INTERNATIONAL STANDARD

ISO 15638-6

First edition
2014-07-15

Intelligent transport systems — Framework for collaborative Telematics Applications for Regulated commercial freight Vehicles (TARV) —

Part 6: Regulated applications

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

Partie 6: Applications réglementées

Reference number
ISO 15638-6:2014(E)

COPYRIGHT PROTECTED DOCUMENT

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 15638-6:2013.

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 Penalties and Levies (VMC)*

Introduction

Many ITS technologies have been embraced by commercial transport *operators* (*4.43*) and freight owners, in the areas of fleet management, safety and security. *Telematics* (*4.54*) applications have also been developed for governmental use. Such regulatory services in use or being considered vary from *jurisdiction* (*4.37*) to *jurisdiction*, but include electronic on-board recorders, collection of penalties and levies, digital *tachograph* (*4.53*), on-board *mass* (*4.41*) monitoring, vehicle *access* (*4.1*) *methods*, hazardous goods tracking and eCall (*4.27*). Additional applications with a regulatory impact being developed include, fatigue management, speed monitoring, and measurement of *mass*, location, distance, and time.

In such an emerging environment of regulatory and *commercial applications* (*4.18*), 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* (*4.52*) 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* (*4.30*) 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* (*4.37*).

This International Standard addresses and defines the *framework* (*4.30*) for a range of cooperative *telematics* (*4.54*) applications for *regulated commercial freight vehicles* (*4.47*), such as *access methods* (*4.2*), driver *f*atigue management, speed monitoring, and on-board *mass* (*4.41*) monitoring. The overall scope includes the concept of operation, legal and regulatory issues, and the generic cooperative provision of services to *regulated commercial freight vehicles*, using an on-board ITS platform. The *framework* is based on a (multiple) *service provider* (*4.50*) oriented approach with provisions for the *approval* (*4.10*) and *auditing* (*4.13*) of *service providers*.

This International Standard

— provides the basis for future development of cooperative *telematics* (*4.54*) applications for *regulated commercial freight vehicles* (*4.47*). Many elements to accomplish this are already available. Existing relevant standards will be referenced, and the *specifications* (*4.52*) 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 commercial freight vehicles*,

— provides a business *architecture* (*4.12*) based on a (multiple) *service provider* (*4.50*) oriented approach, and

— addresses legal and regulatory aspects for the *approval* (*4.10*) 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* (*4.54*) 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 general *specifications* (*4.52*) for communications and data exchange aspects of candidate *regulated applications* (*4.45*) which are specified in ISO 15638-8 to ISO 15638-19 (at the time of developing this part of ISO 15638, but further parts may be added later if a requirement for additional regulated applications to be standardized are identified), the selection and implementation for all or any of which remain a decision for the implementing *jurisdiction* (*4.37*).

NOTE 1 The definition of what comprises a 'regulated' vehicle is regarded as an issue for national decision and might vary from *jurisdiction* (*4.37*) to *jurisdiction*. This International Standard does not impose any requirements on nations in respect of how they define a *regulated vehicle* (*4.47*).

NOTE 2 The definition of what comprises a 'regulated' service is regarded as an issue for national decision, and might vary from *jurisdiction (4.37)* to *jurisdiction*. This International Standard does not impose any requirements on nations in respect of which services for *regulated vehicles (4.47) 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 collaborative Telematics Applications for Regulated commercial freight Vehicles (TARV) —

Part 6: Regulated applications

1 Scope

This part of ISO 15638 specifies the common roles and responsibilities of actors providing *regulated application (4.45)* systems which use *TARV* to provide *regulated application services (4.46)* for *regulated commercial freight vehicles (4.47)* and the interoperability of key operational steps and actions required to support all *TARV regulated application service* systems.

This part of ISO 15638 specifies the general conditions for data exchanges between an *application service provider (4.7)* and vehicle *IVS (4.32)*, and from other *ITS-stations (4.34)* to the *IVS* of the *regulated commercial freight vehicle (4.47)*, and specifies generic data concepts for identified services, but it does not define the detailed aspects of the *application services (4.6)* or their implementation (application specific aspects being defined in ISO 15638-8 to ISO 15638-19 for each identified application service).

This part of ISO 15638 addresses the general and common requirements for the provision of *regulated application services (4.46)* that require data in addition to, or instead of, *basic vehicle data (4.16)* and *core application data (4.23)* (application specific aspects being defined in ISO 15638-8 to ISO 15638-19 for each identified application service).

The scope of this part of ISO 15638 is to provide common aspects of *specifications (4.52)* for communications and data exchange aspects of identified *application services (4.6)* (as defined in ISO 15638-8 to ISO 15638-19) that a *regulator (4.38)* may elect to require or support as an option, including

a) high-level definition of the service that a *service provider (4.50)* 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 common to all parts as defined in ISO 15638-8 to ISO 15638-19, naming content and quality that an *IVS (4.32)* has to deliver.

The definition of what comprises a 'regulated' service is regarded as an issue for national decision and may vary from *jurisdiction (4.37)* to *jurisdiction*. This International Standard does not impose any requirements on nations in respect of which services for *regulated commercial freight vehicles jurisdictions* will require, or support as an option, but provides standardized sets of requirements descriptions for identified services to enable consistent and cost efficient implementations where instantiated.

ISO 15638 has been developed for use in the context of regulated commercial freight vehicles [hereinafter referred to as 'regulated vehicles' *(4.47)*]. 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 (4.37)* 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.

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 14816, *Road transport and traffic telematics — Automatic vehicle and equipment identification — Numbering and data structure*

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

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

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

ISO/TS 15638-4:—[1)], *Intelligent transport systems — Framework for collaborative Telematics Applications for Regulated commercial freight Vehicles (TARV) — Part 4: 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 15638-8, *Intelligent transport systems — Framework for cooperative telematics applications for regulated vehicles (TARV) — Part 8: Vehicle access management and monitoring*

ISO/TS 15638-9, *Intelligent transport systems — Framework for collaborative Telematics Applications for Regulated commercial freight Vehicles (TARV) — Part 9: Remote electronic tachograph monitoring (RTM)*

ISO/TS 15638-10, *Intelligent transport systems — Framework for collaborative Telematics Applications for Regulated commercial freight Vehicles (TARV) — Part 10: Emergency messaging system/eCall (EMS)*

ISO 15638-11, *Intelligent transport systems — Framework for cooperative telematics applications for regulated vehicles (TARV) — Part 11: Driver work records*

ISO 15638-12, *Intelligent transport systems — Framework for cooperative telematics applications for regulated vehicles (TARV) — Part 12: Vehicle mass monitoring*

ISO 15638-13:—[1)], *Intelligent transport systems — Framework for cooperative telematics applications for regulated vehicles (TARV) — Part 13: Mass Penalties and Levies (VMC)*

ISO 15638-14, *Intelligent transport systems — Framework for cooperative telematics applications for regulated vehicles (TARV) — Part 14: Vehicle access control*

ISO 15638-15, *Intelligent transport systems — Framework for cooperative telematics applications for regulated vehicles (TARV) — Part 15: Vehicle location monitoring*

ISO 15638-16, *Intelligent transport systems — Framework for cooperative telematics applications for regulated vehicles (TARV) — Part 16: Vehicle speed monitoring*

ISO 15638-17, *Intelligent transport systems — Framework for cooperative telematics applications for regulated vehicles (TARV) — Part 17: Consignment and location monitoring*

1) To be published.

ISO/TS 15638-18, *Intelligent transport systems — Framework for collaborative Telematics Applications for Regulated commercial freight Vehicles (TARV) — Part 18: ADR (Dangerous Goods) transport monitoring (ADR)*

ISO/TS 15638-19, *Intelligent transport systems — Framework for collaborative Telematics Applications for Regulated commercial freight Vehicles (TARV) — Part 19: Vehicle parking facilities (VPF)*

ISO 17262, *Intelligent transport systems — Automatic vehicle and equipment identification — Numbering and data structures*

ISO 24534-3, *Intelligent transport systems — Automatic vehicle and equipment identification — Electronic registration identification (ERI) for vehicles — Part 3: Vehicle data*

ISO/TS 26683-1, *Intelligent transport systems — Freight land conveyance content identification and communication (FLC-CIC) — Part 1: Context, architecture and referenced standards*

ISO/TS 26683-2, *Intelligent transport systems — Freight land conveyance content identification and communication (FLC-CIC) — Part 2: Application interface profiles*

4 Terms and definitions

For the purposes of this document, the 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 methods
procedures and protocols to provision and retrieve data

4.3
access monitoring
observation and recording of vehicle related data when using the road network and/or associated infrastructure (bridges, tunnels etc.)

4.4
Accord européen relatif au transport international des marchandises Dangereuses par Route
ADR
UNECE regulations and declaration systems for agreements relating to dangerous goods/hazardous goods

4.5
app
small (usually) Java™[2)] applets, organized as software bundles, that support *application services (4.6)* by keeping the *data pantry (4.24)* of the *IVS(4.32)* provisioned with up to date data

4.6
application service
service provided by a *service provider (4.50)* enabled by accessing data from the *IVS (4.32)* of a *regulated vehicle (4.47)* through a wireless communications network

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

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

4.8
app library
separately secure area of memory in *IVS (4.32)* where apps are stored, with different access controls to *data pantry (4.24)*

4.9
application service data file
ASD file
file held in the *data pantry (4.24)* of the *IVS (4.32)* containing data specific to an *application service (4.6)*

4.10
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 delivers the required service levels

4.11
approval authority (regulatory)
organization (usually independent) which conducts *approval (4.10)* and on-going *audit (4.13)* for *service providers (4.50)* on behalf of a *jurisdiction (4.37)*

4.12
architecture
formalized description of the design of the structure of *TARV* and its *framework (4.30)*

4.13
audit
auditing
review of a party's capacity to meet, or continue to meet, the initial and on-going approval agreements as a *service provider (4.50)*

4.14
auditor
person or organization approved to *audit (4.13)* parts of a *regulated application service (4.46)* by an approval *authority (regulatory) (4.11)*

4.15
authentication
function intended to establish and verify a claimed identity

4.16
basic vehicle data
data that shall be maintained/provided by all *IVS (4.32)*, regardless of *jurisdiction (4.37)*

4.17
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 (4.55)* 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 (4.34)* to provide wireless support for applications, such that the application is independent of any particular wireless medium

4.18
commercial application(s)
ITS applications in *regulated vehicles (4.47)* for commercial (non-regulated) purposes

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

4.19
consignment
shipment of goods/cargo to a destination

4.20
consignment and location monitoring
CLM
collection, collation, and transfer of data from an *in-vehicle system* (*4.32*) to an *application service provider* (*4.7*) concerning the content of the load being carried and/or its condition and/or location

4.21
conveyance
vehicle or trailer used transport from one place to another

4.22
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* (*4.34*) 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* (*4.33*)

4.23
core application data
core data
basic vehicle data (*4.16*) plus any additional data required to provide an implemented *regulated application service* (*4.46*)

4.24
data pantry
secure area of memory in *IVS* (*4.32*) where data values are stored, with different access controls to *app library* (*4.8*)

4.25
driver
person driving the *regulated vehicle* (*4.47*) at any specific point in time

4.26
driver work records
DWR
collection, collation, and transfer of *driver* (*4.25*) work and rest hours data from an *in-vehicle system* (*4.32*) to an *application service provider* (*4.7*)

4.27
eCall
specialized instantiation of an *EMS* (*4.28*) that provides incident messaging and communication with a public service assistance point through priority wireless telephone communications using its emergency call capabilities

4.28
emergency message system
EMS
collection, collation, and transfer of emergency message data from an *in-vehicle system* (*4.32*) to an *application service provider* (*4.7*)

4.29
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

4.30
framework
particular set of beliefs, or ideas referred to in order to describe a scenario or solve a problem

4.31
host management centre
central point for *TARV-ROAM* management of *TARV* applications executing on the *TARV-ROAM* host; *HMC* enables remote management of vehicle applications by a trusted party

4.32
in-vehicle system
IVS
ITS-station (4.34) and connected equipment on board a vehicle

4.33
ITS service
communication functionality offered by an *ITS-station (4.34)* to an *ITS-station* application

4.34
ITS-station
ITS-s
entity in a communication network, comprised of application, *facilities (4.29)*, networking and access layer components specified in ISO 21217 that operate within a bounded secure management domain

4.35
IVS installer
actor who installs *IVS (4.32)* on behalf of the vehicle manufacturer or the initial *prime service provider (4.44)*

4.36
IVS maintainer
actor who maintains *IVS (4.32)* on behalf of the *prime service provider (4.44)*

4.37
jurisdiction
government, road, or traffic authority which owns the *regulatory applications (4.45)*

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

4.38
jurisdiction regulator
regulator
agent of the *jurisdiction (4.37)* appointed to regulate and manage *TARV* within the domain of the *jurisdiction*; may or may not be the *approval authority (regulatory) (4.11)*

4.39
local data tree
LDT
frequently updated data concept stored in the on on-board *data pantry (4.24)* containing a collection of data values deemed essential for either a) *TARV regulated application service (4.46)*, or b) *cooperative intelligent transport systems (4.22)*

4.40
map
spatial dataset that defines the road system

4.41
mass
mass of a given heavy vehicle as measured by equipment affixed to the *regulated vehicle (4.47)*

4.42
'mass' information for jurisdictional control and enforcement
MICE
MRC
collection, collation, and transfer of *vehicle mass (4.41)* data from an *in-vehicle system (4.32)* to an appli*cation service provider (4.7)* to enable data provision to *jurisdictions (4.37)* for the control and management of equipped vehicles based on the mass of the *regulated vehicle (4.47)* or use of such data to enable compliance with the provisions of regulations

4.43
operator
fleet manager of a *regulated vehicle (4.47)*

4.44
prime service provider
service provider (4.50) who is the first contractor to provide *regulated application services (4.46)* to the *regulated vehicle (4.47),* or a nominated successor on termination of that initial contract; the *prime service provider (4.44)* is also responsible to maintain the installed *IVS (4.32)*; 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 (4.32)*

4.45
regulated application
regulatory application
application arrangement using TARV utilised by *jurisdictions (4.37)* 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*

4.46
regulated application service
TARV application service to meet the requirements of a regulated application that is mandated by a regulation imposed by a *jurisdiction (4.37),* or is an option supported by a *jurisdiction*

4.47
regulated commercial freight vehicle
regulated vehicle
vehicle that is subject to regulations determined by the *jurisdiction (4.37)* 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 through *TARV* or provide the option to do so

4.48
regime for open application management
ROAM
facilities (4.29) layer for *TARV*, within the ISO 15638 suite of standards deliverables, providing an open access, yet secure runtime environment for *TARV* and other applications, including cooperative vehicle applications, on top of the *CALM* communications environment

4.49
remote tachograph monitoring
RTM
collection, collation, and transfer of data from an on-board electronic *tachograph (4.53)* system to an *application service provider (4.7)*

4.50
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)*

4.51
session
wireless communication exchange between the *ITS-station (4.34)* of an *IVS (4.32)* 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 (4.32)* from any other *ITS-station*

4.52
specification
explicit and detailed description of the nature and functional requirements and minimum performance of equipment, service or a combination of both

4.53
tachograph
sender unit mounted to a vehicle gearbox, a tachograph head and a digital driver card, which records the *regulated vehicle (4.47)* speed and the times at which it was driven and aspects of the *driver's (4.25)* activity selected from a choice of modes

4.54
telematics
use of wireless media to obtain and transmit (data) from a distant source

4.55
user
individual or party that enrols in and operates within a regulated or *commercial application (4.18) service (4.6)*

EXAMPLE *Driver (4.25),* transport *operator (4.43),* freight owner, etc.

4.56
vehicle access control
VAC
control of *regulated vehicles (4.47)* ingress to and egress from controlled areas and related systems

4.57
vehicle access management
VAM
monitoring and management of *regulated vehicles (4.47)* approaching or within sensitive and controlled areas

4.58
vehicle location monitoring
VLM
collection, collation, and transfer of vehicle location data from an *in-vehicle system (4.32)* to an *application service provider (4.7)*

4.59
vehicle parking facility
VPF
parking facility for regulated and other commercial vehicles that meets the requirements of the local *jurisdiction (4.37)* in its ability and associated administration and management esp. often to provide safe and secure parking for regulated and other commercial vehicles

4.60
vehicle mass monitoring
VMM
collection, collation, and transfer of vehicle *mass (4.41)* data from an *in-vehicle system (4.32)* to an *application service provider (4.7)*

4.61
vehicle speed monitoring
VSM
collection, collation, and transfer of vehicle speed data from an *in-vehicle system (4.32)* to an *application service provider (4.7)*

5 Symbols and abbreviated terms

ADR	accord européen relatif au transport international des marchandises dangereuses par route (dangerous goods)
app	applet (Java™[a] application or similar) *(4.5)*
AS	application service
ASD file	application service data file *(4.9)*
ASP	*application service provider (4.7)*
CALM	*communications access for land mobiles (4.17)*
CAN	controller area network
C-ITS	*cooperative intelligent transport systems (4.22)*
CLM	*consignment and location monitoring (4.20)*
CONOPS	concept of operations
DRD	driver records device
DWR	*driver work records (4.26)*
EMS	*emergency message system (4.28)*
HMC	*host management centre (4.31)*
ID	identity
IP	internet protocol
ISMS	information security management system
ITS-S	*ITS station (4.34)*
IVS	*In-vehicle system (4.32)*
Java™[a]	object-oriented open-source operating language developed by SUN systems
LDT	*local data tree (4.39)*
MICE	*'mass' information for jurisdictional control and enforcement (4.42)*
OID	object identifier
OSGi™[a]	open services gateway initiative
QMS	quality monitoring station

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

RAS	*regulated application service (4.46)*
RFID	radio frequency identification device
ROAM	*regime for open application management (4.48)*
RTM	*remote tachograph monitoring (4.49)*
SE	service element
TARV	*telematics (4.54)* applications for *regulated vehicles (4.47)*
UNECE	United Nations Economic Commission for Europe
VAC	*vehicle access control (4.56)*
VAM	*vehicle access management (4.57)*
VLM	*vehicle location monitoring (4.58)*
VMM	*vehicle mass monitoring (4.60)*
VSM	*vehicle speed monitoring (4.61)*
VPF	*vehicle parking facility (4.59)*

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

ISO 15638-1 provides a *framework (4.30)* 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 (4.52)* of the roles of the actors involved, the reader is referred to ISO 15638-1.

In summary, Figure 1 shows the role model conceptual *architecture (4.12)* showing the key actors and their relationships.

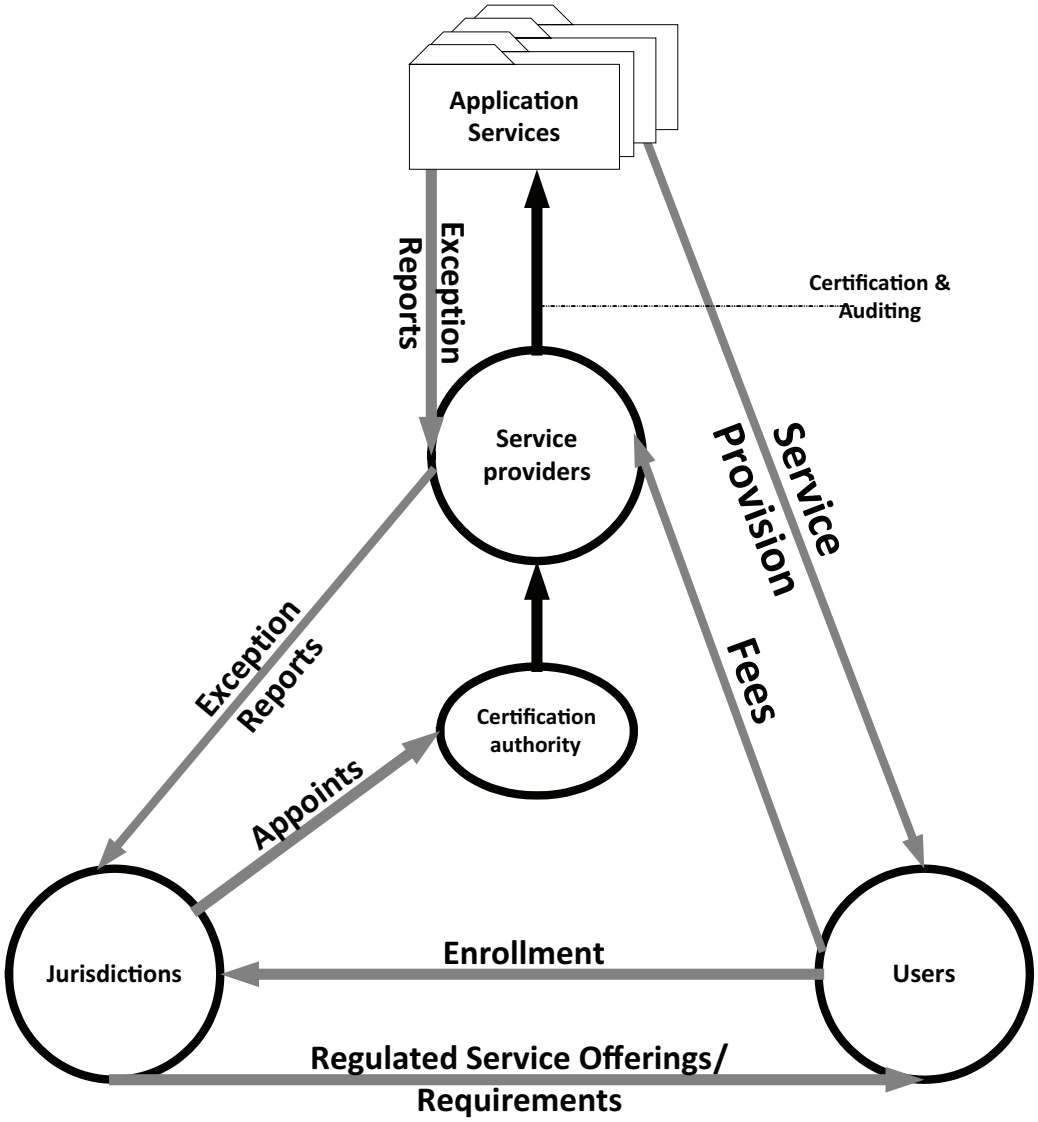


Figure 1 — Role model conceptual architecture
(Source: **ISO 15638-1**)

ISO 15638 provides a suite of International Standard deliverables which addresses and defines the *framework (4.30)* for a range of cooperative *telematics (4.54)* applications for *regulated vehicles (4.47)* [such as electronic *tachograph (4.53)* monitoring, *Driver work records (4.26)*, emergency messaging/*eCall (4.27)*; mass monitoring, HGV *mass (4.41)* monitoring, speed monitoring, *access (4.1)*, *access methods (4.2)*, location monitoring, etc.]. The overall scope includes the concept of operation, legal and regulatory issues, and the generic *cooperative ITS (4.22)* service platform. The *framework (4.30)* is based on a (multiple) *service provider (4.50)* oriented approach including provisions for the *approval (4.10)* and *auditing (4.13)* of *service providers*. This part of ISO 15638 is one of a suite of standards deliverables that provide a standardized approach for *telematics* aspects for *regulated vehicles (4.47)*:

— ISO 15638-1;

— ISO 15638-2;

— ISO 15638-3;

— ISO 15638-4:—[3)];

3) To be published.

— ISO 15638-5;

— this part of ISO 15638;

— ISO 15638-7.

ISO 15638-8 to ISO 15638-19 specifies application and specific aspects for identified TARV regulated application services. At the time of developing this part of ISO 15638, the following parts have been developed for the identified regulated application services, but further parts may be added later if additional TARV regulated application services are identified:

— ISO 15638-8;

— ISO 15638-9;

— ISO 15638-10;

— ISO 15638-11;

— ISO 15638-12;

— ISO 15638-13:—[4)];

— ISO 15638-14;

— ISO 15638-15;

— ISO 15638-16;

— ISO 15638-17;

— ISO 15638-18;

— ISO 15638-19.

This part of ISO 15638 provides common *specifications (4.52)* for the generic telematics and data requirements for candidate *regulated applications (4.45)* for *TARV*, and defines the generic modus of operations.

A *regulated application service (4.46)* shall be a *TARV application service (4.6)* that is mandated by a regulation imposed by a *jurisdiction (4.37)* [government, road or traffic authority, which owns the *regulatory applications (4.45)*], in which case, all vehicles of a class defined by the *jurisdiction* shall support and provide this service; or is an option supported by a *jurisdiction,* in which case, it provides a voluntary electronic means of satisfying a requirement of a *jurisdiction.*

A *regulated application service (4.46)* is provided by a *service provider (4.50)*, also called an *application service provider (4.7)* (*ASP*) who is a party which is approved by an approval *authority (regulatory) (4.11)* as suitable to provide regulated or commercial ITS *application services (4.6)*.

NOTE An *approval authority (regulatory) (4.11)* is an agency of, or function within a *jurisdiction regulator (4.38)*, who approves that the requirements of the *jurisdiction (4.37)* have been met, and should not be confused with an *certification authority (digital)* which is an organization which issues digital certificates for use by other parties (specifically in the context of communications security).

The *service provider (4.50)* provides the *application service (4.6)* to/for a *user (4.55)* who is an individual or party that enrols in and operates within a *regulated application service (4.46)* or *commercial application (4.18)* service in order to meet specific aspects of the requirements of a *jurisdiction (4.37)* for the operation of the *regulated vehicle (4.47)* within that *jurisdiction.*

Examples of a *user (4.55)* are transport *operator (4.43)*, *driver (4.25)*, freight owner, etc. Most commonly, the *user (4.55)* is the transport *operator*.

4) To be published.

For further information, refer to ISO 15638-1.

The *jurisdiction (4.37),* for reasons of efficiency, interoperability, ability to operate within multiple *jurisdictions*, ability to deploy rapidly, and maintenance, may elect to use one of the *regulated application services (4.46)* defined in this part of ISO 15638, to meet defined communications and data aspects of its requirement(s).

Regulated application services (4.46) require clear definition in terms of the requirements laid on the *service provider (4.50).* The responsibility to make such requirements clearly defined and make such requirements available to the *application service providers (4.7)* shall rest with the *jurisdiction (4.37).*

The service definition for each *application service (4.6)* supported by this part of ISO 15638 comprises

a) a clear description of the generic high-level service provided and its inputs, outputs, and results, including a given service level,

b) generic data, naming content, and quality that an *IVS (4.32)* has to deliver,

c) specific data, naming content, and quality for the provision of that particular service,

d) generic service elements definition,

e) *access methods (4.2)* to provision and retrieve data,

f) provisions for quality of service,

g) provisions for test requirements, and

h) provisions for (but not the detailed requirements and arrangements for) the *approval (4.10)* of *IVSs (4.32)* and s*ervice providers (4.50)*.

7 Requirements for services using generic vehicle data

7.1 General

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 (4.46),* and defines general requirements to ensure data interoperability.

7.1.1 Regulated application services using only generic *basic vehicle data*

Where all of the required data can be obtained through the access commands for generic *basic vehicle data (4.16)* specified in ISO 15638-5, the *access methods (4.2)*defined in ISO 15638-5 shall be used consistently to obtain the values for the *TARV LDT (4.39)* [and *C-ITS (4.22) LDT* data concepts where required]. No further international standardization is required; and *jurisdictions (4.37)*, subject to the privacy regulations pertaining within the *jurisdiction,* may develop, operate, and update their regulated or supported regulated voluntary services according to local design; international interoperability being maintained through the provisions of ISO 15638-5 (*TARV* generic vehicle information). All vehicles that are equipped to support ISO 15638 shall be able to support such service provision.

ISO 15638-5, Clause 7 defines the following relevant commands:

a) GETTARVLDT [*local data tree (4.39)*] data;

b) GETC-ITS *(4.22)* (co-operative vehicle systems) *LDT* data.

See ISO 15638-5 for details of these commands.

7.1.2 Regulated application services using both generic vehicle data and additional regulated application specific data

Where the *regulated application service (4.46)* requires both generic vehicle information *and* additional data, the generic vehicle information shall be through the access commands for generic vehicle information specified in ISO 15638-5. The *access methods (4.2)* defined in ISO 15638-5 for 'CREATE core data' and 'GET core data ' shall be used consistently, and additional data and *application service (4.6)* requirements shall be provided as specified in the general methods defined in Clause 8 of this part of ISO 15638, and a subsequent clause pertaining to the appropriate *application service specification (4.52)* provided in ISO 15638-8 to ISO 15638-19.

ISO 15638-5, Clause 8 defines the following relevant commands:

a) `CREATEcoredata`;

b) `GETcoredata`.

See ISO 15638-5 for detail of these commands.

See ISO 15638-5, Clause 8 for the generic sequence of operations for *regulated application services (4.46)* using generic vehicle data and unstandardized additional *regulated application (4.45)* specific data.

7.1.3 'Instigated' and 'Interrogated' data

Data are sent either because its collation, and send is 'instigated' by the app for the specific application service that is running in the IVS [for example, to defined time cycles, or on the occurrence of an event outside of defined limits (cargo temperature, an alarm etc.)]; or it is sent because an interrogating ITS-station has requested the data ('interrogated' data).

7.1.4 Get commands for specific TARV regulated application services

In respect of providing standardized specific data relating to a particular regulated application service (defined in ISO 15638-8 to ISO 15638-19) as the result of an interrogation, one common command shall be used to request application-specific data specified in any of the regulated application services defined in ISO 15638-8 to ISO 15638-19.

The command is

`GET` *`xxx`*

where `xxx` is a three or four character code uniquely identifying the application service data requested. The codes are shown in Table 1.

Table 1 — Unique 'GET' codes for specific application services defined in ISO 15638-8 to ISO 15638-19

ISO 15638	Local data tree (LDT)	`LDT`
ISO 15638	Core Application Data/`CoreData` (CD)	`CD`
ISO 15638-8	Vehicle access management and monitoring	`VAM`
ISO 15638-9	Remote electronic tachograph monitoring	`RTM`
ISO 15638-10	Emergency messaging system/eCall	`EMS`
ISO 15638-11	Driver work records	`DWR`

[a] To be published.

Table 1 *(continued)*

ISO 15638-12	Vehicle mass monitoring NOTE There are multiple ACKs used as defined in ISO 15638-12.	VMM VMMA VMMB VMMX
ISO 15638-13:—[a]	'Mass' information for jurisdictional control and enforcement	MRC
ISO 15638-14	Vehicle access control	VAC
ISO 15638-15	Vehicle location monitoring	VLM VLX
ISO 15638-16	Vehicle speed monitoring	VDSM VDSI VSMX
ISO 15638-17	Consignment and location monitoring	CLM CLX
ISO 15638-18	ADR (Dangerous Goods) monitoring	ADR
ISO 15638-19	Vehicle parking facilities	VPF

[a] To be published.

Where multiple possibilities exist, the explanation and definition of which to use is defined in the appropriate part of ISO 15638 for that regulated application service.

7.2 Conveyance identifiers

The *regulated vehicle (4.47) conveyance (4.21)* type shall be identified in accordance with ISO 26683-2/ISO 14816/ISO 17262/ISO 24534-3.

7.3 Consignment data

Any *regulated vehicle (4.47) consignment (4.19)* data shall be identified in accordance with ISO 26683-2/ISO 14816/ISO 17262/ISO 24534-3.

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

8.1 General

Regulated application services using only generic *basic vehicle data (7.1.1)* provided means, by which two of the access commands specified in ISO 15638-5, can be used to provide all of the data required in order to support a *regulated application service (4.46).*

Where the *regulated application service (4.46)* requires only *basic vehicle data (4.16)*, so long as the *access methods (4.2)*, defined in ISO 15638-5, are used consistently, no further international standardization is required, and *jurisdictions (4.37)* may develop, operate, and update their regulated, or supported voluntary services according to local design. International interoperability is being maintained through the provisions of ISO 15638-5.

However, a number of *regulated application services (4.46)* have been identified that require additional data in order to perform the *application service (4.6)* and where benefit has been identified for such additional data to be standardized. For detail of the reference to International Standards for these regulated application services, see Clause 10.

8.2 Concept of operations for identified regulated application services with additional data requirements

8.2.1 General

This Clause describes the characteristics of a proposed system from the viewpoint of a user *(4.55)* who will employ that system. Its objective is to communicate the quantitative and qualitative system characteristics to all stakeholders.

This Clause defines the general concept of operations for 'standardized' *regulated application services (4.46)* for *TARV*s that require data in addition to that available from the *basic vehicle data (4.16)*, and provides the generic modus operandi for the provision of the *application services (4.6)* defined in the subsequent clauses of this part of ISO 15638 that relate to provisions for specific *regulated application services*.

A 'concept of operations' (*CONOPS*) generally evolves from a concept and is a description of how a set of capabilities may be employed to achieve desired objectives. In ISO 15638, the concept of operations concerns the standardization of data concepts to be exchanged and the wireless means of the exchange of that data. To be clear, ISO 15638 does not specify the capabilities nor form of any product/system offering to the market, nor the form of the instantiation of the *application service (4.6)*. Those aspects are defined by the *jurisdiction (4.37)* and the *application service provider (4.7)*.

8.2.2 Statement of the goals and objectives of the system

The overall objective of *TARV regulated application services (4.46)* with additional data requirements, this part of ISO 15638, is the control of *regulated vehicle*s to meet the requirements of the *jurisdiction (4.37)* within its domain, using *telematics (4.54)*, in circumstances where data are required in addition to that provided by the *basic vehicle data (4.16)* data concept and where the additional data and its methods of transfer can be standardized.

The TARV architecture is based on a triumvirate relationship between the *jurisdiction (4.37)*, *user (4.55)*, and an *application service provider* (4.7). In TARV, it is assumed that most of the service provision is provided as a result of a contract between the service provider and a user (to meet the requirements of the *jurisdiction*).

In order to minimize the load on the limited capacity of the vehicle IVS [which may be supporting several *application services (4.6)* simultaneously, and may be also simultaneously supporting or providing other *C-ITS (4.22)* services], and in line with much current 'cloud' service provision thinking, the principal *application service* provision takes place between the *application service provider (4.7)* and the user and/or *jurisdiction (4.37)*, landside, 'somewhere in the cloud'. The shape and form of the *application service* is determined by the *application service provider (4.7)* and where and how 'in the cloud' the service is performed, is outside of the scope of ISO 15638. What is important is that, while data provisioning takes place on the *regulated vehicle (4.47)*, the actual *application service* is provided somewhere else. The function of the TARV specification to support a particular type of *application service* is to provide relevant data from the *regulated vehicle* to the *application service provider*, and in some circumstances, for the *regulated vehicle* IVS to receive data from the *application service provider* or other *ITS-stations (4.34)*.

Thus, TARV does not specify the *application service (4.6)* itself [enabling the differing requirements of different *jurisdictions (4.37)* to be met within the standard, and for different commercial offerings to provide market differentiation], but specifies, in a standardized form, the key generic data concepts required to enable the service provision and their transfer through a wireless communication to the *application service provider (4.7)*, and the provision of key data to the IVS of the *regulated vehicle (4.47)* from the *application service provider* or another *ITS-station (4.34)*, such as that of a *jurisdiction* or manager of a restricted zone.

It is an underlying concept (described in ISO 15638-1) that these services are provided by agreement with the *user (4.55)*, and using an approved *service provider (4.50)* to meet the requirements of the

jurisdiction (*4.37*) through *in-vehicle system* (*4.32*) (*IVS*) with communications capability between the *regulated vehicle* (*4.47*) and the *service provider*, and access to relevant data from the *regulated vehicle*.

It is an underlying assumption that the *regulated vehicle* (*4.47*) is equipped with the means to acquire and provide the data [additional to the '*basic vehicle data'* (*4.16*)], required by the specific *application service* (*4.6*). The generic requirements for additional data for the specified service is defined in the relevant clause below, defining the particular *application service* (defined in ISO 15638-8 to ISO 15638-19), as is the functional source of the means of such data provision. However, the actual equipment to be installed in order to provide that data provision functionality is not standardized and is a commercial decision of the *application service provider* (*4.7*), unless it is specified by the *jurisdiction* (*4.37*).

That is to say, that this part of ISO 15638 determines the nature of the data and how it is to be received/sent by the *IVS* (*4.32*), but does not standardize the equipment used to obtain the data.

EXAMPLE Refrigerated trailer temperature. The International Standard may define that the temperature was measured and transmitted to the *IVS* (*4.32*) either on demand or at prescribed intervals and reported to the *IVS* using a defined interface as degrees Celsius or Fahrenheit, and the degrees of precision of that temperature measurement. It would not specify the location nor type of thermometer, only the form and frequency in which the data are made available. However, it is possible that a *jurisdiction* (*4.37*) may additionally specify that the equipment of a particular type, or operates within some parameters that it has specified, but such *specification* (*4.52*) is outside the scope of this part of ISO 15638.

While this part of ISO 15638 determines the role of a 'approval authority' (*4.11*) function as part of the basic architecture, it is a basic tenet that the *jurisdiction* (*4.37*) has freedom to determine how its approval requirements are met, and, that function may be instantiated as an independent body, a department of the *jurisdiction*, or self-approval if the *jurisdiction* deems this to be appropriate.

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

Strategies, tactics, policies, and constraints, and indeed, the services that are regulated as mandatory or optionally supported, may vary from *jurisdiction* (*4.37*) to *jurisdiction.* Such definition is beyond the scope of this part of ISO 15638, which defines only the generic data and protocols to support a 'standard' *application service* (*4.6*), where such an *application service* is elected by a *jurisdiction* to meet their requirements.

A core strategy of this part of ISO 15638, and a central facet of its security, is to ensure that an *app* (*4.5*) is only loaded legitimately, and that this priorly loaded *app* contains a prior determined destination address where the *basic vehicle data* (*4.16*) or *core data* (*4.23*) is to be sent.

Instigating a 'GET*TARVLDT*' or 'GETCoreData' command therefore only results in that data being sent to the previously determined destination address, and not to a potentially spoof enquirer.

8.2.4 Organisations, activities, and interactions among participants and stakeholders

The classes, attributes, and key relationships are described in ISO 15638-1 and in Clause 6 of this part of ISO 15638.

8.2.5 Clear statement of responsibilities and authorities delegated

The responsibilities and authorities are described in ISO 15638-1 and application-specific aspects of the relevant specific *application service* (*4.6*) in ISO 15638-8, Clause 9 and 8.4.

8.2.6 User

The '*user* (*4.55*)' is most usually the *operator* (*4.43*) of the *regulated vehicle* (*4.47*), but in some cases, may be the *driver* (*4.25*). He shall enrol with the *jurisdiction* (*4.37*) to have his service provided automatically by wireless communications. He shall appoint an approved *service provider* (*4.50*) to provide the *regulated application service* (*4.46*) for the *regulated vehicle* [or *driver* (*4.25*) where appropriate].

It shall be the responsibility of the *operator (4.43)* of the *regulated vehicle (4.47)* to enrol and to have his vehicle equipped, to enable it to provide the service [regardless of whether the *user (4.55)* of the service is the *regulated vehicle (4.47) operator (4.43)* or the *driver (4.25)* of the *regulated vehicle (4.47)*]. So long as he uses approved service providers, *IVS installers (4.35)*, and *IVS maintainers (4.36)*, the *operator (4.43)* may then assume that the *application service (4.6)* shall be provided in accordance with the legislation/regulations.

The *user (4.55)* shall be responsible to pay any fees for the provision of the service agreed with the *service provider (4.50)* to the *service provider*. The means by which this is achieved is a subject for the commercial marketplace and is outside the scope of this part of ISO 15638.

8.2.7 Application service provider

In the case of the standardized *application services (4.6)* defined below (defined in ISO 15638-8 to ISO 15638-19), the *application service provider (4.7)* shall offer to *users (4.55)* to provide the specific *application service* to the requirements of a *jurisdiction (4.37)*, using the TARV standardized data concepts and data exchanges with the *regulated vehicle (4.47)* defined herein (one of defined in ISO 15638-8 to ISO 15638-19).

8.2.8 Application service

This shall be a service defined in one standardized *application services (4.6)* defined below (defined in ISO 15638-8 to ISO 15638-19) and provided by the *application service provider (4.7)* to the *jurisdiction (4.37)* to meet the requirements of the *jurisdiction.*

8.2.9 Operational processes for the system

The operational processes for the exchange of data over a wireless medium are described at a generic level in 8.3 [Sequence of operations for identified regulated *application services (4.6)* with additional data requirements], in Clause 9 (Common features of regulated TARV services), and at an *application service* specific level in the clause (defined in ISO 15638-8 to ISO 15638-19 below) defining the communication and data requirements at a generic level for the particular 'standard' *application service.*

8.2.10 Service requirements definition

A *jurisdiction (4.37)* passes legislation/regulation to require, or support, the provision of a particular *application service (4.6)* using wireless media. The legislation/regulation may require that an *application service* is provided in accordance with one of the standardized *regulated application services (4.46)* defined below (defined in ISO 15638-8 to ISO 15638-19). Doing it significantly improves the probability that a *TARV* equipped vehicle will be able to support the *application service.* This is particularly important when *regulated vehicle*s from a different *jurisdiction* are operating within the territory of a *jurisdiction.*

8.3 Sequence of operations for identified regulated application services with additional data requirements

8.3.1 Framework for operations

The security requirements are such that a common and secure provision for security needs to be provided on all *cooperative ITS (4.22)* systems in order to both maintain security and offer interoperability, common use and reuse of data. These aspects are dealt with in ISO 15638-4:—[5] and all instantiations claiming compliance with this part of ISO 15638 shall also comply with ISO 15638-4:—[3] (*TARV* system security requirements).

ISO 15638-5 provides the *specifications (4.52)* for generic *basic vehicle data (4.16)* that it is required for all *TARV IVSs (4.32)* to support and make available to *application service providers (4.7)* through a wireless

5) To be published.

communications link supported by the *IVS (4.32)*, in order to support the provision of regulated and commercial *application services (4.6)*.

Some further data concepts, while not required in all cases for every *TARV* in every *jurisdiction (4.37)*, may be required generically for all equipment within a particular *jurisdiction,* or class of *TARV* within a *jurisdiction,* in order for the *jurisdiction* to achieve its regulation of *TARV*s and provide the *regulated application services (4.46)*, defined in ISO 15638-8 to ISO 15638-19.

The combination of *basic vehicle data (4.16)* and those additional data concepts required within a particular *jurisdiction (4.37)* (or class of *TARVS)* are known as *core application data (4.23)* for an *application service (4.6)* within a particular *jurisdiction. Basic vehicle data* shall therefore be found in all equipped *TARV*s, while *core application data* may be required in all equipped *TARV*s (or class of *TARVS*) within a particular *jurisdiction.*

Equipped vehicles operating internationally shall need to carry all of the additional data concepts required by all of the *jurisdictions (4.37)* within which they operate, in order to determine their *core application data (4.23)*. By providing standard definitions for these commonly expected additional data concepts, this will be easy to achieve and provide international interoperability.

The *ROAM (4.48)* (Regime for Open Application Management) *architecture (4.12),* defined in ISO 15638-1, provides the *framework (4.30)* and operational environment for developing and deploying platforms for *TARV* applications within a general *framework (4.30)* of cooperative vehicle *telematics (4.54)* systems, and is designed not only to support *TARV* application systems (defined herein), but also to support other commercial and safety cooperative systems for commercial vehicles beyond the scope of the *TARV regulated applications (4.45)* (See ISO 15638-7), and general C-ITS systems for all classes of vehicles. It is therefore designed to be compatible and interoperable with other C-ITS standards, and has used the successful results of research programmes and applications in these areas as is source of inspiration.

ROAM (4.48) provides an open execution environment in which *TARV* applications can be developed, delivered, implemented and maintained during the life cycle of both service applications and equipment. *Drivers (4.25)* and fleet *operators (4.43)* shall be able to rely on their integrated *in-vehicle system (4.32)* to allow *TARV*s to operate within the requirements of *jurisdictions (4.37)* within which they drive their vehicles, and gain advantages from direct co-operative management of transport safety and efficiency wherever they drive.

Within the *TARV* environment, *regulated applications (4.45)* are developed by *jurisdictions (4.37)* and deployed by *application service providers (4.7)* to '*Host management centres (4.31)*' (*HMC*). The *host management centre* provides a service gateway that supervises the secure provision of software and services *TARV*s. *HMC*s manage the provisioning of applications to any authorized and subscribed *user (4.55)* through its client system. After it is properly provisioned and installed on the client system, it can enact the application. Mechanisms for flexible software deployment and management are provided by Java/OSGi™ (open services gateway initiative). See ISO 15638-1, 6.1.3.

8.3.2 ROAM 'App' library and data pantry

A layer below these applications is the provision of data for the *data pantry (4.24)*. This data provisioning is not generated by a single application, but by a number of small task specific 'Facilities *Apps*', which are generally small Java™ applets [*apps (4.5)*], organized as software bundles, that generally busy themselves keeping the *data pantry (4.24)* provisioned with up to date data. This data provisioning is envisaged to be carried out by the 'Facilities *Apps*', each of which shall service the updating of individual data elements in the *basic vehicle data (4.16)* concept, and for the *core application data (4.23)* concept where a *jurisdiction (4.37)*/application service *(4.6)* has specified or provided an *app* to do this. The process is defined in ISO 15638-1,*(4.12*).

A key feature of this 'layering' is the principal that a particular layer can only communicate with the adjacent layer immediately above or below it or to its side. The communication infrastructure is therefore hidden from the application by the middleware, and the 'apps' are separated from the resultant data.

It is crucial also that the *data pantry (4.24)* contains just end data. The *data pantry (4.24)* is accessible to an *app (4.5),* so long as it has authorization, but the software *app (4.5)* that generated the data are not available to the *app (4.5)* during an online *session (4.51)*.

This data are calculated by *apps (4.5),* placed by the *application service provider (4.7)* in the on-board data library, and stored as discrete data concept values in the on-board '*data pantry (4.24)*'. The frequency of such updates is determined by the *app.* ISO 15638-5 defines that additional *apps* in the library collate the data into data concepts containing collated data element values, stored as discrete files in the *data pantry (4.24)*. The processes are illustrated in Figure 2.

Figure 2 shows apps being uploaded into the *app library (4.8)*, and the execution environment running the *apps (4.5)* and updating the data concept values in the *data pantry (4.24)*. It shows the *LDT (4.39)* values being updated to the instructions of the appropriate *app*. It then shows a *jurisdiction (4.37)/ application service (4.6)* uploading an *app* [which it does through the *application service provider (4.7)* or *prime service provider (4.44)*] for its *core data (4.23)*, which then demands that the *core data* concept values be updated. This is done. The *jurisdiction* then requests the *core data* values which are supplied.

An example of an *app (4.5)* demanding the *TARV LDT (4.39)* is then shown, with the *app* in the execution environment stimulating a refresh of the *TARV LDT* values, updating the file in the *data pantry (4.24)* and then supplying them to the *application service provider (4.7)* through the wireless interface.

Finally, the example of a safety *app (4.5)* requesting the *C-ITS (4.22)* (cooperative vehicle systems) *LDT* is shown, it is not relevant within this part of ISO 15638, other than to show how this can also be achieved with a similar mechanism.

The overall sequence of service provision for all of the specified standardized *application services (4.6)*, defined in ISO 15638-8 to ISO 15638-19, is similar, and is conformant to the process defined in ISO 15638-1, Clause 12.

All *application services (4.6)*, defined in ISO 15638-8 to ISO 15638-19, of this part of ISO 15638 shall operate in the *CALM-ROAM* environment as specified in ISO 15638-1.

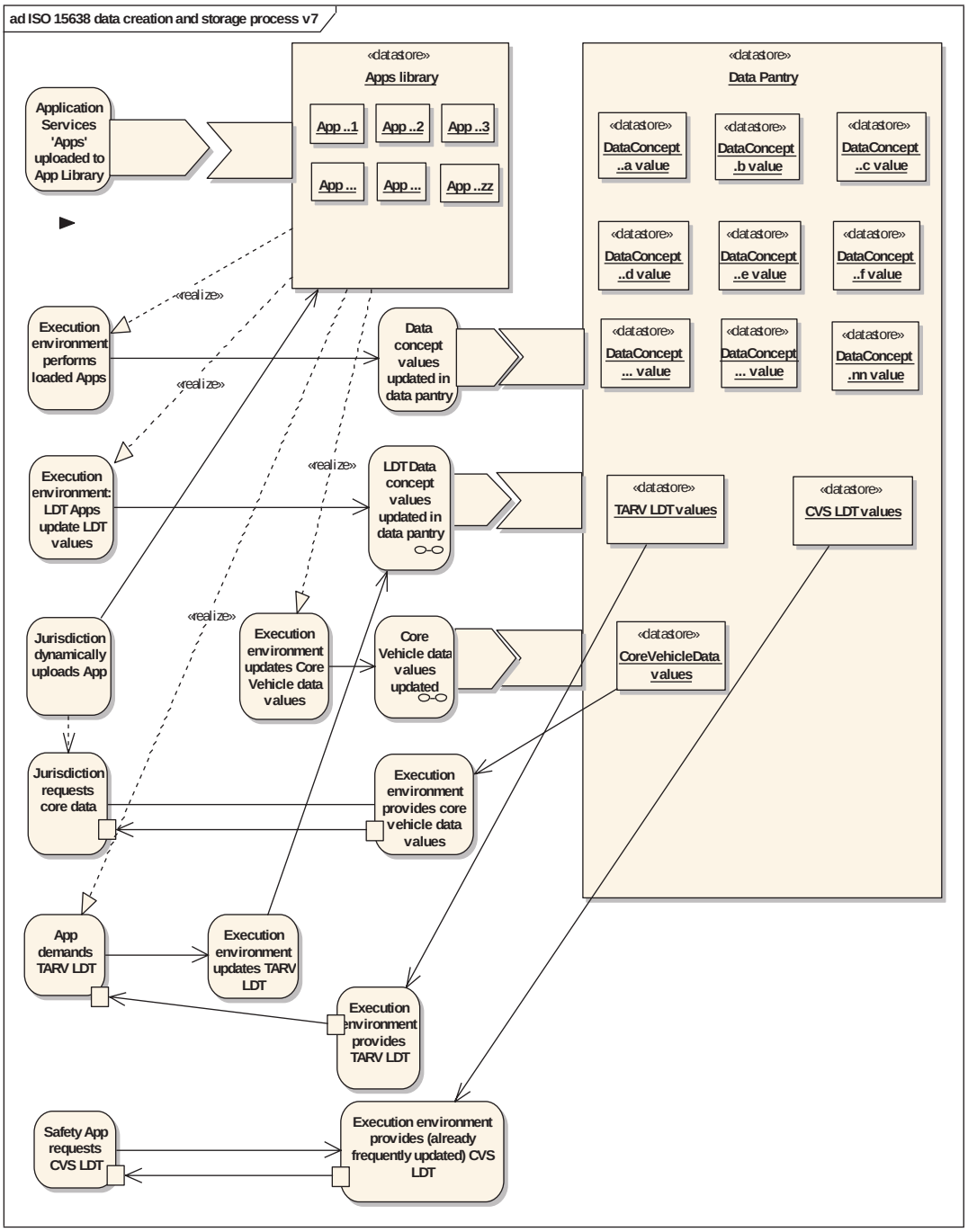


Figure 2 — The ISO 15638 data creation and storage process
(Source: **ISO 15638-5**)

Figure 3 shows the generic environment in which standardized *application services (4.6)* are provided.

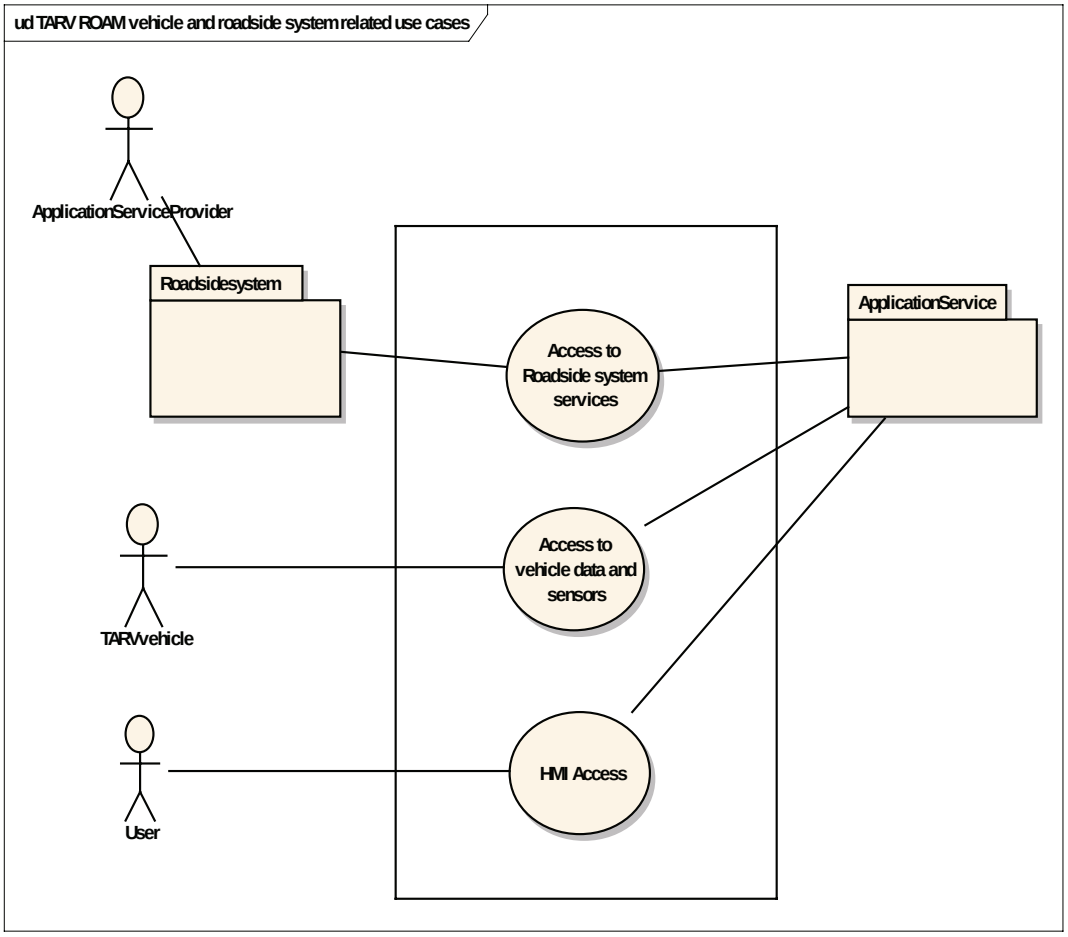


Figure 3 — TARV-ROAM vehicle and roadside system related use cases
(Source: **ISO 15638-1**)

8.3.3 Concurrent multiple 'apps' and 'core data'

It is important to understand that, whereas *basic vehicle data (4.16)* [*TARV LDT (4.39)* always provides current values for the same data concept, *core data (4.23)* is a transient data concept. It is created by an *app (4.5)* at a point in time, and its content is the content determined by that *app* (subject to the constraints of ISO 15638, various parts and this part of ISO 15638]. Although separate commands, the '`CREATE core data`' and '`GETcoredata`' commands are used together in sequence. The first populates the transient *core data (4.23)* data concept with values, the second sends those values to a previously determined address.

In this manner, this single command services multiple applications that are concurrent in the 'apps' library in a way that simplifies the application system and *app (4.5)*, and makes efficient use of the limited memory of the *IVS (4.32)*, (i.e. the single command and file can service multiple 'apps', even if running concurrently).

NOTE In the event that a *service provider (4.50)* issues a '`GETcoredata`' command without preceding it with a `CREATEcoredata`' command, this would only result in the current values of the *core data (4.23)* data concept being sent to their legitimate predetermined IPv6 address, and not to the instigator of the '`GETcoredata`' command.

8.3.4 General sequence of operations

The first step in all *regulated application service (4.46)* provision is that the *jurisdiction (4.37)* shall instruct an *application service provider (4.7)* to provide the *regulated application service (4.46)*. This may be the *application service provider* appointed by the *jurisdiction* (in some cases may even be a functional arm of

the *jurisdiction*) or it may be an *application service provider (4.7)* contracted to the *user (4.55)* to meet the requirements of the *jurisdictions* within/through which the *user (4.55)* is operating the *regulated vehicle (4.47)*.

The '*regulated application service (4.46)*' is a software application system comprising two parts.

a) 'landside' application software system;

b) on-board *app (4.5)* to generate the *core data (4.23)* for the system.

The landside application software system that provides the *regulated application service (4.46)* may, at the election of the *jurisdiction (4.37)*, either be provided by the *jurisdiction* to *application service providers (4.7)*, or the *jurisdiction* may provide its requirements and allow the *application service provider* to develop the software; but shall use one of these two approaches.

The on-board *app (4.5)* may, at the election of the *jurisdiction (4.37)*, either be provided by the *jurisdiction* to *application service providers (4.7)*, or the *jurisdiction* may provide its requirements and allow the *application service provider* to develop the software, but shall use one of these two approaches.

In the event that the *jurisdiction (4.37)* provides the *app (4.5)*, it has two ways to provision the on-board data library with the *app.* It can provide the *app* to the *application service provider (4.7)*, and it is then the responsibility of the *application service provider to* load it onto the *IVS (4.32)* of the *regulated vehicle (4.47)*, or, using *TARV-ROAM,* it can dynamically request the *application service provider* to upload the app directly to the *regulated vehicle (4.47)* as it enters the *jurisdiction.*

In domestic situations, the *jurisdiction (4.37)* may prefer to have the *application service provider (4.7)* install the *app (4.5)* to the *regulated vehicle (4.47)*, however, where a vehicle is roaming through different *jurisdictions*, the *jurisdiction* will probably want to dynamically request the *application service provider* to upload the *app* to the *regulated vehicle (4.47)* as it enters the *jurisdiction* and act as the *application service provider,* or have an agent it appoints do so on its behalf, while the *regulated vehicle (4.47)* remains within its domain.

This is possible because of *TARV-ROAM,* and is secure because the *application service (4.6)* only has access to the values in the *data pantry (4.24)* of the *IVS (4.32)* which it is authorized to access, and does not have access to other *apps (4.5)* or equipment or data in the *regulated vehicle (4.47)*.

Figure 4 shows the routes that the *application service (4.6)* software is provided to the *application service provider (4.7),* and the two routes that the *app (4.5)* can be provisioned in the *app* library of the *IVS (4.32)*. See ISO 15638-1, Clause 12 for further detail.

NOTE In Figure 4, the abbreviation *RAS* stands for '*regulated application service (4.46)*'.

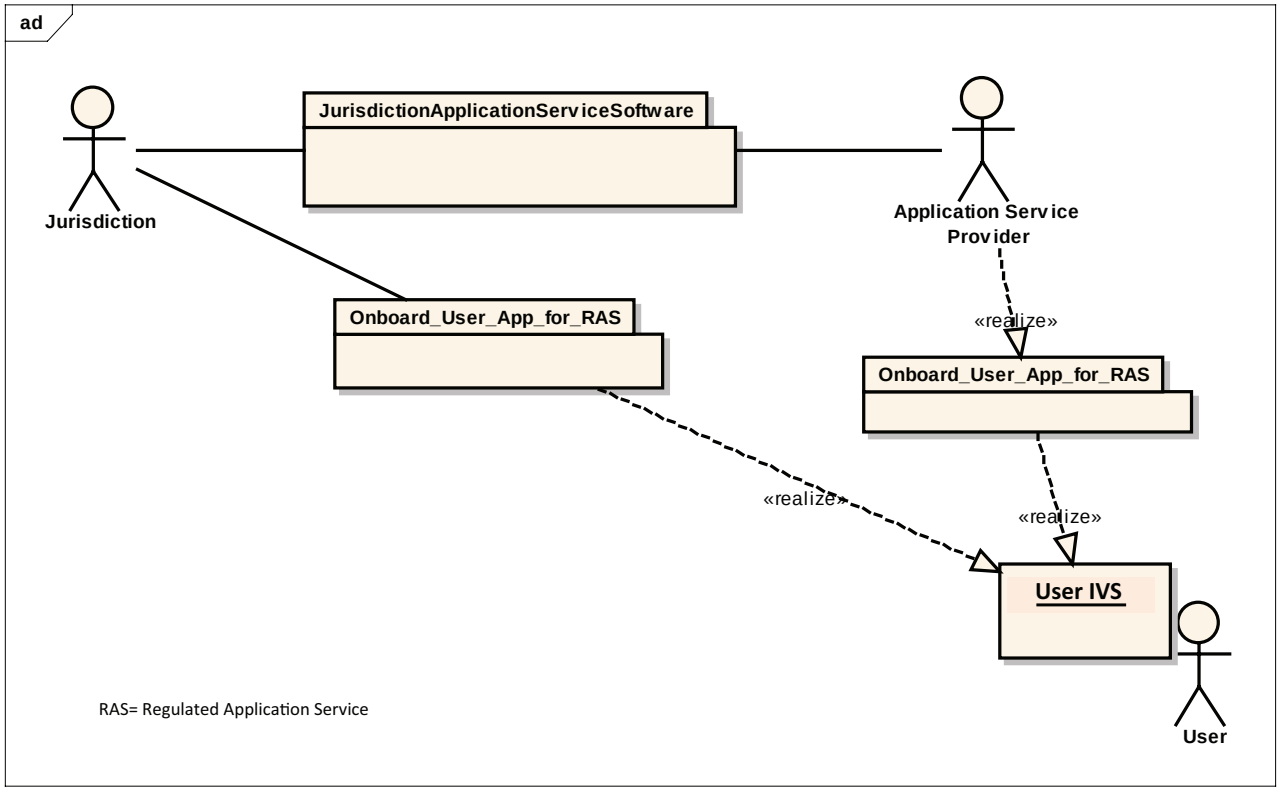


Figure 4 — Provisioning the 'app' into the IVS

The first stage shown in Figure 5 also represents this process as the first step in the sequence of operations.

8.3.4.1 Commands

Providing a regulated *TARV* service is envisaged as one or a series of short transactions, in which, in order to obtain *basic vehicle data (4.16)* or *core application data (4.23)*, one or two (of four) commands is invoked.

— `GETTARVLDT data`

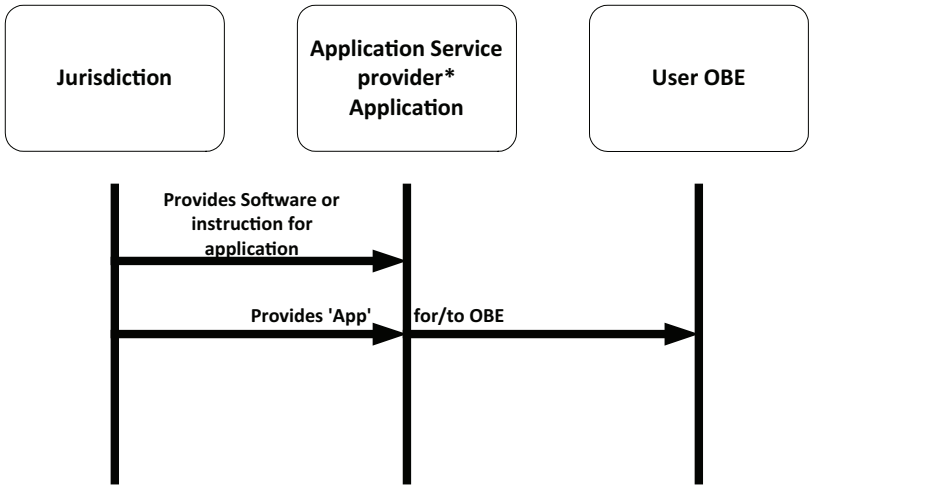
— `CREATE core data`

— `GET core data`

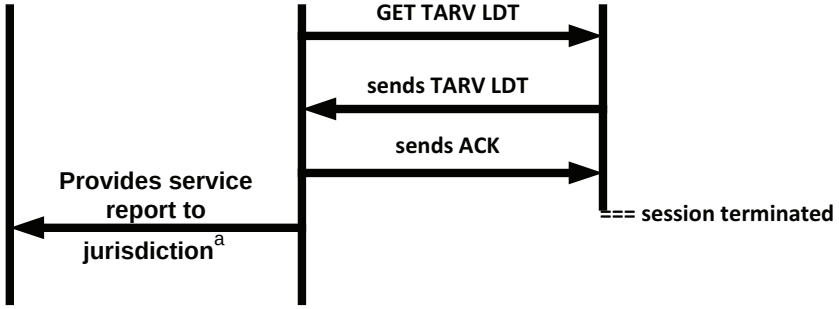
— `GET xxx` (where xxx is an option defined in 7.1)

The objective is to invoke the shortest possible link with the vehicle to obtain the required data, and then close the communication. If data are required at several geographical points or several points in time, this comprises a series of short *sessions (4.51)* [and where required by the *regulated application (4.45)*, further detail of generic data specification for identified *regulated application services (4.46)* is provided in ISO 15638-8 to ISO 15638-19, which may, or may not, require *basic vehicle data (4.16)* or *core application data (4.23)* as part of that service provision].

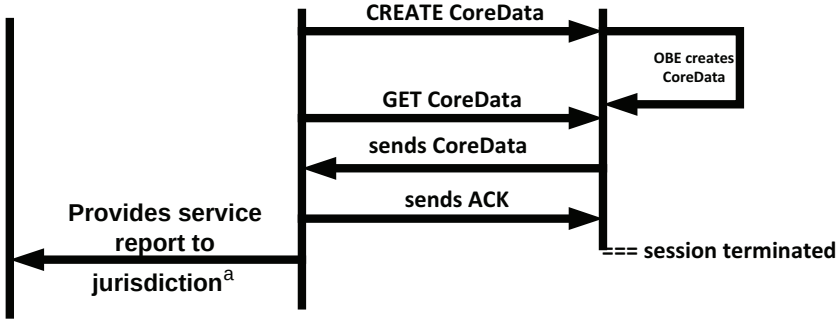
Figure 5 shows the high level conceptual sequence of operations.



Where only Essential vehicle data (TARV LDT) is required



Where Core vehicle data (LDT + application specific data) is required



a In some instantiations, the *application service provider (4.7)* will be the *jurisdiction (4.37)* or its agent.

Figure 5 — Sequences to obtain *TARV LDT* and CoreData

Building the *application service (4.6)* results, and providing required information to *jurisdictions (4.37)*, is architecturally conceived as a process that is performed by the *application service (4.6)* software and hosted in the landside system of the *application service provider (4.7),* and is not transacted while the communication with the *regulated vehicle (4.47)* is in progress, nor is the service directly provided by the *IVS (4.32)*, except for the transaction 'CREATE' to update the on-board *data pantry (4.24)*, or to 'GET' the data.

If further data are subsequently required, or the data obtained is in any way deficient, this is solved by a subsequent communication *session (4.51)* wih the *regulated vehicle (4.47)*.

All further data processing of the application service is effected by the *application service provider (4.7)*, landside, using the application provider application service software, not on-board by the *IVS (4.32)* (and therefore outside the scope of ISO 15638).

This is designed to minimize the duty on the wireless interface (and with several wireless media charging models, also to minimize its cost), and to maximize on-board security.

The resulting communications sequence is therefore, in realization, more staccato, as shown in Figures 6 and 7.

8.3.4.2 GET TARV LDT

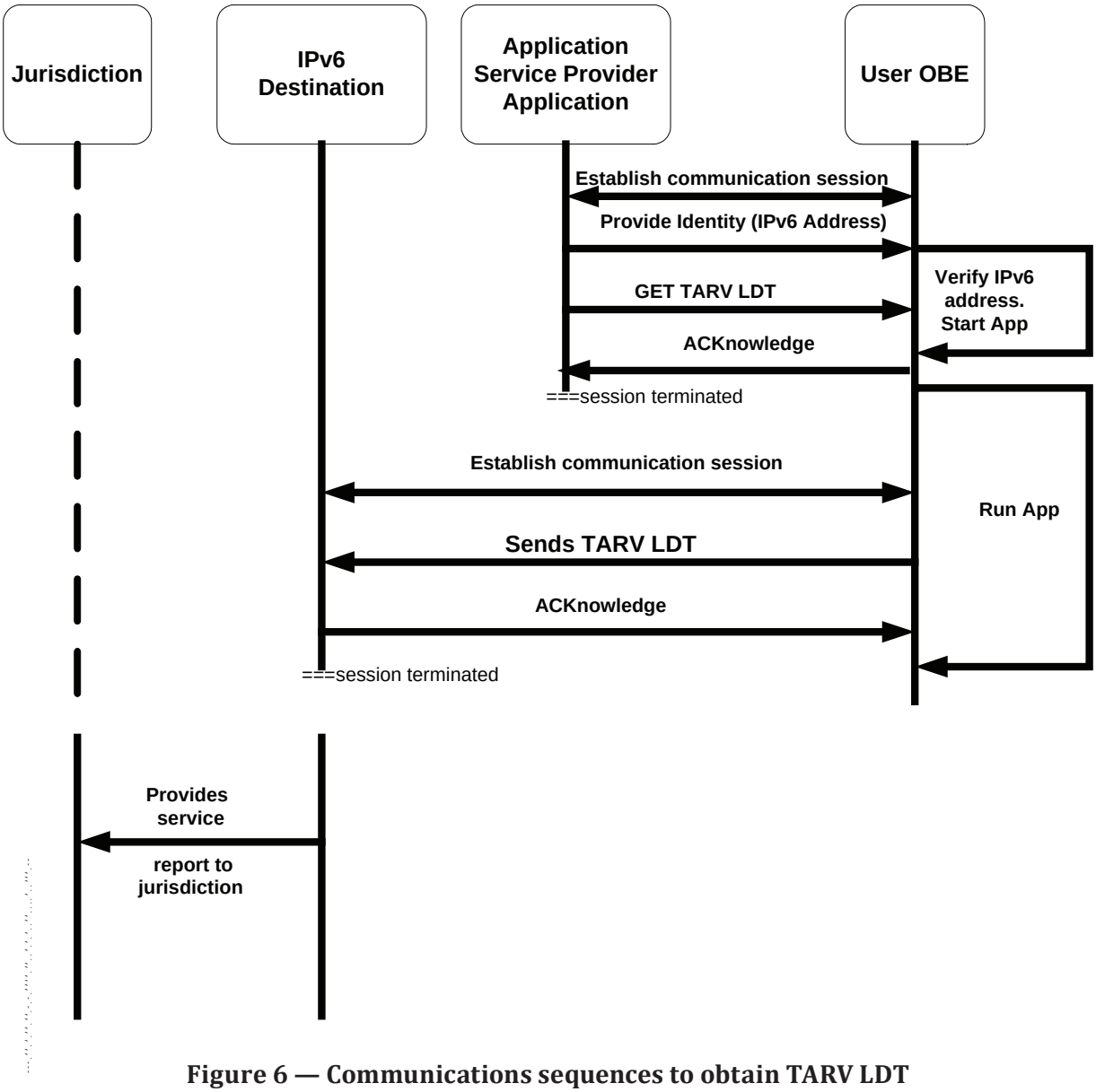


Figure 6 — Communications sequences to obtain TARV LDT

If only the *basic vehicle data (4.16)* is required, the application operating system shall simply establish the communication link in accordance with ISO 15638-2, and shall issue the command 'GETTARVLDT *(4.39)* data' in accordance with ISO 15638-5. The *IVS (4.32)* sends an acknowledgement (see 8.3.5) that the command has been received and the *session (4.51)* is closed. The *IVS* then sends the *TARV LDT* to the predetermined IPv6 address. The receiving IPv6 address sends an ACKnowledgement <LDX>. Once

the *IVS (4.32)* receives the ACKnowledgement) <LDX>, that *TARV LDT* is successfully received by the destination address, the *session (4.51)* shall be closed. (See Figure 6 and Table 3).

8.3.4.3 CREATE and GET CoreData

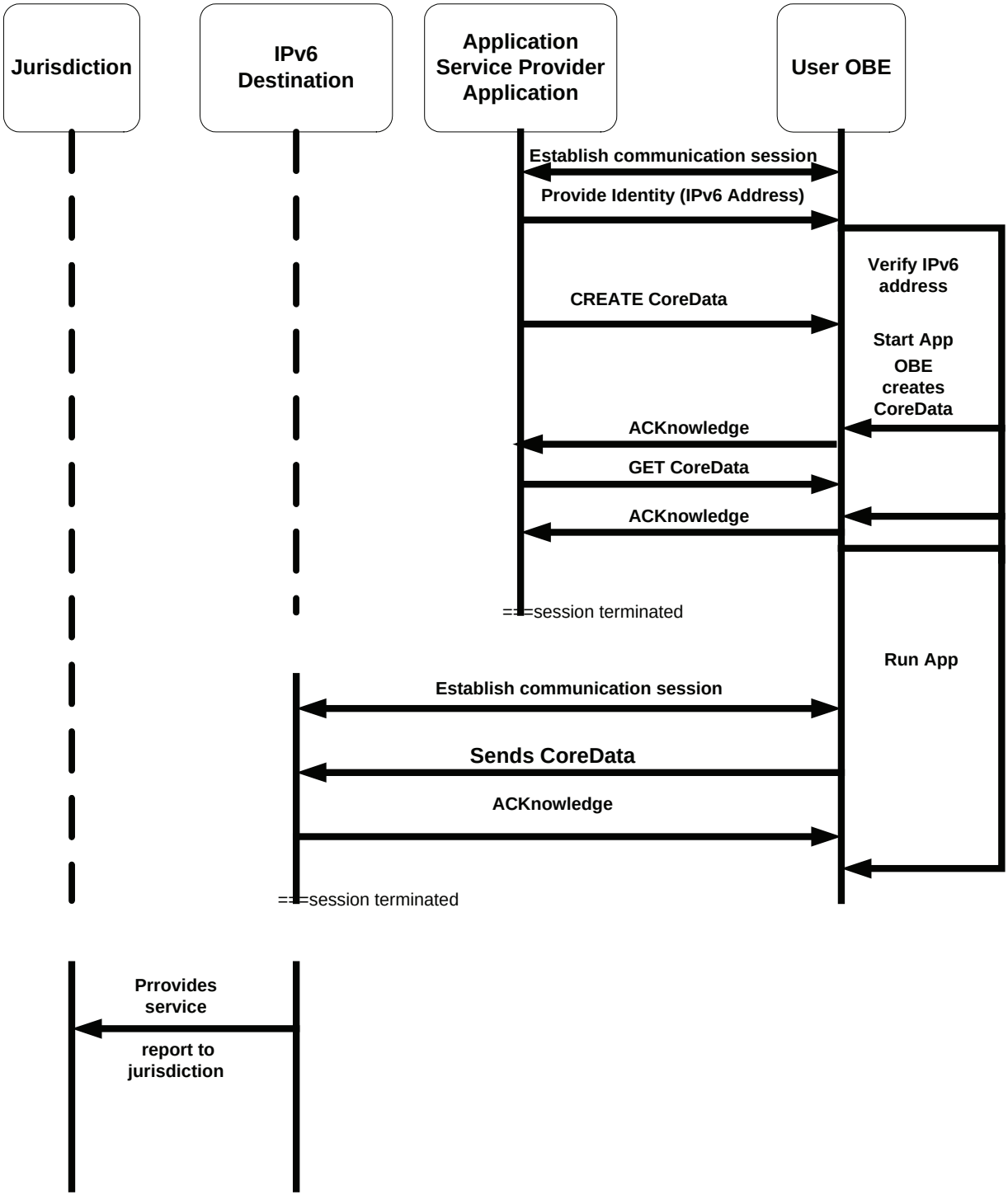


Figure 7 — Communications sequences to obtain CoreData

Most of the *application services (4.6),* defined in this part of ISO 15638, require data in addition to the *basic vehicle data (4.16)*, and therefore, before the data can be obtained, the *data pantry (4.24)* has to be updated. Figure 8 shows a hypothetical example of `CoreData`.

NOTE In the *TARV-ROAM architecture (4.12),* the application system has no direct access to the source of data, only data in the *data pantry (4.24)* that it is authorized to access.

In this event, the application operating system shall establish the communication link in accordance with ISO 15638-2), and shall issue the command '`CREATE core data`', The *IVS (4.32)* then populates the `CoreData` data concept with data as instructed by the on-board *app (4.5)* associated with the *app*. The *IVS* sends an acknowledgement `<D>` (see 8.3.5) that the command has been received and the *session (4.51)* is closed.

The *IVS (4.32)* then sends the `CoreData` to the predetermined IPv6 address contained in the content of the `CoreData`. The receiving IPv6 address sends an ACKnowledgement `<CDX>` (see 8.3.5).

NOTE *Core data (4.23)* includes the *TARV LDT (4.39)* data.

Once the *IVS (4.32)* receives an acknowledgement (ACK) `<CDX>` that the '`CoreData`' has been successfully received by the enquirer, the *session (4.51)* shall be closed. (See Figure 7). An example of the construct of '`core data` *(4.23)*' is provided in Figure 8.

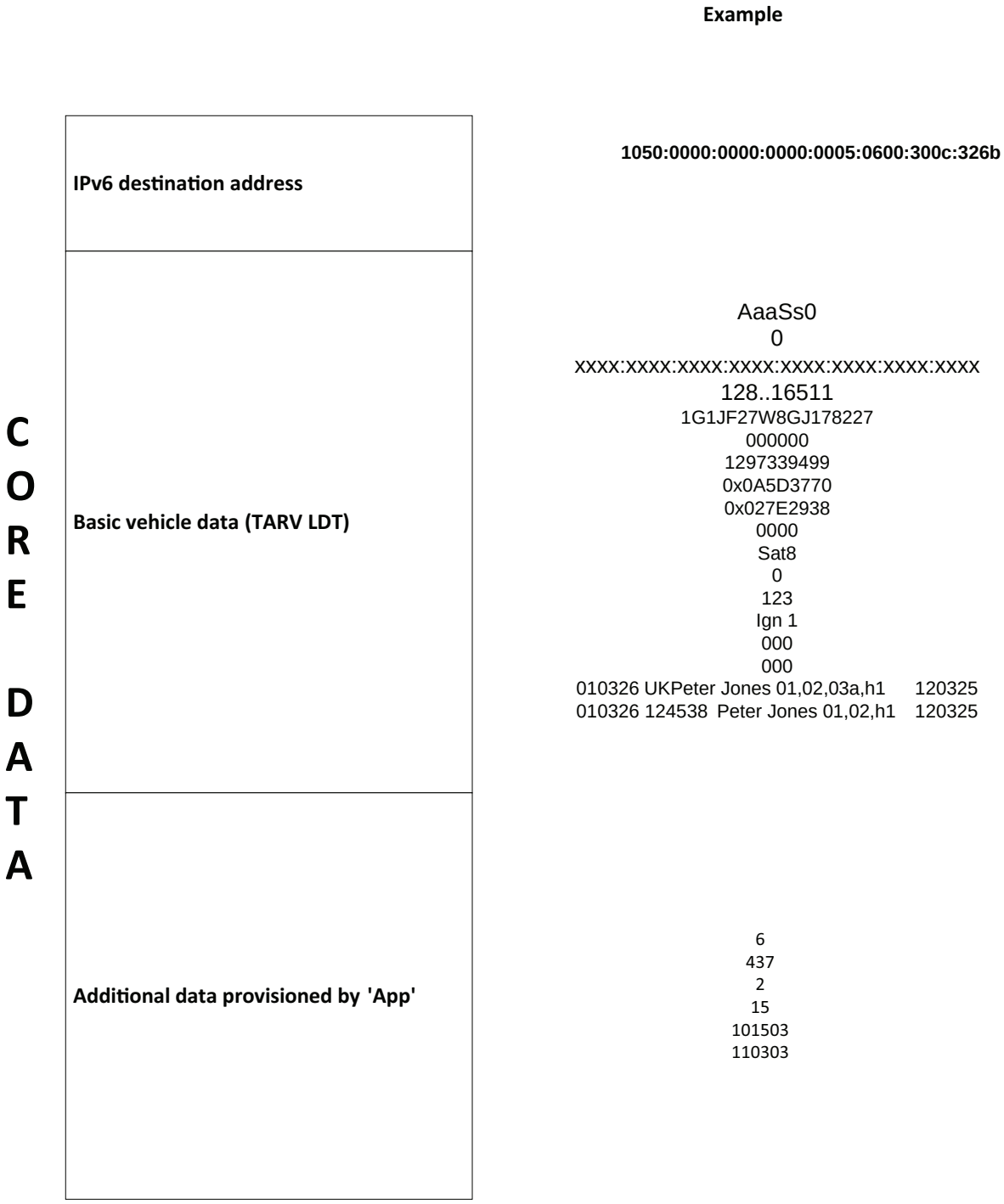


Figure 8 — Core application data example

8.3.5 ACKnowledgements

ACKnowledgements (ACK) are made at the application level and are additional to any ACKs passed at the media communication level. ACKs are unique to enable the recipient to confirm that the correct action has been taken by the IVS.

There are two types of ACKnowledgement.

a) Acknowledgement (by the IVS) that a request for data has been received. These shall be as defined in Table 2.

The acknowledgement is unique to the application service data being requested, confirming to the interrogator that its request for a specific set of data are acknowledged, and that, the correct action has been taken by the IVS.

b) Acknowledgement (from the receiving IPv6 address) that the data has been received. These shall be as defined in Table 3.

The acknowledgement is unique to the application service data being requested, confirming to the interrogator that its request for a specific set of data are acknowledged, and that, the correct action has been taken by the IVS.

Table 2 — Acknowledgement by the IVS (to Interrogator) that a request for information has been received

ISO 15638	Local data tree (LDT)	L
ISO 15638	Core Application Data/`CoreData` (CD)	D
ISO 15638-8	Vehicle access management and monitoring	A
ISO 15638-9	Remote electronic tachograph monitoring	T
ISO 15638-10	Emergency messaging system/eCall	E
ISO 15638-11	Driver work records	W
ISO 15638-12	Vehicle mass monitoring	M
ISO 15638-13:—[a]	'Mass' information for jurisdictional control and enforcement	R
ISO 15638-14	Vehicle access control	L or D
ISO 15638-15	Vehicle location monitoring	X
ISO 15638-16	Vehicle speed monitoring	S
ISO 15638-17	Consignment and location monitoring	C
ISO 15638-18	ADR (Dangerous Goods) monitoring	Y
ISO 15638-19	Vehicle parking facilities	P

[a] To be published.

Table 3 — Acknowledgement by the receiving IPv6 destination that a datafile has been received

ISO 15638	Local data tree (LDT)	LDX
ISO 15638	Core Application Data/`CoreData` (CD)	CDX
ISO 15638-8	Vehicle access management and monitoring	VAX
ISO 15638-9	Remote electronic tachograph monitoring	RTX
ISO 15638-10	Emergency messaging system/eCall	EMX
ISO 15638-11	Driver work records	DWX
ISO 15638-12	Vehicle mass monitoring NOTE: there are multiple ACKs used as defined in ISO 15638-12)	VMX MAX MBX MXX
ISO 15638-13:—[a]	'Mass' information for jurisdictional control and enforcement	MRX
ISO 15638-14	Vehicle access control	VCX

[a] To be published.

Table 3 *(continued)*

ISO 15638-15	Vehicle location monitoring	VLX LXX
ISO 15638-16	Vehicle speed monitoring	VSX VDX SMX
ISO 15638-17	Consignment and location monitoring	CLX CXX
ISO 15638-18	ADR (Dangerous Goods) monitoring	ADX
ISO 15638-19	Vehicle parking facilities	VPX

[a] To be published.

NOTE These ACK codes mirror the 'GET' codes defined in 7.1.1.

If a new application service is defined in a new part of ISO 15638, not covered in the above tables in this subclause, that new part of ISO 15638 shall specify a unique one letter ACK for acknowledgement by the IVS (to Interrogator) that a request for information has been received, and shall specify a unique three letter ACK for acknowledgement by the receiving IPv6 destination that a data file has been received.

8.3.6 Application specific sequences of operations

A sequence of operations is provided for each of the *regulated application service (4.46) specifications (4.52)* in parts of ISO 15638, referenced in Clause10.

8.4 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 (4.37)* as part of its *specification (4.52)* for any particular *regulated application service (4.46).* However, where a specified *regulated application service (4.46)* has specific Q of S requirements essential to maintain interoperability, these aspects shall be defined in the specific part of ISO 15638 (ISO 15638-8 to ISO 15638-19) relating to that *regulated application service.*

8.5 Test requirements

This part of ISO 15638 contains no general requirements concerning test requirements. Such aspects shall be determined by a *jurisdiction (4.37)* as part of its regulation for any particular *regulated application service (4.46),* and issued as a formal test requirements *specification (4.52)* document. However, where a specified *regulated application service (4.46)* has specific test requirements essential to maintain interoperability, these aspects shall be specified in the specific part of ISO 15638 (ISO 15638-8 to ISO 15638-19) relating to that *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.

8.6 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 (4.37)* 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

9.2 Generic operational processes for the system

The details of the instantiation of *regulated application service (4.46)* are as designed by the application service system to meet the requirements of a particular *jurisdiction (4.37)* and are not defined herein. This part of ISO 15638 specifies the generic roles and responsibilities of actors in the systems, and the interoperability of key operational steps and actions required to support all *TARV regulated application service* systems, and this Clause addresses the generic provision of *regulated application services* that require data in addition to, or instead of, *basic vehicle data (4.16)* and *core application data (4.23)*, and specifies the generic form and content of such data required to support such systems, and *access methods (4.2)* to that data. Clause 10 references relevant parts of ISO 15638 where particular data and data exchange requirements for specific identified regulated service provision are further defined.

It shall not be possible for collected or stored *regulated application service (4.46)* data in any software or non-volatile memory within the application service system to be accessible or capable of being manipulated by any person, device or system (including through any self-declaration device), other than that authorized by the *application service provider (4.7).*

The means by which data are provisioned into the *data pantry (4.24)*, and the means to obtain the *TARV LDT (4.39)* and *core data (4.23)* are described in Clause 8.

Specific *regulated application services (4.46)* (referenced parts of ISO 15638 defined in Clause 10), shall collect and transfer application specific data. Sometimes, this shall be or shall include the *TARV LDT (4.39)* or *core data (4.23)*, in many cases additional application specific data will be required. This data are defined in the specific *regulated application services* (referenced parts of ISO 15638 defined in Clause 10).

Different *application services (4.6)* may require connection to different application-specific equipment, for example, a *tachograph (4.53)*, or some form of driving licence reading equipment. However, there are common basic processes behind *TARV regulated application services (4.46)*.

In order to minimize demand on the *IVS (4.32)* (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 (4.46)*.

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 (4.7) (ASP),* pass that data to the *ASP.* All of the actual application service processing shall occur in the mainframe system of the *ASP* (in the 'cloud').

At a conceptual level, the *TARV* system is therefore essentially simple, as shown in Figure 9. The process is similar to that for `CoreData`, but data are supplied to a different on-board file in the *data pantry (4.24)*.

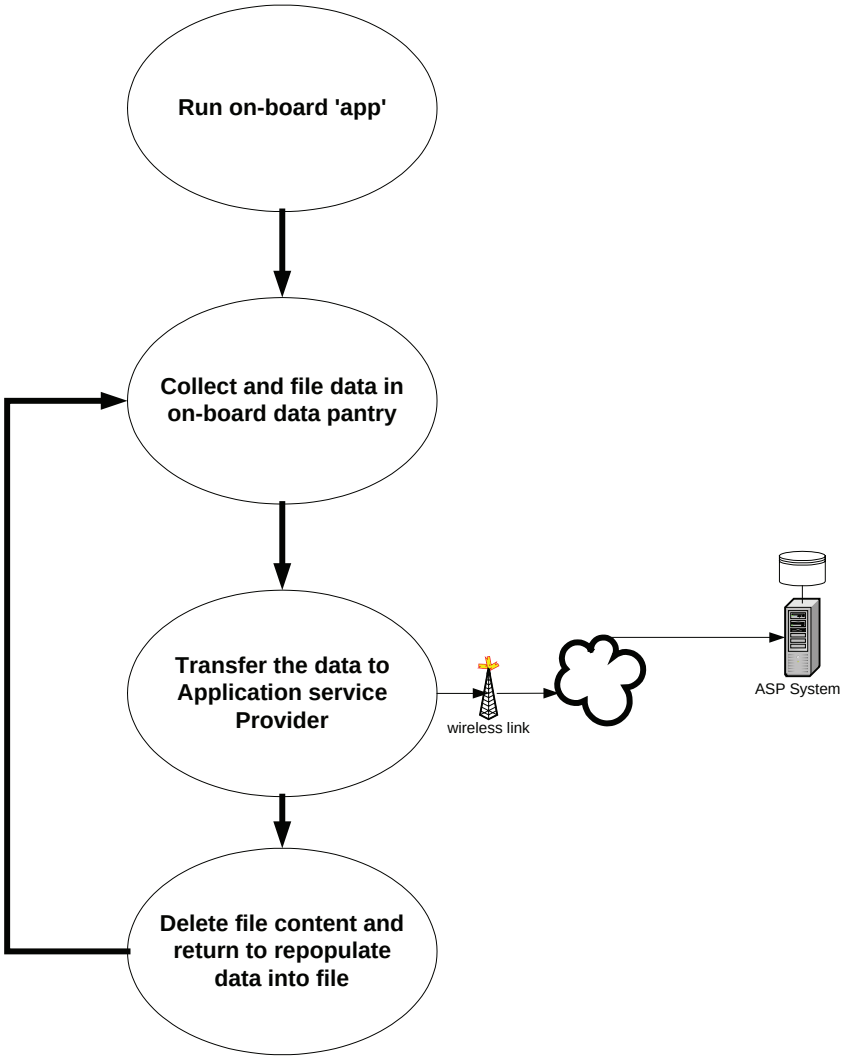


Figure 9 — TARV regulated application service on-board procedure

At a common generic functional level, the process may be seen as shown in Figure 10 below, however, the connected equipment may/may not be required in all cases.

9.3 Common role of the jurisdiction

9.3.1 General

In this environment of specified *regulated application services (4.46)*, the *jurisdiction (4.37)* provides the role of developing the laws and enforcement as determined by the *jurisdiction.*

9.3.2 Common role of the 'agent of the jurisdiction'

An agent of the *jurisdiction (4.37)* is a party appointed by the *jurisdiction* to be responsible for providing one of the aspects under the responsibility of the jurisdiction.

9.3.3 Common role of the 'approval authority'

This part of ISO 15638 has been developed on the premise that there will be multiple *application service providers (4.7)* providing *TARV regulated application services (4.46)*. As the *specification (4.52)* is performance-based, except in the case where service provision is made using software provided by the *jurisdiction (4.37),* it is also expected that each *application service provider* will have a unique solution

and offering. It is expected that *application service providers (4.7)* will update their offerings from time to time.

The *jurisdiction (4.37)* has to be satisfied that each instance of a specified *regulated application service (4.46)* meets its requirements, provides the data required by this and any other relevant part of ISO 15638, and provides reports to the *specifications (4.52)* that it issues. This is undertaken by a function known within *TARV* as the '*approval authority (regulatory) (4.11)*'. This body may be an independent body appointed by the *jurisdiction,* or may be a department of the *jurisdiction,* depending on the regime imposed by the *jurisdiction.* See ISO 15638-1, or may be some other instantiation determined by the *jurisdiction* to provide the functionality described herein as the '*approval authority (regulatory)*'. It may even be that the *jurisdiction* elects to derogate the approval process to the service provider in a self-approval environment.

Each new *regulated application service (4.46)* 'product' developed and intended for use by an *application service provider (4.7),* and each 'variation' to an existing approved specified *regulated application service* shall be approved by the *approval authority (regulatory) (4.11)* prior to it being recognized and approved as a specified *regulated application service* system in accordance with the regime of the *jurisdiction (4.37).*

The responsibility of the *approval authority (regulatory) (4.11)* shall be to technically assess whether the specified *regulated application service (4.46)* systems offered by an *application service provider (4.7)* meets the performance-based *specification (4.52)* (i.e. are initially approved) and continue to meet their purpose after upgrades and changes are made (i.e. on-going approval) and provide this advice to the *jurisdiction (4.37).* The *approval authority (regulatory)* shall be required to make such assessment consistently across approvals and assist applicants where information or interpretation is required.

The *approval authority (regulatory) (4.11)* may also be engaged by the *jurisdiction (4.37)* to audit the *application service provider's (4.7)* specified *regulated application service (4.46)* systems for operation and provide assurance that the specified *regulated application service* system continues to operate as it was initially approved.

The means by which this *approval authority (regulatory) (4.11)* function is instantiated, its formality, and powers, shall be entirely at the discretion of the *jurisdiction (4.37)*, and some or all functions may, at the discretion of the *jurisdiction,* be derogated to be self-approval processes.

9.4 Common role of the prime service provider

To facilitate the correct installation and monitoring of *TARV IVS (4.32)*, a *prime service provider (4.44)* has been contracted by the *user (4.55)*. See ISO 15638-1. The *prime service provider (4.44)* is the technical expert of their system and shall be responsible for its installation, maintenance and as necessary upgrade, but unless also appointed as an *application service provider (4.7)* for a particular service, is not responsible for the operation of *application service (4.6)* software.

The *prime service provider (4.44)* shall be responsible to ensure that the multiple applications operate properly, and do not adversely impact each other.

It is envisaged that the *IVS (4.32)* operating systems may require updating from time to time to improve functionality, fix software 'bugs', or update the protection from electronic threats such as software viruses and it shall be the responsibility of the *prime service provider (4.44)* to undertake such tasks, possibly in collaboration with *application service providers (4.7).*

The role of the *prime service provider (4.44)* shall be to ensure that the *IVS (4.32)* performs during day to day operation in the same manner as it did when it was approved. The *prime service provider (4.44)* shall put in place a regime to the satisfaction of the *approval authority (regulatory) (4.11)* which shall periodically monitor the *IVS (4.32)* through a number of means including receiving test application service data files generated by the on-board *app (4.5)* for that *application service (4.6).* The *prime service provider (4.44)* shall be responsible to determine the *IVS (4.32)* operational state, perform any necessary enhancements and efficiently deal with malfunctions when they occur.

The *prime service provider (4.44)* shall report any malfunctions to the *driver (4.25)* and *application service provider (4.7)* as appropriate, and as technically possible [for example it may not be possible, during a

working *session* (*4.51*), to advise the *driver* (*4.25*) if the *IVS* (*4.32*) has failed entirely, and such advice would have to be by post event 'offline' means].

The *prime service provider* (*4.44*) shall work closely with the *application service provider* (*4.7*) and vehicle *operator* (*4.43*) to permit and enable the prompt repair and rectification of any malfunction with a *TARV IVS* (*4.32*).

9.5 Common role of the application service provider

The *application service provider* (*4.7*) is the actor who is responsible for providing and operating the approved *vehicle location monitoring* (*4.58*) system.

The *application service provider* (*4.7*) provides the *application service* (*4.6*), as approved by an approval *authority (regulatory)* (*4.11*) to the parties specified in the regime of the *jurisdiction* (*4.37*) [normally the *operator* (*4.43*), *jurisdiction* and *driver* (*4.25*)] undertaken under the terms of a contract with the *user* (*4.55*). The *application service provider* is responsible for receiving, processing, and storing the data generated from their clients *IVS* (*4.32*).

Either the *prime service provider* (*4.44*) or *application service provider* (*4.7*) shall be responsible for providing the *driver* (*4.25*) with an identification and *authentication* (*4.15*) method that works with their *IVS* (*4.32*) in accordance with the agreement between the *prime service provider,* and *application service provider* (*4.7*) in respect of these issues.

The *application service provider* (*4.7*) shall be responsible to ensure that the *regulated application service* (*4.46*) system is correctly installed and performs during day to day operation in the same manner as it did when it was approved. The *application service provider* shall monitor the operation of the *regulated application service* (*4.46*) system and shall report malfunctions to the *driver* (*4.25*), the *prime service provider* (*4.44*), and if required, to the *jurisdiction* (*4.37*). The *application service provider* shall maintain operational knowledge of the system to determine its operational state, perform any necessary enhancements and deal efficiently with malfunctions if they occur.

Where physical maintenance of the *IVS* (*4.32*) is required, the *application service provider* (*4.7*) shall notify the *prime service provider* (*4.44*) and they shall jointly rectify the problem according to their defined and agreed responsibilities.

It is envisaged that the *regulated application service* (*4.46*) systems may require updating from time to time to improve functionality, update *maps* (*4.40*), fix software 'bugs', or update the protection for the *regulated application service* systems from electronic threats such as software viruses and it shall be the responsibility of the *application service provider* (*4.7*) to undertake such tasks, possibly in collaboration with the *prime service provider* (*4.44*).

9.6 Common role of the user

In the case of the most *regulated application services* (*4.46*), the *user* (*4.55*) may be the fleet *operator* (*4.43*), or the *driver* (*4.25*), or both, depending on the specific application service as defined by the regime imposed by the *jurisdiction* (*4.37*). Within this part of ISO 15638, '*operator* (*4.43*)' and '*driver*' are therefore considered as sub-classes of the class '*user* (*4.55*)'.

9.6.1 Role of the driver

The *driver* (*4.25*) shall be responsible, where required by the system, for using the identification and *authentication* (*4.15*) method supplied by the *prime service provider* (*4.44*)/*application service provider* (*4.7*). The declaration of his/her personnel details such as name, *driver's* (*4.25*) licence number and issuing *jurisdiction* (*4.37*) shall be automatically declared by the method of identification and *authentication* (*4.15*). However, the technical means of provision (electronic driving licence identification device, keyboard, iris recognition, barcode, RFID, DRD, etc.) of this information, shall be a function of system/equipment design (or a requirement of the *jurisdiction*) and is not standardized within this part of ISO 15638.

The *driver (4.25)* shall be responsible for reporting any system malfunction alerts, or apparent system failures to the *operator (4.43)* and/or *application service provider (4.7)* as per the instructions provided to them at the commencement of their contract. The *driver (4.25)* is not responsible for *IVS (4.32)* or other equipment malfunction or rectification processes beyond these actions.

The *driver (4.25)* shall be responsible for any equipment (such as a *DRD*, smart card, *RFID* device, barcode) provided to him to identify him/herself to the *IVS (4.32)* when in control of the *regulated vehicle (4.47)*. If the *driver (4.25)* loses any such device, he/she shall be responsible to immediately advise the *regulated vehicle (4.47) operator (4.43)* and *application service provider (4.7).*

NOTE Some *regulated application services (4.46)* may only enable the *regulated vehicle (4.47)* to operate once the identification of the *driver (4.25)* is recorded.

9.6.2 Role of the operator

The *operator (4.43)* of the *regulated vehicle (4.47)* shall be responsible to advise and request action from the *application service provider (4.7)* in the event that the *driver (4.25)* advises him of a potential or actual system malfunction and shall make the *regulated vehicle (4.47)* reasonably accessible to the *application service provider* in order that they may rectify the problem.

If required, and according to the regime of the *jurisdiction (4.37),* the *operator (4.43)* shall identify the *driver (4.25)* of the *regulated vehicle (4.47)* at a particular point of time, to the *jurisdiction* or its agents.

9.7 Common characteristics for instantiations of regulated application services

9.7.1 A *regulated application service (4.46)* is approved; it utilizes a *TARV IVS (4.32)* which communicates to the *prime service provider (4.44)/application service provider (4.7)* and may have the ability to insert a means to provide *driver (4.25)* licence details, or link to another device such as a digital *tachograph (4.53)*.

NOTE The TARV IVS may be a general ITS-station IVS as defined in ISO 21217, or may be a specific device for TARV.

9.7.2 The *application service provider (4.7)* shall load an *app (4.5)* for a *regulated application service (4.46)* into the *IVS (4.32)* of the *operator's (4.43)* vehicles.

9.7.3 The *app (4.5)* for the *regulated application service (4.46)* shall run whenever the *regulated vehicle (4.47)* is operating, or to the instruction of the *application service provider (4.7)* or *operator (4.43)*.

9.7.4 The *app (4.5)* for the *regulated application service (4.46)* shall record the data specified within the appropriate clauses of this part of ISO 15638, in a uniquely named file (to a naming convention specified herein) {the 'application service data file *(4.9)* [ASD file *(4.9)*]} in the *data pantry (4.24)* of the *IVS (4.32)*.

9.7.5 The *application service provider (4.7)* shall design/install/operate its' regulated system as approved by the *approval authority (regulatory) (4.11)*.

9.7.6 The *IVS (4.32)* shall provide the ASD file *(4.9)* to the *application service provider (4.7)* using the *TARV IVS* wireless link, on demand from the *application service (4.6)* system or at the instigation by the on-board *app (4.5)* for the *regulated application service (4.46),* or at least once every 24 h.

Every transfer shall include framing data that identifies its sequential order, IVS ID, version number of IVS, and version number of the *app (4.5)* for the *regulated application service (4.46).*

The system shall acknowledge receipt of the data through the *TARV IVS (4.32)* wireless link. Once the data has been acknowledged, it shall be deleted from the *IVS* memory unless the *operator (4.43)* chooses to retain it in the *IVS* memory for other openly declared purposes with the assent of the user .

9.7.7 The application service system shall retain and back up the 'ASD file *(4.9)*' data to the requirements of the *jurisdiction (4.37).*

9.7.8 The *application service provider (4.7)* shall provide reports to the *jurisdiction (4.37)* or its agents as specified and required by the *jurisdiction* when approving the product.

Where required by the application service *specification (4.52)* approved by the *approval authority (regulatory) (4.11)*, the *driver (4.25)* shall provide their identification to the system at commencement of a *session (4.51)* using the identification and *authentication (4.15)* method provided by the *application service provider (4.7)*. When the *regulated vehicle (4.47)* ignition is turned off, the system shall automatically close the *session*. Each time the *regulated vehicle* ignition is turned on, the *driver* shall be required to identify and authenticate himself/herself.

If *drivers (4.25)* change without turning the engine off, the new *driver* shall identify himself/herself by the means provided by the *application service provider (4.7).*

Where required by the application service *specification (4.52)* approved by the *approval authority (regulatory) (4.11)*, the *application service provider (4.7)* provides the *driver (4.25)* (i.e. *driver* specific) with their identification and *authentication (4.15)* method for the *IVS (4.32)*. The method of identification and *authentication (4.15)* may be unique to each *application service provider.*

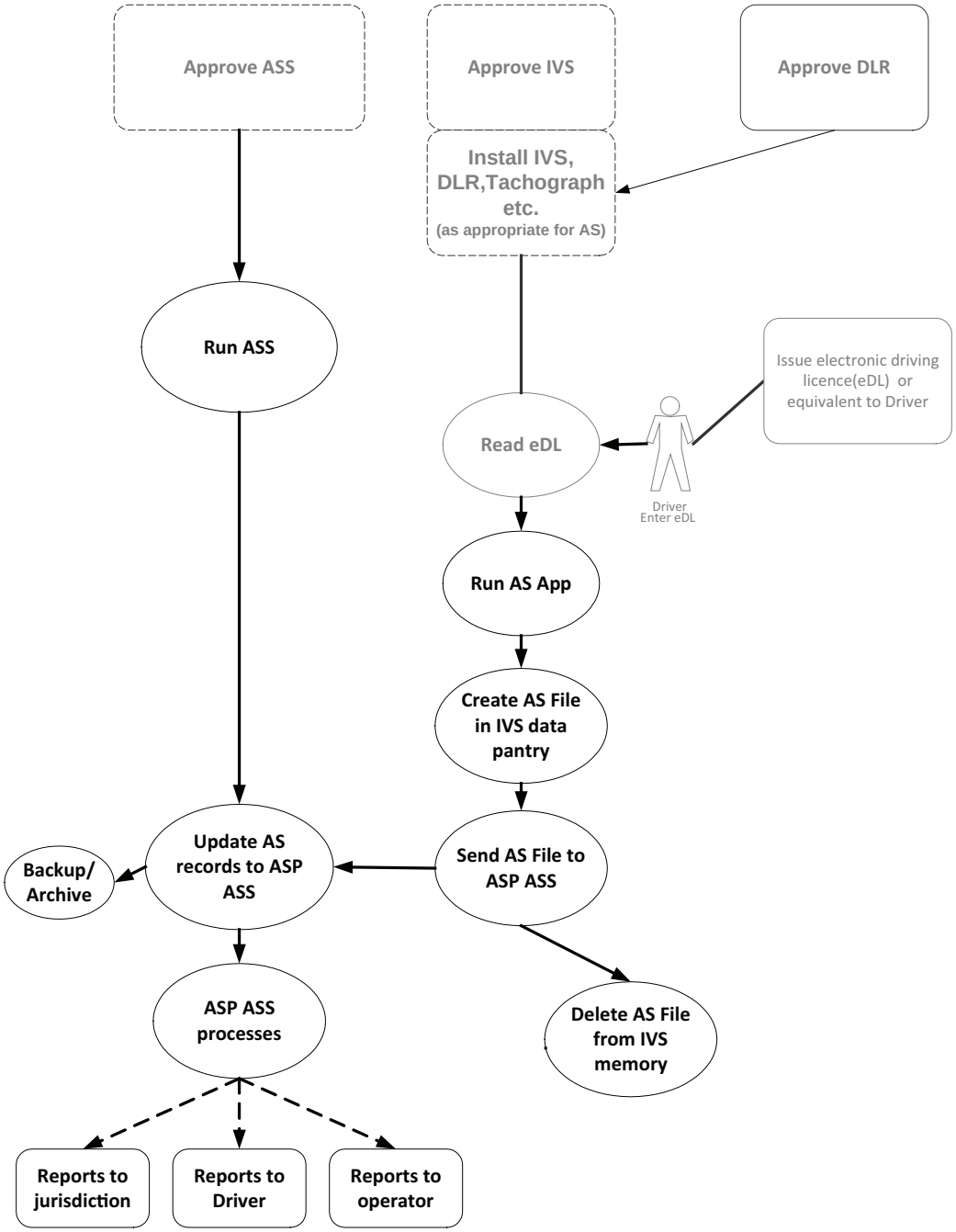
9.7.9 Electronic records are generated periodically by the *IVS (4.32)* when the *regulated vehicle (4.47)* is moving. The electronic record contains accurate time and location data as defined herein. These ASD file *(4.9)* records are generated automatically during the *session (4.51)* and also stored in the *IVS*.

9.7.10 'ASD files' *(4.9)* generated by the *IVS (4.32)* are sent to the predetermined address of the *application service provider (4.7)*, and only to that address. The *application service provider* transmits reports/data to the *regulated vehicle (4.47) operator (4.43)* [in accordance with the system *specification (4.52)*], and in the event of contravention, to the *jurisdiction (4.37),* in accordance with the regime of the *jurisdiction.*

9.8 Common sequence of operations for regulated application services

The business process and sequence of operations are shown in Figure 10.

In understanding Figure 10, it is important to understand that different *jurisdictions (4.37)* will require their own form of a *regulated application service (4.46),* and that *application service provider (4.7)* service offerings will also vary. The specific detail of these *application services (4.6)* are not defined within this part of ISO 15638, and for this part of ISO 15638, at a generic level, the 'business process' is to collate the required data [as specified by the on-board *app (4.5)*], and provide a uniquely named file containing that data to the *application service provider (4.7)* system through a wireless interface to a predetermined email address.



Key

AS application service
ASP application service provider
ASS application service system
eDL electronic driver license
DLR driving license reader
IVS in-vehicle system (including ITS-station)

Figure 10 — Generic regulated application service business process and procedure

9.9 Quality of service

Generic quality of service provisions for *application services (4.6)* are provided for

a) information security (see 9.10),

b) data naming content and quality (see 9.11),

c) software engineering quality systems (see 9.12),

d) quality monitoring station (see 9.13),

e) audits (see 9.14), and

f) access control policy (see 9.16).

Variations for specific *application services (4.6)* are shown in the clauses describing that particular application service (below).

9.10 Information security

The *prime service provider (4.44)* and *application service providers (4.7)* shall both be required to implement an 'Information Security Management system' (*ISMS*) necessary for the on-going operation of the system.

The *ISMS* shall provide assurance that the risks to evidentially-significant information will be managed appropriately by the *users (4.55)* of the system.

This *ISMS* shall be in alignment with a National or International Standard for information security management systems and implement control mechanisms in accordance with such standards. The *ISMS* shall give specific care and focus to

a) *driver (4.25)* identification and *authentication (4.15),*

b) the management of cryptographic elements of the system including hardware, software, and keys,

c) physical and environmental security,

d) access control, especially access from privileged *users (4.55)* and the mechanisms to provide controlled access to functions and information based upon a *user's* legitimate tasks on a need-to-know basis,

e) network and communications security, and

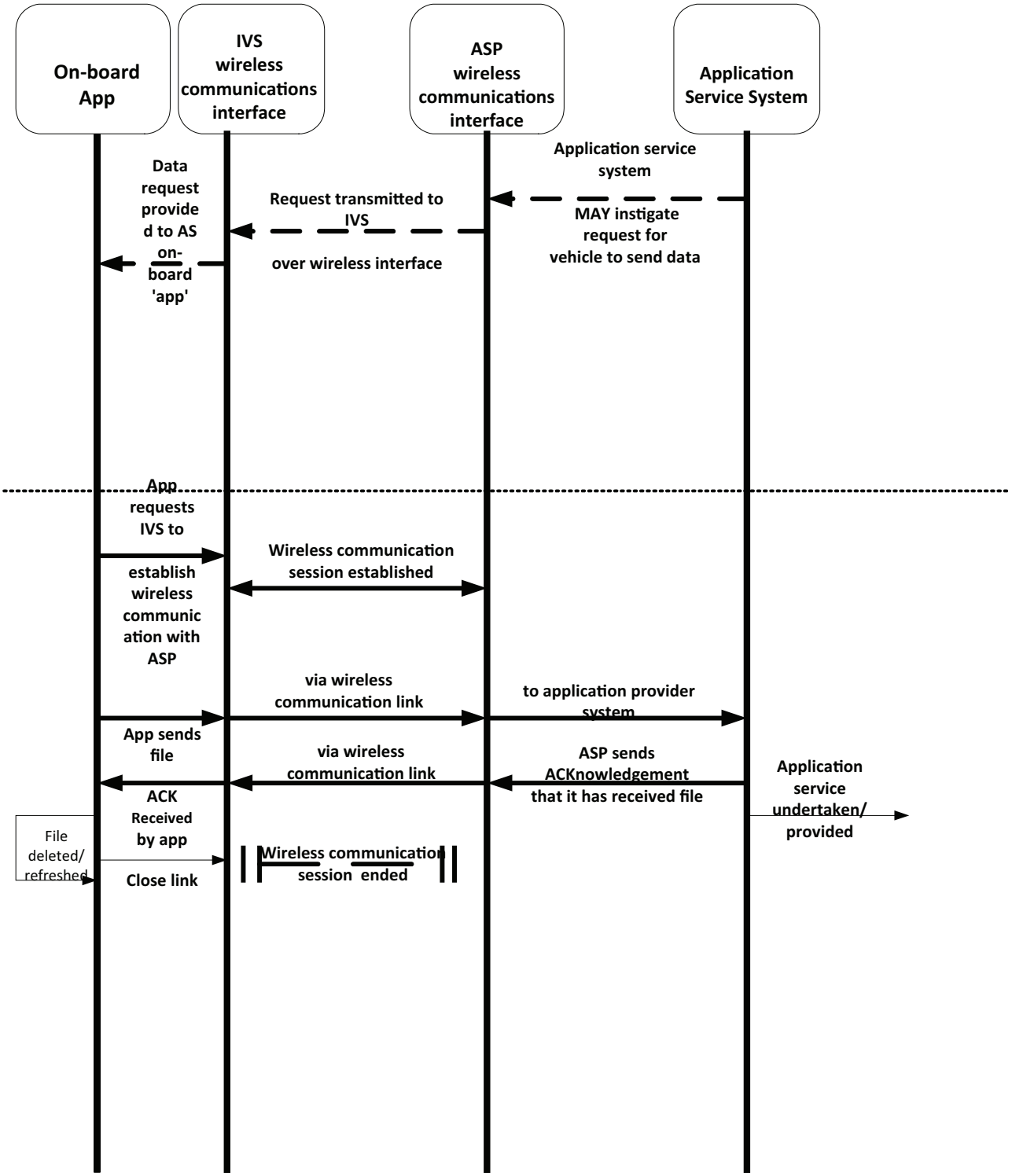
f) incident detection and management.

9.11 Data naming content and quality

TARV application services (4.6) are built around short communication *sessions (4.51)* that simply transfer a file of data to the predetermined address of an *application service provider (4.7)* at intervals/times determined by the application, and receive back a confirmation that the data has been received. Figure 11 illustrates the generic sequence. Figure 11 is illustrative of the process, but individual *application services* may have slightly more complex transactions.

An *application service provider (4.7)* may stimulate the transfer of a file from the *IVS (4.32)* to the application service system. In other situations, it is the on-board *app (4.5)* that stimulates the file to be sent, in some *application service (4.6)* instantiations it may be a combination of both.

Variations for specific *application services (4.6)* are shown in the clauses describing that particular application service (below).



Key

AS application service

ASP application service provider

Figure 11 — Generic file transfer sequence from IVS to application service provider system

The process to obtain *basic vehicle data (4.16)* [*TARV LDT (4.39)*] data content shall be as defined in 8.3.4.1, 8.3.4.2, and ISO 15638-5.

The electronic records declared and stored by the *IVS (4.32)* shall be authenticated, have integrity and be secure from interception or corruption.

In order to enable the application service to identify files received, the files are named to the following convention:

```
<service name><date><time><vehicle registration number><driver licence number>
```

EXAMPLE VDLM 110316 070603 GB 1 KV76WRR WILLI502139RK9MA85

As:

VDLM110316070603KV76WRR WILLI502139RK9MA85

Vehicle registration number shall be as specified in ISO 14816, CS4.

Driver (4.25) licence number shall be as specified by the issuing *driver (4.25)* licence *jurisdiction (4.37).*

Some *application services (4.6)* may not require either the vehicle registration number or the drivers licence number in which case that element of the data concept name may be omitted, however there shall always be at least one of these two elements present. Such issues shall be explicitly defined in the relevant Application Service part of ISO 15638 (ISO 15638-8 to ISO 15638-19).

The clauses defining the specific *application services (4.6)* (below) specify the precise naming convention for that *application service.*

9.12 Software engineering quality systems

The *specification (4.52)*, design, development and testing of the *IVS (4.32)*, *application service provider (4.7)* system and on-board application service *(4.6) app (4.5)* shall employ a recognized software engineering quality system methodology declared to and approved by the approving authority.

The quality system shall also control the process of updates and changes and shall be in alignment with a recognized International quality standard.

9.13 Quality monitoring station

As the *application service provider's (4.7)* end-to-end system comprises a complex arrangement of components (i.e. IVS, wireless communications provider, *application service provider* system etc.), the *prime service provider (4.44)* shall provide, maintain and make available to the *application service provider* a 'Quality Monitoring Station' (*QMS*). The *QMS* provides the *application service provider* with a working example of an *IVS (4.32)* and enables them to monitor each of the components of their end to end system.

9.14 Audits

The *prime service provider (4.44)* shall undergo both internal and external audits at intervals defined by the *jurisdiction (4.37)/approval authority (regulatory) (4.11)* function to ensure that they continue to provide high quality services. The results of these audits shall be provided into the quality systems of the *prime service provider* for continuous improvement actions, and the results shall be provided to the *jurisdiction/approval authority (regulatory)* where so required by the jurisdiction.

The *application service provider (4.7)* shall undergo both internal and external audits at intervals defined by the *jurisdiction (4.37)/approval authority (regulatory) (4.11)* function to ensure that they continue to provide high quality services. The results of these audits shall be provided into the quality systems of the *application service provider* for continuous improvement actions, and the results shall be provided to the *jurisdiction/approval authority (regulatory)*.

9.15 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.

9.16 Approval of IVSs and service providers

Generic provisions for the *approval (4.10)* of *IVSs* and *service providers (4.50)* shall be as specified in ISO 15638-3. Detailed provisions for specific *regulated applications (4.45)* shall be as specified by the regime of the *jurisdiction (4.37).*

10 Specified TARV regulated application services

10.1 General

This Clause identifies and provides reference for the specifications of recognized TARV regulated application services.

10.2 Vehicle access monitoring (VAM)

The framework, architecture, and data definition shall be as specified in ISO 15638-8.

10.3 Remote electronic tachograph monitoring (RTM)

The framework, architecture, and data definition shall be as specified in ISO 15638-9.

10.4 Emergency messaging system/eCall (EMS)

The framework, architecture, and data definition shall be as specified in ISO 15638-10.

10.5 Driver work records (work and rest hours compliance) (DWR)

The framework, architecture, and data definition shall be as specified in ISO 15638-11.

10.6 Vehicle mass monitoring (VMM)

The framework, architecture, and data definition shall be as specified in ISO 15638-12.

10.7 'Mass' data for regulatory control and management (MRC)

The framework, architecture, and data definition shall be as specified in ISO 15638-13:—[6)].

10.8 Vehicle access control (VAC)

The framework, architecture, and data definition shall be as specified in ISO 15638-14.

10.9 Vehicle location monitoring (VLM)

The framework, architecture, and data definition shall be as specified in ISO 15638-15.

10.10 Vehicle speed monitoring (VSM)

The framework, architecture, and data definition shall be as specified in ISO 15638-16.

---

6) To be published.

10.11 Consignment and location monitoring (CLM)

The framework, architecture, and data definition shall be as specified in ISO 15638-17.

10.12 Accord Dangereuses par Route (Dangerous Goods) monitoring (ADR)

The framework, architecture, and data definition shall be as specified in ISO 15638-18.

10.13 Vehicle secure parking (VPF)

The framework, architecture, and data definition shall be as specified in ISO 15638-19.

10.14 Other TARV regulated application services

The framework, architecture, and data definition of other yet to be identified, and specified TARV regulated application services shall be as specified in additional parts of this International Standard that may be developed at some future date.

Subsequent versions/issues of this part of this International Standard may therefore include additional *regulated application services (4.46)* where these have been subsequently identified and specified.

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 in this part of ISO 15638 and ISO 15638-7 contain no direct patents nor intellectual property other than the copyright of ISO in respect of reproduction of this document. 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:—[7], 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 (4.37)* and its regulations for instantiation in this respect.

7) To be published.

Bibliography

[1] ISO/IEC/TR 10000-1, *Information technology — Framework and taxonomy of International Standardized Profiles — Part 1: General principles and documentation framework*

[2] ISO 10241-1, *Terminological entries in standards — Part 1: General requirements and examples of presentation*

[3] ISO 128-30, *Technical drawings — General principles of presentation — Part 30: Basic conventions for views*

[4] ISO 128-34, *Technical drawings — General principles of presentation — Part 34: Views on mechanical engineering drawings*

[5] ISO 128-40, *Technical drawings — General principles of presentation — Part 40: Basic conventions for cuts and sections*

[6] ISO 128-44, *Technical drawings — General principles of presentation — Part 44: Sections on mechanical engineering drawings*

[7] ISO 80000 (all parts), *Quantities and units*

[8] IEC 60027 (all parts), *Letter symbols to be used in electrical technology*

[9] ISO 690, *Information and documentation — Guidelines for bibliographic references and citations to information resources*

[10] ISO 21210, *Intelligent transport systems — Communications access for land mobiles (CALM) — IPv6 Networking*

[11] ISO 21217, *Intelligent transport systems — Communications access for land mobiles (CALM) — Architecture*

[12] ISO/TR 12859, *Intelligent transport systems — System architecture — Privacy aspects in ITS standards and systems*

ICS 03.220.20;35.240.60

Price based on 44 pages