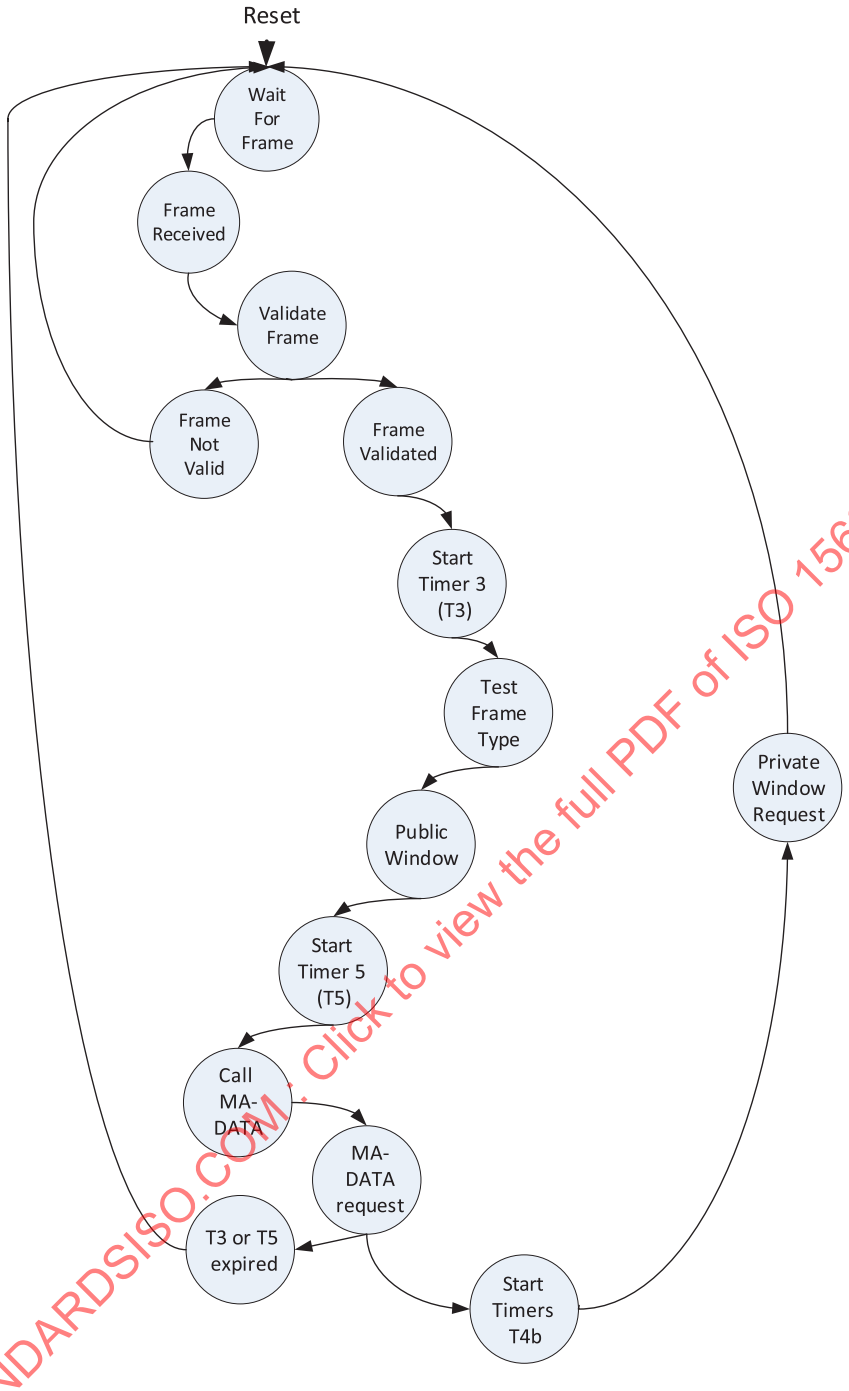


Figure B.9 — State machine concerning only the Public Uplink

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. It 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.

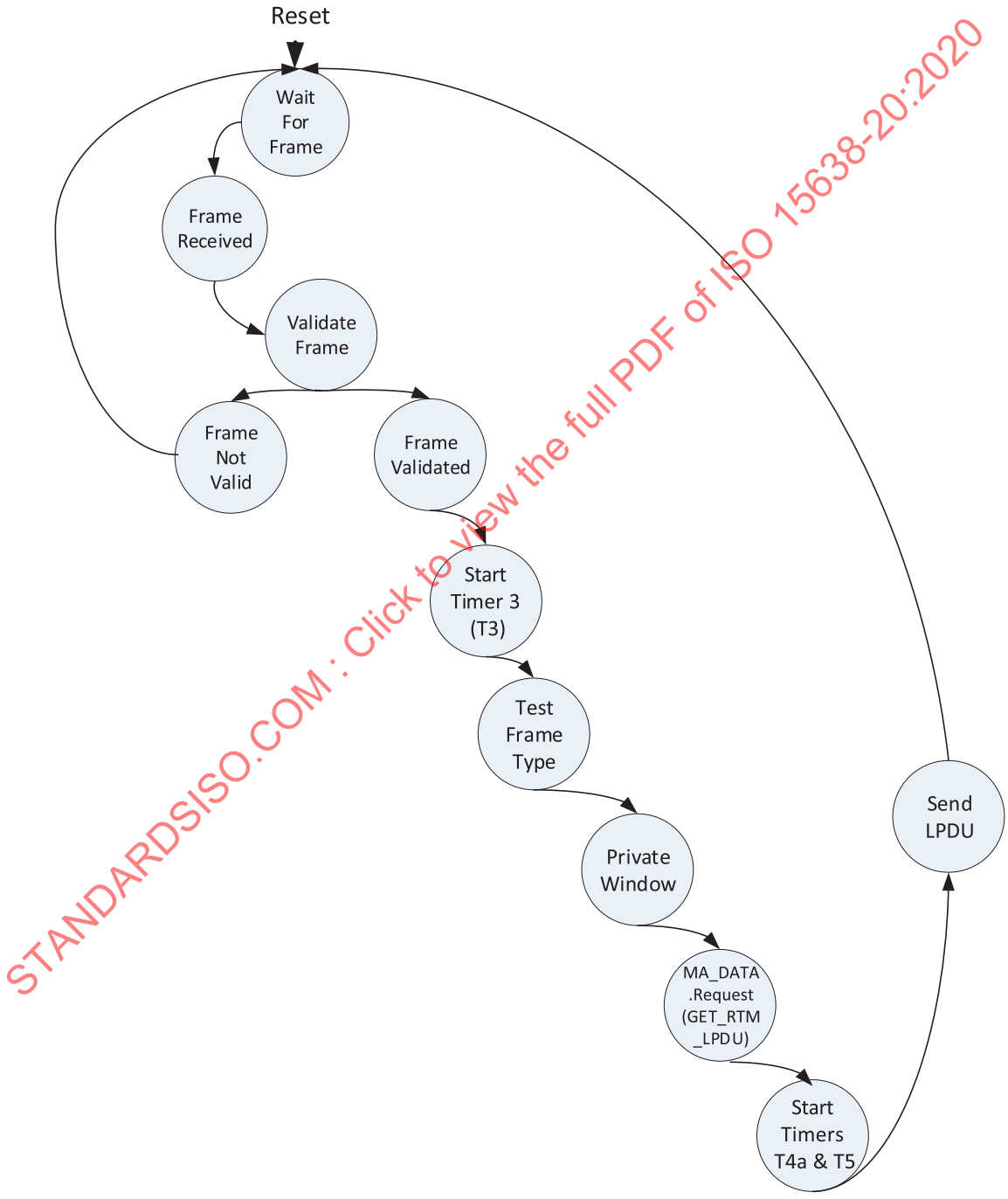


Figure B.10 — State machine concerning only the Private Uplink branch

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 Timer 4a (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 WIM applications.

B.2 5,8 GHz DSRC functions for weigh-in-motion

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 CEN 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 outside 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 (e.g. keys) which 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, or 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 WIM 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 above.

B.2.1.5 Data transfer mechanism

Payload data defined previously are requested by the interrogator after the 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).

The ASN.1 module definition for WIM is defined as follows:


```
TarvWIM {iso(1) standard(0) 15638 part20(20) version1(1)} DEFINITIONS AUTOMATIC TAGS

::= BEGIN

IMPORTS

-- Imports data attributes and elements from EFC which are used for WIM

LPN, Provider

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,
Set-Request, Set-Response, Time, T-APDUs, VST

FROM EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)};

-- Imports data elements from RTM

Rtm-ContextMark

FROM TarvRtm {iso(1) standard(0) 15638 part9(9) version1(1)}

-- Definitions of the WIM functions

WIM-InitialiseComm-Request ::= BST

WIM-InitialiseComm-Response ::= VST

WIM-DataRetrieval-Request    ::=    Get-Request    (WITH    COMPONENTS    {eid,    attrIdList,
accessCredentials ABSENT})

WIM-DataRetrieval-Response ::= Get-Response {WimContainer} (WITH COMPONENTS {..., eid, iid
ABSENT})

WIM-DataTx-Request::= Set-Request {WimContainer} (WITH COMPONENTS {..., accessCredentials
ABSENT, iid ABSENT})

WIM-DataTx-Response::= Set-Response (WITH COMPONENTS {..., iid ABSENT, ret PRESENT})

WIM-Upload-Request ::= Action-Request {WimContainer} (WITH COMPONENTS {…, Actiontype(15),
accessCredentials ABSENT, iid ABSENT )

WIM-Upload-Response ::= Action-Response {WimContainer} (WITH COMPONENTS {…, iid ABSENT )

WIM-TerminateComm::=  Event-Report-Request  {WimContainer}(WITH  COMPONENTS  {mode  (FALSE),
eid (0),

eventType (0)})

WIM-TestComm-Request::=  Action-Request  {WimContainer}  (WITH  COMPONENTS  {...,  eid  (0),
actionType

(15), accessCredentials ABSENT, iid ABSENT})
```

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

-- Definitions of the WIM attributes:

WimData ::= SEQUENCE {

    encryptedWimPayload OCTET STRING (SIZE(51)) (CONSTRAINED BY { -- calculated encrypting
WimOData as per Tachograph Regulations Appendix 11 --}),

    DSRCSecurityData OCTET STRING

    }


WimOData ::= SEQUENCE {

                  wimRegistrationPlate LPN,

                  wimRecordedWeight INTEGER (0..65535), -- Total measured weight with 10
Kg resolution.

                  wimAxlesConfiguration OCTET STRING SIZE (2),-- 10 bits for recorded
number of axles

                  wimAxlesRecordedWeight SEQUENCE (SIZE (10)) OF INTEGER (0..65535),--
Weight for each axle

                  wimTimestamp INTEGER(0..4294967295), -- Timestamp of current record

                  }

WimRData ::= SEQUENCE {

                  registeredData WimOData, -- data measured in the same format as data
on board

                  wimRLocation Provider  -- Country code followed by a Country-assigned
unique INTEGER

                  }

WimDestRef::=SEQUENCE{

  DEST  IA5String (SIZE(80)) -- requested destination IP address url for the data

  REF   IA5String (SIZE(020))      -- reference of unique significance for the inspector

  }


WimActionParameter ::= SEQUENCE {

  destRef RtmDestRef,

  attributeList SEQUENCE OF {AttributeId} SIZE (10)

  }

WimContextMark ::= RtmContextMark

WimTransferAck ::= INTEGER {

                Ok     (1),
```

```
                NoK     (2)
                } SIZE (1..255)

WimContainer ::= 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{WimContainer},
    wimData                     [10] WimData,
    wimContextmark              [11] Rtm-ContextMark,
    wimRData                    [12] WimRData,
    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.2.1.6 WIM Transaction to obtain data

Communication between ITS-stations of the interrogator / roadside and the vehicle and the DSRC lilnk requirements are as described in B.1 above.

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

Initialisation is performed according to the provisions of B.2.1.6 and Tables B.12 to B.25. In the initiation phase, the interrogator starts sending a frame containing a BST (Beacon Service Table) according to EN 12795 and EN 13372:2012, 6.3.2, 7.1.1, and 7.1.2. The following tables give a practical example of an interrogation session.

In the Initialisation phase, the interrogator starts sending a BST. See Table B.12.

Table B.12 — 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.13.

Table B.13 — Initialisation _ BST frame contents

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 indicator BeaconID	0	NonMand applications not present
	SEQUENCE { ManufacturerId INTE-		
	GER(0..65535)	xxx	Manufacturer Identifier
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 of mandApplications = 1
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

Table B.13 *(continued)*

Octet #	Attribute field	bits in octet	Description
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 13372:2012, 7.1.1, with no specific WIM settings. Table B.14 provides an example of bit encoding.

Table B.14 — 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 13372:2012, 7.1.1 with no specific WIM settings.

Table B.15 provides an example of bit encoding.

Table B.15 — 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 13372:2012, 6.3.2, 7.1.1, and 7.1.3 with settings as specified Table B.16, using the allocated transmission window.

Table B.16 — 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

Table B.16 *(continued)*

Field	Settings
Parameter	No extension, Container choice 11, followed by WIM 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 Wim Context mark, which is composed of an OBJECT IDENTIFIER representing the related standard, its part (20 for WIM) 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.17, with an indication of bit encodings, is given in Table B.17, where the IVS-DSRC only supports Communication Profile C1.

Table B.17 — 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 {	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 0001	No extension, 1 application
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 IVS DSRC function and identifying the application instance.
14	Parameter Container	0000 0010	No extension, Container Choice = 02_{10}, Wim Context Mark, Octet string
15		0000 1000	No extension, Wim Context Mark length = 8_{10}

Table B.17 *(continued)*

Octet #	Attribute field	bits in octet	Description
16	Wim-ContextMark ::= SEQUENCE {	0000 0110	Object Identifier of the supported standard, part, and version. Example: ISO (1) Standard (0) TARV (15638) part20(20) Version1 (1). First octet is 06H, which is the Object Identifier Second octet is 06H, which is its length. Subsequent 6 octets encode the example Object Identifier
17	StandardIdentifier,	0000 0110	
18	}	0010 1000	
19		1000 0000	
20		1111 1010	
21		0001 0110	
22		0001 0100	
23		0000 0001	
24	ObeConfiguration Sequence { OPTION indicator	0	ObeStatus not present
25	EquipmentClass INTEGER (0..32767)	xxxx xxxx	
26	ManufacturerId INTEGER (0..65535) }	xxxx xxxx	Manufacturer identifier for the IVS-DSRC. See ISO 14816 Register.
27		xxxx xxxx	
28	FCS	xxxx xxxx	Frame check sequence
29		xxxx xxxx	
30	Flag	0111 1110	End Flag

The following Table B.18 shows an example of VST generated by an IVS-DSRC that supports Communication Profile C1 and Communication Profile C2.

Table B.18 — Initialisation — 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
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	00 0010	No extension. AID= 2 Freight&Fleet
	AID DSRCApplicationEntityID		
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}, Wim Context Mark, Octet string
15		0000 1001	No extension, Wim Context Mark length = 9_{10}

Table B.18 *(continued)*

Octet #	Attribute field	bits in octet	Description
16	Wim-ContextMark ::= SEQUENCE	0000 0110	Object Identifier of the supported standard, part, and version. Example: ISO (1) Standard (0) TARV (15638) part20(20) Version1 (1). First octet is 06H, which is the Object Identifier Second octet is 06H, which is its length. Subsequent 6 octets encode the example Object Identifier
17	{	0000 0110	
18	StandardIdentifier,	0010 1000	
19	WimCommProfile }	1000 0000	
20		1111 1010	
21		0001 0110	
22		0001 0100	
23		0000 0001	
24		0000 0001	Communication Profile C1
25	SEQUENCE {	1	EID present
	OPTION indicator	1	Parameter present
	OPTION indicator AID DSRCApplicationEntityID	00 0010	No extension. AID= 2 Freight&Fleet
26	EID Dsrc-EID	xxxx xxxx	Generated by the OBU and identifying the application instance.
27	Parameter Container {	0000 0010	No extension, Container Choice = 02_{10}, Wim Context Mark, Octet string
28		0000 1001	No extension, Wim Context Mark length = 9_{10}
29	Wim-ContextMark ::= SEQUENCE	0000 0110	Object Identifier of the supported standard, part, and version. Example: ISO (1) Standard (0) TARV (15638) part20(20) Version1 (1). First octet is 06H, which is the Object Identifier Second octet is 06H, which is its length. Subsequent 6 octets encode the example Object Identifier
30	{	0000 0110	
31	StandardIdentifier,	0010 1000	
32	WimCommProfile }	1000 0000	
33		1111 1010	
34		0001 0110	
35		0001 0100	
36		0000 0001	
37		0000 0010	Communication Profile C2
38	ObeConfiguration Sequence { OPTION indicator	0	ObeStatus not present
39	EquipmentClass INTEGER (0..32767)	xxxx xxxx	
40	ManufacturerId INTEGER (0..65535) }	xxxx xxxx	Manufacturer identifier for the IVS-DSRC. See ISO 14816 Register.
41	FCS	xxxx xxxx	Frame check sequence
42		xxxx xxxx	
43	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.19.

Table B.19 — Presentation — GET request frame settings

Field	Settings
Invoker Identifier (IID)	Not present
Link Identifier (LID)	Link address of the specific IVS DSRC
Chaining	No

Table B.19 *(continued)*

Field	Settings
Element Identifier (EID)	As specified in the VST. No extension
Access Credentials	No
AttributeIdList	No extension, 1 attribute, AttributeID = 1 (WimData)
Fragmentation	No
Layer2 settings	Command PDU, Polled ACn command

Table B.20 shows an example of reading the WIM data that belong to the ISO TARV series of standards.

Table B.20 — Presentation — Get 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
9	Get.request SEQUENCE { Option Option Option Fill BIT STRING(SIZE(1)) }	0110	Get request
		0	Access Credentials not present
		0	IID not present
		1	Attribute List present
		0	Set to 0.
10	EID (INTEGER(0..127)	xxxx xxxx	The EID of the WIM 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, WimData. 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 GET request, sends a GET response with the requested data conforming to the GET response defined in EN 12834, with settings as specified in Table B.21.

Table B.21 — Presentation — GET 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.22 shows an example of reading the WIM data that belong to the TARV suite of standards.

Table B.22 — 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
10	Get.response SEQUENCE {	0111	Get response
	Option Option Option Fill }	0	IID not present
		1	Attribute List present
		0	Return status not present
		0	Not used
11	EID	xxxx xxxx	Responding from the WIM application instance. No extension.
12	AttributeIdList SEQUENCE OF {	0000 0001	No extension, number of attributes = 1
13	Attributes SEQUENCE { AttributeId	0000 1010	No extension, AttributeId=1 (WimData)
14	AttributeValue CONTAINER	0000 1010	No extension, Container Choice = 10_{10}, Octet string
15		0110 0100	No extension, example OCTET STRING length = 100
16		xxxx xxxx	Up to 110 octets including 50 octets for Security data
17		xxxx xxxx	
18		xxxx xxxx	
...		....	
126	FCS	xxxx xxxx	Frame check sequence
127		xxxx xxxx	
128	Flag	0111 1110	End Flag

In the case of Communication Profile C2, the interrogator then instructs the IVS-DSRC to deliver requested data to a specified URL of Service Provider, by issuing an UPLOAD command, conforming to the ACTION command defined in EN 12834, with no specific settings for WIM.

Table B.23 shows an example of UPLOAD request.

Table B.23 — Presentation — UPLOAD Request frame example

Octet #	Attribute field	Bits in octet	Description
1	FLAG	0111 1110	Start flag

Table B.23 *(continued)*

Octet #	Attribute field	Bits in octet	Description
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
9	ACTION.request SEQUENCE {	0000	Action request (TRANSFER CHANNEL)
	Option indicator	0	Access Credentials not present
	Option indicator	1	Action parameter present
	Option indicator	0	IID not present
	Mode BOOLEAN }	1	Response expected
10	EID INTEGER (0..127)	xxxx xxxx	Generated by the OBU and identifying the application instance.
11	ActionType INTEGER (0..127)	0000 1000	No extension, Action type TRANSFER CHANNEL request
12	ActionParameter CONTAINER {	0000 0010	No extension, Container Choice = 2
13		0000 0000	No extension. OctetString length = 100 octets
16	WimActionParameter SEQUENCE { WimDestRef SEQUENCE { dest	xxxx xxxx	70 characters for the requested URL of the data, right aligned and padded with blanks
86	ref }	xxxx xxxx	20 characters as unique reference for the inspector
106	Attributes SEQUENCE OF {	0000 1010	No extension, number of attributes to be transferred (example of max 10 attributes)
107	AttributeId }	xxxx xxxx	Attributes Id's
116	FCS	xxxx xxxx	Frame check sequence
117		xxxx xxxx	
118	Flag	0111 1110	End Flag

In the Communication Profile C2, the IVS-DSRC, when receiving the UPLOAD request, sends an ACTION response as defined in EN 12834, with no specific settings.

Table B.24 shows an example of reading the WIM data that belong to the ISO TARV series of standards.

Table B.24 — Presentation — ACTION 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 VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1101 0000	Response PDU
7	LLC Control field	n111 0111	ACn command n bit

Table B.24 *(continued)*

Octet #	Attribute field	Bits in octet	Description
8	LLC status field	0000 0000	Response available
9	Fragmentation header	1xxx x001	No fragmentation
10	ACTION.response SEQUENCE {	0001	ACTION response (TRANSFER CHANNEL)
	Option indicator	0	IID not present
	Option indicator	1	Response parameter present
	Option indicator	0	Return status not present
	Fill BIT STRING (SIZE (1))	0	Not used
11	EID INTEGER (0..127)	0000 xxxx	No extension, EID as set in the VST
12	ResponseParameter CONTAINER {	0000 0010	No extension, container choice = 2
13		0000 0001	No extension, string length = 1 octets
16	WimTransferAck }	0000 0001	No extension, example positive ack
14	FCS	xxxx xxxx	Frame check sequence
15		xxxx xxxx	
16	Flag	0111 1110	End Flag

The interrogator then closes the connection by issuing a RELEASE command conforming to EN 12834:2003, 7.3.8, with no specific WIM settings. Table B.25 shows a bit encoding example of the RELEASE command.

Table B.25 — Termination — Release command 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	1000 s000	The frame contains a command LPDU
7	LLC Control field	0000 0011	UI command
8	Fragmentation header	1xxx x001	No fragmentation
9	EVENT_REPORT.request SEQUENCE {	0010	EVENT_REPORT (Release)
	Option indicator	0	Access Credentials not present
	Option indicator	0	Event parameter not present
	Option indicator	0	IID not present
	Mode BOOLEAN	0	No response expected
10	EID INTEGER (0..127)	0000 0000	No extension, EID = 0 (System)
11	EventType (INTEGER (0..127) }	0000 0000	Event type 0 = Release
12	FCS	xxxx xxxx	Frame check sequence
13		xxxx xxxx	
14	Flag	0111 1110	End Flag

The interrogator terminates the communication with the command "**RELEASE**".

The IVS DSRC is not expected to answer to the RELEASE command. The communication is then closed.

B.3 Error handling

B.3.1 Recording of the data in the IVS

The data shall be provided, already encrypted, by the IVS.

B.3.2 Communication errors

Communication error handling shall be as defined in the related DSRC standards, namely EN 300 674-1, EN 12253, EN 12795 and EN 12834.

B.3.3 Encryption and signature errors

Data is passed across the DSRC interface already encrypted and together with security data. If the interrogator fails to successfully decrypt data, the incident shall be recorded in the interrogator for quality control purposes. If the data is technically decrypted but makes no sense to the operator of the interrogator, the operator shall be provided with means to record that the decryption was unsuccessful for quality control purposes. The means by which these events are reported are a function of product design and not specified in this document.

B.3.4 Recording of errors

B.3.4.1 Dynamic wireless communication

The DSRC medium is a dynamic wireless communication in an environment of uncertain atmospheric and interference conditions, particularly in the 'portable interrogator' and 'moving vehicle' combinations involved in this application. It is therefore necessary to ascertain the difference between a 'read failure' and an 'error' condition. In a transaction across a wireless interface, read failure is common and the consequence is usually to retry, i.e. rebroadcast the BST and reattempt the sequence, which will in most circumstances lead to a successful communication connection and transfer of data, unless the target vehicle moves out of range during the time required to retransmit. (A 'successful' instance of a 'read' may have involved several attempts and retries).

Read failure may be because the antennas were not paired properly (failure of 'aiming'), because one of the antennas is shielded – this may be deliberate, but also can be caused by the physical presence of another vehicle, radio interference, especially from circa 5,8 GHz WIFI or other public access wireless communications, or may be caused by radar interference, or difficult atmospheric conditions (e.g. during a thunderstorm), or simply by moving out of the range of the DSRC communication. Individual instances of read failures, by their nature, cannot be recorded, simply because the communication simply did not occur.

However, if the agent of the jurisdiction targets a vehicle and attempts to interrogate its IVS, but no successful transfer of data ensues, this failure could have occurred because of deliberate tampering, and therefore the agent of the jurisdiction needs a means to log the failure, and alert colleagues downstream that there may be a violation. The colleagues can then, for example, stop the vehicle and carry out a physical inspection. However, as no successful communication has taken place, the DSRC system cannot provide data concerning the failure.

B.3.4.2 Recommendation to use digital imaging in support of DSRC

It is therefore recommended that interrogators are equipped with a digital camera of good resolution that, in the event that the agent of the competent control authority triggers a read, and no read ensues, a digital photograph is automatically taken and the image provided to the agent of the jurisdiction, or colleagues downstream. It is also recommended that interrogators are equipped with optical recognition software to recognize and digitize the licence plate of the targeted vehicle.

It is also recommended that interrogators match the vehicle registration number obtained via the IVS with the digital representation of that optically recorded by the digital camera of the interrogator, and report any anomaly to the operator of the interrogator.

The means by which such failure to reconcile are reported are not specified and are a matter for product design or data requirements of the jurisdiction.

B.3.4.3 Failure to read

'Failure to read' is technically different to an 'error'. In this context an 'error' is the acquisition of a wrong value.

Data transferred to the IVS is supplied encrypted, therefore shall be verified by the supplier of the data (see B.5).

Data subsequently transferred across the air interface is checked by cyclic redundancy checks at the communications level. If the CRC validates, then the data is correct. If the CRC does not validate, the data is retransmitted. The probability that data could successfully pass through a CRC incorrectly is statistically so highly improbable that it may be discounted.

If the CRC does not validate and there is no time to retransmit and receive the correct data, then the result will not be an error, but an instantiation of a specific type of read failure.

The only meaningful 'failure' data that can be recorded is that of the number of successful initiations of transactions that occur, that do not result in a successful transfer of data to the interrogator.

The interrogator shall therefore record, time-stamped, the number of occasions where the 'initialisation' phase of a DSRC interrogation is successful, but the transaction terminated before the data was successfully retrieved by the interrogator. This data shall be available to the operator and shall be stored in the memory of the interrogator equipment. The means by which this is achieved shall be a product of product design or the specification of a jurisdiction.

B.4 Commissioning and periodic inspection tests for the DSRC

B.4.1 General

Commissioning and periodic inspection tests that require decrypting and comprehension of the decrypted data content shall take into consideration the requirements of the jurisdiction in which the vehicle is registered and within which the vehicle is operating.

The WIM DSRC interface is a secure, protected communication, as described above in this Annex. Commissioning, and more particularly any periodic inspection of the IVS, may need to test that the DSRC interface is functioning. However, as the DSRC data is provided to the DSRC module encrypted, and the parties carrying out commissioning, and, particularly, periodic inspection tests, are not party to the security mechanisms, therefore without such access will be unable to effect normal interrogator >>-:-<IVS transactions.

B.4.2 Tests which validate data content

Commissioning and periodic inspection tests that require decrypting and comprehension of the decrypted data content shall take into consideration the requirements of the jurisdiction in which the vehicle is registered.

B.4.3 ECHO

This clause contains provisions specifically made to test only that the interrogator>>-:-<IVS is functionally active.

The objective of the ECHO command is to enable workshops or test facilities to test that the DSRC link is working without needing access to security credentials.

The tester's equipment therefore only needs to be able to initialise a DSRC communication (sending a BST with AID = 2) and then send the ECHO command, and, assuming the DSRC is working, will receive

the ECHO response. See B.6 for details. Assuming it receives this response correctly, the DSRC link (interrogator>>-:-<IVS) may be certified as functioning correctly.

B.5 Data transfer between the IVS-DSRC and VU remote communication

B.5.1 Physical connection and interfaces

The connection between the IVS and the IVS-DSRC-VU can be either by physical cable or short-range wireless communication based on Bluetooth v4.0 BLE.

Regardless of the choice of the physical connection and interface, the following requirements shall be satisfied:

a) In order that different suppliers may be contracted to supply the IVS and the IVS-DSRC, and indeed different batches of IVS-DSRC-VU, the connection between the IVS and the IVS-DSRC shall be an open standard connection. The VU shall connect with the IVS-DSRC-VU either:

   1) using fixed cable of 2 m, using a Straight DIN 41612 H11 Connector – 11 pin approved male connector from the IVS-DSRC to match a similar DIN/ISO approved Straight DIN 41612 H11 Connector female connector from the VU device;

   2) using Bluetooth Low Energy (BLE);

   3) using a standard ISO 11898-1 or SAE J1939 connection.

b) the definition of the interfaces and connection between the VU and IVS-DSRC must support the application protocol commands defined in Annex B above; and

c) the IVS and IVS-DSRC shall support the operation of the data transfer via the connection in regard to performance and power supply.

B.5.2 Application protocol

The application protocol between the IVS Remote Communication facility and IVS-DSRC is responsible for periodically transferring the remote communication data from the IVS to the DSRC.

The following main commands are identified:

a) Initialisation of the communication link – Request;

b) Initialisation of the communication link – Response;

c) Send Data with Identifier of the WIM application and Payload defined by WIM-O and/or WIM-R Data;

d) Acknowledgment of the data;

e) Termination of the communication link - Request;

f) Termination of the communication link - Response.

In ASN1.0, the previous commands may be defined as:

```
Remote Communication DT Protocol DEFINITIONS ::= BEGIN

RCDT-Communication Link Initialisation - Request ::= SEQUENCE {

    LinkIdentifier INTEGER

}
```