INTERNATIONAL STANDARD

ISO 15638-14

First edition
2014-07-15

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

Part 14: Vehicle access control

Systèmes intelligents de transport — Cadre pour applications télématiques collaboratives pour véhicules réglementés (TARV) —

Partie 14: Contrôle de l'accès des véhicules

Reference number
ISO 15638-14:2014(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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 on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 204, *Intelligent transport systems*.

This first edition cancels and replaces ISO/TS 15638-14:2013.

ISO 15638 consists of the following parts, under the general title *Intelligent transport systems — Framework for cooperative telematics applications for regulated vehicles (TARV)*:

— *Part 1: Framework and architecture*

— *Part 2: Common platform parameters using CALM*

— *Part 3: Operating requirements, 'Approval Authority' procedures, and enforcement provisions for the providers of regulated services*

— *Part 5: Generic vehicle information*

— *Part 6: Regulated applications*

— *Part 7: Other applications*

— *Part 8: Vehicle access management and monitoring*

— *Part 9: Remote electronic tachograph monitoring (RTM)*

— *Part 10: Emergency messaging system/eCall (EMS)*

— *Part 11: Driver work records*

— *Part 12: Vehicle mass monitoring*

— *Part 14: Vehicle access control*

— *Part 15: Vehicle location monitoring*

— *Part 16: Vehicle speed monitoring*

— *Part 17: Consignment and location monitoring*

— *Part 18: ADR (Dangerous Goods) transport monitoring (ADR)*

— *Part 19: Vehicle parking facilities (VPF)*

The following parts are under preparation:

— *Part 4: System security requirements*

— *Part 13: 'Mass' information for jurisdictional control and enforcement*

Introduction

Many ITS technologies have been embraced by commercial transport *operators (4.36)* and freight owners, in the areas of fleet management, safety and security. *Telematics (4.48)* applications have also been developed for governmental use. Such regulatory services in use or being considered vary from *jurisdiction (4.32)* to *jurisdiction*, but include electronic on-board recorders, digital *tachograph (4.47)*, on-board *mass (4.34)* monitoring, 'mass' penalties and levies, vehicle *access (4.1) methods*, *hazardous goods (4.22)* tracking, and e-call. Additional applications with a regulatory impact being developed include, fatigue management, speed monitoring, and heavy vehicle penalties imposed based on location, distance, and time.

In such an emerging environment of regulatory and *commercial applications (4.17)*, it is timely to consider an overall *architecture (4.12)* (business and functional) that could support these functions from a single platform within a commercial freight vehicle that operate within such regulations. International Standards will allow for a speedy development and *specification (4.46)* of new applications that build upon the functionality of a generic specification platform. A suite of standards deliverables is required to describe and define the *framework (4.28)* and requirements so that the on board equipment and back office systems can be commercially designed in an open market to meet common requirements of *jurisdictions (4.32)*.

This International Standard addresses and defines the *framework (4.28)* for a range of cooperative *telematics (4.48)* applications for *regulated commercial freight vehicles (4.40)* [such as *access methods (4.3)*, driver fatigue management, speed monitoring, on-board *mass (4.34)* monitoring, penalties and levies]. 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 (4.44)* oriented approach with provisions for the *approval (4.9)* and *auditing (4.13)* of *service providers*.

This International Standard will

— provides the basis for future development of cooperative *telematics (4.48)* applications for *regulated vehicles (4.40)*. Many elements to accomplish this are already available. Existing relevant standards will be referenced, and the *specifications (4.46)* will use existing standards (such as *CALM*) wherever practicable,

— allows for a powerful platform for highly cost-effective delivery of a range of *telematics* applications for *regulated vehicles*,

— provide a business *architecture (4.12)* based on a (multiple) *service provider (4.44)* oriented approach, and

— addresses legal and regulatory aspects for the *approval (4.9)* and *auditing (4.13)* of *service providers.*

This International Standard is timely as many governments (Europe, North America, Asia, and Australia/New Zealand) are considering the use of *telematics (4.48)* for a range of regulatory purposes. Ensuring that a single in-vehicle platform can deliver a range of services to both government and industry through open standards and competitive markets is a strategic objective.

This part of ISO 15638 provides *specifications (4.46)* for vehicle access control.

NOTE 1 The definition of what comprises a "regulated commercial freight vehicle" is regarded as an issue for national decision, and may vary from *jurisdiction (4.32)* to *jurisdiction*. This International Standard does not impose any requirements on nations in respect of how they define a *regulated vehicle (4.40)*.

NOTE 2 The definition of what comprises a "regulated" service is regarded as an issue for national decision, and may vary from *jurisdiction (4.32)* to *jurisdiction*. This International Standard does not impose any requirements on nations in respect of which services for *regulated vehicles (4.40) jurisdictions* will require, or support as an option, but will provide standardized sets of requirements descriptions for identified services to enable consistent and cost efficient implementations where implemented.

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

Part 14: Vehicle access control

1 Scope

This part of ISO 15638 addresses the provision of *"vehicle access control"* and specifies the form and content of such data required to support such systems, and *access methods (4.3)* to that data.

The scope of this part of ISO 15638 is to provide *specifications (4.46)* for common communications and data exchange aspects of the *application service (4.6)* vehicle access control that a regulator may elect to require or support as an option, including

a) high-level definition of the service that a *service provider (4.44)* has to provide, [The service definition describes common service elements; but does not define the detail of how such an *application service (4.6)* is instantiated, not the acceptable value ranges of the data concepts defined.],

b) means to realize the service, and

c) application data, naming content and quality that an *IVS (4.29)* has to deliver.

The definition of what comprises a "regulated" service is regarded as an issue for National decision, and may vary from *jurisdiction (4.32)* to *jurisdiction*. This International Standard does not impose any requirements on nations in respect of which services for *regulated commercial freight vehicles (4.40) jurisdictions* will require, or support as an option, but provides standardized sets of requirements descriptions for identified services to enable consistent and cost efficient implementations where instantiated.

This International Standard has been developed for use in the context of *regulated commercial freight vehicles (4.40)*. There is nothing however to prevent a jurisdiction extending or adapting the scope to include other types of regulated vehicles, as it deems appropriate.

2 Conformance

Requirements to demonstrate conformance to any of the general provisions or specific *application services (4.6)* described in this part of ISO 15638 shall be within the regulations imposed by the *jurisdiction (4.32)* where they are instantiated. Conformance requirements to meet the provisions of this International Standard are therefore deemed to be under the control of, and to the specification of, the *jurisdiction* where the *application service*(s) is/are instantiated.

The protocols defined in this part of ISO 15638 have been independently tested. Annex B provides results of these tests. In any conformance assurance process undertaken by candidate systems, where appropriate, the results may be used as part of its process of conformance compliance.

3 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

ISO 15638-2, *Intelligent transport systems — Framework for collaborative telematics applications for regulated commercial freight vehicles (TARV) — Part 2: Common platform parameters using CALM*

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

ISO 15638-4:—[1], *Intelligent transport systems — Framework for cooperative telematics applications for regulated vehicles (TARV) — System security requirements*

ISO 15638-5, *Intelligent transport systems — Framework for collaborative telematics applications for regulated commercial freight vehicles (TARV) — Part 5: Generic vehicle information*

ISO 15638-6, *Intelligent transport systems — Framework for collaborative telematics applications for regulated commercial freight vehicles (TARV) — Part 6: Regulated applications*

ISO 15638-8, *Intelligent transport systems — Framework for cooperative telematics applications for regulated vehicles (TARV) — Part 8: Vehicle access management*

4 Terms and definitions

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

4.1
access
admittance, entry, permit to use the road network and/or associated infrastructure (bridges, tunnels etc.)

4.2
access control
procedures and measures to control admittance, entry, permit to use the road network and/or associated infrastructure (bridges, tunnels etc.)

4.3
access methods
procedures and protocols to provision and retrieve data

4.4
access monitoring
observation and recording of vehicle related data when using the road network and/or associated infrastructure (bridges, tunnels etc.)

4.5
app
small (usually) Java™[2] applets, organized as software bundles, that support *application services (4.6)* by keeping the *data pantry (4.23)* of the *IVS (4.29)* provisioned with up-to-date data

4.6
application service
service provided by a *service provider (4.44)* enabled by accessing data from the *IVS (4.29)* of a *regulated vehicle (4.40)* via a wireless communications network

1) To be published.

2) This information is given for the convenience of users of this document and does not constitute an endorsement by ISO.

4.7
application service provider
ASP
party that provides an *application service (4.6)*

4.8
app library
separately secure area of memory in *IVS (4.29)* where apps are stored (with different access controls to *data pantry (4.23)*)

4.9
approval
formal affirmation that an applicant has satisfied all the requirements for appointment as an *application service provider (4.7)* or that an *application service (4.6)* delivers the required service levels

4.10
approval agreement
written agreement made between an *approval authority (regulatory) (4.11)* and a *service provider (4.44)*

Note 1 to entry: *Approval authority (regulatory) (4.11)* approval agreement recognizes the fact that a *service provider (4.44)*, 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*.

4.11
approval authority (regulatory)
organization (usually independent) which conducts *approval (4.9)* and ongoing *audit (4.13)* for *service providers (4.44)* on behalf of a *jurisdiction (4.32)*

4.12
architecture
formalized description of the design of the structure of *TARV* and its *framework (4.28)*

4.13
audit
auditing
review of a party's capacity to meet, or continue to meet, the initial and on-going *approval agreements (4.10)* as a *service provider (4.44)*

4.14
basic vehicle data
data that shall be maintained/provided by all *IVS (4.29)* regardless of *jurisdiction (4.32)*

4.15
BigBubble
zones, such as metropolitan area, which include within them several *sensitive/restricted zones (4.42)*

4.16
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 (4.49)* determined parameters, by using a suite of International Standards based on ISO 21217 (*CALM* architecture) and ISO 21210 (*CALM* networking), that provide a common platform for a number of standardized media using *ITS-stations (4.31)* to provide wireless support for applications, such that the application is independent of any particular wireless medium

4.17
commercial application(s)
ITS applications in *regulated vehicles (4.40)* for commercial (non-regulated) purposes

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

4.18
consignment and load monitoring
monitoring of shipment of goods/cargo throughout or at specific points of a journey to a destination

4.19
controlled zone
controlled access zone
defined physical area which the *jurisdiction (4.32)* or controlled zone manager determines require *access control (4.2)* for *regulated vehicles (4.40)*

4.20
cooperative ITS
C-ITS
ITS applications for both regulatory and commercial purposes that require the exchange of data between uncontracted parties using multiple *ITS-stations (4.31)* communicating with each other and sharing data with other parties with whom they have no direct contractual relationship to provide one or more *ITS services (4.29)*

4.21
core data
basic vehicle data (4.14) plus any additional data required to provide an implemented *regulated application service (4.39)*

4.22
dangerous goods
hazardous goods
HAZMAT
substances or articles which are potentially hazardous (for example, poisonous to humans, harmful to the environment, explosive, flammable, or radioactive) that require regulatory control when transported

4.23
data pantry
secure area of memory in *IVS (4.29)* where data values are stored with different access controls to *app library (4.8)*

4.24
driver
person driving the *regulated vehicle (4.40)* at any specific point in time

4.25
driver work records
DWR
collection, collation, and transfer of *driver (4.24)* work and rest hours data from an *in-vehicle system (4.29)* to an *application service provider (4.7)*

4.26
emergency message system
EMS
collection, collation, and transfer of emergency message data from an *in-vehicle system (4.29)* to an *application service provider (4.7)*

4.27
facilities
layer that sits on top of the communication stack and helps to provide data interoperability and reuse, and to manage applications and enable dynamic real time loading of new applications

4.28
framework
particular set of beliefs, ideas referred to in order to describe a scenario or solve a problem

4.29
in-vehicle system
IVS
ITS-station (4.31) and connected equipment on board a vehicle

4.30
ITS service
communication functionality offered by an *ITS-station (4.31)* to an *ITS-station* application

4.31
ITS-station
ITS-s
entity in a communication network, comprised of application, *facilities (4.27)*, networking, and access layer components specified in ISO 21217 that operate within a bounded secure management domain

4.32
jurisdiction
government, road, or traffic authority which owns the r*egulatory applications (4.38)*

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

4.33
local data tree
LDT
frequently updated data concept stored in the on-board *data pantry (4.23)* containing a collection of data values deemed essential for either a) *TARV regulated application service (4.39)*, or b) *cooperative intelligent transport systems (4.20)*

4.34
mass
mass of a given heavy vehicle as measured by equipment affixed to the *regulated vehicle (4.40)*

4.35
'mass' information for jurisdictional control and enforcement
MICE
MRC
collection, collation, and transfer of vehicle *mass (4.34)* data from an *in-vehicle system (4.29)* to an *application service provider (4.7)* to enable data provision to *jurisdictions (4.32)* for the control and management of equipped vehicles based on the *mass* of the *regulated vehicle (4.40)*, or use of such data to enable compliance with the provisions of regulations

4.36
operator
fleet manager of a *regulated vehicle (4.40)*

4.37
prime service provider
service provider (4.44) who is the first contractor to provide *regulated application services (4.39)* to the *regulated vehicle (4.40)*, or a nominated successor on termination of that initial contract; the prime service provider is also responsible to maintain the installed *IVS (4.29)*; if the *IVS* was not installed during the manufacture of the vehicle the prime service provider is also responsible to install and commission the *IVS*

4.38
regulated application
regulatory application
application arrangement using TARV utilized by *jurisdictions (4.32)* 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*; may be mandatory or voluntary at the discretion of the *jurisdiction*

4.39
regulated application service
TARV application service (4.6) to meet the requirements of a regulated application that is mandated by a regulation imposed by a *jurisdiction (4.32),* or is an option supported by a *jurisdiction*

4.40
regulated commercial freight vehicle
regulated vehicle
vehicle that is subject to regulations determined by the *jurisdiction (4.32)* 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; at the option of *jurisdictions*; this may require the provision of information via *TARV* or provide the option to do so

4.41
remote tachograph monitoring
RTM
collection, collation, and transfer of data from an on-board electronic *tachograph (4.47)* system to an *application service provider (4.7)*

4.42
sensitive/restricted zone
defined physical area which the *jurisdiction (4.32)* or sensitive/restricted zone manager determines require special monitoring (e.g. urban pedestrian areas, school and hospital surroundings, ...), freight villages, ports, road sensitivity infrastructure (bridges, tunnels, ...)., weight restricted areas, width restricted areas, areas where there has been an accident or incident, etc.

4.43
sensitive/restricted zone management
monitoring and management of *regulated vehicles (4.40)* in additional to normal traffic management, as specified by the *jurisdiction (4.32)* or its agents to apply to *regulated vehicles*

4.44
service provider
party which is approved by an approval *authority (regulatory) (4.11)* as suitable to provide regulated or commercial ITS *application services (4.6)*

4.45
session
wireless communication exchange between the *ITS-station (4.31)* of an *IVS (4.29)* and the *ITS-station* of its *application service provider (4.7)* to achieve data update, data provision, upload apps, or otherwise manage the provision of the *application service (4.6),* or a wireless communication provision of data to the *ITS-station* of an *IVS (4.29)* from any other *ITS-station*

4.46
specification
explicit and detailed description of the nature and functional requirements and minimum performance of equipment, service, or a combination of both

4.47
tachograph
sender unit mounted to a vehicle gearbox, a tachograph head, and a digital driver card, which records the *regulated vehicle (4.40)* speed and the times at which it was driven and aspects of the *driver's (4.24)* activity selected from a choice of modes

4.48
telematics
use of wireless media to obtain and transmit (data) from a distant source

4.49
user
individual or party that enrols in and operates within a regulated or *commercial application (4.17)* service

EXAMPLE *Driver (4.24),* transport *operator (4.36),* freight owner, etc.

4.50
vehicle access control
VAC
control of *regulated commercial freight vehicles (4.40)* ingress to and egress from controlled areas and associated penalties and levies

4.51
vehicle access management
VAM
monitoring and management of *regulated vehicles (4.40)* approaching or within sensitive and controlled areas

4.52
vehicle location monitoring
VLM
collection, collation, and transfer of vehicle location data from an *in-vehicle system (4.29)* to an *application service provider (4.7)*

4.53
vehicle mass monitoring
VMM
collection, collation, and transfer of vehicle *mass (4.34)* data from an *in-vehicle system (4.29)* to an *application service provider (4.7)*

4.54
vehicle parking facility
VPF
system for booking and *access (4.1)* to and egress from a vehicle parking facility (VPF)

4.55
vehicle speed monitoring
VSM
collection, collation, and transfer of vehicle speed data from an *in-vehicle system (4.29)* to an *application service provider (4.7)*

5 Symbols and abbreviated terms

AA *approval authority (regulatory) (4.11)*

ADR *Accord Européen relatif au transport international des marchandises Dangereuses par Route* [*dangerous goods (4.22)*]

app applet (Java™ application or similar) *(4.5)*

AS	application service
ASP	*application service provider (4.7)*
CALM	*communications access for land mobiles (4.16)*
C-ITS	*cooperative intelligent transport systems (4.20)*
CZM	*controlled access zone (4.19)* management/manager
Dr	*driver (4.24)*
DWR	*driver work records (4.25)*
EMS	*emergency message system (4.26)*
ID	identity
IP	internet protocol
ITS-S	*ITS station (4.31)*
IVS	*in-vehicle system (4.29)*
J	*jurisdiction (4.32)*
Java™[a]	object-oriented open-source operating language developed by SUN systems
LDT	*local data tree (4.33)*
MICE/ MRC	*'Mass' information for jurisdictional control and enforcement (4.35)/'Mass' regulation and control*
Op	*operator (4.36)*
PSP	*prime service provider (4.36)*
RTM	*remote tachograph monitoring (4.40)*
SE	service element
SPF	secure parking facility
SZM	*sensitive/restricted zone management (4.43)*/manager
TARV	*telematics (4.48)* applications for *regulated vehicles (4.40)*
VAC	*vehicle access control (4.50)*
VAM	*vehicle access management (4.51)*
VLM	*vehicle location monitoring (4.52)*
VMM	*vehicle mass monitoring (4.53)*
VPF	*vehicle parking facilities (4.54)*
VSM	*vehicle speed monitoring (4.55)*

[a] This information is given for the convenience of users of this document and does not constitute an endorsement by ISO.

6 General overview and framework requirements

ISO 15638-1 provides a *framework (4.28)* and *architecture (4.12)* for *TARV*. It provides a general description of the roles of the actors in *TARV* and their relationships.

To understand clearly the *TARV* framework, *architecture (4.12)*, and detail and *specification (4.46)* 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. To understand clearly the general context in to which the provision of this application service, the reader is referred to ISO 15638-6.

In order to be compliant with this part of ISO 15638, the overall architecture employed shall comply with ISO 15638-1.

In order to be compliant with this part of ISO 15638, the communications employed shall comply with ISO 15638-2.

In order to be compliant with this part of ISO 15638, the operating requirements employed shall comply with ISO 15638-3.

In order to be compliant with this part of ISO 15638, the security employed shall comply with ISO 15638-4.

In order to be compliant with this part of ISO 15638, the basic vehicle data shall comply with ISO 15638-5.

In order to be compliant with this part of ISO 15638, the generic conditions for this application service shall comply with ISO 15638-6.

This International Standard has been developed for use in the context of regulated commercial freight vehicles [hereinafter referred to as '*regulated vehicles*' *(4.40)*]. There is nothing, however, to prevent a jurisdiction extending or adapting the scope to include other types of regulated vehicles, as it deems appropriate.

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 (4.39)* shall be as defined in ISO 15638-6.

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

8.1 General

Application services that require data in addition to basic vehicle data shall be conducted as defined in ISO 15638-6.

8.2 Quality of service requirements

This part of ISO 15638 contains no general requirements concerning quality of service. Such aspects shall be determined by a *jurisdiction (4.32)* as part of its *specification (4.46)* for any particular *regulated application service (4.39)*. However, where a specified *regulated application service (4.39)* has specific quality of service requirements essential to maintain interoperability, these aspects shall be as specified in Clause 10.

8.3 Test requirements

This part of ISO 15638 contains no general requirements concerning test requirements. Such aspects shall be determined by a *jurisdiction (4.32)* as part of its *specification (4.46)* for any particular *regulated application service (4.39)*, and issued as a formal test requirements *specification (4.46)* document.

However, where a specified *regulated application service (4.39)* 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 deliverable referenced within that clause. 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 deliverable.

8.4 Marking, labelling and packaging

This part of ISO 15638 has no specific requirements for marking labelling or packaging.

However, where the privacy of an individual can be potentially or actually compromised by any instantiation based on this International Standard, the contracting parties shall make such risk explicitly known to the implementing *jurisdiction (4.32)* and shall abide by the privacy laws and regulations 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 the instantiation of *regulated application service (4.39)* are as designed by the application service system to meet the requirements of a particular *jurisdiction (4.32)* and are not defined herein. ISO 15638-6 specifies the generic roles and responsibilities of actors in the systems, and instantiations that claim compliance with this part of ISO 15638 shall also be compliant with the requirements of ISO 15638-6.

The means by which data are provisioned into the *data pantry (4.23)*, and the means to obtain the *TARV LDT (4.33)* and *core data (4.21)* are described in ISO 15638-6, Clause 8 (esp. 8.3).

In order to minimize demand on the *IVS (4.29)* [which it is assumed will be performing multiple *application services (4.6)* 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 (4.39)*.

The *TARV* approach is for the on-board *app (4.5)* 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) (4.7),* 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, Clause 9.

At a conceptual level, The *TARV* system is therefore essentially simple, as shown in Figure 1. The process is similar to that for `CoreData`, but data are supplied to a different on-board file in the *data pantry (4.23)*.

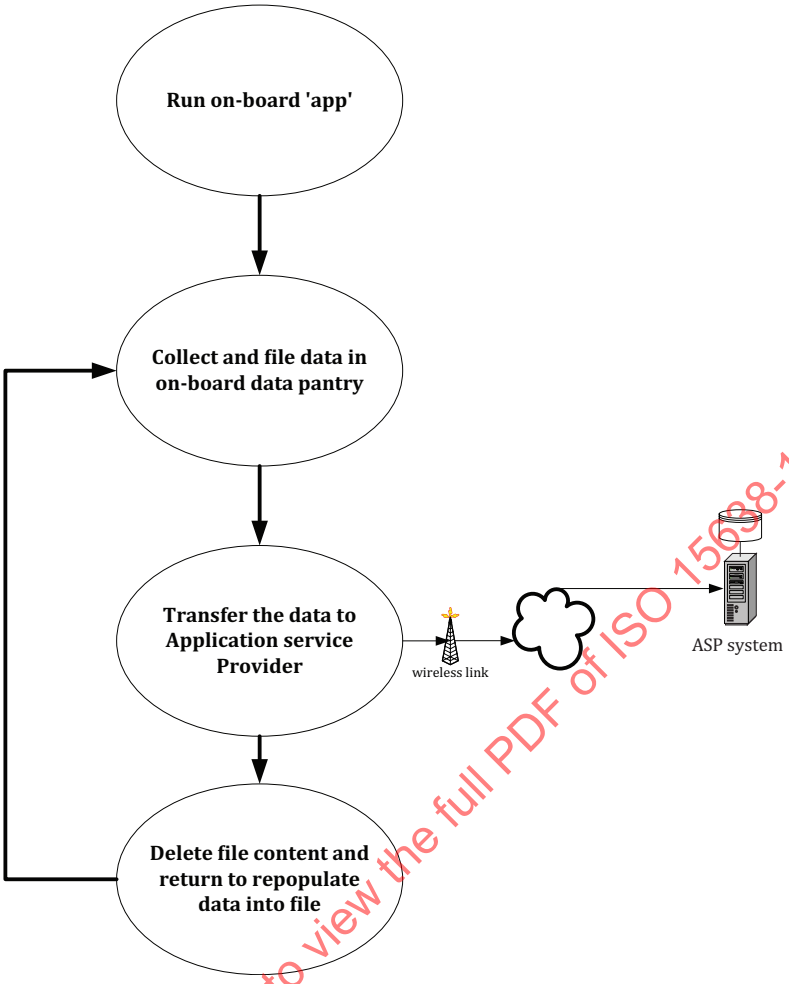

Figure 1 — TARV regulated application service on-board procedure

At a common generic functional level for this application service, the process may be seen as shown in Figure 2 below, however, the connected equipment may/may not be required in all cases.

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

The common role of the jurisdiction, approval authority, application service provider, and user shall be as defined in ISO 15638-6, 10.2.4 and 10.2.5.

9.3 Common characteristics for instantiations of regulated application services

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

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 (4.6)* shall be as defined in ISO 15638-6.

9.6 Information security

Information security shall be as defined in ISO 15638-6.

9.7 Data naming content and quality

Data naming and quality shall be as defined in ISO 15638-6.

Variations specific to the vehicle access control *application service (4.6)* shall be as defined below.

9.8 Software engineering quality systems

Software engineering quality systems shall be as defined in ISO 15638-6.

9.9 Quality monitoring station

The availability of quality monitoring stations shall be as defined in ISO 15638-6.

9.10 Audits

Audits shall be as defined in ISO 15638-6.

9.11 Data access control policy

To protect the data and information held by the *application service provider (4.7)*, each provider shall adopt a risk based data access control policy for employees of the provider.

9.12 Approval of IVSs and service providers

Generic provisions for the *approval (4.9)* of *IVSs* and *service providers (4.44)* shall be as specified in ISO 15638-3. Detailed provisions for specific *regulated applications (4.38)* shall be as specified by the regime of the *jurisdiction (4.32)*.

10 Vehicle access control (VAC)

10.1 TARV VAC service description and scope — VAC use cases

10.1.1 Jurisdiction — Safety enhancement

Jurisdictions (4.32) define *controlled zones (4.19)* by issuing specific *access (4.1)* policies in order to enhance the level of road safety in special situations by preserving the traffic efficiency and respecting the environment. *Controlled zones* might be special inner city areas (e.g. urban pedestrian areas, school, and hospital surroundings, ...), freight villages, ports, road sensitivity infrastructure (bridges, tunnels, ...)., weight restricted areas, width restricted areas, areas where there has been an accident or incident, or zones and roadways where *regulated vehicles (4.40)* have to pay levies for *access*, etc. or temporary zones created to protect VIP movement (movement of president, senior ministers, a public gathering/procession etc.). Public authorities are normally required to publish the *access* rules and the restriction policy. '*Vehicle access control*' *(VAC) (4.50)* is a specialized use case of '*vehicle access management*' *(VAM) (4.51)*, where the '*Controlled Zone* Manager' (*CZM*) has the right/ability to permit or refuse entry of a *regulated vehicle* to a defined *controlled zone*.

10.1.2 Controlled zone managers — Access control monitoring and management

In the *VAC (4.50)* use case, *controlled zone (4.19)* managers (*CZM*) [who may be an organ of a *jurisdiction (4.32)*, local authority or licensed/contracted *operator (4.36)*] have the ability to grant or prevent *access (4.1)* of *regulated vehicles (4.40)* according to some stipulated criteria (such as type, size, weight, status,

condition, payment of fees, etc.). They may also solicit and obtain data from the *regulated vehicle (4.40)* when approaching, when within or when leaving the *controlled zone*.

10.1.3 Vehicle operators — Access control monitoring and management

Vehicle *operators (4.36)* may be required to pay fees for *regulated vehicles (4.40)* to enter *controlled zones (4.19),* or meet other conditions such as seek prior permission or make data submission, and/or may need to monitor the progress of their vehicle as it passes through the *controlled zone*.

10.1.4 Jurisdiction — Levy

In the case where a levy is applied for a *regulated vehicle (4.40)* to gain permission to enter the controlled area, *jurisdictions (4.32)* may need to have access to suitable tools to permit or prevent *access (4.1)* to designated roadways based on the payment of levies, as a tax, subscription, or either on entry to the roadway, at the exit from the roadway, or by prior agreement between the parties.

10.1.5 Controlled zone managers — Assessment of levies

In the case where a levy is applied for a *regulated vehicle (4.40)* to gain permission to enter the controlled area, 'road operators' may need to have access to suitable tools to permit or prevent *access (4.1)* to designated roadways based on the payment of fees, either on the payment of levies, as a tax, subscription or either on entry to the roadway, at the exit from the roadway, or by prior agreement between the parties and may use *access control (4.2)* techniques such as barriers and traffic control lights to achieve this objective. The *CZM* may also need to have access to suitable tools to differentiate fees among fleet *operators (4.36)* depending on their performance over time.

10.1.6 Jurisdiction — Access control enforcement

Jurisdictions (4.32) need to have access to suitable tools and regulation for the enforcement of the published *access (4.1)* rules to restricted/dangerous areas.

10.1.7 Controlled zone managers — Enforcement

CZMs need to have access to suitable tools for the enforcement of the published *access (4.1)* rules to restricted/dangerous areas.

10.2 Concept of operations for vehicle access control

10.2.1 General

The general goal of an *access control (4.2)* system is a specialized case of vehicle access monitoring (*VAM*) specified in ISO 15638-8, that additionally has the ability to control (permit entry/deny entry) of *regulated vehicles (4.40)* to the sensitive or *controlled zone (4.19)* or zone where *access (4.1)* is granted according to matching acceptable criteria, or by payment for use of, or a combination of these factors. See ISO 15638-8 for detail of *access methods (4.3)* provisions and capabilities.

These *specifications (4.46)*, in the case of fee collection, apply to special provisions that are specific to '*regulated vehicles*'*(4.40)* and require either different control parameters or different data to general ITS electronic fee collection.

For general electronic fee collection for all classes of vehicles for the use of roads, for reasons of interoperability and consistency, the standards specifically designed for ITS electronic fee collection based around ISO 17573 and ISO 12855 should normally be used and take precedence.

NOTE The system *architecture (4.12)* defined in ISO 17573 is the basis for all standards that relate to tolling systems in the toll domain. From this system *architecture* standard, other standards have consistently reused

— common definitions of terms and concepts and basic system functionalities and structure,

— common terminology, and

— identified interfaces that are or need to be defined.

ISO 17573 uses ISO/IEC 10746-3 for the description of the *architecture (4.12)*.

A given transport service for a given vehicle is fully identified by one or several toll declarations, made available to the Toll Charger (TC). Toll declarations have to be made available according to the rules of the toll regime of the toll domain.

The amount due for a given transport service used by a vehicle liable to toll is concluded by the Toll Charger with the use of toll declarations (as described above) and calculation is made according to the rules of the toll regime (formula, tariff tables, specific situations rules, traffic conditions, etc.).

The information above, associated with a given transport service, is named billing details; for a given transport service, the billing details are referring to one or several toll declarations.

Depending on the toll regime, billing details are elaborated with information collected by the Toll Charger and/or the relevant Toll Service Provider (TSP); they are concluded by the Toll Charger.

The Toll Charger elaborates and makes the payment claims (or toll payment claims) available to each Toll Service Provider, according to the bilateral agreements it has with each Toll Service Provider, referring to billing details. These payment claims include an amount due taking into account any specific commercial conditions applicable to a vehicle, a fleet of vehicles or a given Toll Service Provider.

(For definition of the use of terms in this example, please see ISO 12855.)

In the case of any fee collection associated with *VAC (4.50)*, it shall either fit within, and therefore use the provisions of standardized ITS EFC standards, or its data or *access (4.1)* conditions will be different in the case of *regulated vehicles (4.40)*, in which case the provisions defined herein shall pertain in respect of communications from the *CZM* to the *regulated vehicle* or between the *regulated vehicle* and its *ASP (4.7)*. It may most frequently control access according to the vehicle class or some parameter of qualification or disqualification that has nothing to do with fees or levies, but in some cases, a qualification condition may include the payment of a levy as a form of taxation, subscription, penalty for wear and tear, or other basis of imposition of a levy.

Taken at its most restrictive interpretation, '*access control*' *(4.2)* is simply the control of '*access*' *(4.1)* of *regulated vehicles (4.40)* to *controlled zones (4.19)* of the road network. As with *VAM* (ISO 15638-8), what constitutes a '*controlled zone*', and what constitutes a *'regulated' vehicle (4.40)*, are liable to many interpretations and will, quite rightly, vary in different jurisdictions around the globe.

VAC (4.50) use cases extend beyond monitoring and fee assessment to generic areas such as asset protection/asset management, traffic management, safety, security, etc., even, in some *jurisdictions (4.32)*, under the guise of "supervisory intervention orders", to vehicle regulation provisions such as alcohol interlocks as a supervisory provision for a *driver (4.24)* with a record of driving under the influence, for whom an alcohol interlock is a condition of permission of '*access*' *(4.1)* to drive.

Many *VAC (4.50)* application service use cases, although functionally with very different objectives, can operate with only *basic vehicle data (4.14)* as defined in ISO 15638-5, and require no specialized standardization, other than the provisions generically specified within ISO 15638-3, ISO 15638-5, and ISO 15638-6, Clauses 8 and 9.

This part of ISO 15638 focuses on the requirements for generic *access methods (4.3)* or management systems whose objective is generically to control (permit/stop) *access (4.1)* for *regulated vehicles (4.40)* to/from or in some circumstances reducing or eliminating movement within, the defined controlled zone.

For applications that simply require vehicle monitoring to enable the *application service provider (4.7)* to achieve provision of the *application service (4.6)*, and do not involve *access control (4.2)* measures, see ISO 15638-8.

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

This part of ISO 15638 focuses on providing standardized support for generic *access control (4.2)* (possibly including monitoring or management) systems to increase the safety and the management efficiency of *controlled zone (4.19) access control*.

The basic concept for *access control (4.2)* is to monitor vehicles approaching *controlled zones (4.19)* in order to control entry to/movement within/egress from the *controlled zone*, and allow/deny the *access (4.1)*, by using wireless communication between incoming vehicles and the infrastructure, combined with a physical means to control *access* (barriers, lights etc.). See Figure 2.

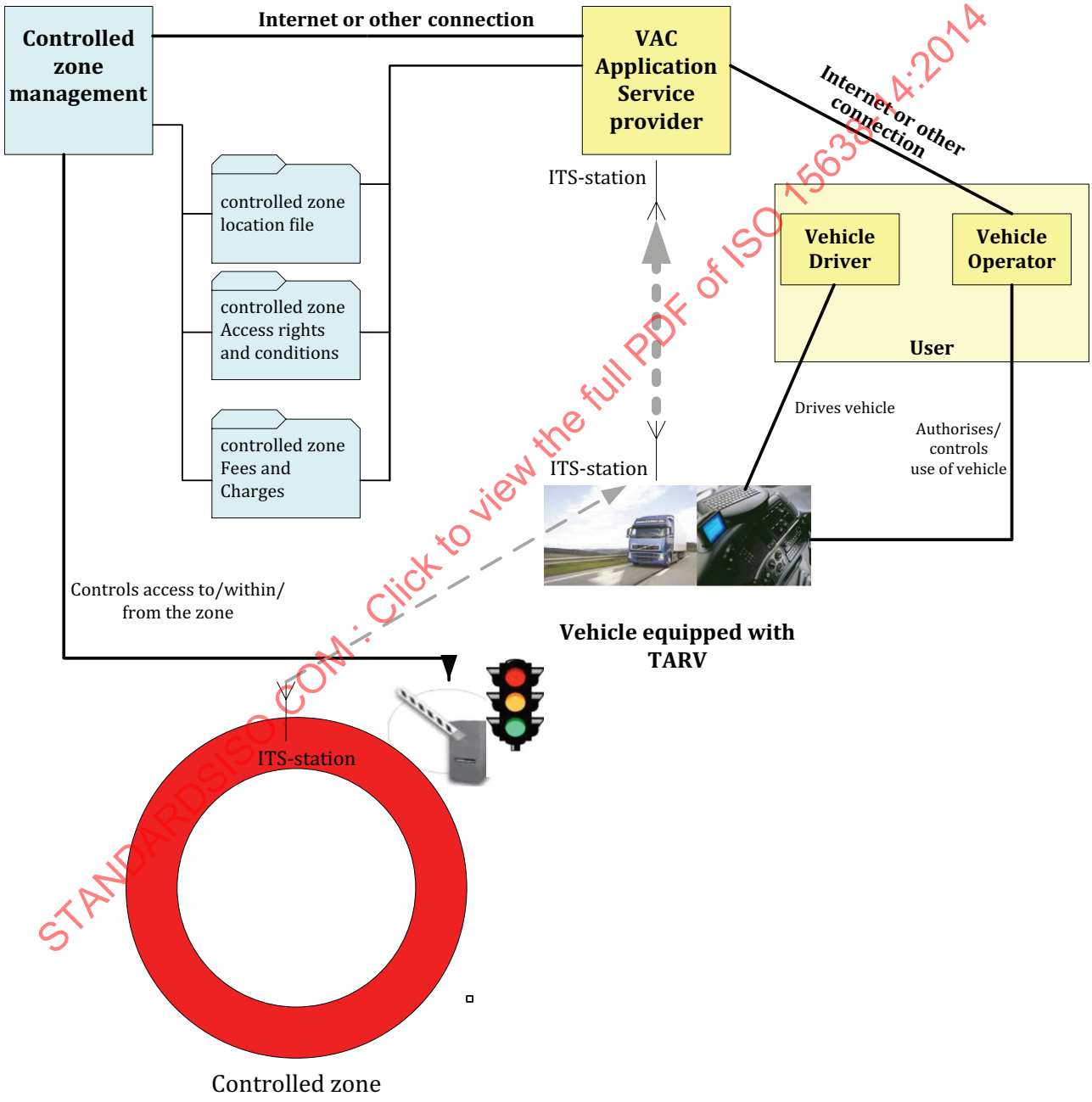

Figure 2 — Vehicle access control, monitoring, and management overview

While support for the application service *vehicle access monitoring* (*VAM*) *(4.51)* as defined in ISO 15638-8, may be said to be normally 'zone centric', monitoring the populations within a zone, *VAC (4.50)* may normally be considered to be 'vehicle centric', in that, it is centred around entry of a particular *regulated vehicle (4.40)* to movement around and egress from the zone. As with *VAM* (ISO 15638-8), the core activity elements that are essential to *VAC* may be considered as

a) define and update *controlled zone (4.19)* definition, *access (4.1)* rights, and any related levying structures,

b) approaching *access control (4.2)*,

c) decision-making and information feedback,

d) monitoring while within the *controlled zone*,

e) fees and levying, and

f) egress from *controlled zone*.

Although in the case of *VAC*, the behaviour for *access control (4.2)* is added.

After detecting the entrance to the *controlled zone (4.19)*, once inside a predefined *access controlled (4.2)* approach zone, the approaching vehicle (automatically or at the instigation of the driver) shall send relevant data to its *application service provider (4.7)*, who obtains relevant information from the 'Controlled Zone Management '(*CZM*) enabling it to provide the required information and information concerning any levy for amounts due and how they are collected, and request entry to the *controlled zone (4.19)*. As with *VAM* and all *TARV* applications, the management and provision of the *application service (4.6)* is undertaken by the *application service provider*. The communication between the *ASP* and the *IVS (4.29)* of the *regulated vehicle (4.40)* shall be as determined in ISO 15638-6, 8.3 with data from the *regulated vehicle* always provided to a predetermined IPv6 address in a separate communication from that of the interrogation. The *ASP* shall then provide the data to the *controlled zone (4.19)* manager by the means determined by the *CZM* (and outside of the scope of this part of ISO 15638).

The *ASP (4.7)* is responsible to provide the *CZM* with the data required by the regulations controlling *access (4.1)* conditions for the *controlled zone (4.19)*. Once the *CZM* is satisfied that it has received the required data/fees, it shall grant *access (4.1)* to the *controlled zone (4.19)*, or if not satisfied shall deny *access*.

This part of ISO 15638 does not attempt to specify how such management or control services are specified nor how their application service provision is designed and installed, only the communications required between the *regulated vehicle (4.40)* and the *application service provider (4.7)*, or from the *CZM* to the *regulated vehicle*. Most communications are between the *ASP* and the *controlled zone (4.19)* management centre, or between the *regulated vehicle operator (4.36)/application service provider/controlled zone* management centre, and all of these communications and exchanges are outside of the scope of this part of ISO 15638.

Control and enforcement in respect of *mass (4.34)* are a special case, defined in ISO 15638-13.

Without specifying the application, the generic *VAC* use case is shown in Figure 3.

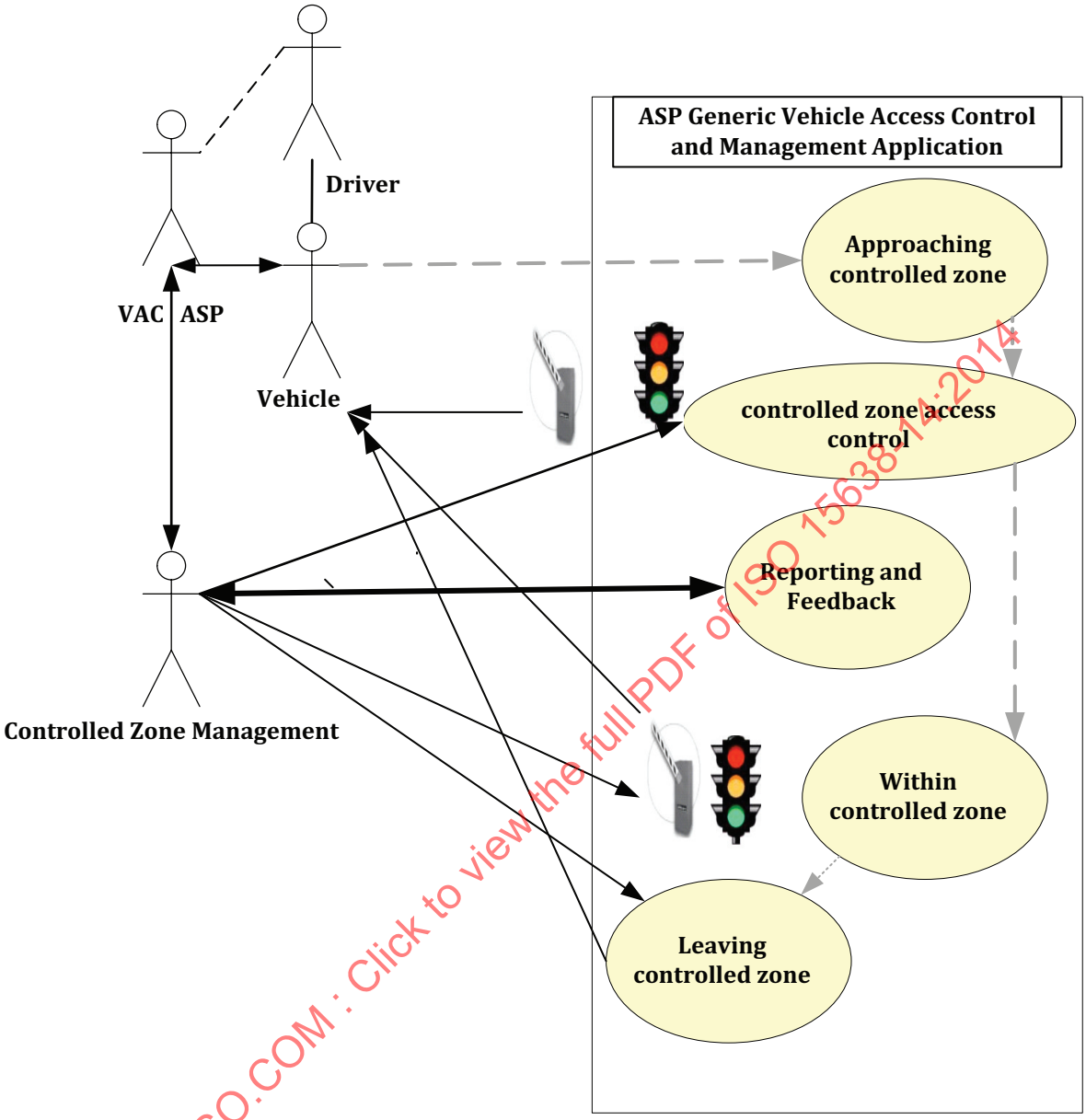

Figure 3 — VAC use case and boundary

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

This application service support is designed for *access control (4.2)* to/within/from *controlled zones (4.19)*. For monitoring of vehicles within these *controlled zones (4.19)*, the provisions of ISO 15638-8 will generally prove more appropriate. For general monitoring of the location of *regulated vehicles (4.40)*, the *vehicle location monitoring (4.52)* provisions specified in ISO 15638-15, or *consignment and load monitoring (4.18)* provisions of ISO 15638-17, or, in the case of monitoring *dangerous goods (4.22)* to meet regulatory requirements, the provisions of ISO 15638-18 will be more appropriate. For support for other specific *application services (4.6)*, the provisions of other parts of this International Standard should also be considered for their relevance. (See 'Foreword' for list of the parts of this International Standard and application services supported.)

Individual *jurisdictions (4.32)* may have specific requirements in respect of issues such as CO^2 emissions, carbon footprint, complex vehicle configurations, noise level, worn suspension air-bags, etc. that are not the subject of the specific application service provisions of ISO 15638-8 to ISO 15638-19, and may find that the ability to develop specific requirements for additional data, provided in ISO 15638-6, 8.3 may be, in many cases, more appropriate than the provisions for *VAC* (this part of ISO 15638) (and where

of common interest such provisions could be added to subsequent versions/releases of this part of ISO 15638).

10.2.4 Organizations, activities, and interactions among participants and stakeholders

The principle actors that comprise the system are

— *driver (4.24)*,

— *regulated vehicle (4.40)*,

— *application service provider (4.7)*, and

— *access control (4.2)* manager.

Four use cases have been identified, namely

a) approaching *controlled zone (4.19)* — Planned,

b) approaching *controlled zone* — Unplanned,

c) decision making,

d) reporting and feedback, and

e) exiting *controlled zone*.

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.

Table 1 provides a list of the actors involved, their activities and interactions.

Table 1 — TARV VAC actors involved, their activities and interactions

Actor	Role	Activities	Interactions
Jurisdiction (J) *(4.33)*	Sets requirements for mandatory and supported *TARV VAC (4.50)*	Publishes *specifications (4.46)*	ALL
		Obtains regulations	ALL: Establish regime and regulations PSP: Register *TARV* equipment ASP Register application, receive reports Op: Vehicle registration Dr: Licence
		Appoints *Approval Authority* (if required)	AA: Contract. Instruct. Receive reports
		Monitors reports	
		Instigates any enforcement	
Approval authority (AA) *(4.11)*	Implements *jurisdiction* policy at equipment and service approval level	Approves *IVS (4.29)*, and vehicle equipment, a*pplication service (4.6)* instantiations	PSP: Approve IVS ASP: *Approve application service*

Table 1 *(continued)*

Actor	Role	Activities	Interactions
		Conducts quality of service maintenance to instruction of *jurisdiction*	
Prime service provider (PSP) *(4.37)*	Responsibility for *IVS*	Installs and/or commissions *IVS*	AA: May apply to approve *IVS* Op; Installation
		Maintains *IVS*, related equipment	Op: Maintain *IVS* and related equipment
Application service provider (ASP) (4.7)	Provides *TARV VAC* application support services	Develops instantiation of *TARV VAC application service*	AA: Applies for approval of service
		Contracts with *users (4.49)*	Op: Contracts
		Provides *TARV VAC application service* to *users* and *jurisdiction*	Op: Provides service Dr: May provide service J: Provides service/reports
Controlled zone (4.19) manager	Manages controlled area	Interfaces with *users* (Dr/Op) and *jurisdiction* Provides *access (4.1)* to/within/from *controlled zone*, may collect fees, collecting the parameters from the monitored vehicles, process them according to the applicable policy and manage the *access* to the area., provides reports, exception reports, violations	ASP: collects data, passes information and instructions, forwards appropriate fees J: Provides reports
Operator (4.36) (Op)	Provides *regulated vehicle (4.40)*	'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, pays appropriate fees
		Receives reports from *ASP*	
Driver (Dr) *(4.24)*	Drives *regulated vehicle* to instruction of *operator (4.36)*		Op: to instructions
		Signs into *TARV VAC* system	IVS: signs *driver* into system
		Drives *regulated vehicle*	

The use case is depicted in Figure 3, and in the collaboration diagram shown in Figure 4.

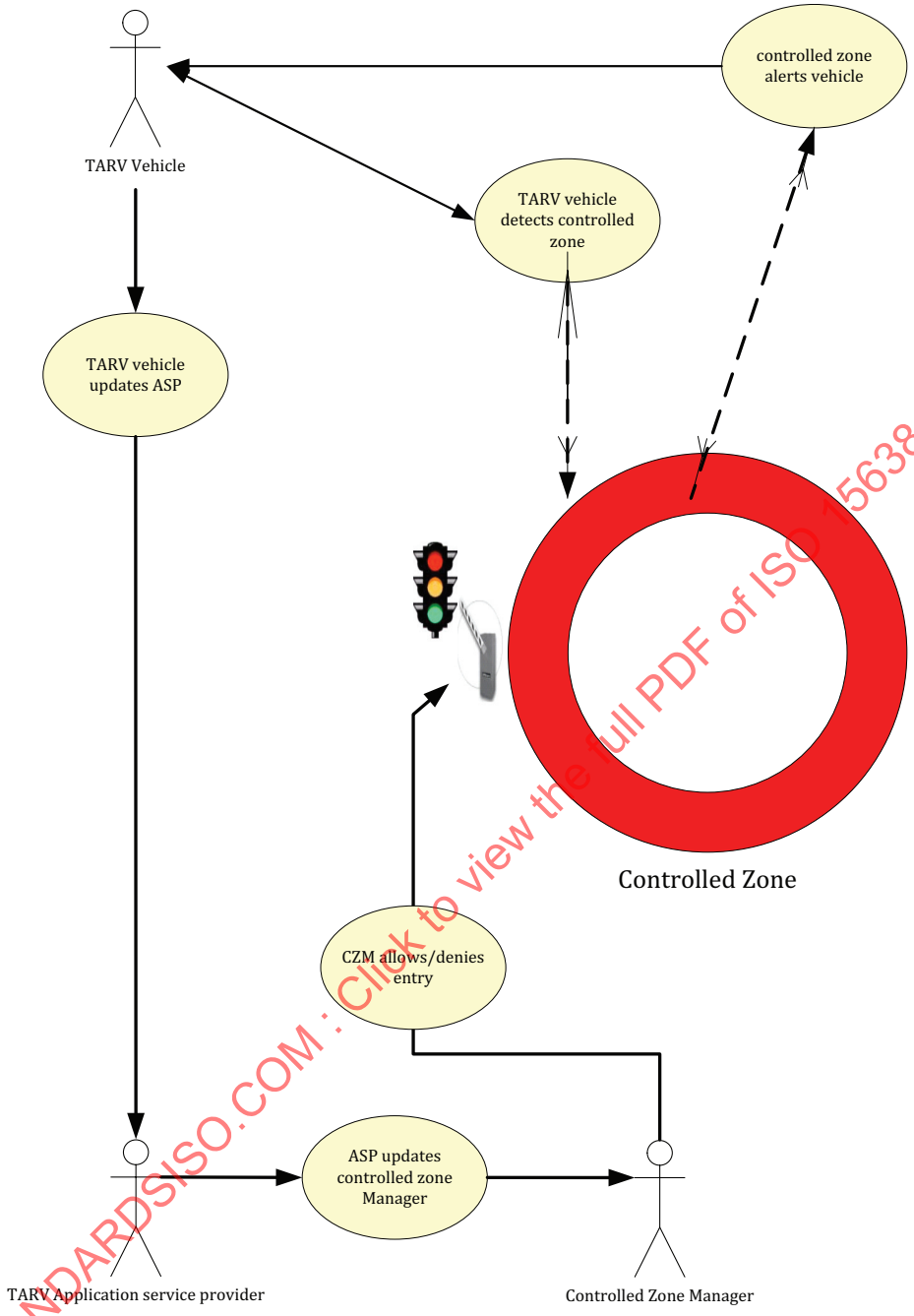

Figure 4 — VAC access control area collaboration diagram

10.2.4.1 Approaching controlled zone — Planned

This use case, the *ASP (4.7)* of the *regulated vehicle (4.40)* shall make contact with the *regulated vehicle* to obtain its current *basic vehicle data (4.14)* as defined in ISO 15638-5. If the *regulated vehicle* is equipped, the *ASP* may also obtain the *driver (4.24)* identification, and possibly obtain data concerning the load and its status if this is information required by the *controlled zone (4.19)* manager. (If the *regulated vehicle* is not equipped to provide *driver* data, or load data, and if this is required information, then the *ASP* has the responsibility to obtain and provide that data by other means).

If the *jurisdiction (4.32)* controlling the *controlled zone (4.19)* requires additional data supplied from the *regulated vehicle (4.40)*, then either it shall provide an *app (4.5)* to the *ASP (4.7)* who shall be responsible to preload the *app* into the memory of the *IVS (4.29)* of the *regulated vehicle*, or the *ASP* shall devise and install such an *app*.

The communication between the *ASP (4.7)* and the *regulated vehicle (4.40)* *IVS (4.29)* shall be as determined in ISO 15638-6, 8.3 with data from the *regulated vehicle* always provided to a predetermined IPv6 address in a separate communication from that of the interrogation. The *ASP* shall then provide the data to the *controlled zone (4.19)* manager (*CZM*) by the means determined by the *CZM* (and outside of the scope of this part of ISO 15638). The *ASP* is responsible to provide the *CZM* with the data required by the regulations controlling *access (4.1)* conditions for the *controlled zone*, and making payment of any fees.

10.2.4.2 Approaching controlled zone — Unplanned

In this use case, there has been no pre-planning regarding the *controlled zone (4.19)*.

The reasons for and conditions of *access (4.1)* to and reporting from a *controlled zone* are entirely within the discretion of the *jurisdiction (4.32)/CZM* who may or may not allow unplanned entry, and such conditions of *access* are outside of the *specifications (4.46)* of this International Standard.

In this circumstance, the *CZM* shall have the responsibility to alert the driver/vehicle that it is approaching a *controlled zone (4.19)*.

The *CZM* may provide this warning by providing a broadcast signal to a wireless communications medium supported by the *TARV* equipped vehicle. In this case, this message shall stimulate an *app (4.5)* provided by the *ASP* to collect and transmit the *basic vehicle data (4.14)* as determined in ISO 15638-5, plus any additional information received from the broadcast to the predetermined IPv6 address provided by the *ASP* as determined in ISO 15638-6, 8.3, and the *session (4.45)* shall then proceed as a planned approach to the *controlled zone (4.19)*, as determined in 10.2.4.1.

In the case that the *CZM* does not have the means to automatically notify the *IVS (4.29)* of the *regulated vehicle (4.40)*, the *CZM* may simply erect a barrier or traffic control lights or other methods of control at the point of entry. The *CZM* shall post a visible and/or audible notification to the *driver (4.24)* of the *regulated vehicle*, and the *driver* of the *regulated vehicle* shall trigger the *IVS* of the *regulated vehicle* to send its *basic vehicle data (4.14)* to the predetermined IPv6 address provided by the *ASP (4.7)*. The means of this triggering are a matter for system design and not standardization. These means may or may not permit the *driver* to provide further information to the *ASP*.

On receipt of an unplanned, unexpected set of *basic vehicle data (4.14)*, the *ASP (4.7)* shall contact an address provided by the *jurisdiction (4.32)* to see if a (probably temporary) *controlled zone (4.19)* has been created and obtain its *access (4.1)* conditions. Armed with the updated *basic vehicle data (4.14)*, the *ASP* shall then meet the information and/or payment provision requirements of the *CZM* by means outside of the scope of this International Standard. If the *CZM* requires an, or regular, updates of the *basic vehicle data*, the *ASP* shall obtain these by the normal means of interrogation of the *IVS (4.29)* as determined in Clause 8.

10.2.4.3 Control, reporting, and feedback

The *controlled zone (4.19)* manager (*CZM*) shall then make a decision whether to permit or deny entry. As well as permitting or denying entry, it shall advise the *ASP (4.7)* of its decision. Where the entry conditions are fulfilled and the *regulated vehicle (4.40)* has entered the *controlled zone*, the *CZM* shall determine any data, and frequency of its provision that it requires form the *regulated vehicle* while in the *controlled zone*. In a planned situation, the *ASP* may have loaded an *app (4.5)* into the memory of the *IVS (4.29)* to provide this information at the intervals required. In an unplanned situation, if the *CZM* requires an, or regular, updates of the *basic vehicle data (4.14)*, it shall obtain these by the normal means of interrogation of the *IVS* as determined in Clause 8 and the relevant provisions of ISO 15638-6, Clauses 8 and 9.

It may be that the *CZM* also requires data when the *regulated vehicle (4.40)* is about to egress from the *controlled zone (4.19)*. As with the situation approaching the *controlled zone*, the *CZM* may provide that

notification via an *ITS-station (4.31)* – *ITS-station* communication to the *IVS (4.29)* of the *regulated vehicle*, or by a visible or audio notification to the *driver (4.24),* or in this case, it could have provided that data to the *ASP* in its exchange of information with them. As the *ASP* has received the updated location of the *regulated vehicle* every time it is provided with the *basic vehicle data (4.14)*, it has the means to provide egress relative data to the *CZM*, or to stimulate a new update of *basic vehicle data* from the *regulated vehicle* to enable it to do so. The means by which it does this are by agreement with the *CZM* and out with the scope of this International Standard.

10.2.5 Clear statement of responsibilities and authorities delegated

10.2.5.1 The *jurisdiction (4.32)* shall be responsible for the regime and regulations.

10.2.5.2 The *jurisdiction (4.32)* shall employ an *approval authority (regulatory) (4.11)* or otherwise provide its function.

10.2.5.3 The *jurisdiction (4.32)* shall provide means for enforcement (where required) to meet the requirements of the regime of the *jurisdiction.*

10.2.5.4 The *prime service provider (4.38)* shall install/commission *IVS (4.29)* and maintain the *IVS*.

10.2.5.5 The *prime service provider (4.37)* shall install/commission, or supervise the installation/commissioning of any on-board equipment connected to the *IVS (4.29)*.

10.2.5.6 The *application service provider (4.7)* (*ASP*) shall develop the *TARV VAC* application service or use a *TARV VAC* application service provided by *CZM*.

10.2.5.7 The *application service provider (4.7)* shall obtain any required *approval (4.9)* of its *TARV VAC* service from the *approval authority (regulatory) (4.11)*

10.2.5.8 The *application service provider (4.7)* shall contract with the *operator (4.36)* of the *regulated vehicle (4.40)*.

10.2.5.9 The *application service provider (4.7)* shall be responsible to provide the application service to *jurisdiction (4.32)*, *operator (4.36)*, and *driver (4.24)* as specified in its service offering. The *ASP* shall be responsible to inform the *driver* (by whatever means the *ASP* deems appropriate and the *jurisdiction* considers adequate), of regulations in respect of *access (4.1)* to the *controlled zone (4.19)* and the rules and procedures for entering the *controlled zone* in as much as this information is required for the *driver* to perform his tasks and remain within the regulations pertaining.

10.2.5.10 The *operator (4.36)* shall be responsible to provide the *regulated vehicle (4.40).*

10.2.5.11 The *operator (4.36)* shall be responsible to abide by requirements of the regime TARV VAC.

10.2.5.12 The operator *(4.36)* shall be responsible to pay penalties and levies required by *jurisdiction (4.32), CZM, prime service provider (4.37),* and *application service provider (4.7).* Where appropriate, the *operator (4.36)* shall pay any penalties and levies due to the *CZM*, or *jurisdiction* via its *ASP*, but it shall always be the *operator (4.36)* who is responsible for the payment of such fees.

10.2.5.13 The *driver (4.24)* shall be responsible to follow instructions, including use of the *IVS (4.29)* and associated equipment.

10.2.5.14 The *CZM* shall, within a regime determined by the *jurisdiction (4.32)*, be responsible for determining the regulation and *access (4.1)* policies and admission practices of the *controlled zone (4.19)*

and making such regulations as required for its management, and shall be responsible for making such regulations readily, freely, and fairly accessible to ASPs, and vehicle *operators (4.36)*.

10.2.5.15 The *CZM* shall be responsible for developing and operating any systems required for the management of the *controlled zone (4.19)* and for all and any equipment, *access control (4.2)* equipment and interfaces associated with the zone required by the regime of the *jurisdiction (4.32)*, and for providing access to *ASPs (4.7)* to provide required data to/from the system, and for making any broadcasts or other communications to the *regulated vehicle (4.40)* in order to request data.

10.2.5.16 In the event that levies are imposed to enter, or for movement within or egress from the *controlled zone (4.19)*, the *CZM* shall provide the *ASP (4.7)* and/or the *regulated vehicle (4.40) operator (4.36)* with receipt for the applied fee including detail of the basis of the levies imposed.

10.2.6 Equipment required for TARV VAC

10.2.6.1 TARV IVS

10.2.6.1.1 The system shall be designed to work using *TARV IVS (4.29)* as defined in this International Standards.

10.2.6.1.2 The *prime service provider* (*4.37*)*/application service provider (4.7)* shall provide to the *approval authority (regulatory) (4.11)*, evidence of compliance from an appropriate body to demonstrate the suitability for use in vehicles for the *IVS (4.29)* and all associated equipment.

10.2.6.1.3 It shall not be possible for collected or stored vehicle data or vehicle data in any software or non-volatile memory within the *IVS (4.29)* to be accessible or capable of being manipulated by any person, device, or system, other than that authorized by the *application service provider (4.7)*.

10.2.6.2 Equipment periphery/connected to IVS

10.2.6.2.1 The requirements of this part of ISO 15638 can be met without the requirement for the use of additional equipment, however, for convenience, or to meet the requirements of other parts of this International Standard, a vehicle may have equipment that is periphery/connected to the *IVS (4.29)* (for example, driver input device, driver identification device, etc.).

Where such equipment is used, it shall have been properly installed by the *prime service provider (4.37)* as approved by the *approval authority (regulatory) (4.11)* of the *jurisdiction (4.32)*.

10.2.6.2.2 This part of ISO 15638 specifies the *framework (4.28)* for the communications requirements with vehicles for the *access control (4.2)* of *regulated vehicles (4.40)* into/within/exiting access controlled zones. It does not specify the specific data collection requirements that such a system may require in addition to *basic vehicle data (4.14)*. That is a matter for local regulation/system design. If these local system *specifications (4.46)* require data to be collected from additional equipment connected to the *IVS (4.29)*, that shall be a local decision which requires clear *specification (4.46)* and control by the *jurisdiction (4.32)*/*CZM* and is outside the scope of this part of ISO 15638. The provisions of ISO 15638-6, Clause 8 may however be used to transmit such data.

10.2.6.3 `TARV VAC 'app'

The *ASP (4.7)* shall design and upload an *app (4.5)* designed to provide data to support the *TARV VAC (4.50)* application or shall install an *app* designed by the *jurisdiction (4.32)* or *CZM*, to provide any data in addition to the *basic vehicle data (4.14)* required by the *jurisdiction*/*CZM*. The *specification (4.46)* of that *app* is a matter for the *ASP* and/or *jurisdiction*/*CZM* and is outside the scope of this part of ISO 15638.

10.2.6.4 CZM levies and penalties applications and systems

TARV support for the *VAC (4.50)* application service is designed for use where such services are restricted to *regulated vehicles (4.40)* [however, these are defined by the *jurisdiction (4.32)*]. Where levies are an intrinsic part of such systems, this part of ISO 15638 is appropriate only for levy systems restricted to *regulated vehicle*s.

For reasons of commercial efficiency, interoperability and reuse, where charging for *regulated vehicle (4.40) access (4.1)* to a *controlled zone (4.19)* is part of a general automatic fee collection system for purposes such as road charging, that apply to all classes of vehicles using a *controlled zone,* implementers shall give precedence to and use the standards designed for ITS electronic fee collection wherever possible, in preference to this *specification (4.46)*.

10.2.7 Operational processes for the system — Define and update controlled access zone

A *controlled access zone (4.19)* shall be defined by the *CZM* [e.g. urban pedestrian areas, school and hospital surroundings, freight villages, ports, road sensitivity infrastructure (bridges, tunnels, etc.), weight restricted areas, width restricted areas, areas where there has been an accident or incident, etc.]. An approach (monitoring) area with adequate range shall be defined and declared, where the *regulated vehicle (4.40)* approaching the *controlled access zone* shall be tracked and monitored in order to notify its entry to the *controlled access zone*.

In respect of the rules/regulations, these are at the determination of the *jurisdiction (4.32)* or *CZM*, but may be for example a requirement to receive vehicle information periodically for monitoring specific goods.

Information requirements may relate to/be dependent on issues such as weight restrictions, number of axles, height restrictions, speed limitation, safety distance between vehicles, etc.

Public authorities and/or *CZM* shall publish/define in advance the critical area definition, the policies/rules and recommendations.

The *CZM* shall make generally available to *ASP*s *(4.7)*, and shall notify *ASP*s each and every time in immediate response to receiving notification that a vehicle is approaching the *controlled access zone (4.19)*, advising the policies/rules/regulations, requirements and recommendations associated to the *controlled access zone* and make available the tariff of levies if applicable.

10.2.8 Operational processes for the system — Approaching controlled access zone (planned and unplanned)

The reference points for the 'approaching *controlled access zone (4.19)*' (planned and unplanned) use case are the following.

10.2.8.1 *ASP (4.7)* determines that vehicle is approaching a *controlled access zone (4.19)* and warns the *driver (4.24)*.

10.2.8.2 Equipment of the *CZM* shall detect that a vehicle is approaching the *controlled access zone (4.19)* and its *ITS-station (4.31)* requests vehicle data.

10.2.8.3 Equipment of the *CZM* broadcasts an approach warning and request for vehicle data to all approaching vehicles.

10.2.8.4 *Regulated vehicle (4.40)* shall detect that it is approaching a *controlled access zone (4.19)* and warns the *driver (4.24).*

10.2.8.5 *Regulated vehicle (4.40)* shall update and send '*basic vehicle data (4.14)* to its *ASP (4.7)*.

10.2.8.6 *ASP (4.7)* determines that vehicle routing is correct and shall send vehicle identification parameters and relevant data to *CZM*.

10.2.8.7 *ASP (4.7)* instructs *driver (4.24)* not to enter *controlled access zone (4.19)* and provides re-routing information to *driver.*

10.2.9 Operational processes for the system — Access, reporting, and feedback

The reference points for the 'reporting and feedback' use case are the following.

10.2.9.1 *CZM* shall advise *ASP (4.7)* of its information requirements for the *regulated vehicle (4.40)* while within the *controlled access zone (4.19)* in advance of journey.

10.2.9.2 *CZM* shall advise *ASP (4.7)* of its information requirements for the *regulated vehicle (4.40)* in response to receipt of notification of vehicle approaching the *controlled access zone (4.19).*

10.2.9.3 *ASP (4.7)* shall send relevant data to *CZM* together with authorization of, and means of, paying, any fees and levies due.

10.2.9.4 *CZM* shall process the received data in order to decide to grant or deny *access (4.1)* to the critical area. In the event that *access* is to be denied, the *CZM* system shall have a means of informing the *driver (4.24), ASP (4.7)*, and *operator (4.36)*, that *access* is being denied to the specific *regulated vehicle (4.40)*. The means by which such notification is provided is a function of system design and is not specified in this part of ISO 15638.

10.2.9.5 *CZM* shall otherwise permit and enables *access (4.1)* (by lifting or lowering barriers, using control lights, or whatever means are appropriate), and during the passage through the *controlled zone (4.19)*, or at the point of exit from the *controlled zone*, may similarly operate multiple *access control (4.2)* mechanisms.

10.2.9.6 *ASP (4.7)* shall download *app (4.5)* into library of *IVS (4.29)* (preferably in advance) to program the *regulated vehicle (4.40) IVS (4.29)* to provide data at requested intervals or triggers.

10.2.9.7 *ITS-station (4.31)* of *CZM* shall interrogate vehicle at points where it requires vehicle data with a request for data and possibly provides some additional reference data to the *regulated vehicle (4.40)*.

10.2.9.8 In response to the installed *app (4.5)* or a prompt from an *ITS-station (4.31)* of the *CZM*, the *IVS (4.29)* of the *regulated vehicle (4.40)* shall update and send *basic vehicle data (4.14)* plus any additional data previously instructed by the *CZM*, together with any reference data provided by the interrogator, to the IPv6 address previously determined by the *ASP (4.7)*, who verifies and forwards the data to the system of the *CZM*.

10.2.10 'BigBubble' approaching and leaving

This configuration adopts a big area, for example, a metropolitan area, which includes several *controlled access zones (4.19)* within its '*BigBubble (4.15)*' *controlled access zone*. The design, nature, and complexity will vary from instantiation to instantiation, and will have significant impact on the design and management of the *CZM* system. In some *C-ITS (4.20)* implementations, this can have significant impact on the data exchange transactions between the *regulated vehicle (4.40)* and the *CZM* system. Within the *architecture (4.12)* of *TARV*, however, all such complications reside in the *CZM* system, or the *ASP* (4.7) system, and do not impact the *regulated vehicle*, which simply responds to the instructions of the relevant *app* (4.5), or to interrogation requests from an *ITS-station (4.31)* of the *CZM*.

10.3 Sequence of operations for TARV VAC

The sequence of operations for *TARV VAC* are therefore as follows:

10.3.1 VAC service element (VAC SE1): Define controlled zone

The *CZM* shall define the *controlled zone (4.19)* and its *access (4.1)* conditions.

10.3.2 VAC service element (VAC SE2): Publish regulation

The *CZM* shall post/make *controlled zone (4.19)* and its *access (4.1)* conditions, penalties, levies, and regulation information available to *ASPs (4.7)* and *users (4.49)*.

10.3.3 VAC service element (VAC SE3): Detect approaching regulated vehicle

By means unspecified in this part of ISO 15638, the approaching point of entry by a *regulated vehicle (4.40)* into a *controlled zone (4.19)* shall be detected and the *ASP (4.7)* advised.

10.3.4 VAC service element (VAC SE4): ASP notifies CZM of approaching vehicle

The *ASP (4.7)* shall notify the *CZM* with relevant vehicle details and agrees to the payment of any relevant fees.

10.3.5 VAC service element (VAC SE5): 'Interrogated' request for vehicle data

10.3.5.1 In the event that the *IVS (4.29)* of a vehicle receives a wireless interrogation requesting the vehicle data, the interrogator shall also provide at the time of the request, a unique 8-byte reference number (`URef`), and a destination IPv6 address (`ReqDest`) where it requests the data to be sent.

10.3.5.2 On receipt of the request, the *IVS (4.29)* shall acknowledge the request with the appropriate acknowledgement defined in ISO 15638-6, 8.3.5 < L > or < D >, which acknowledges that a request for LDT or `CoreData` has been received.

10.3.5.3 The *IVS (4.29)* shall then close the communication session.

10.3.5.4 The *IVS (4.29)* shall then open a new communication session using an available and appropriate CALM wireless medium.

10.3.5.5 The *IVS (4.29)* shall then send the data file (as defined in 10.5) to a predetermined destination IPv6 (internet) address that has previously been stored in the memory of the data pantry by its *ASP (4.7)*, together with the `URef` and `ReqDest` provided by the interrogator.

10.3.5.6 On successful receipt of the data, the recipient at the predetermined destination IPv6 address shall send an acknowledgement < `VAX` > to the *IVS (4.29)*.

10.3.5.7 On receipt of the acknowledgement < `VAX` >, the *IVS (4.29)* shall close its communication session.

10.3.5.8 The *ASP (4.7)* 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 part of ISO 15638.

10.3.6 VAC service element (VAC SE6): Grant/deny access

The *CZM* shall decide whether to permit *access (4.1)* and informs the *driver (4.24)*, *ASP (4.7)* and *operator (4.36)* [if *access (4.1)* is denied].

The *CZM* shall otherwise permit and enables entry of the *regulated vehicle (4.40)* to the *controlled zone (4.19)* (by lifting or lowering barriers, using control lights, or whatever means are appropriate).

10.3.7 VAC service element (VAC SE7): Periodic or requested updates

During the passage through the *controlled zone (4.19)*, or at the point of exit from the *controlled zone*, the *CZM* may similarly operate multiple *access control (4.2)* mechanisms (by lifting or lowering barriers, using control lights, or whatever means are appropriate). Whenever it receives such a request from an *ITS-station (4.31)* of the *CZM*, the *IVS (4.29)* of the *regulated vehicle (4.40)* shall update and send its *basic vehicle data (4.14)* together with other predetermined required data, and reference data provided by the *CZM*, to its *ASP (4.7)*. The *ASP* updates the *CZM* with the requested data.

The *CZM* decides whether to permit continued progress through the *controlled zone (4.19)* and shall inform the *driver (4.24)*, *ASP (4.7)*, and *operator (4.36)* if continued *access (4.1)* is denied. In these circumstances, it shall be the *CZMs* responsibility to instruct the *driver* what to do, and the *CZM* shall also bear the responsibility to keep the *ASP* informed. The means by which the *CZM* performs these tasks is not specified in this part of ISO 15638.

The *CZM* shall otherwise permit and enables progress of the *regulated vehicle (4.40)* through the *controlled zone (4.19)* (by lifting or lowering barriers, using control lights, or whatever means are appropriate).

10.3.8 VAC service element (VAC SE8): 'Interrogated' request for vehicle consignment data

10.3.8.1 An interrogating *ITS-station (4.31)* shall request specific data as determined in ISO 15638-6, 7.1 and 8.1.2.

10.3.8.2 In the event that the *IVS (4.29)* of a vehicle receives a wireless interrogation requesting the `VAC` data, the interrogator shall also provide at the time of the request, a unique 8-byte reference number (`URef`), and a destination IPv6 address (`ReqDest`) where it requests the data to be sent.

10.3.8.3 On receipt of the request, the *IVS (4.29)* shall acknowledge the request with the appropriate `ACK`nowledgement defined in ISO 15638-6, 8.3.5 < C >, which acknowledges that a request for `VAC` data has been received.

10.3.8.4 The *IVS (4.29)* shall then close the communication session.

10.3.8.5 The *IVS (4.29)* shall then open a new communication session using an available and appropriate CALM wireless medium.

10.3.8.6 The *IVS (4.29)* shall then send the VAC data file (as defined in 10.5) to a predetermined destination IPv6 (internet) address that has previously been stored in the memory of the data pantry by its *ASP (4.7)*, together with the `URef` and `ReqDest` provided by the interrogator.

10.3.8.7 On successful receipt of the data, the recipient at the predetermined destination IPv6 address shall send an acknowledgement < `VAX` > to the *IVS (4.29)*.

10.3.8.8 On receipt of the acknowledgement < `VAX` >, the *IVS (4.29)* shall close its communication session.

10.3.8.9 The *ASP (4.7)* 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 part of ISO 15638.

10.3.9 VAC service element (VAM SE9): Vehicle egress

The *regulated vehicle (4.40)* leaves the *controlled zone (4.19)*.

10.4 Generic TARV VAC data naming content and quality

The process to obtain *basic vehicle data (4.14)* [*TARV LDT (4.33)*] data content shall be as defined in ISO 15638-6, 8.3 and ISO 15638-5.

10.5 Specific TARV VAC data naming content and quality

VAC data principally comprises the LDT which identifies the key identification and characteristics of the vehicle, as specified in ISO 15638-5.

Controlled zone (4.19) specific additional data for the provision of that particular service shall be as specified by the *jurisdiction (4.32)/CZM*.

In the event that data are sent in response to an interrogation requesting data, the following data shall be appended:

Number	Data concept name	Use	Format	Notes/Source
VAC001	Uref	Mandatory	AN (8)	An 8-byte reference provided by the interrogator requesting the data. The alphanumeric or binary content of which is unspecified by this International Standard, but is intended to be used by the interrogator to provide a unique reference to its request for data.
VAC002	ReqDest	Mandatory	35 Bytes	Requested destination IPv6 address for the data to be sent as: scheme://domain:port/path?query_string#fragment_id i.e.: The scheme name (commonly called protocol), followed by:// then, depending on scheme, a domain name (alternatively, IP address): a port number, and / the path of the resource to be fetched or the program to be run. If the scheme name is http, the 'http://' is assumed e.g: www.example.com/path/to/name https://example.com/47.35868 telnet://192.0.2.16:80/

10.6 TARV VAC application service specific provisions for quality of service

The integrity of the data are 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, as specified in 10.4, are defined in ISO 15638-6, 8.3 and ISO 15638-5.

Application specific requirements shall be part of the regulation of the *jurisdiction (4.32)/CZM* for the *sensitive/restricted zone (4.43)*. However, in defining such requirements, *jurisdictions* shall wherever

possible, use performance-based or functionally *specifications (4.46)* 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.

10.7 TARV VAC application service specific provisions for test requirements

There are no specific provisions for test requirements specified in this version of this International Standard.

10.8 TARV VAC application specific rules for the approval of IVSs and 'service providers'

See 9.12.

11 Declaration of patents and intellectual property

This part of ISO 15638 contains no known patents or intellectual property other than that which is implicit in the media standards referenced herein and in ISO 15638-2. While the *CALM* standards themselves are free of patents and intellectual property, *CALM* in many cases relies on the use of public networks and IPR exists in many of the public network media standards. The reader is referred to those standards for the implication of any patents and intellectual property.

Application services (4.6) specified within this part of ISO 15638 and ISO 15638-7 contain no direct patents or intellectual property other than the copyright of ISO. However, national, regional, or local instantiations of any the applications services defined in this part of ISO 15638 and ISO 15638-7, or of the generic vehicle information defined in ISO 15638-5, the security requirements contained in ISO 15638-4, or the requirements of ISO 15638-3, may have additional requirements which may have patent or intellectual property implications. The reader is referred to the regulation regime of the *jurisdiction (4.32)* and its regulations for instantiation in this respect.

Annex A
(informative)

ASN.1 modules for ISO 15638-14 data concepts

A.1 Use of ASN.1

ISO TC204 requires that data concepts defined in ISO TC204 ITS standards deliverables are elaborated in ASN.1 (ISO 14813-6).

ISO 21217 (ITS- CALM -ITS-station communications architecture) and its associated standards require the exchange of data using ASN.1 PER or UPER.

The following example provides a definition for the data concepts used in this part of ISO 15638.

A.2 ASN.1 modules for ISO 15638-14 (vehicle access control)

A.2.1 Data concepts defined in ISO 15638-5 and used in this part of ISO 15638

```
TARVLocalDataTree DEFINITIONS AUTOMATIC TAGS::=
   BEGIN
        LDTData::= SEQUENCE
        {dataFormatVersion      DataFormatVersion,
         messageID              MessageIdentifier,
         primeSPID              PrimeServiceProviderIdentifier,
         applicationSPAddress   ApplicationServiceProviderAddress,
         sessionControlData     SessionControlData OPTIONAL,
         vehicleUniqueID        VehicleUniqueIdentifier OPTIONAL,
         vehicleClassID         VehicleClassIdentification OPTIONAL,
         vin                    VIN,
         propulsionStorageType  PropulsionStorageType,
         time                   TimeAndTimestamp DEFAULT 0,
         location               Location,
         direction              DirectionOfTravel,
         ignition               Ignition,
         movementSensors        OtherMovementSensors,
         driverID               DriverIdentification,
         trailerID              TrailerIdentification OPTIONAL,
         loadData               LoadData
         }

        DataFormatVersion::= VisibleString (SIZE (6))

        MessageIdentifier::= INTEGER

        PrimeServiceProviderIdentifier::= VisibleString (PATTERN "\w#4:\w#4:\w#4:\w#4:\
w#4:\w#4:\w#4:\w#4") -IPv6 address in the format xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx

        ApplicationServiceProviderAddress::= CHOICE {
        content   [0] INTEGER (128..16511), -contained in two octets
        extension [1] OCTET STRING(SIZE (2))
        }

        SessionControlData::= VisibleString

        VehicleUniqueIdentifier::= SEQUENCE {
        countryCode       VisibleString,
        alphabetIndicator VisibleString,
        licPlateNumber    NumericString
        }
```

```
        VehicleClassIdentification::= NumericString (SIZE (2))

        VIN::= VisibleString (SIZE (17))

        PropulsionStorageType::= BIT STRING {
        gasoline (0),
        diesel   (1),
        cng      (2),
        lpg      (3),
        electric (4),
        hydrogen (5)
        } -Enter type value with curly bracket at beginning and end, assignment type will
accept word and binary forms of storage type

        TimeAndTimestamp::= INTEGER

        Location::= SEQUENCE {
                              latitude  VisibleString (SIZE (10)),
                              longitude VisibleString (SIZE (10)),
                              altitude  VisibleString (SIZE (4..5)) DEFAULT "0000",
                              noOfSats  VisibleString (PATTERN "Sat\d+"), -Type value
must be in the format "SatN", where N = the number of satellites present
                              trust     INTEGER {
                                                false (0),
                                                true  (1)
                                                } (0 | 1) -accepts true, false, 0 or 1
                              }

        DirectionOfTravel::= INTEGER (0..360) -degrees clockwise

        Ignition::= VisibleString ("Ign 1" | "Ign 0" | "Ign d") -where 1=on, 0=off,
d=disconnected

        OtherMovementSensors::= SEQUENCE
        {sensorOne VisibleString (PATTERN "\d+\s\Mvt\s[m,n,d]"|"000") DEFAULT "000", -Type
value must be in the format "[SensorNumber] Mvt [m/n/d]", where m=movement, n=no movement,
d=disconnected
        sensorTwo  VisibleString (PATTERN "\d+\s\Mvt\s[m,n,d]"|"000") DEFAULT "000"
        }

        DriverIdentification::= SEQUENCE
        {jurisdictionID    VisibleString (PATTERN "\d#6\s\w+\s\w+\s(\w+,)*\s\d#6"), -
Must be in the format "[IssueDate(yymmdd)] [IssuingJurisdiction] [Driver'sName]
[VehicleClasses(comma separated)] [ExpiryDate(yymmdd)]"
        userAuthorisation VisibleString (PATTERN "\d#6\s\w+\s\w+\s(\w+,)*\s\d#6"|"000000")
DEFAULT "000000" -Same format as jurisdictionID
        }

        TrailerIdentification::= VisibleString

        LoadData::= VisibleString
   END
```

A.2.2 Data concepts defined in ISO 15638-14 (VAC)

```
-Type definition for 15638-14 module
VehicleAccessControl DEFINITIONS AUTOMATIC TAGS::=
   BEGIN

      VACData::= SEQUENCE
      {vAC001 Uref,
       vAC002 ReqDes
      }

      Uref::= VisibleString (SIZE (8))

      ReqDes::= VisibleString (SIZE (35))

   END
```

Annex B
(informative)

Independent testing of the protocols defined in this part of ISO 15638

B.1 Objectives

To test the validity of TARV standards it is necessary to simulate the TARV transactions. These are of two types

B.1.1 Instigation

a) The IVS of a vehicle establishes a new communication using one of (and shall be tested for each of) several wireless media defined below.

b) The IVS of a vehicle internally triggers a requirement to send a packet of data to a predetermined destination IPv6 (Internet) address.

c) The vehicle sends the data file to the predetermined destination IPv6 (Internet) address.

d) The recipient address sends acknowledgement.

e) The IVS closes the communication on receipt of acknowledgement.

B.1.2 Interrogation

a) The IVS of a vehicle receives a wireless interrogation requesting a packet of data.

b) The IVS of a vehicle is switched on but is not connected.

c) The IVS of a vehicle receives a wireless interrogation requesting a packet of data..

d) On receipt, it acknowledges the request (`ACK`).

e) It closes the communication.

f) It opens a new communication session using one of (and shall be tested for each of) several wireless media defined below.

g) It sends the data file to a predetermined destination IPv6 (Internet) address.

h) The recipient address sends acknowledgement.

i) The IVS closes the communication on receipt of acknowledgement.

These scenarios need to be tested using each of 2G, 3G, WiFi, 5,9 GHz (IEEE 802.11) using the same data.

A number of different data files (of different length) and acknowledgements need to be sent, which differ according to the application service. Each of the sequences defined below need to be tested.

In respect of 'interrogation' scenarios, the ability to receive the interrogation on one medium (esp. 5,9 GHz) and to instigate the subsequent message using a different medium needs to be tested.

B.1.3 Preconditions, assumptions, and simulations

a) The S.U.T. concerns only the communication between the IVS and the application service provider address. No other part of the system specifications are to be tested (they appear in the figures below for context, and because they are copied from the base standards.)

b) CALM and media choice are assumed, and not S.U.T.

c) The vehicle is equipped with wireless communications that enable it to make communications using 2G, 3G, Mesh WiFi, 5,9 GHz (IEEE 802.11p).

d) The means to trigger the sending of a message from the vehicle is a function of IVS design, not S.U.T., therefore, may be simulated.

e) The destination address is intended to be an IPv6 address, but may be simulated with an IPv4 address as this is an Internet issue, not S.U.T.

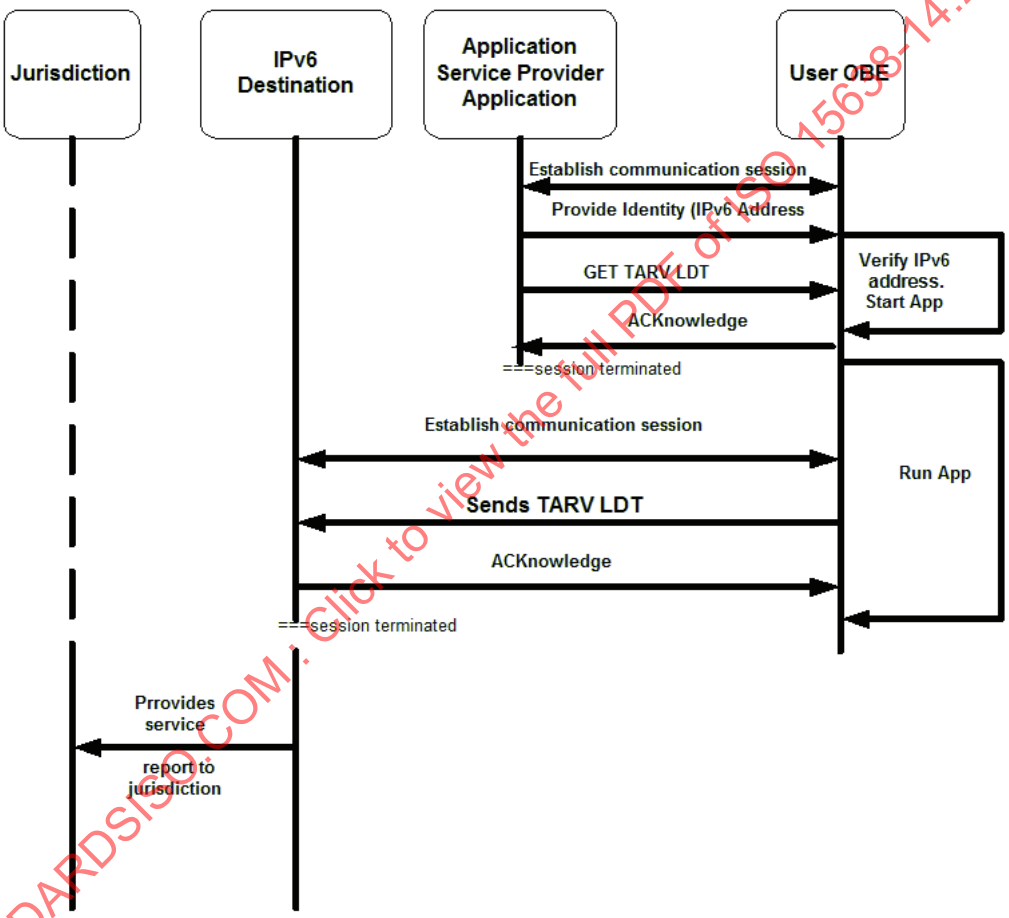

Figure B.1 — Communications sequences to obtain TARV LDT

B.1.4 Application Services where the verity of the communication needs to be physically tested

a) *VAM* *vehicle access monitoring*

b) *RTM* *remote electronic tachograph monitoring*

c) EMS *emergency messaging system*

d) *DWR* *driver work records* (work and rest hours compliance)

e) *VMM* *vehicle mass monitoring*

f) MRC *'mass' data for regulatory control and management (no test - data as VMM)*

g) *VAC vehicle access control (no test - data as VAM)*

h) *VLM vehicle location monitoring*

i) *VSM vehicle speed monitoring*

j) *CLM consignment and location monitoring*

k) *ADR Accord Dangereuses par Route (Dangerous Goods) monitoring*

l) *VPF vehicle parking facilities*

B.2 Test script 1 LDT service: VAM vehicle access monitoring (LDT)

CTP 1.1.1 Instigated LDT using 2G

S.U.T. reference	**Instigated send of LDT data using 2G**		
CTP/1.1.1			
S.U.T. test objective	The IVS of a vehicle establishes a new communication using one of (and shall be tested for each of) several wireless media defined below. The IVS of a vehicle internally triggers a requirement to send a packet of data to a predetermined destination IPv6 (Internet) address. The vehicle sends the datafile to the predetermined destination IPv6 (Internet) address. The Recipient address sends acknowledgement. The IVS closes the communication on receipt of acknowledgement.		
CTP origin	CSI		
Reference requirement	ISO 15638-8 and ISO 15638-6, 8.3.4.2		
Initial conditions	The S.U.T. concerns only the communication between the IVS and the application service provider address. No other part of the system specifications are to be tested (they appear in the figures below for context, and because there are copied from the base standards). CALM and media choice are assumed and not S.U.T. The vehicle is equipped with wireless communications that enable it to make communications using 2G, 3G, WiFi, 5,9 GHz (IEEE 802.11p). The means to trigger the sending of a message from the vehicle is a function of IVS design, not S.U.T., therefore may be simulated. The destination address is intended to be an IPv6 address, but may be simulated with an IPv4 address as this is an Internet issue, not S.U.T.		
Stimulus and expected behaviour			
Test point		**Tester action**	**Pass condition**
1.1.1.1	1	IVS instigates a communication session using selected media (2G) to predetermined destination IP address	Session established

1.1.1.2	2	IVS sends file named < 44EMV03WRRLDT > < START > < AaaSs0,,0,xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx,128..16511,1G1JF27W8GJ178227,000000,1297339499,0x0A5D3770,0x027E2938,0000,Sat8,0,123,Ign 1,000,000,010326 UKPeter Jones,01,02,03a,h1,120325,010326 124538, Peter Jones 01,02,h1120325 > < END >	File sent and arrives correctly at destination
1.1.1.3	3	Destination address sends ACK < LDX >	
1.1.1.4	4	IVS receives ACK < LDX >	File received and ACK < LDX > sent
1.1.1.5	5	IVS closes communication session	Communication session closed
			If ALL individual pass conditions listed in this column above have been met THEN CTP PASS ELSE CTP FAIL

Test result: CTP 1.1.1	**Pass/Fail**	**Date: 28th June 2102**
Signature/initials 	**PASS**	 k4, MIRA, Watling St, Nuneaton, Warwickshire, CV10 0TU, UK Tel: +44 (0)7730 922 810 Web: www.innovits.com/advance

CTP 1.1.2 Interrogated LDT using 2G

S.U.T. reference	**Interrogated send of LDT data using 2G**
CTP/1.1.2	
S.U.T. test objective	The IVS of a vehicle receives a wireless interrogation requesting a packet of data. The IVS of a vehicle is switched on but is not connected. The IVS of a vehicle receives a 2G wireless interrogation requesting a packet of data. On receipt, it acknowledges the request (ACK). It closes the communication. It opens a new communication session using one of (and shall be tested for each of) several wireless media defined below. It sends the datafile to a predetermined destination IPv6 (Internet) address. The recipient address sends acknowledgement. The IVS closes the communication on receipt of acknowledgement.

CTP origin		CEN	
Reference requirement		ISO 15638-8 and ISO 15638-6, 8.3.4.2	
Initial conditions		The S.U.T. concerns only the communication between the IVS and the application service provider address. No other part of the system specifications are to be tested (they appear in the figures below for context, and because there are copied from the base standards). CALM and media choice are assumed and not S.U.T. The vehicle is equipped with wireless communications that enable it to make communications using 2G, 3G, WiFi, 5,9 GHz (IEEE 802.11p). The means to trigger the sending of a message from the vehicle is a function of IVS design, not S.U.T., therefore may be simulated. The destination address is intended to be an IPv6 address, but may be simulated with an IPv4 address as this is an Internet issue, not S.U.T.	
Stimulus and expected behaviour			
Test point		**Tester action**	**Pass condition**
1.1.2.1	1	Session connected (incoming call)	Call in progress
1.1.2.2	2	Caller sends data request command (GPRS, EDGE, etc.) GET VAM	Data request sent
1.1.2.3	3	IVS acknowledges request by returning ACKnowledgement < A >	ACK < A > received
1.1.2.4	4	IVS closes communication session	Communication session closed
1.1.2.5	5	IVS instigates a communication session using selected media to predetermined destination IP address	Communication session successfully opened
1.1.2.6	6	IVS sends file named < 44EMV0 < START > < AaaSs0,,0,xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx,128..16511,1G1JF27W8GJ178227,000000,1297339499,0x0A5D3770,0x027E2938,0000,Sat8,0,123,Ign 1,000,000,010326 UKPeter Jones,01,02,03a,h1,120325,010326 124538, Peter Jones 01,02,h1120325 > < END >	File sent and arrives correctly at destination
1.1.2.7	7	Destination address sends ACK < LDX >	
1.1.2.8	8	IVS receives ACK < LDX >	File received and ACK < LDX > sent
1.1.2.9	9	IVS closes communication session	Communication session closed
			If ALL individual pass conditions listed in this column above have been met THEN CTP PASS ELSE CTP FAIL

Test result: CTP 1.1.2	Pass/Fail	Date: 28th June 2102
Signature/initials 	**PASS**	k4, MIRA, Watling St, Nuneaton, Warwickshire, CV10 0TU, UK Tel: +44 (0)7730 922 810 Web: www.innovits.com/advance

CTP 1.1.3 Interrogated LDT using 5,9 GHz and responding using 2G or 3G

S.U.T. reference	Interrogated LDT using 5,9 GHz and send of LDT data using 2G or 3G
CTP/1.1.3	
S.U.T. test objective	The IVS of a vehicle receives a wireless interrogation requesting a packet of data. The IVS of a vehicle is switched on but is not connected. The IVS of a vehicle receives a 5,9 GHz (IEEE 802.11p) wireless interrogation requesting a packet of data. On receipt, it acknowledges the request (ACK). It closes the communication. It opens a new communication session using 2G or 3G. It sends the datafile to a predetermined destination IPv6 (Internet) address. The recipient address sends acknowledgement. The IVS closes the communication on receipt of acknowledgement.
CTP origin	CEN
Reference requirement	ISO 15638-8 and ISO 15638-6, 8.3.4.2
Initial conditions	The S.U.T. concerns only the communication between the IVS and the application service provider address. No other part of the system specifications are to be tested (they appear in the figures below for context, and because there are copied from the base standards). CALM and media choice are assumed and not S.U.T. The vehicle is equipped with wireless communications that enable it to make communications using 2G, 3G, WiFi, 5,9 GHz (IEEE 802.11p). The means to trigger the sending of a message from the vehicle is a function of IVS design, not S.U.T., therefore may be simulated. The destination address is intended to be an IPv6 address, but may be simulated with an IPv4 address as this is an Internet issue, not S.U.T.

Stimulus and expected behaviour

Test point		Tester action	Pass condition
1.1.3.1	1	Session connected (incoming call) using 5,9 GHz (IEEE 802.11p)	Call in progress
1.1.3.2	2	Caller sends data request command GET LDT	Data request sent
1.1.3.3	3	IVS acknowledges request by returning ACKnowledgement < A >	ACK < L > received

1.1.3.4	4	IVS closes communication session	Communication session closed
1.1.3.5	5	IVS instigates a communication session using 2G or 3G	Communication session successfully opened
1.1.3.6	6	IVS sends file named < 44EMV03WRRLDT > < START > < AaaSs0,,0,xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx,128..16511,1G1JF27W8GJ178227,000000,1297339499,0x0A5D3770,0x027E2938,0000,Sat8,0,123,Ign 1,000,000,010326 UKPeter Jones,01,02,03a,h1,120325,010326 124538, Peter Jones 01,02,h1120325 > < END >	File sent and arrives correctly at destination
1.1.3.7	7	Destination address sends ACK < LDX >	
1.1.3.8	8	IVS receives ACK < LDX >	File received and ACK < LDX > sent
1.1.3.9	9	IVS closes communication session	Communication session closed
			If ALL individual pass conditions listed in this column above have been met THEN CTP PASS ELSE CTP FAIL

Test result: CTP 1.1.3	**Pass/Fail**	**Date: 28th June 2102**
Signature/initials 	**PASS**	 k4, MIRA, Watling St, Nuneaton, Warwickshire, CV10 0TU, UK Tel: +44 (0)7730 922 810 Web: www.innovits.com/advance

CTP 1.2.1 Instigated LDT using 3G

S.U.T. reference	**Instigated send of LDT data using 3G**
CTP/1.2.1	
S.U.T. test objective	The IVS of a vehicle establishes a new communication using one of (and shall be tested for each of) several wireless media defined below. The IVS of a vehicle internally triggers a requirement to send a packet of data to a predetermined destination IPv6 (Internet) address. The vehicle sends the datafile to the predetermined destination IPv6 (Internet) address. The recipient address sends acknowledgement. The IVS closes the communication on receipt of acknowledgement.
CTP origin	CSI