INTERNATIONAL STANDARD

ISO 15638-5

First edition
2013-06-15

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

Part 5:
Generic vehicle information

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

Partie 5: Informations génériques sur le véhicule

Reference number
ISO 15638-5:2013(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

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

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

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

ISO 15638 consists of the following parts, under the general title *Intelligent transport systems — Framework for collaborative Telematics Applications for Regulated commercial freight 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* [Technical Specification]

— *Part 7: Other applications*

— *Part 8: Vehicle access monitoring (VAM)* [Technical Specification]

— *Part 9: Remote electronic tachograph monitoring (RTM)* [Technical Specification]

— *Part 10: Emergency messaging system/eCall (EMS)* [Technical Specification]

— *Part 11: Driver work records (work and rest hours compliance) (DWR)* [Technical Specification]

— *Part 12: Vehicle mass monitoring (VMM)* [Technical Specification]

— *Part 14: Vehicle access control (VAC)* [Technical Specification]

— *Part 15: Vehicle location monitoring (VLM)* [Technical Specification]

— *Part 16: Vehicle speed monitoring (VSM)* [Technical Specification]

- *Part 17: Consignment and location monitoring (CLM)* [Technical Specification]
- *Part 18: ADR (Dangerous Goods) transport monitoring (ADR)* [Technical Specification]
- *Part 19: Vehicle parking facilities (VPF)* [Technical Specification]

The following parts are under preparation:

- *Part 4: System security requirements* [Technical Specification]
- *Part 13: Mass Penalties and Levies (VMC)*

Introduction

Many *ITS* technologies have been embraced by commercial transport operators and freight owners, in the areas of fleet management, safety and security. Telematics applications have also been developed for governmental use. While the regulatory services in use or being considered varies from country to country, these include services such as charging, digital tachograph, hazardous goods tracking and e-call. Additional applications with a regulatory impact being developed include access monitoring, on-board mass monitoring, fatigue management, speed monitoring and heavy vehicle charging based on mass, location, distance and time.

In such an emerging environment of regulatory and commercial applications, it is timely to consider an overall architecture (business and functional) that could support these functions from a single platform within a commercial vehicle that operate within such regulations. Such International Standards will allow for a speedy development and specification of new applications that build upon the functionality of a generic specification platform. This suite of standards deliverables describes and defines the framework and requirements so that the *in-vehicle system* [4.7] can be commercially designed in an open market to meet common requirements.

This suite of standards deliverables will provide the basis for future development of cooperative telematics applications for *regulated commercial freight vehicles* [4.14]. Many elements to accomplish this are already available. Existing relevant standards will be referenced, and the specifications will use existing standards (such as *CALM*) wherever practicable.

This suite of standards deliverables will also allow for a powerful platform for highly cost-effective delivery of a range of telematics applications for *regulated commercial freight vehicles* [4.14].

Finally, a business architecture based on a (multiple) *service provider* [4.15] oriented approach will also require consideration of legal and regulatory aspects for the *approval authority* [4.3] approval and auditing of *service providers [4.7].*

This suite of standards deliverables is timely as many governments (Europe, North America, Asia and Australia/New Zealand) are considering the use of telematics for a range of regulatory purposes. 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 suite of standards deliverables addresses and defines the framework for a range of cooperative telematics applications for *regulated commercial freight vehicles* [4.14] (such as access monitoring, driver fatigue management, speed monitoring, on-board mass monitoring and charging). The overall scope includes the concept of operation, legal and regulatory issues, and the generic cooperative *ITS* service platform. The framework will be based on a (multiple) *service provider* [4.15] oriented approach provisions for the *approval authority* [4.3] approval and auditing of *service providers.*

This part of the ISO 15638 family of standards deliverables provides specifications for generic *basic vehicle data* [4.4] that it is required for all *IVSs* to support and make available to application *service providers* [4.15] using the *IVS* wireless communications link(s), in order to support the provision of regulated and commercial application services for *TARVs*; and provides *basic vehicle data* for cooperative intelligent transport systems.

NOTE The definition of what comprises a ‘regulated’ vehicle is regarded as an issue for national decision, and may vary from country to country. This suite of standards deliverables does not impose any requirements on nations in respect of how they define a regulated vehicle.

NOTE The definition of what comprises a ‘regulated’ service is regarded as an issue for national decision, and may vary from country to country. This suite of standards deliverables does not impose any requirements on nations in respect of which services for regulated vehicles countries will require, or support as an option, but will provide standardised sets of requirements descriptions for identified services to enable consistent and cost efficient implementations where implemented.

NOTE Cooperative *ITS* applications, in this context, are defined as the use of an in-vehicle *ITS* platform to meet both commercial and regulatory needs from a (functionally) single on-board platform.

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

Part 5:
Generic vehicle information

1 Scope

This part of ISO 15638 defines generic basic vehicle and *core application data* [4.5] provision to application *service providers* [4.15] to be supported by *in-vehicle system* [4.7] (*IVS*) for cooperative telematics applications for *regulated commercial freight vehicles* [4.14] (*TARV*), and to provide *basic vehicle data* [4.4] for cooperative intelligent transport systems.

This part of ISO 15638 provides the specifications for generic *basic vehicle data* [4.4] that it is required for all *TARV IVSs* to support and make available to application *service providers* [4.15] via a wireless communications link supported by the *IVS*, in order to support the provision of regulated and commercial application services.

Some further data concepts, while not required in all cases for every *TARV* in every *jurisdiction* [4.9], may be required generically for all equipment within a particular *jurisdiction* [4.9], or class of *TARV* within a *jurisdiction* [4.9], in order for the *jurisdiction* to achieve its regulation of *TARVs*.

Equipped vehicles operating internationally will need to carry all of the additional data concepts required by all of the *jurisdictions* [4.9] within which they operate, in order to determine their *core application data* [4.5]. This part of ISO 15638 provides standard definitions for these commonly expected additional data concepts.

A second set of (largely complementary) 'basic vehicle' data is required to support interoperable cooperative intelligent transport systems and this is also determined and provided within this part of ISO 15638. The framework architecture and many of the protocols are common between both (*TARV* and *C-ITS*) sets of requirements, and also with those being adopted by the wider cooperative *ITS* sector.

2 Conformance

This part of ISO 15638 defines specifications for generic *basic vehicle data* [4.4] that it is required for all *IVSs* to support and make available to application *service providers* [4.15] using the *IVS* wireless communications link(s), in order to support the provision of regulated and commercial application services for *TARVs*; and provides *basic vehicle data* for cooperative intelligent transport systems., and has no specific conformance tests defined herein, however Clause 10 specifies which tests may be required. Some aspects defined within may have conformance tests defined in other parts of ISO 15638.

Conformance to any other International Standard or specification referenced in this part of ISO 15638 shall be ascertained according to the requirements of the referenced deliverable.

Conformance to this part of ISO 15638 is therefore a matter of self-declaration of compliance, or by submission to a test house to ascertain that the provisions of the clauses of this part of ISO 15638 have been adhered to.

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

3 Normative references

The following referenced 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 3166-1	*Codes for the representation of names of countries and their subdivisions — Part 1: Country codes*
ISO 3166-2	*Codes for the representation of names of countries and their subdivisions — Part 2: Country subdivision codes*
ISO 3779	*Road vehicles — Vehicle identification number (VIN) -- Content and structure*
ISO/IEC 8824-1	*Information processing systems — Open Systems Interconnection —Specification of abstract syntax notation one (ASN.1) — Part 1: Specification of the Basic Notation*
ISO/IEC 8824-2	*Information processing systems — Open Systems Interconnection — Specification of abstract syntax notation one (ASN.1) — Part 2: Information Object Specification*
ISO/IEC 8824-3	*Information processing systems — Open Systems Interconnection — Specification of abstract syntax notation one (ASN.1) — Part 3:Constraint Specification*
ISO/IEC 8824-4	*Information processing systems — Open Systems Interconnection — Specification of abstract syntax notation one (ASN.1) — Part 4:Parameterisation of the ASN.1 Specifications*
ISO/IEC 8825-2	*Information technology — ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)*
ISO 10918-1	*Information technology — Digital compression and coding of continuous-tone still images: Requirements and guidelines).*
ISO 13183	*Intelligent transport systems — Communications access for land mobiles (CALM) — Broadcast communications*
ISO 14816	*Road transport and traffic telematics — Automatic vehicle and equipment identification — Numbering and data structure*
ISO 15638-1	*Intelligent transport systems — Framework for cooperative telematics applications for regulated commercial freight vehicles (TARV) — Part 1: Framework and architecture*
ISO 15638 -2	*Intelligent transport systems — Framework for cooperative telematics applications for regulated commercial freight vehicles (TARV) — Common platform parameters using CALM*
ISO 15638 -3	*Framework for cooperative telematics applications for regulated commercial freight vehicles TARV — Operating requirements, 'Approval authority' procedures, and enforcement provisions for the providers of regulated services*
ISO 15638 -4	*Intelligent transport systems — Framework for cooperative telematics applications for regulated commercial freight vehicles (TARV) — System security requirements*
ISO 17262	*Intelligent transport systems — Automatic vehicle and equipment identification — Numbering and data structures*
ISO 21210	*Intelligent transport systems — Communications access for land mobiles — IPv6 Networking*

ISO 21212	*Intelligent transport systems — Communications access for land mobiles (CALM) — 2G Cellular systems*
ISO 21213	*(CALM) — 3G Cellular systems*
ISO 21214	*Intelligent transport systems — Communications access for land mobiles (CALM) — Infra-red systems*
ISO 21215	*Intelligent transport systems — Communications access for land mobiles (CALM) -- M5*
ISO 21216	*Intelligent transport systems — Wireless communications — CALM using millimetre communications — Air interface*
ISO 21217	*Intelligent transport systems — Communications access for land mobiles (CALM) — Architecture*
ISO 21218	*Intelligent transport systems — Communications access for land mobiles (CALM) — Medium service access points*
ISO 25111	*Intelligent transport systems — Communications access for land mobiles (CALM) — General requirements for using public networks*
ISO 25112	*Intelligent transport systems — Communications access for land mobiles (CALM) — Mobile wireless broadband using IEEE 802.16*
ISO 25113	*(CALM) — Mobile wireless broadband using HC-SDMA*
ISO TS 26683-2	*Intelligent transport systems — Freight land conveyance content identification and communication — Part 2: Application interface profiles*
ISO 29281	*Intelligent transport systems — Communications access for land mobiles (CALM) — Non-IP networking*
ISO 29282	*Intelligent transport systems — Communications access for land mobiles (CALM) — Applications using satellite networks*
ISO 29283	*ITS CALM Mobile Wireless Broadband applications using Communications in accordance with IEEE 802.20*
ETSI TS 102 894	*Intelligent Transport System (ITS);Users & Applications requirements;Facility layer structure, functional requirements and specifications;Facility layer structure, functional requirements and specifications*
ETSI TS 102 890-1	*Intelligent Transport Systems (ITS);Facilities layer function;Communication Management specification Facilities Communication Management*
ETSI TS 102 890-2	*Intelligent Transport Systems (ITS);Facilities layer function;Services announcement specification-Facilities Service Announcement*
EN 302 895	*Intelligent Transport Systems (ITS);Vehicular Communications;Basic Set of Applications; Local Dynamic Map (LDM) Specification*

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
A/D voltage
analogue to digital converter voltage

4.2
application service
service provided by a *service provider* [4.15] accessing data from the *IVS* of a *regulated commercial freight vehicle* [4.14] via a wireless communications network

4.3
approval authority
organization (usually independent) which conducts 'Approval Authority' approval and ongoing audit for *service providers* [4.15]

4.4
basic vehicle data
data maintained/provided by all *IVS*

4.5
core application data
basic vehicle data [4.4] plus any additional data required to provide an implemented *regulated application services* [4.13]

4.6
G's
gravitational force
object's acceleration relative to free-fall

4.7
in-vehicle system (IVS)
equipment on-board a vehicle that can provide the specified telematics functionality

NOTE This equipment may comprise a single physical *on-board unit* [4.11], or a telematics functionality within one or multiple equipments on-board a vehicle

4.8
Java™
object oriented open source operating language developed by 'SUN Microsystems'™

4.9
jurisdiction
government, road or traffic authority which owns the '*regulatory applications* [4.12]

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

4.10
local data tree
LDT
frequently updated data concept stored in the on on-board data pantry containing a collection of data values deemed essential for either a) *TARV regulated applications* [4.12], or b) cooperative intelligent transport systems

4.11
on-board unit
OBU
integrated telematics unit installed on-board which provides the specified telematics functionality required for the *IVS*

4.12
regulated/regulatory application
approval arrangement utilized by *jurisdictions* [4.9] for granting certain categories of commercial vehicles rights to operate in regulated circumstances subject to certain conditions

NOTE Each *jurisdiction* may use their own terminology including, but not limited to, permit, application, scheme, concession, exemption, gazettal and notice

4.13
regulated application service
TARV application service [4.2] that is mandated by a regulation imposed by a *jurisdiction* [4.9], or is an option supported by a *jurisdiction*

4.14
regulated commercial freight vehicle
vehicle designed to haul commercial freight that is subject to regulations determined by the *jurisdiction* [4.9] as to the use of the road system of the *jurisdiction* and the compliance with specific regulations for that class of *regulated commercial freight vehicle*, often through the provision of information via *TARV*

4.15
service provider
party which is approved by a *approval authority* [4.3] as suitable to provide regulated or commercial *ITS* services

4.16
unique vehicle identification
unambiguous identification of the vehicle

5 Symbols (and abbreviated terms)

ACK
acknowledgement

API
application program interface

app
application programme

AS
application service

CALM
communications access for land mobiles

C-ITS
cooperative intelligent transport systems

CVIS
'Cooperative Vehicle-Infrastructure Systems' (EC Project)

DDS
distributed directory service

FOAM
framework for open applications (standards deliverable within CVIS)

G
gravitational force

GNSS
global navigation satellite system

HMC
host management centre

ITS
intelligent transport systems

IVS
in-vehicle system [4.7]
LDM
local dynamic map

LDT
local data tree [4.10]

JAVA
JAVA™ [4.8]

OBU
on-board unit [4.11]

OEM
original equipment manufacturer

OMA
open mobile alliance

OSGi™
open services gateway initiative

PSP
prime service provider

RAM
random access memory

SI
Système international d’unité

ROAM
regime for open application management

TARV
telematics applications for *regulated commercial freight vehicles* [4.14]

URI
uniform resource identifier

UTC
universal time coordinated

6 General overview and framework

6.1 General overview

6.1.1 Context

6.1.1.1 Framework and architecture

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

Figure 1 shows the role model conceptual architecture showing the key actors and their relationships.

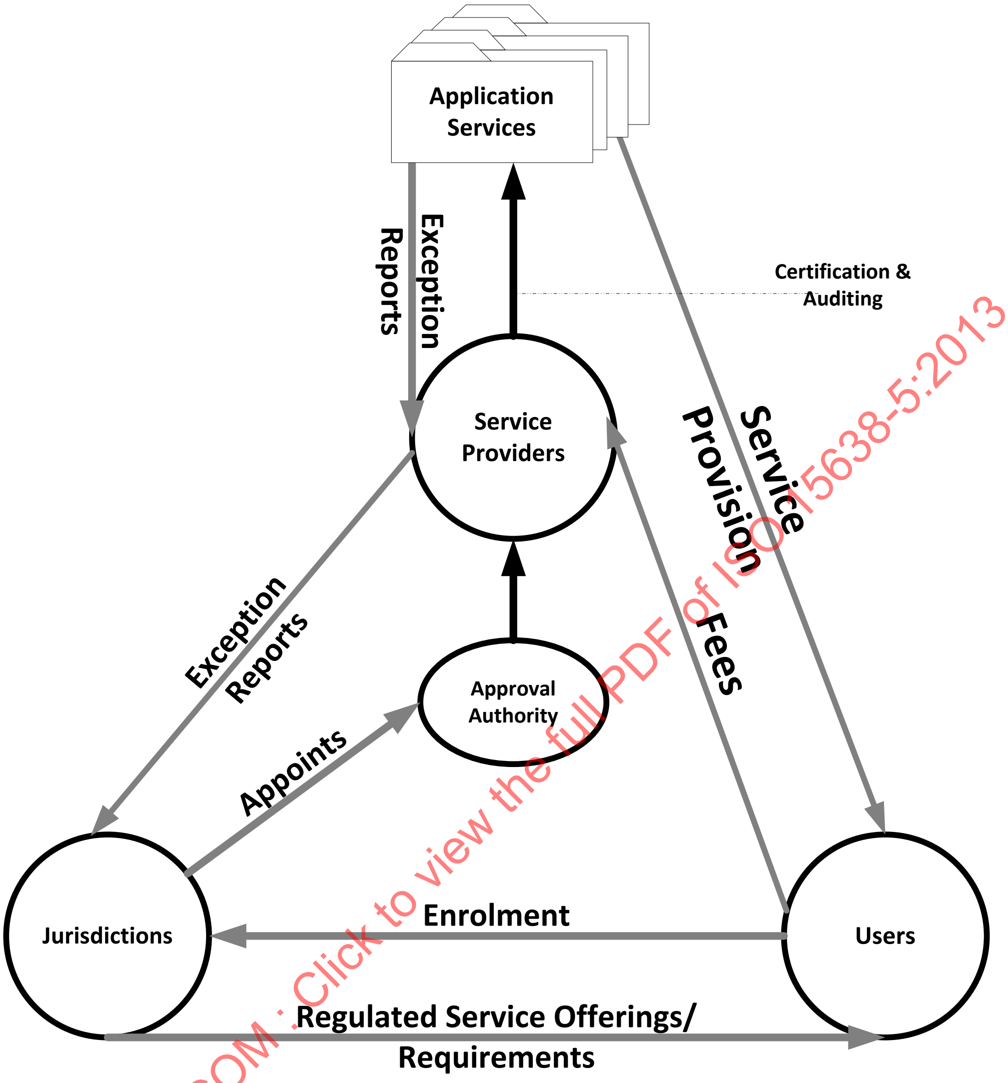

Figure 1 — Role model conceptual architecture

(Source: ISO 15638-1)

To understand more clearly the *TARV* framework in detail the reader is referred to ISO 15638-1.

ISO 15638 provides a suite of standards deliverables addresses and defines the framework for a range of cooperative telematics applications for regulated commercial freight vehicles (such as access monitoring, driver fatigue management, speed monitoring, on-board mass monitoring and charging). The overall scope includes the concept of operation, legal and regulatory issues, and the generic cooperative *ITS* service platform. The framework is based on a (multiple) *service provider* [4.15] oriented approach provisions for the *approval authority* [4.3] approval and auditing of *service providers*.

ISO 15638 is comprised of seven framework parts and twelve application specific parts. The framework parts are:

- 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 4: System security requirements
- Part 5:Generic vehicle information
- Part 6: Regulated applications [Technical Specification]
- Part 7: Other applications

While specific *application services* [4.2], both regulated and commercial, will have their own application specific requirements for data provided by the *IVS* or harvested by the *IVS* from connected equipment and instruments, some generic data is required by many, if not most, and in some cases all, application services for regulated commercial vehicles.

It is therefore required that, while not designing the functionality or physical form of any *IVS* (which is considered a function of the marketplace or *jurisdictions* [4.9] who are regulating in order to implement), that the generic information known within the ISO 15638 suite of standards deliverables as *basic vehicle data* [4.4], shall be supported by all *IVSs*.

(for example, shall have a unique identifier, collect time and location data, etc.)

Some further data concepts, while not required in all cases for every *TARV* in every *jurisdiction* [4.9], 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 *TARVs*. A number of these data concepts, which are expected to frequently be required are, for reasons of interoperability, defined within this part of ISO 15638.

The combination of *basic vehicle data* [4.4] and those additional data concepts required within a particular *jurisdiction* [4.9] (or class of *TARVs*) are known as *core application data* [4.5] for that *jurisdiction. Basic vehicle data [4.4]* will therefore be found in all equipped *TARVs*, while *core application data* [4.5] will be found in all equipped *TARVs* (or class of *TARVs*) within a particular *jurisdiction*.

Equipped vehicles operating internationally will need to carry all of the additional data concepts required by all of the *jurisdictions* [4.9] within which they operate, in order to determine their *core application data* [4.5]. By providing standard definitions for these commonly expected additional data concepts, this will be easy to achieve and provide international interoperability.

This part (15638-5) provides definition for generic vehicle information, and simple means for authorised actors to download that information. This information comprises:

- *basic vehicle data* [4.4] provided by the *TARV LDT* [4.10]* for *TARV* applications (*local data tree* [4.10]);
- *basic vehicle data* [4.4] provided by the *C-ITS LDT* [4.10]* for cooperative intelligent transport systems (particularly cooperative safety related systems);
- *core application data* [4.5] which comprises *basic vehicle data* [4.4] (from the *TARV LDT* [4.10]) together with additional data requirements in a particular *jurisdiction* [4.9];
- Archive data, which enables the prime *service provider* [4.15] to maintain a complete record of data calculated and recorded on-board.

NOTE **LDT* (*local data tree* [4.10]) is a data concept stored in the on on-board data pantry containing a collection of data values deemed essential for either a) *TARV regulated applications* [4.12], or b) cooperative intelligent transport systems.

ISO 15638-1 (*TARV* Framework and architecture) recognises that different *jurisdictions* [4.9] will have different requirements and that they may require in addition to the *basic vehicle data* [4.4]. This additional data together with the *basic vehicle data* is known as *core application data* [4.5] or '`CoreData`' within ISO 15638.

But within the global *TARV* context, for a transcontinental journey (examples UK to Russia via France, Belgium, Holland, Germany, Poland, Belarus; Hungary to France via Austria and Germany; China to Malaysia via Laos and Thailand etc.) it is impracticable to just rely on the user or *application service* [4.2] provider to both know and be able to technically provide the additional data to meet the requirements of all of the *jurisdictions* [4.9] of all of the transit countries, particularly as such requirements may also vary over time and from freight type to freight type.

Some of the data on-board the vehicle will also be commercially sensitive and measures need to be taken to prevent it being useful by, or accessed by, the wrong hands.

Further, and most importantly, in a 'co-operative *ITS'* environment, much of this data could be used by, or obtained from, other '*Apps'* on-board, and so it is not efficient just to simply define it as a constituent element of a single data concept *core application data* [4.5] or *basic vehicle data* [4.4] . There is nothing wrong with grouping data elements into data concepts such as *basic vehicle data* or *core application data*, but it is not efficient to have these elements only available within these defined major data concepts.

Finally, the security requirements are such that a common and secure provision for security needs to be provided on all cooperative *ITS* systems in order to both maintain security and offer interoperability, common use and reuse of data.

This data is calculated by *apps* in the on-board data library, and stored as discrete data concept values in the on-board 'data pantry'. The frequency of such updates is determined by the app. This part of ISO 15638 defines that additional *apps* in the library collate the data into two data concepts containing collated data element values:

a) *TARV LDT* [4.10] values
b) *C-ITS LDT* [4.10] values

A further app creates an archive of the history and values of data, stored in a file called '`RecentArchive`'.

6.1.1.2 Data creation process and architecture

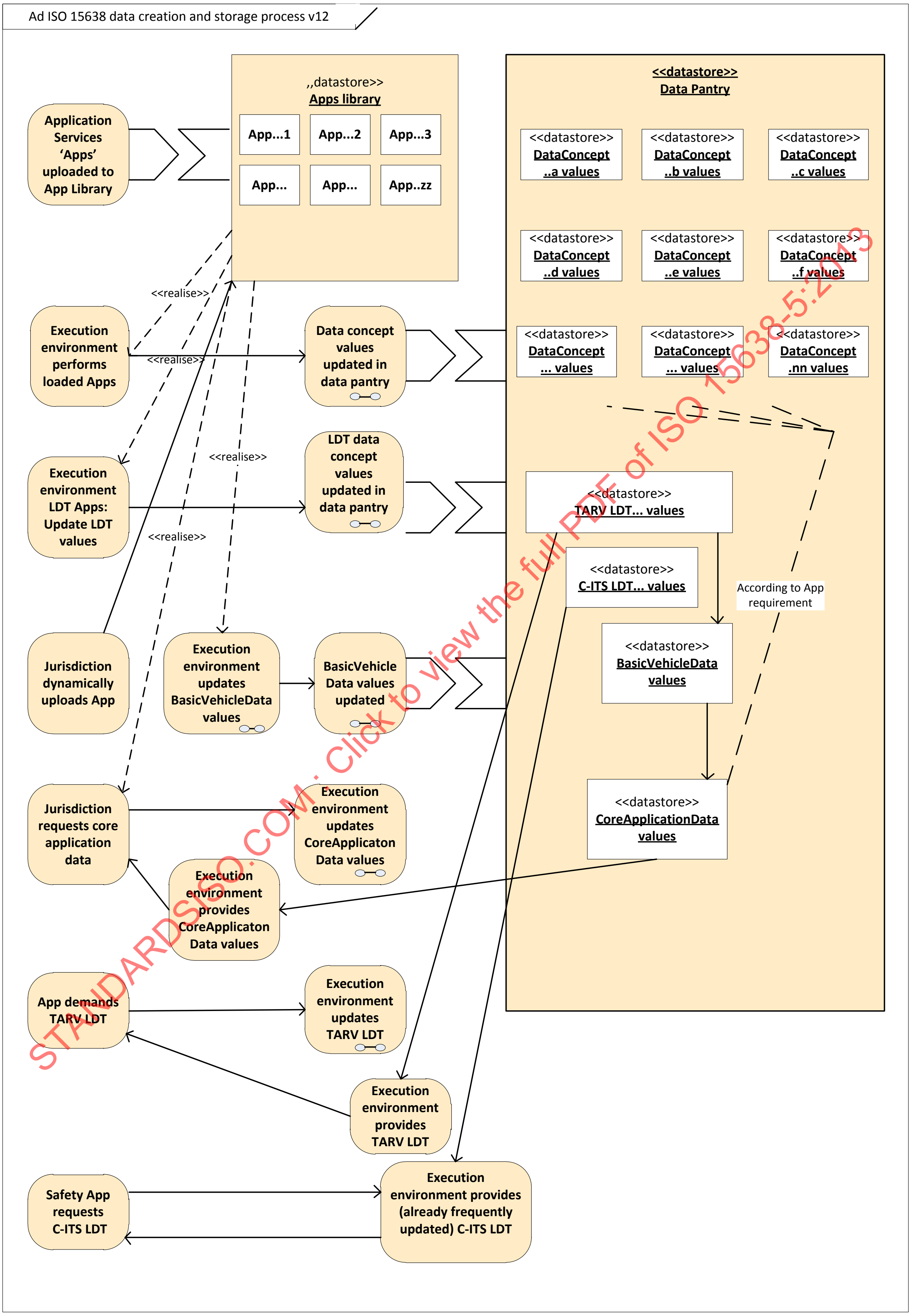
Ad ISO 15638 data creation and storage process v12
Application Services 'Apps' uploaded to App Library
,,datastore>>
Apps library
App...1
App...2
App...3
App...
App...
App..zz
<<datastore>>
Data Pantry
<<datastore>> DataConcept ..a values
<<datastore>> DataConcept ..b values
<<datastore>> DataConcept ..c values
<<datastore>> DataConcept ..d values
<<datastore>> DataConcept ..e values
<<datastore>> DataConcept ..f values
<<datastore>> DataConcept ... values
<<datastore>> DataConcept ... values
<<datastore>> DataConcept .nn values
<<realise>>
<<realise>>
<<realise>>
<<realise>>
Execution environment performs loaded Apps
Data concept values updated in data pantry
Execution environment LDT Apps: Update LDT values
LDT data concept values updated in data pantry
<<datastore>> TARV LDT... values
<<datastore>> C-ITS LDT... values
<<datastore>> BasicVehicleData values
<<datastore>> CoreApplicationData values
According to App requirement
Jurisdiction dynamically uploads App
Execution environment updates BasicVehicleData values
BasicVehicle Data values updated
Jurisdiction requests core application data
Execution environment updates CoreApplicaton Data values
Execution environment provides CoreApplicaton Data values
App demands TARV LDT
Execution environment updates TARV LDT
Execution environment provides TARV LDT
Safety App requests C-ITS LDT
Execution environment provides (already frequently updated) C-ITS LDT

Figure 2 — The ISO 15638 data creation and storage process

Figure 2 shows *apps* being uploaded into the app library, and the execution environment running the *apps* and updating the data concept values in the data pantry. It shows the *LDT* [4.10] values being updated to the instructions of the appropriate *app*. It then shows a *jurisdiction* [4.9] uploading an app for its *core application data* [4.5], which then demands that the *core application data* concept values be updated. This is done. The *jurisdiction* then requests the *core application data* values which are supplied.

An example of an app demanding the *TARV LDT* [4.10] is then shown, with the app in the execution environment stimulating a refresh of the *TARV LDT* values, then supplying them to the application.

Finally the example of a safety app requesting the *C-ITS LDT* [4.10] is shown. As these safety events are frequently time critical, it is assumed that an app in the data library is ensuring that the data is always current, and so it is provided instantaneously on request.

6.1.1.3 Commands

This part of ISO 15638 defines (see Clause 7) five generic commands for use by any application:

a) GET TARV LDT data (`GETTARVLDT`)

b) GET C-ITS LDT data (`GETC-ITSLDT`)

c) CREATE core application data (CREATECoreData)

d) GET core application data (GETCoreData)

e) GET Archive (GETArchive)

GET TARV LDT data provides a means for any application to get the current mix of permanent and situation/time dependent data.

GET core application data provides a means for any application to get the current mix of permanent and situation/time dependent data.

GET Archive, provides a means to upload all data collected in the memory of the *OBU* since the last instance of this command, and to transfer the data to the interrogator.

Certification procedures and enforcement provisions for the providers of regulated services shall be found in ISO 15638-3 Clause 12.

Security aspects are dealt with in ISO 15638-4 TARV system security requirements. Specific *application service* [4.2] provision aspects are defined in ISO 15638-6 TARV regulated application services, and ISO 15638-7 TARV other applications.

Basic vehicle data [4.4] and *core application data* [4.5] aspects are specified in Clause 8 of this part of ISO 15638.

6.1.1.4 IVS requirements

IVS requirements shall be as defined in clause 9 of ISO 15638-3 (TARV – Operating requirements, 'Approval authority' procedures, and enforcement provisions for the providers of regulated services).

6.1.2 ROAM

6.1.2.1 ROAM framework and architecture

The *ROAM* (Regime for Open Application Management) architecture provides the framework and operational environment for developing and deploying platforms for *TARV* applications within a general framework of cooperative intelligent transport telematics systems and shall be as defined in ISO 15638-1.

ROAM 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.

TARV applications for regulated commercial vehicles can be implemented according to the regulations of implementing *jurisdictions* [4.9], and at their discretion, via an app provided by the *jurisdiction*.

A number of generic and interoperable *regulated application services* [4.13] are provided as a toolbox to *jurisdictions* [4.9] in ISO 15638-6 (*TARV* Regulated application services). The methodology to support commercial services for *TARVs*, and to cooperate/interoperate with the provision of general safety services for all classes of vehicles is provided in ISO 15638-7).

Within the *TARV* environment, *regulated applications* [4.12] are developed by *jurisdictions* [4.9] and deployed by *application service* [4.2] providers to 'Host Management Centres' (*HMC*). The *HMC* provides a service gateway that supervises the secure provision of software and services for *TARVs*. *HMCs* manage the provisioning of applications to any authorised and subscribed user via 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™* [4.7] /*OSGi™* (open services gateway initiative), and the overall framework and architecture is therefore already well proven in use in other domains, such as mobile telephony.

While the requirements for regulated commercial vehicles are very specific to the domain of a *jurisdiction* [4.9], and will vary from one *jurisdiction* to another, equipped *TARVs*, in a world of cooperative *ITS* systems, do not operate in isolation, and the on-board platform designed to support *TARV regulated application services* [4.13] will also provide other commercial services to *TARVs* and interoperate and support general cooperative safety services for all classes of vehicles.

ROAM defines an architecture (based on CVIS/*OSGi*™) that connects *in-vehicle systems* [4.7], roadside infrastructure and back-end infrastructure necessary for co-operative management of transport safety and efficiency. This provides an architecture and specification that is implementation independent, i.e. to allow implementation using various client and back-end server technologies.

TARV-ROAM is therefore a specific instantiation of a common approach for secure data provision in a cooperative *ITS* environment, adapted to the needs of *TARV*.

While the reader is referred to ISO 15638-1 for an explanation of the architecture and functioning of *TARV-ROAM*, the following Figures are reproduced as a reference précis.

Figure 3 illustrates *TARV* service provision with *ROAM* Identified.

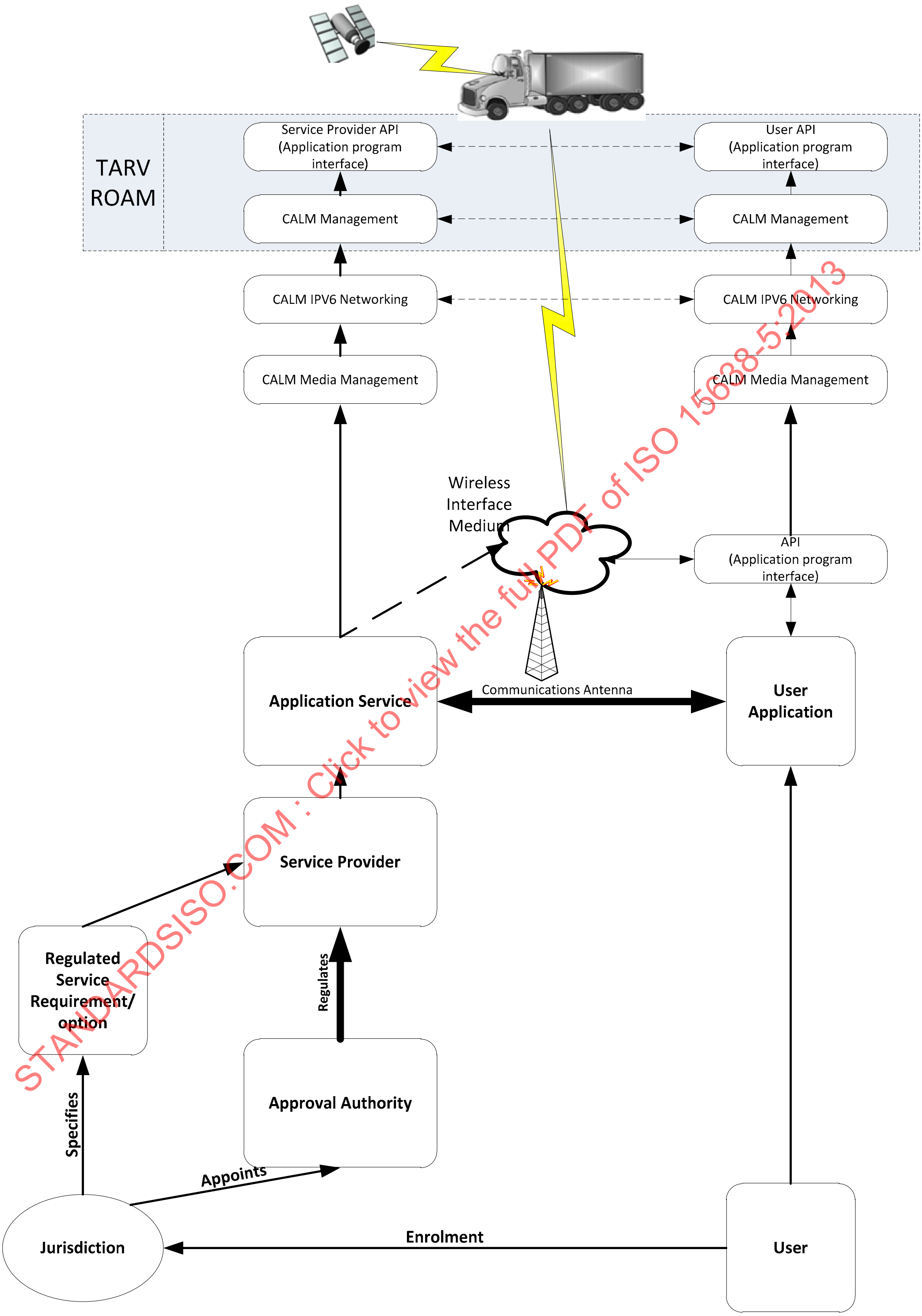

Figure 3 — TARV service provision with ROAM identified

(Source: ISO15638-1, modified)

Figure 4 provides a view of the **IVS** component disposition.

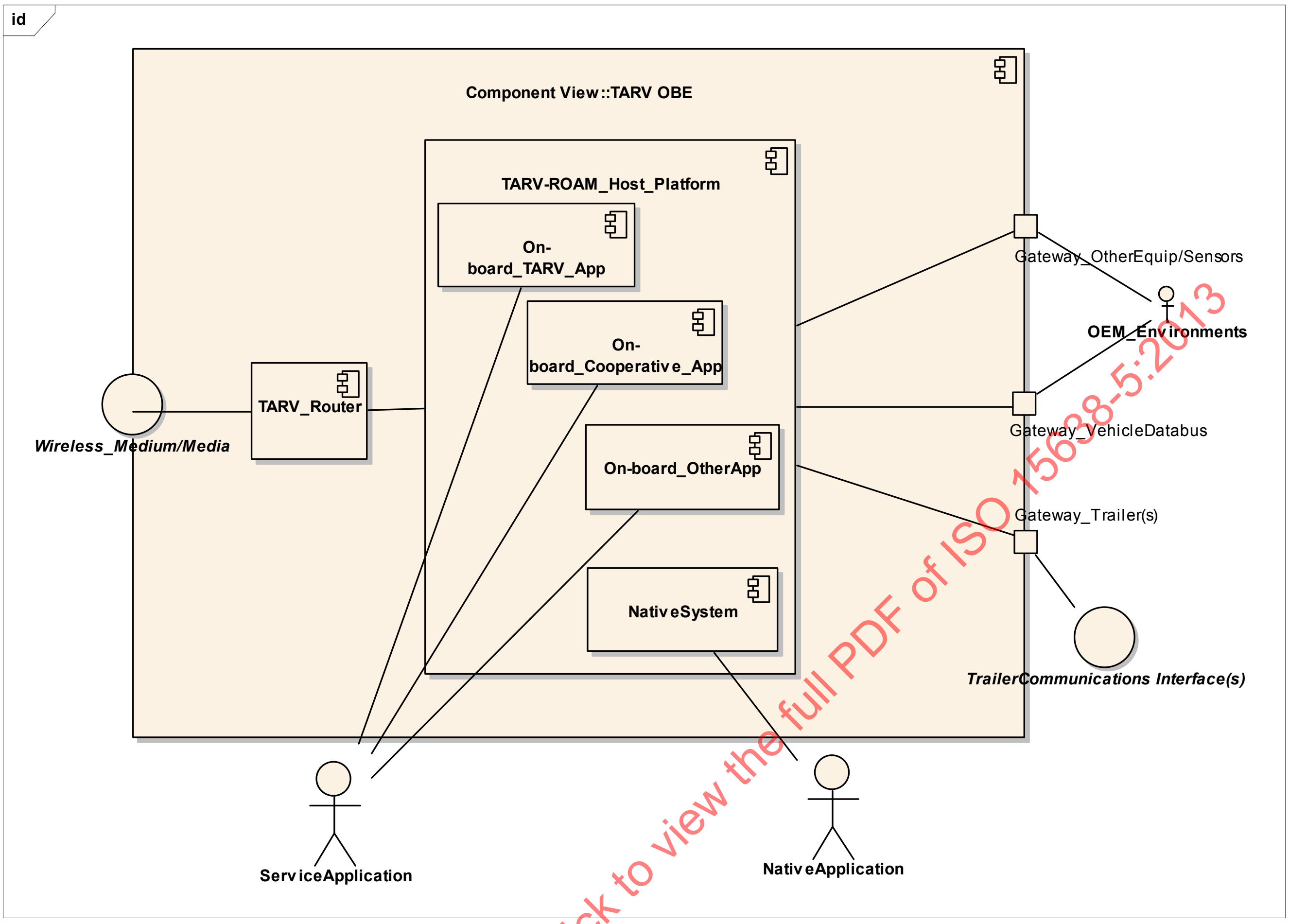

Figure 4 — TARV IVS component decomposition

Figure 5 provides a view of the communications.

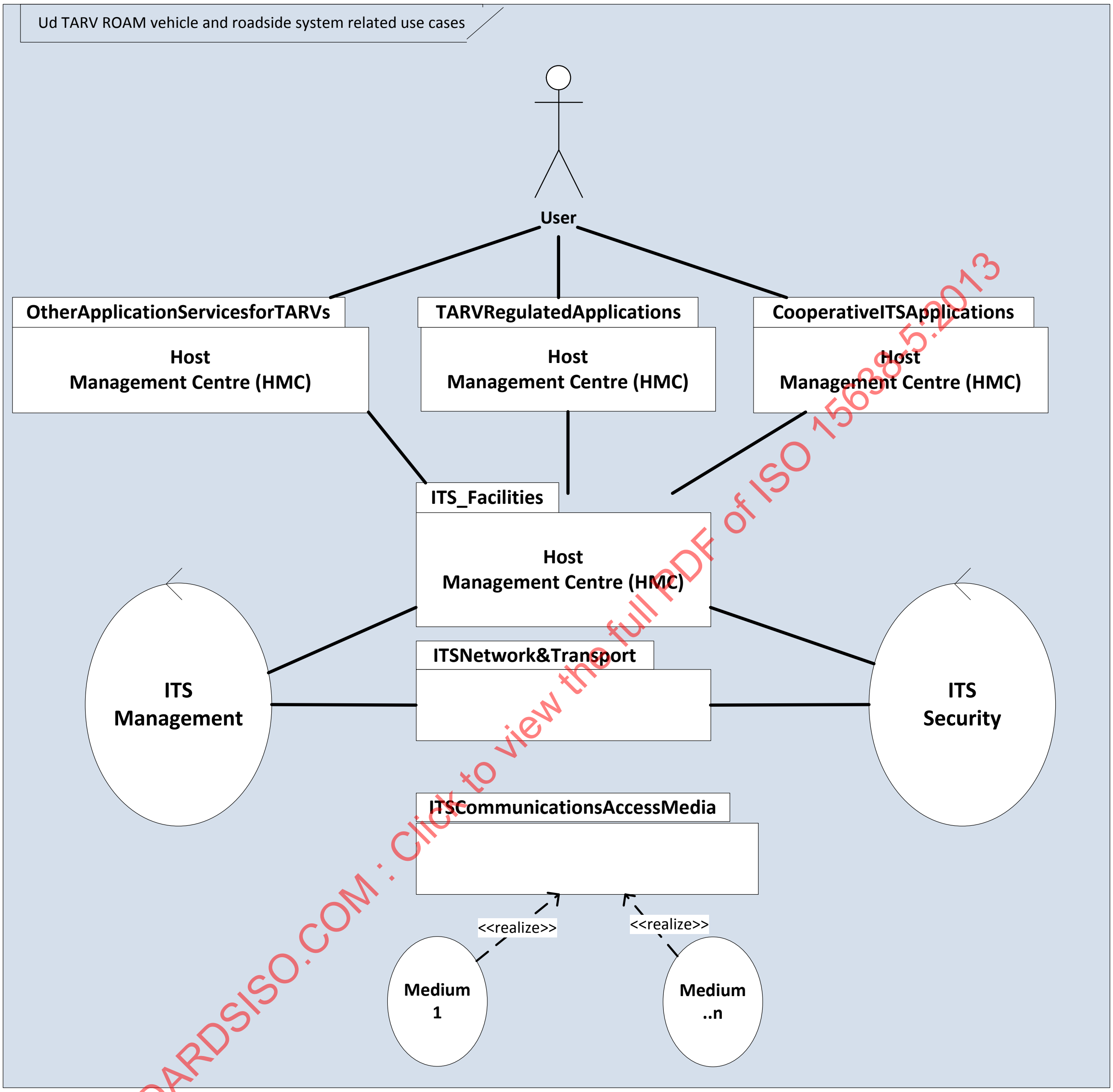

Figure 5 — UML representation of TARV-ROAM communication diagram

Figure 6 shows a UML view of TARV–ROAM service platform components.

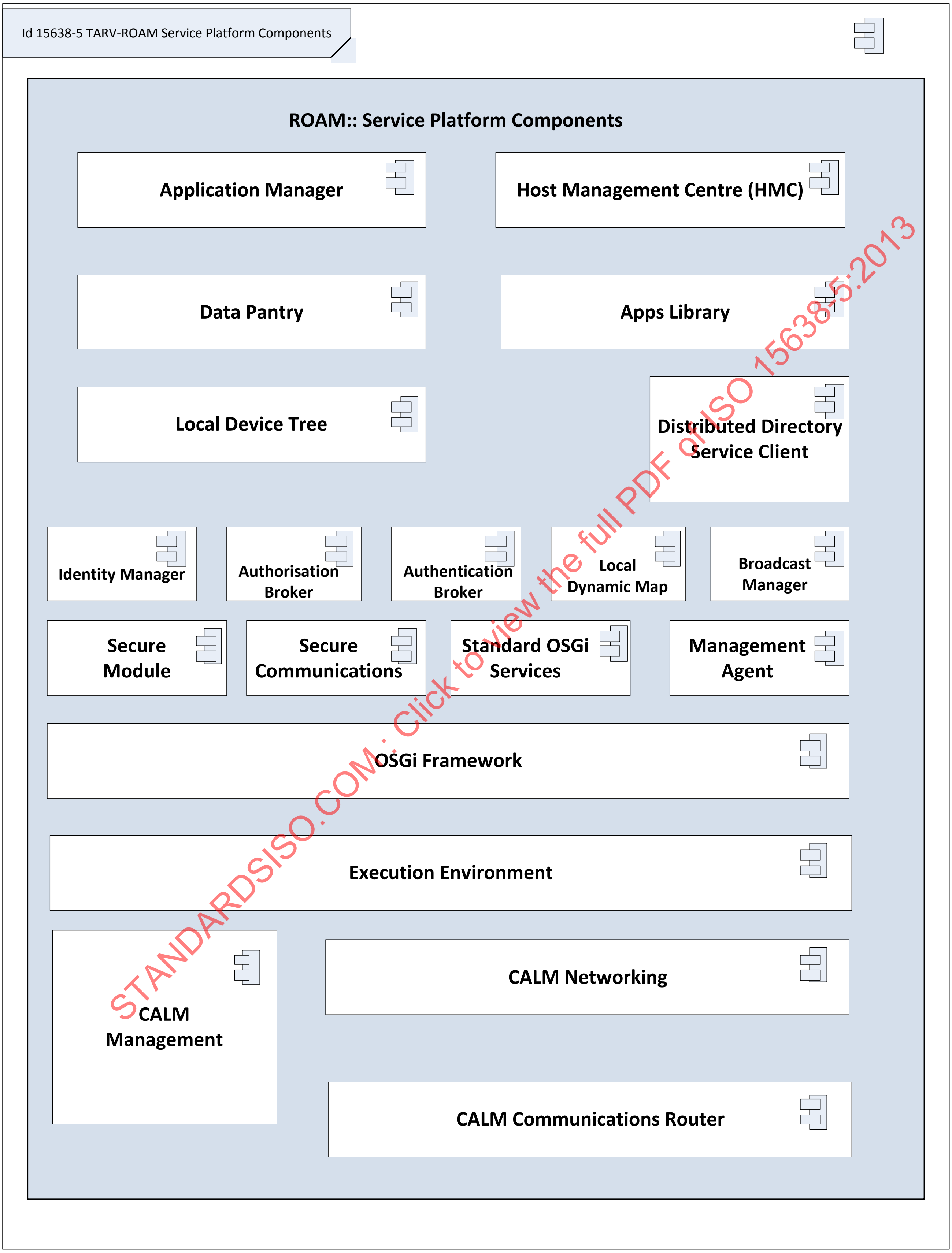

Figure 6 — TARV–ROAM service platform components

6.1.2.2 TARV supported LDTs

This version of *TARV* supports two *LDT* [4.10] *basic vehicle data* [4.4] concepts

1) TARV LDT
2) C-ITS LDT

The *TARV LDT* [4.10] *basic vehicle data* [4.4] is focussed to the specific requirements for regulated commercial vehicles.

The *C-ITS* (co-operative intelligent transport systems) *LDT* [4.10] *basic vehicle data* [4.4] is focussed to the requirements for cooperative intelligent transport systems for all classes of vehicle, and is safety application centric.

Figure 7 provides a representation of the *C-ITS local data tree* [4.10].

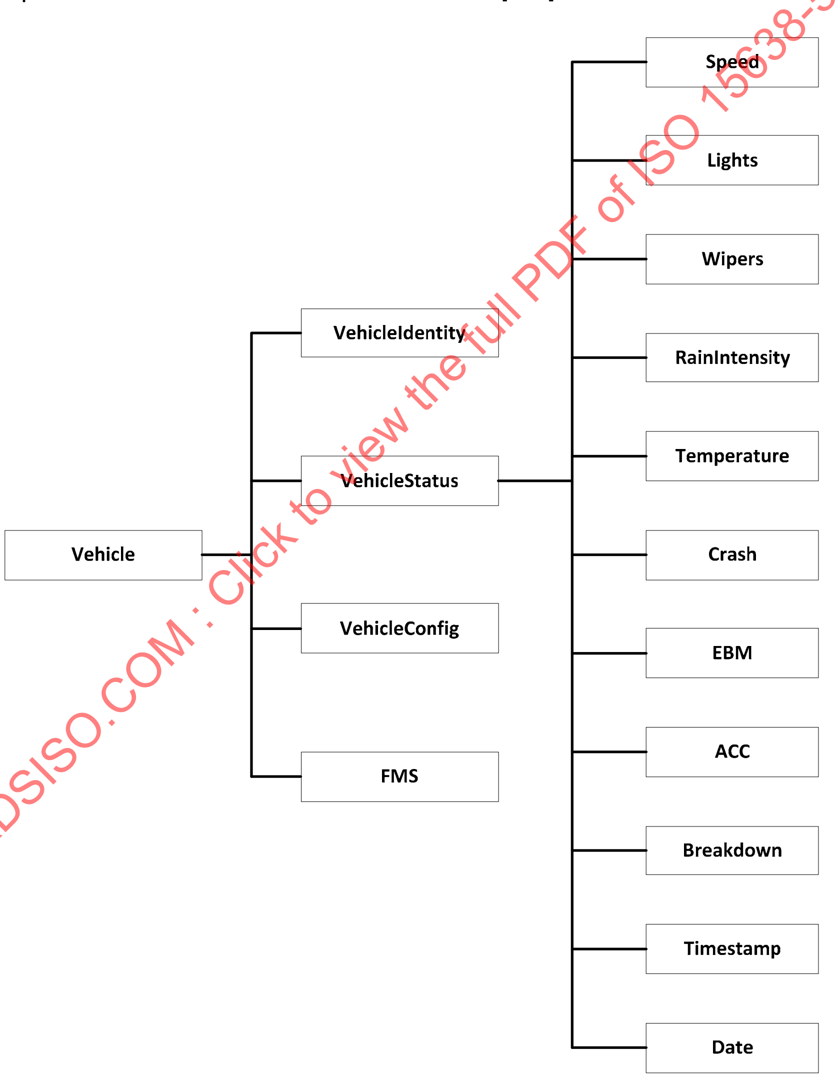

Figure 7 — C-ITS local data tree

(From project CVIS)

Figure 8 shows the TARV *local data tree* [4.10].

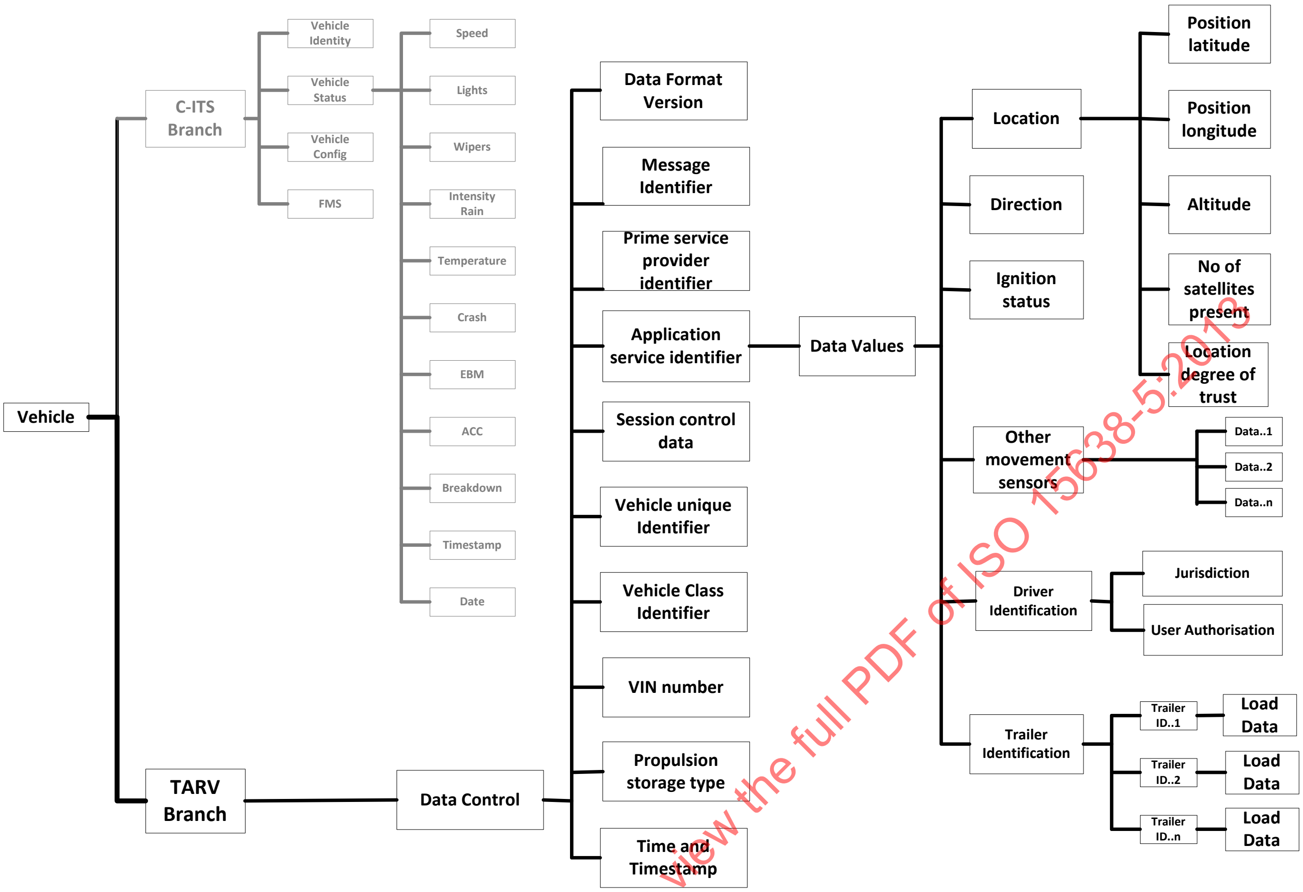

Figure 8 — TARV local data tree

7 System requirements

7.1 Communications requirements

TARV-ROAM communications layers shall conform to ISO 15638-2.

7.2 TARV-ROAM Security requirements

TARV-ROAM security aspects shall conform to ISO 15638-4.

7.3 TARV-ROAM facilities layer requirements

TARV-ROAM facilities layer functions shall conform to:

- ETSI TS 102 894 Intelligent Transport System (*ITS*); Users & Applications requirements; Facility layer structure, functional requirements and specifications.
- ETSI TS 102 890-1 Intelligent Transport Systems (*ITS*); Facilities layer function; Communication management specification.
- ETSI TS 102 890-2 Intelligent Transport Systems (*ITS*); Facilities layer function; Services announcement specification.

Any *TARV-ROAM* local dynamic map specifications shall conform to EN 302 895 'Intelligent Transport Systems (ITS);Vehicular Communications;Basic Set of Applications; Local Dynamic Map (LDM) Specification'.

7.4 7Host management centre (HMC) requirements

The *HMC* shall operate in compliance with the basic Java bundle that includes a management agent. See http://www.osgi.org/javadoc/r4v42/org/osgi/service/provisioning/ProvisioningService.html, together with the process devised by CVIS, to automate and secure this process. These extra additional Java classes are found in:

http://www.itscommunity.eu/cvisproject/download/Deliverables/DEL_CVIS_3.4_Final_Architecture_and_System_Specifications_v1.0.pdf

(Chapter 3.1).- See Annex B.

8 Generic vehicle data requirements

8.1 Data provision

8.1.1 Location of on-board data

On-board data calculated or obtained by the *IVS* shall be stored as individual data concept values in the 'data pantry' defined in ISO 15638-1.

Apps shall be provided by the prime *service provider* [4.15], *application service* [4.2] providers and *jurisdictions* [4.9] to the *IVS* and shall be stored in the non-volatile memory in an 'application library'. This is described as a function and the physical manifestation shall be a function of product design, not standardisation.

The' Host Management Centre'/execution environment shall host and run the *apps*.

TARV data shall be calculated by *apps* in the on-board data library, and stored as discrete data concept values in the 'data pantry'. The frequency of such updates is determined by the app.

The means by which data is collected shall be at the determination of the prime *service provider* [4.15], but shall be capable to meet the relevant requirements of 8.3.

The specifications shown in this part of ISO 15638 are shown below in semantic representation. Data presentation shall be as determined in ISO 15638-2 (Common platform parameters using CALM).

The real position of the element in the data-stream is defined by the ASN1 definition. Such elaboration should be provided by the *jurisdiction* [4.9] or its agent (in conformance to ISO 15638-2).

Example ASN.1 definitions may be provided in ISO 15638-6 and ISO 15638-7.

It should therefore be noted that data elements therefore do not necessarily start or end on a byte boundary.

8.1.2 Naming of 'Apps'

An '*App'* is created by or to the instruction of a *jurisdiction* [4.9] to obtain data from the vehicle (`CoreData`).

The *App* name shall always be the IPv6 address of the destination that the data creates is to be sent.

As IPv6 addresses are unique, this means that multiple '*Apps'* can be safely sent to the on-board '*Apps'* library by multiple parties (who are unaware of each other) and can be stored in the on-board '*Apps'* library without fear of naming conflicts.

It also provides additional security for `CoreData` over and above that provided by ISO 15638-4.

8.1.3 Local data trees

Additional *apps* in the library shall be provided by the prime *service provider* [4.15] and shall collate the data into two collated data concepts:

a) TARV LDT values
b) C-ITS LDT values

8.1.4 C-ITS LDT

See Figure 7 above.

The *C-ITS* (co-operative intelligent transport systems) *LDT* [4.10] *basic vehicle data* [4.4] is focussed to the requirements for cooperative intelligent transport systems for all classes of vehicle, and is safety application centric.

For the interoperability and efficient operation of cooperative safety services (for example collision avoidance; ice, fog and obstacle alerts; incident warnings; etc.), the *basic vehicle data* [4.4] available needs to be the same for all vehicles, of whatever class.

The data content of the *C-ITS LDT* [4.10] shall therefore be as determined in a future standard to be developed by ISO or ETSI.

Apps from the on board *Apps* library shall therefore update the data concepts in the 'data pantry' and the *C-ITS-LDT* [4.10] either at frequencies specified in that Standard, or as determined by the *app*. Where not predetermined by the standard, the means by which, and frequency at which, that data is populated and refreshed shall be determined by the app installed in the app library by the prime *service provider* [4.15] or *application service* [4.2] provider and is not determined in this part of ISO 15638, but the form of the data stored in the data pantry, and the access rights, shall be as determined in ISO 15638-4, and a future standard to be developed by ISO or ETSI in respect of the final data payload of the *C-ITS LDT* [4.10].

8.1.5 TARV LDT

See Figure 8 above.
The *TARV LDT* [4.10] is focussed on the specific requirements for the provision of application services to regulated commercial vehicles.

TARV LDT [4.10] *basic vehicle data* [4.4] shall consist of at least the data specified in Clauses 8.3 and stored in the 'data pantry' in formats specified in these subClauses.

The scope of this section is to define core generic *basic vehicle data* [4.4] provision to *application service* [4.2] providers to be supported by *in-vehicle system* [4.7] (*IVS*) for cooperative telematics applications for *regulated commercial freight vehicles* [4.14] (*TARV*). This data shall be represented in the *TARV LDT* [4.10]. 8.3 below provides specification of the data concepts. 8.4 provides the organisation within the *TARV LDT*.

While specific application services, both regulated and commercial, will have their own application specific requirements for data provided by the *IVS* or harvested by the *IVS* from connected equipment and instruments, some generic data is required by many, if not most, and in some cases all, *TARV* application services. (*basic vehicle data* [4.4] for all classes of vehicles for safety and other cooperative intelligent transport systems is specified in the *C-ITS-LDT* [4.10] defined in 8.1.4 above).

It is therefore required that, while not designing the functionality or physical form of any *IVS* (which is considered a function of the marketplace or *jurisdictions* [4.9] who are regulating in order to implement), the generic information known within the ISO 15638 suite of standards deliverables as '*TARV basic vehicle data* [4.4] ', shall be supported by all *TARV IVSs*:

(for example, shall have a unique identifier, collect time and location data, etc.)

Apps from the on board *apps* library shall update the data concepts in the 'data pantry' and the *TARV-LDT* [4.10] either at frequencies specified in this part of ISO 15638, or as determined by the *app*. Where not predetermined by this part of ISO 15638, the means by which, and frequency at which, that data is populated and refreshed shall be determined by the app installed in the app library by the prime *service provider* [4.15] or *application service* [4.2] provider, and is not determined within this part of ISO 15638, but the form of the data stored in the data pantry for these data concepts shall be as determined within this Clause 8 (this Clause), and the access rights, shall be as determined in ISO 15638-4. The app shall also predetermine the IPv6 destination address for the prime *service provider* and *application service* provider(s) for the receipt of data and in the case of '*apps'* to create *core application data* [4.5] the *apps* shall be named as the destination address for the *core application data* (see 8.1.2 above).

Where required, the prime *service provider* [4.15], *application service* [4.2] providers and *jurisdictions* [4.9] can provide new *apps* to the app library on board the *IVS* by the methods described in ISO 15638-1, this part of ISO 15638 (ISO 15638-5), and its referenced standards.

This part of ISO 15638 therefore provides the specifications for generic *basic vehicle data* [4.4] that it is required for all *TARV IVSs* to support and make available to *application service* [4.2] providers via a wireless communications link supported by the *IVS*, in order to support the provision of regulated and commercial application services. This is achieved through the *TARV local data tree* [4.10] (*LDT*).

Some further data concepts, while not required in all cases for every *TARV* in every *jurisdiction* [4.9], 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 *TARVs*. A number of these data concepts, which are expected to frequently be required are, for reasons of interoperability, defined within this part of ISO 15638 (Clause 9) to provide the *core application data* [4.5] concept.

8.1.6 Recent data archive

A further app shall be provided by the prime *service provider* [4.15] and shall create an archive of the history and values of data, stored in a file called '`RecentArchive`'.

8.2 Commands for vehicle data

ISO 15638-3 provides for 5 generic commands for use by any application:

1) GET TARV LDT data

2) GET C-ITS LDT data

3) CREATE core application data

4) GET core application data

5) GET Archive

8.2.1 GET TARV LDT data

On receipt of the command '`GETTARVLDT`' the system shall provide the values of the *TARV LDT* [4.10] data concept, together with the requested destination address provided by the requestor, to the previously advised destination address of the requesting *application service* [4.2] provider or *jurisdiction* [4.9]**.** The data shall be sent to no other destination. The *IVS* shall not, under any circumstances, provide data to an address provided at the same time as the request for data, and the *IVS* shall only provide data to previously predetermined addresses. The system shall send an ACK to the requesting address and close the communication with that address immediately.

NOTE By responding to a command by sending the response (data) only to a predetermined IPv6 address, the possible phishing (attempting to acquire information by masquerading as a trustworthy entity) and other unauthorised third party access to the data is significantly reduced.

8.2.2 GET C-ITS LDT data

On receipt of the command '`GETC-ITSLDT`' the system shall make the values of the *C-ITS LDT* [4.10] data concept (specified in this part of ISO 15638) available to authorised users and shall provide the values to the previously advised destination address of the requesting *application service* [4.2] provider or *jurisdiction* [4.9]**.** The data shall be sent to no other destination. It is not allowed to provide a destination address at the time of requesting the data. The *IVS* shall not, under any circumstances, provide data to an address provided at the same time as the request for data, and the *IVS* shall only provide data to previously predetermined addresses.

8.2.3 CREATE core application data

In order to obtain *core application data* [4.5] the *IVS* first has to create that data. There is one single command to create *core application data*, but there may be multiple '*apps'* concurrent in the vehicle whose *core application data* [4.5] is different.

The application therefore first provides the *IVS* system with the destination IPv6 for the *core application data* [4.5].

It then provides the command '`CREATECoreData`'.

On receipt of the command '`CREATECoreData`' the system shall run the previously provided 'app' which bears the same name as the destination IPv6 address (see 8.1.2 above) which will populate the *core application data* [4.5] data concept with the current values of the *TARV LDT* [4.10] together with any additional data concept values specified in the 'app',

and on request (GET CoreData See 8.2.4 below) shall provide the values to the previously advised destination address of the requesting *application service* [4.2] provider or *jurisdiction* [4.9], as determined in the previously uploaded 'app'.

The data shall be sent to no other destination. (i.e. it is not returned to the address of the enquirer conducting the communication session, but is sent via the internet to the previously advised IPv6 address programmed into the previously provided 'app').

core application data [4.5] comprises the *TARV LDT* data defined in 8.1 above, plus the data for any mandated or supported *regulated application service* [4.13] for *TARV* and the IPv6 address (app filename) of the destination address.

Figure 9 shows an example. For explanation of the detail of the content see clauses 8.3, 8.4 and 9 below.

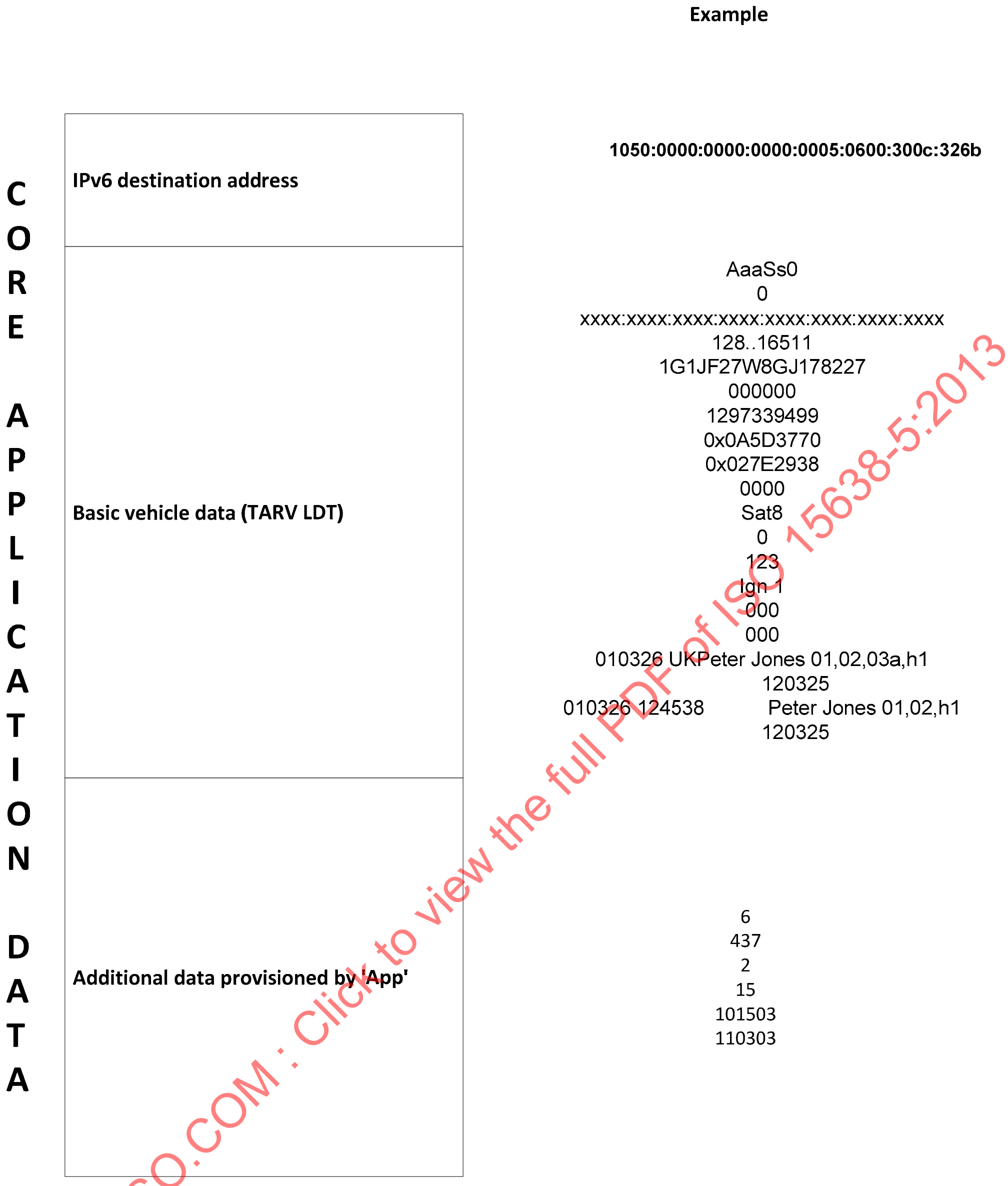
Example
C O R E A P P L I C A T I O N D A T A
IPv6 destination address
1050:0000:0000:0000:0005:0600:300c:326b
Basic vehicle data (TARV LDT)
AaaSs0
0
xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
128..16511
1G1JF27W8GJ178227
000000
1297339499
0x0A5D3770
0x027E2938
0000
Sat8
0
123
Ign 1
000
000
010326 UKPeter Jones 01,02,03a,h1
120325
010326 124538 Peter Jones 01,02,h1
120325
Additional data provisioned by 'App'
6
437
2
15
101503
110303

Figure 9 — Core application data

However, whilst 8.3.1 – 8.3.17 determine the *basic vehicle data* [4.4] that shall be supported by all *IVS* for regulated commercial vehicles in all cases and countries, *jurisdictions* [4.9] may impose additional requirements for additional data, regardless of the *regulated application services* [4.13], that it requires or supports at any point in time. This part of ISO 15638 provides some candidates in Clause 9.

The use of all or any of these candidates in additional to the *TARV LDT* [4.10] to form the *core application data* [4.5] is at the election of the *jurisdiction* [4.9].

The purpose of defining these additional data concepts is to provide international interoperability so that where used, they are used consistently.

It is important to understand that the *core application data* [4.5] field is a transient data concept. There is just one data concept *core application data* [4.5] and it is populated according to the most recent use of the '`CREATE Core application data`' command. This both keeps the application programming simple and uses the limited memory of the *IVS* efficiently.

8.2.4 GET core application data

On receipt of the command ‘GETCoreData’ the system shall send the values of the *core application data* [4.5] data concept (see 8.2.3 above) which has just been provisioned into the CoreData by the ‘CREATECoreData’ command (see 8.2.3 above), together with the requested destination address provided by the requestor.to the previously advised destination IPv6 address of the *application service* [4.2] provider or *jurisdiction* [4.9], The data shall be sent to no other destination. The *IVS* shall not, under any circumstances, provide data directly to an interrogating party, and the *IVS* shall only provide data to the previously predetermined IPv6 address provided by the previously provisioned ‘app’. The system shall send an ACK to the requesting address and close the communication with that address immediately.

NOTE In this way spoof, ‘phishing’ or other fraudulent attempts to access vehicle data are avoided. The only way to get *core application data* [4.5] is via the “GETCoreData’ command and that command can only send the data via the internet to the previously determined IPv6 address. Other security measures, provided by *TARV-ROAM* and ISO 15638-4 (*TARV* system security requirements) prevent the unauthorised loading of ‘*apps’* into the on-board ‘app’ library. Therefore, even if a spoof *application service* [4.2] provider manages to gain access to the *IVS* and successfully conducts a communication session, its attempt to get *core application data* [4.5] will only result in that data being sent to its legitimate destination, not back to the enquirer.

8.2.5 GET Archive

On receipt of the command ‘GETArchive’ the system shall provide the contents of the ‘RecentArchive’ file stored in the non volatile memory of the *IVS* to the IPv6 address previously provided by the prime *service provider* [4.15]. The ‘RecentArchive’ file shall only be accessed by the application or prime *service provider* via the IPv6 address that it has previously provided to the *IVS* and the RecentArchive’ file shall be protected against access in any other way or by any other party whatsoever except during an *IVS* maintenance operation, and then only by the prime *service provider* or his agent. It is not allowed to provide a destination address at the time of requesting the data. The *IVS* shall not, under any circumstances, provide data to an address provided at the same time as the request for data, and the *IVS* shall only provide data to previously predetermined addresses.

On successful receipt of the receipt of the ‘RecentArchive’ data, the prime *service provider* [4.15] shall send an ACK to the *IVS* acknowledging, in the form prescribed in ISO 15638-3, that it has received the data.

On receipt of the ACK by the *IVS*, the *IVS* shall clear the data in the ‘RecentArchive’ file and shall commence to repopulate that file with a record of the clearance of the file in the format yyyymmddhhmmss.

8.3 Presentation of the ‘basic vehicle data’ concept

The definitions shown in this part of ISO 15638 are shown below in semantic representation. Data presentation shall be as determined in ISO 15638-2 (Common platform parameters using CALM).

The real position of the element in the data-stream is defined by the ASN1 definition. It is recommended that such definition is specified by the *jurisdiction* [4.9] or its agent in its downloaded *App*. Example ASN.1 definitions may be provided in ISO 15638-6 and ISO 15638-7.

It should therefore be noted that data elements therefore do not necessarily start or end on a byte boundary.

Basic vehicle data [4.4] shall consist of at least the data 8.3.1- 8.3.16 in this clause, together with the data specified in 8.3.17 if available. The data shall be stored in the data pantry, and as required by *Apps*, shall be used to update the *TARV LDT* [4.10].

8.3.1 Data format version

The ‘data pantry’ of the *IVS* shall:

- carry a data format version identification which shall comprise the three letter country identification code of the *jurisdiction* [4.9] as defined in ISO 3166-1 (Codes for the representation of names of countries and their subdivisions — Part 1: Country codes),

- followed by a two letter identification of the state (or other sub partition of the *jurisdiction* [4.9]) as defined in ISO 3166-2 (Codes for the representation of names of countries and their subdivisions — Part 2: Country subdivision codes) or as determined by the *jurisdiction* if it deems that subdivision not to be appropriate)

- followed by a sequential version number starting from version 1 to discriminate from later *TARV* data formats for that *jurisdiction* [4.9]**.**

- Where there is no subpartition the element may be omitted

EXAMPLES AUSVA1 USACA2 GB1 NL4
(Australia Victoria version 1) (USA California version 2) (Great Britain version 1) (Netherlands version 4)

Later versions shall be backwards compatible with existing versions.

Systems receiving *TARV regulated commercial freight vehicle* [4.14] data concepts shall support all standardised *TARV* versions within that *jurisdiction* [4.9], which are each uniquely identified using the *TARV* data format version parameter, defined herein, which shall always be contained in the first byte of all [current and future] *TARV LDT* [4.10] data concepts.

8.3.2 Message identifier

The ‘data pantry’ of the *IVS* shall carry a message identifier, starting with 1, incremented for each repeated *TARV LDT* [4.10] data transfer attempt until the receipt of the data concept is acknowledged upon which the message identifier reverts to 1.

8.3.3 Prime service provider identifier

The ‘data pantry’ of the *IVS* shall carry the IPv6 address of the prime *service provider* [4.15] (to enable the *IVS* to establish a communication session with the prime *service provider* when required).

The data shall be stored in the format:

PSP ***IPv6 address***
As *PSP* xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
Example: *PSP* 1050:0000:0000:0000:0005:0600:300c:326b
NOTE The preferred format for an IPv6 address is xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx where each x is a hexadecimal digit representing 4 bits. IPv6 addresses range from 0000:0000:0000:0000:0000:0000:0000:0000 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.

An alternative format for IPv6 addresses combines the colon and dotted notation, so the IPv4 address may be embedded in the IPv6 address. Hexadecimal values are specified for the left-most 96 bits, and decimal values are specified for the right-most 32 bits indicating the embedded IPv4 address. This format ensures compatibility between IPv6 nodes and IPv4 nodes when you are working in a mixed network environment.
These two types of IPv6 addresses use this alternative format:

IPv4-mapped IPv6 address
This type of address is used to represent IPv4 nodes as IPv6 addresses. It allows IPv6 applications to communicate directly with IPv4 applications. For example, 0:0:0:0:0:ffff:192.1.56.10 and ::ffff:192.1.56.10/96 (shortened format).

IPv4-compatible IPv6 address
This type of address is used for tunnelling. It allows IPv6 nodes to communicate across an IPv4 infrastructure. For example, 0:0:0:0:0:0:192.1.56.10 and ::192.1.56.10/96 (shortened format).

8.3.4 Application service provider identifier

The ‘data pantry’ of the *IVS* shall carry the IPv6 address for each of the application services to which the user has subscribed (to enable the *IVS* to establish a communication session with the appropriate *service provider* [4.15] when required).

In order to identify the particular application service, the identifier shall additionally provide an *application service* [4.2] programme identifier in addition to the IPv6 address of the *application service* provider.

The *application service* [4.2] program identifier shall be stored in the format specified by IEEE 1609 (*ITS* AID addressing)

```
ITSaid1ext::=CHOICE{
              content   [0]  INTEGER(128..16511), -- contained in two octets of ITSaid
              extension[1]  ITSaid2ext
              }
```

and shall use *API's* issued by an international registration authority.

APIs for generic *regulated application services* [4.13] shall be obtained and issued via provisions made in ISO 15638-6.

For additional *application service* [4.2] provider specific application services, *application service* providers shall be required to register their application with the registration authority and obtain a unique *API* for each *application service*.

The data shall be stored in the format:

AS *API* IPv6 address
As *AS* 00000000 00000000 xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
Example: *PSP* 128..16511 1050:0000:0000:0000:0005:0600:300c:326b

8.3.5 Session control data

Shall be presented as specified in ISO 15628-2 (*TARV*- Common platform parameters using *CALM*) and the media appropriate *CALM* Media standard(s).

The *CALM* media standards at the time of development of this part of ISO 15638 are:

ISO 21210	*Intelligent transport systems — Communications access for land mobiles — IPv6 Networking*
ISO 21212	*Intelligent transport systems -- Communications access for land mobiles (CALM) -- 2G Cellular systems*
ISO 21213	*(CALM) -- 3G Cellular systems*
ISO 21214	*Intelligent transport systems -- Communications access for land mobiles (CALM) -- Infra-red systems*
ISO 21215	*Intelligent transport systems -- Communications access for land mobiles (CALM) -- M5*
ISO 21216	*Intelligent transport systems -- Wireless communications -- CALM using millimetre communications -- Air interface*
ISO 21217	*Intelligent transport systems -- Communications access for land mobiles (CALM) – Architecture*
ISO 21218	*Intelligent transport systems -- Communications access for land mobiles (CALM)-- Medium service access points*
ISO 25111	*Intelligent transport systems -- Communications access for land mobiles (CALM) -- General requirements for using public networks*
ISO 25112	*Intelligent transport systems -- Communications access for land mobiles (CALM) -- Mobile wireless broadband using IEEE 802.16*
ISO 25113	*(CALM) -- Mobile wireless broadband using HC-SDMA*
ISO 29281	*Intelligent transport systems -- Communications access for land mobiles (CALM) -- Non-IP networking*
ISO 29282	*Intelligent transport systems -- Communications access for land mobiles (CALM) -- Applications using satellite networks*
ISO 29283	*ITS CALM Mobile Wireless Broadband applications using Communications in accordance with IEEE 802.20*

ISO 13183 *Intelligent transport systems — Communications access for land mobiles (CALM) — Broadcast communications*

8.3.6 Vehicle unique identifier

The ‘data pantry’ of the *IVS* of the *regulated commercial freight vehicle* [4.14] shall carry a *unique vehicle identification* [4.16]. The *IVS* shall be programmed by the prime *service provider* [4.15] with a file containing the vehicle registration number as defined in ISO 14816 (Automatic Vehicle Identification – Numbering and data structure, Clause4.10 CS4 Vehicle license coding.

```
 CS4 ::= SEQUENCE {
    countryCode
    CountryCode, alphabetIndicator
    AlphabetIndicator, licPlateNumberLicPlateNumber
}
```

8.3.7 Vehicle class identification

The ‘data pantry’ of the *IVS* of the *regulated commercial freight vehicle* [4.14] shall carry a vehicle class identification which shall be elaborated in accordance with ISO 17262 (Intelligent transport systems — Automatic vehicle and equipment identification –Intermodal goods transport numbering and data structures) or ISO 26683-2 (Intelligent transport systems — Freight land conveyance content identification and communication — Part 2: Application interface profiles) or the specific and defined vehicle classification determined by the *jurisdiction* [4.9].

8.3.8 VIN number

The ‘data pantry’ of the *IVS* of the *regulated commercial freight vehicle* [4.14] shall carry the ‘Vehicle Identification (VIN) Number’ according ISO 3779 (Road vehicles -- Vehicle identification number (VIN) -- Content and structure).

World Manufacturer Index (WMI)
Vehicle Type Descriptor (VDS)
Vehicle Identification Sequence (VIS).

As:

1st-3rd digit - World Manufacturer Indicator, ISO 3780	Who made the vehicle
4th-8th digit - Manufacturer Specific	Model of vehicle, engine, bodystyle, etc.
9th digit - Check digit	Mathematical Formula to determine if VIN is real
10th digit – Year	Model year of the vehicle
11th digit - Assembly Plant - Manufacturer Specific	The assembly plant that built the car
12th - 17th digit - Sequence Number	Usually starts at 100001,200002,A0000A, B0000B, etc.

Example: 1G1JF27W8GJ178227

See ISO 24534 for VIN variant provisions

8.3.9 Propulsion storage type

The ‘data pantry’ of the **IVS** shall carry an identification of the type of vehicle energy storage(s) present. For each storage type the following coding applies:

false = indicates a type of storage not present

true = indicates type of storage which is present

The following storage types are supported:

- Gasoline tank
- Diesel tank
- Compressed natural gas (CNG/LNG)
- liquid propane gas (LPG)
- Electric energy storage
- Hydrogen storage

All bits shall be set to zero to indicate an unknown or other type of energy storage.

NOTE This information may be unreliable if there has been a change of vehicle propulsion type (e.g. from gasoline to CNG).

NOTE More than one bit may be set if there is more than one type of energy storage present.

8.3.10 Time and timestamp (UTC sec)

The 'data pantry' of the *IVS* shall carry a timestamp of first transmission of any specific communication of data from the *regulated commercial freight vehicle* [4.14] to the *jurisdiction* [4.9] or its agent using the *IVS* via a wireless network.

As seconds elapsed since midnight January 1st, 1970 *UTC*.

Failure value for time stamp set to "0".

The date and time shall be stored with a resolution of 1 second.

8.3.11 Location

8.3.11.1 General

The 'data pantry' of the *IVS* shall carry a location of the vehicle which shall be regularly updated and shall be in a format shall be as determined in WGS84. The frequency of update is not defined in this part of ISO 15638 and may be a feature of product design or regulation of the *jurisdiction* [4.9]**.**

It shall be at the responsibility of the *IVS* provider to determine how the location data is established.

The confidence bit is only used for an eCall message.

For error estimation in TARV see 8.3.12.

Latitude and longitude

±DD.DDDD±DDD.DDDD	degrees
±DDMM.MMM±DDDMM.MMM	degrees and minutes
±DDMMSS.SS±DDDMMSS.SS	degrees, minutes and seconds
+DD > +00	north latitudes
+DD = +00	equator
-DD < +00	south latitudes
+000 < +DDD < +180	east longitudes
+000 = +DDD	prime meridian
-180 < -DDD < +000	west longitudes
-180 = -DDD	180th meridian

In the event of interruption to and subsequent reacquisition of *GNSS* satellite signals, the *IVS GNSS* receiver shall on the reacquisition of *GNSS* satellite signals, commence to collect and store vehicle position:

a) if the interruption is for a period of less than seven days, within 60 seconds of reacquisition of *GNSS* satellite signals; and

b) if the interruption is for a period of seven days or more, within five minutes of reacquisition of *GNSS* satellite signals.

Altitude

The representation of altitude is optional. The unit is the metre unless the foot is specified. As:
+mmmm ≥ 0000
-mmmm <0000

Examples
Paris +48.52+002.20/
Eiffel Tower +48.8577+002.295/
Statue of Liberty +40.6894-074.0447/
Mount Everest +27.5916+086.5640+8850/
North Pole +90+000/
South Pole -90+000+2800/

8.3.11.2 Position latitude

8.3.11.2.1 Position latitude shall be as determined in WGS84.

Units: Miliarcsec
Value range (-324000000 to 324000000)

Maximum value Latitude = 90°00'00.000" = 90*60*60.000" = 324000.000" = 324 000 000 Miliarcseconds
= 0x134FD900

Minimum value Latitude = -90°00'00.000" = -90*60*60.000" = -324000.000" = -324 000 000 Miliarcseconds
= 0xECB02700

EXAMPLE 48°18'1.20" N = 48.3003333 lat= (48*3600)+(18*60)+1.20}'' = 173881,200''
which encodes to the following value:
= 173881200d = 0x0A5D3770

If latitude is invalid or unknown, the value 0x7FFFFFFF shall be transmitted

8.3.11.2.2 The latitude position calculated by the *IVS GNSS* receiver shall not deviate by more than 13 metres from the absolute horizontal position country average for 95% of the observations when using at least four satellites and a 'Horizontal Dilution of Precision' of < 4.

8.3.11.2.3 The resolution of the stored latitude position calculated by the *IVS GNSS* receiver shall be to 1 degree or better.

8.3.11.2.4 The longitude position calculated by the *IVS GNSS* receiver shall not deviate by more than 13 metres.

8.3.11.3 Position longitude

8.3.11.3.1 Position longitude shall be as determined in WGS84.

Units: Miliarcsec

Value range (-648000000 to 648000000)

Maximum value Longitude = 180°00'00.000" = 180*60*60.000" = 648000.000" = 648 000 000 Miliarcseconds= 0x269FB200

Minimum value Longitude = -180°00'00.000" = -180*60*60.000" = -648000.000" = -648 000 000 Miliarcseconds= 0xD9604E00

EXAMPLE. 11°37'2.52" E = 11.6173666 long= (11*3600)+(37*60)+2.52}'' = 41822.520''
which encodes to the following value:
= 41822520d = 0x027E2938

If longitude is invalid or unknown, the value 0x7FFFFFFF be used:
res from the absolute horizontal position country average for 95% of the observations when using at least four satellites and a 'horizontal dilution of precision' of < 4.

8.3.11.3.2 The resolution of the stored longitude position calculated by the *IVS GNSS* receiver shall be to 1 degree or better.

8.3.11.3.3 The longitude position calculated by the *IVS GNSS* receiver shall not deviate by more than 13 metres.

8.3.11.4 Position altitude

Position altitude shall be as determined in WGS84.

Units: Metre (unless foot is specified by the *jurisdiction* [4.9])
+mmmm ≥ 0000
-mmmm <0000

Where altitude data is not available, 0000 shall be provided.

8.3.11.5 Number of satellites present

When providing or recording location data the *IVS* shall also record and present the number of satellites present during the calculation in the format:

Sat*N*

Where *N*= the number of satellites present

Example Sat8

8.3.11.6 Location/direction degree of trust

This confidence bit is only used for an eCall message.
For error estimation in TARV see 8.3.12.

8.3.12 Error estimation (covariance matrix)

Error estimation of location is calculated within GNSS by a Kalman filter (described in ISO 15638-1).

By taking the sources available, both from the GNSS and other on-board equipment an error estimate, known as a 'covariance matrix) can be established.

This part of ISO 15638 does not interpret the significance of the values in the covariance matrix, as these will vary according to the context. Such interpretation is deemed to be calculated by the relevant system of the application service provider.

This part of ISO 15638 determines the format of the covariance matrix data.

How the data is calculated is a matter for system design, subject to it being consistent with the mathematical concepts of the Kalman filter. Figure 10 shows how the covariance matrix is calculated

NOTE The Kalman filter utilises control inputs to the system, and measurements (such as from sensors) to form an estimate of the system's varying quantities (its state) that is better than the estimate obtained by using any one measurement alone. It can be described as a common sensor fusion algorithm.

The inputs to a Kalman filter are measurements of system inputs and outputs and statistical parameters such as the input process and measurement noise covariance matrices, and the outputs of the filter are (optimal) estimates of the state variables and an estimate of the covariance matrix of the estimation error of the state vector. The advantage (and reason for longevity of the Kalman filter) is that under a rather loose set of conditions, the estimates are provably optimal; that is, they are the best that you can do with the information you have.

All measurements and calculations based on models are estimates to some degree. Noisy sensor data, approximations in the equations that describe how a system changes, and external factors that are not accounted for introduce some uncertainty about the inferred values for a system's state. The Kalman filter averages a prediction of a system's state with a new measurement using a weighted average.

The weights are calculated from the covariance, a measure of the estimated uncertainty of the prediction of the system's state, and may be described as a linear quadratic estimation. The result of the weighted average is a new state estimate that lies in between the predicted and measured state, and has a better estimated uncertainty than either alone. The Kalman filter works recursively and requires only the last "best guess" - not the entire history - of a system's state to calculate a new state.

The state estimate and covariances are coded into matrices to handle the multiple dimensions involved in a single set of calculations. This allows for representation of linear relationships between different state variables (such as position, velocity, and acceleration) in any of the transition models or covariances.

This data field shall comprise a variable length data object (because the number of states in the kinematic state vector can vary) to contain the covariance matrix of the estimation error of the kinematic state (and possibly other relevant parameters), recorded within a two byte data concept. The means by which the data is obtained and interpreted shall be a matter of system design, and is not standardised to enable best performance of available data and improvement over time as data sources improve.

The recorded and transmitted covariance matrix data object shall contain a state vector ID which will identify the number of states (N) and their meaning, followed by N variance values (square-roots of the diagonal elements D of the covariance matrix R), followed by the N(N-1)/2 single precision (2-octets each max) non-zero values of the lower triangular matrix L, where R = LDL.

NOTE Thus, the number of elements to be stored is N(N+1)/2 and two bytes should be sufficient for at least N(N-1)/2 of them. The encoding of the N diagonal elements will depend on the choice of units for the state variables and whether or not dynamic scaling is used.

All covariance matrices are positive semi-definite meaning that that one can propagate (calculate directly) a square-root of the covariance matrix rather than the matrix itself which saves a factor of two in the number of octets required to achieve a given precision

The final data shall be transmitted in 4 bytes, with any unused bits as padded zeros.

8.3.13 Direction of travel

The *IVS* shall determine direction of travel of the vehicle in WGS84 or GDA94.

The direction of travel determined by the *IVS GNSS* receiver shall not deviate from the actual direction of travel by more than 4 degrees for 95% of the observations when using at least four satellites and a horizontal dilution of precision of < 4.

The resolution of direction of travel determined by the *IVS GNSS* receiver and recorded by the *IVS* shall be to 1 degree or better.

The ‘data pantry’ of the *IVS* shall store the identification of direction of travel of the vehicle which shall be regularly updated and shall be in a direction of travel in 2°-degrees steps from magnetic north (0– 358, clockwise).

If direction of travel is invalid or unknown, the value 0xFF shall be used.

The frequency of update is not defined in this part of ISO 15638 and may be a feature of product design or regulation of the *jurisdiction* [4.9].

The requirement to provide data in the form prescribed in this subClause is an operational requirement; however the means of calculating the direction of travel shall be at the discretion of the *IVS* provider.

The current vehicle heading value shall represent the vehicle's real direction of travel; random fluctuations of *GNSS* signals shall not affect the value sent.

Manufacturers of *IVS* shall ensure that, except where the objective of a *regulated application service* [4.13] is the monitoring or reporting of speed, the information provided in the recent location parameters is not sufficient for this information to be used for determining vehicle speed, the means to ensure this are not defined within this part of ISO 15638.

8.3.14 Ignition status

When providing or recording location data the *IVS* shall also record and present the status of the vehicle ignition (on / off / disconnected) as:

Ign 1/0/d

Where 1=on, 0=off, d=disconnected.

8.3.15 Other movement sensors

When providing or recording location data, the *IVS* shall also record and present the status of any other independent movement sensors present (movement/no movement/disconnected) as:

S (sensor number) Mvt m/n/d

Where m=movement, n=no movement, d=disconnected.

8.3.16 IVS identification

The functionality known within the ISO 15638 suite of standards as the *IVS* (*in-vehicle system* [4.7]) may be performed by a single *on-board unit* [4.11] (*OBU*) or a combination of equipment installed on-board within different locations.

Nonetheless, whatever the configuration, it performs the functionality of the *IVS* as defined in the relevant ISO 15638 standards deliverable, or combination of ISO 15638 standards deliverables.

For some *TARV* application services it is required or desirable to identify the *IVS* uniquely and unambiguously, and an 'app' in the facilities layer shall provide an' **IVS**ID' file in the data pantry of the *IVS* that shall contain a unique and unambiguous identification of the *IVS*.

NOTE The unique identification of the *IVS* is not the same as the unique identification of the vehicle, and a vehicle, through its working life may have its *IVS* replaced or updated or changed in a material way in order to accommodate new requirements for additional application services. Additionally, in a situation where both the prime mover and one or several trailers each have their own *IVS*, there may be multiple *IVS* assigned to a single vehicle on any journey.

The *IVS* identification shall be unique and unambiguous and shall be permanent so long as the functionality of the *IVS* remains the same. Any material change to the function of the *IVS*, be that accommodated in one *OBU* or several equipments, other than extension of the memory of the *IVS*, shall create a new *IVS* and it shall be given a new identity.

Registration procedures including the structures that are with National issuing authorities are mandatory for this structure. Provisions for registration can be found in Annex A (normative) of ISO 14816 (also reproduced as Annex A of this part of ISO 15638).

The identity shall be consistent to ISO 14816 CS1 (Clause 4,7 of ISO 14816) and shall provide an unambiguous identification element of 56 bits (PER encoding) as:

8.3.16.1 ISO 14816 CS1 definition (IVS identification data concept)

```
 CS1 ::= SEQUENCE {
      countryCode                CountryCode,                    issuerIdentifier
                                 IssuerIdentifier,                 serviceNumber
                                 ServiceNumber
      }
```

8.3.16.2 Country code definition

```
CountryCode ::= BIT STRING(Size(10))
 -- Value assignment is done in accordance with ISO 3166 and by using
 -- the ITA.2 alphabet. For value assignment, please refer to
 -- http://www.nni.nl/cen278/14816_NRAI_register_by_country.html
```

8.3.16.3 Issuer identifier definition

```
IssuerIdentifier ::= INTEGER(0 .. 16383)
```

Refer to Annex A of the current version of ISO 14816 for registration.

NOTE the version current at the time of publication of this part of ISO 15638 is reproduced as Annex A of this part of ISO 15638 for the convenience of the reader.

8.3.16.4 Service number definition

```
ServiceNumber ::= BIT STRING(Size(32))
```

8.3.17 Manufacturer identification

Where a manufacturer wishes to include its own unique identity (largely for batch identification and quality of service purposes, it may use this option in addition to, but not in place of the *IVS* unique identification defined in 8.3.15.

Manufacturer identification of *OBU's* used as all or part of the *IVS* shall be in accordance with ISO 14816 CS2 (Clause 4.8 of ISO 14816).

'Manufacturers Numbering' enables manufacturers to provide, if they so choose, a numbering system that is independent of a particular country. It is expected that this numbering scheme will primarily be used as an electronic serial number in systems requiring direct knowledge of manufacturer and equipment versions (e.g. for QA/QC purposes). This number may also be used as a cryptographic hidden identity in systems with a combination of anonymity and strong security requirements.

The structure defined in ISO 14816 details the content of the manufacturers numbering data 'primitive' and is to be read in conjunction with the notes shown below the structure.

Registration procedures are similar to the procedures of CS1, with the exception that the structures are not registered with any National Issuing Authority. Provisions for registration can be found in Annex A (normative) of ISO 14816.

The Numbering Scheme views the ID as a data element, and the common basic data structure is only a data identifier code.

As:

8.3.17.1 CS2 definition (manufacturer identification data concept)

```
CS2 ::= SEQUENCE {
issuerIdentifier                    ManufacturerIdentifier,  serviceNumber
ServiceNumber
}
```

8.3.17.2 Manufacturer Identifier definition

```
ManufacturerIdentifier ::= INTEGER(0 .. 65535)
```

8.3.17.3 Service number definition

`ServiceNumber` is defined in 8.3.15.4.

8.3.18 Driver(s) identification

The ‘data pantry ’of the *IVS* shall record the identification of each and every driver of the vehicle.

The drivers’ identification is in two parts, the first part (*jurisdiction* [4.9] identification) is mandatory and shall be the current drivers driving licence number, and the second identification (user authorisation) is optional at the discretion of the *jurisdiction* [4.9], or the user, as appropriate.

NOTE Driver identification is considered essential ‘vehicle’ data as it shows who is in control of the vehicle at any point in time. It may also be required for applications not directly connected with any driver monitoring application service

NOTE This implies that the *IVS* shall have the capability to record the identification of the driver of the vehicle each and every time that the ignition is turned on, or when drivers change during a journey (even if the ignition is not switched off at the point of change of driver.(See ISO 15638-3).

NOTE The means of capturing the driver driving licence is not specified within this part of ISO 15638, but should be a design parameter for both *jurisdictions* [4.9] and equipment manufacturers. The driver of a vehicle will change frequently. In many cases a vehicle is sent on a journey with two drivers, who rotate in order to abide with driving hours regulations. Careful attention should be given to this aspect. However, the types of driving licence vary greatly around the world, as do their physical formats. Where the driving licence regime of the *jurisdiction* does not support an easily machine readable format the *jurisdiction* may wish to consider providing *regulated commercial freight vehicle* [4.14] drivers with a barcode or an RFID or USB device that can be quickly machine read. Other aspects that a *jurisdiction* may consider are facial recognition techniques (such as those commonly found on personal computers), or iris recognition, to assure that the driver matches the driving licence number provided. At this point in time these aspects have to be determined by each *jurisdiction*, and bilateral agreements made for cross border journeys.

The driver’s driving licence number shall be provided each time a new/replacement driver takes the wheel to drive the vehicle. The means for capturing that data is not determined in this part of ISO 15638.

The format of the driver identification is in two parts:

a) Jurisdiction identification
b) User authorisation

8.3.18.1 Jurisdiction identification

The *jurisdiction* [4.9] identification shall be the driver license identification shall be stored in the format:

Issue date Issuing *jurisdiction* [4.9] Driver name Vehicle classes Expiry date

The vehicle classes that a driver is licensed to drive to be listed in alphanumeric form as determined by the issuing *jurisdiction* [4.9]**.** Listed in sequence as shown on the driving license, with classes separated by a comma.

Issue and expiry date to be listed in yymmdd format.

EXAMPLE

010326	UK	Peter Jones	01,02,03a,h1	120325

8.3.18.2 User authorisation

User authorisation of the driver may or may not be required at the discretion of the *jurisdiction* [4.9], or the user. If not required, 000000 shall be recorded.

User authorisation of the driver may be required where, for example for insurance reasons, a driver, though technically licensed to drive a class of vehicle by the *jurisdiction* [4.9], may need additional experience and training to haul a particular type of load, such as dangerous chemicals or abnormal loads etc.

Where required, the driver user authorisation shall be stored in the format:

Issue date	Issuing organisation	Driver name	vehicle classes	Expiry date

Vehicle classes to be listed in alphanumeric form in the same formats as the driving license. Authorised vehicle classes listed in sequence as shown on the driving license, with classes separated by a comma.

The issuing organisation to be the company registration number or employer registration number that is unique within the *jurisdiction* [4.9], as determined by the *jurisdiction***.**

Issue and expiry date to be listed in yymmdd format.

EXAMPLE

010326	124538	Peter Jones	01,02,h1	120325

8.3.19 Trailer identification

The ‘data pantry’ of the *IVS* shall carry an identification of each of its trailers (if any) in a format In accordance with ISO 17262 CS9 (Clause 7.3).

8.3.20 Load data

The ‘data pantry’ of the *IVS* shall, whenever possible, carry a profile of the load of the vehicle/ each trailer in a format of one of the profile options specified in ISO 26683-2 (Intelligent transport systems — Freight land conveyance content identification and communication — Part 2: Application interface profiles).

8.4 Organisation of the TARV LDT

LDT [4.10] data shall be transferred within the security and communication provisions of ISO 15638-4 and ISO 15638-2. Data presentation aspects at the point of transfer of the *LDT* [4.10] data concept are dealt with within those standards deliverables and are not specified herein.

As data shall be transferred using ASN.1 PER (ISO 8824 (Parts 1-4)/8825) the form of presentation defined herein is semantic. The actual data presentation shall be as required by ISO/IEC 8825-2, Information technology — ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)

TARV LDT [4.10] data shall be presented as in Table 1:

Table 1 — TARV LDT Data

Concept name	Concept format	Concept semantic content	Clause Ref	Delimiter
DataFormatVersion	AaaSs*0*	Country, Subpartition, Version	8.3.1	;
MessageIdentifier	*0*	Send attempt number	8.3.2	;
PrimeServiceProviderIdentifier	xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx	IPv6 address	8.3.3	;

ApplicationServiceProviderAddress	ITSaid1ext::=CHOICE{
	content [0] INTEGER(128..16511), -- contained in two octets of ITSaid
	extension [1] ITSaid2ext
	}
	And shall use **APIs** issued by an international registration authority.
			8.3.4	;

SessionControlData		As specified in ISO 15638.2 for specific media	8.3.5	;

VehicleUniqueIdentifier	Registration number of the regulated commercial vehicle	vehicle registration number as defined in ISO 14816 (Automatic Vehicle Identification – Numbering and data structure, Clause4.10 CS4 Vehicle license coding:
		CS4 ::= SEQUENCE {
		countryCode CountryCode,
		alphabetIndicator AlphabetIndicator,
		licPlateNumberLicPlateNumber
		}
			8.3.6	;

VehicleClassIdentifier	51	As specified in ISO 24534 Clause 5.5.1 (ISO 3833 vehicle type)	8.3.7	
VinNumber	*1G1JF27W8GJ178227* See ISO 24534 for VIN variant provisions	World Manufacturer Index (WMI) Vehicle Type Descriptor (VDS) Vehicle Identification Sequence (VIS) 1st-3rd digit - World Manufacturer Indicator, ISO 3780 Who made the vehicle 4th-8th digit - Manufacturer Specific Model of vehicle, engine, bodystyle, etc. 9th digit - Check digit Mathematical Formula to determine if VIN is real 10th digit – Year Model year of the vehicle 11th digit - Assembly Plant - Manufacturer Specific The assembly plant that built the car 12th - 17th digit - Sequence NumberUsually starts at 100001,200002,A0000A, B0000B, etc.	8.3.8	;
PropulsionStorageType	000000	0 nonpresence or 1 presence Gasoline;Diesel;CNG;LPG;Electric;Hydrogen	8.3.9	;
Time&Timestamp	1297339499	*UTC* seconds since 1970/01/01	8.3.10	;
Location	0x0A5D3770 0x027E2938 0000 Sat8 *0*	Latitude, Longitude, Altitude, No of satellites present, Trust (true/false)	8.3.11	;
Error Estimation (covariance matrix	00000000 00000000 00000000 00000000	4 bytes, installed equipment specific value	8.3.12	

Concept name	Concept format	Concept semantic content	Clause Ref	Delimiter
`DirectionOfTravel`	123	0-358 degrees clockwise	8.3.13	;
`Ignition`	Ign 1/0/d	On/off/disconnected	8.3.14	;
`OtherMovementSensors`	S (sensor number) Mvt m/n/d S (sensor number) Mvt m/n/d	Sensor number Mvt m/n/d Where m=movement, n=no movement, d=disconnected.	8.3.15	;

`IVSIdenification`	BIT STRING (Size(10);
	Integer (0-13683);
	BIT STRING (Size(32);
		ISO 148816 CS1 definition;
		Country code definition;
		Issuer Identifier definition
			8.3.16	;

`ManufacturerIdentification`	INTEGER (0..65535)	ISO 14816 Manufacturer identifier	8.3.17	;
`DriverIdentification`	010326 UKPeter Jones 01,02,03a,h1 120325 010326 124538 Peter Jones 01,02,h1 120325	*Jurisdiction* [4.9];User J=alphanumeric form as determined by the issuing *jurisdiction*. Listed in sequence as shown on the driving license, with classes separated by a comma. U= Issue date Issuing organisation Driver name vehicle classes Expiry date	8.3.18	;
`TrailerIdentification`		In accordance with ISO 17262 CS9	8.3.19	;
`LoadData`		One of profile options specified in ISO 26683-2	8.3.20	;

The recipients of the *TARV LDT* [4.10] are *application service* [4.2] providers and *jurisdictions* [4.9].

The data content of *TARV LDT* [4.10] is self identifying in respect of vehicle identification and instance, and needs no specific titling. The implementer is free to use its own internal conventions for internal purposes to distinguish between multiple instances of *TARV LDTs* for internal use.

As part of security and privacy provisions, the prime *service provider* [4.15] or the application provider recipient of a *TARV LDT* [4.10] shall not pass this data concept to any third party whatsoever other than the user to whom it is contracted to provide the *application service* [4.2] or as specified by its contract with the user.

As part of security and privacy provisions, any *jurisdiction* [4.9], who is the recipient of a *TARV LDT* [4.10] shall not pass this data concept to any third party whatsoever other than the user except in the pursuance of legal action by the *jurisdiction* in which case the provisions of the legislation under which such action is being taken shall determine the rules of access to the *TARV LDT* [4.10] data.

9 Additional data provision options for ‘core application data’ and regulated applications

9.1 General

It is assumed within this part of ISO 15638 that a *jurisdiction* [4.9] is responsible to decide the data that it requires from a regulated commercial vehicle when that vehicle is operating within its *jurisdiction*.

Basic vehicle data [4.4] that is always available for *TARV* application systems, and *basic vehicle data* for cooperative intelligent transport systems of all classes of vehicles (for safety and other cooperative intelligent transport systems), are specified in Clause 8 above. The *basic vehicle data* [that shall be supported by all *IVS* for regulated commercial vehicles in all cases and countries is stored in the *TARV LDT* [4.10].

But *jurisdictions* [4.9] may impose additional requirements for additional data, regardless of the *regulated application services* [4.13], or to support its instantiation of a *regulated application services* that it requires or supports, at any point in time.

Specific application services, both regulated and commercial, will have their own application specific requirements for data provided by the *IVS* or harvested by the *IVS* from connected equipment and instruments, and these will be specified in the specific *application service* [4.2] specification. They will obtain this by using an app to obtain the *TARV LDT* [4.10] together with data generated by *apps* for the onboard aspects of the regulated service provision, which will be stored in the data pantry with restricted access rights to the app for the *regulated application services* [4.13]**.** This can be provided by ‘push’ from the on-board app, or ‘pull’ from the *application service* providers app providing the *application service*.

Basic vehicle data [4.4] ' will therefore be found in the main branch of the *LDT* [4.10] of all equipped *TARVs*, while *core application data* [4.5] will be found in the data pantry of all equipped *TARVs* (or class of *TARVs*) when they are within a particular *jurisdiction* [4.9], and added to a purpose designed ’side-branch’ of the *LDT* by an app provided or approved by the *jurisdiction* requiring the data.

Like the additional data required by different *jurisdictions* [4.9], some of these additional data concepts will be specific to one particular application service, others, although not required by all or most application services (and therefore not in the *TARV LDT* [4.10]), may be required by several or many application services.

There is therefore also a class of data which is not ‘basic vehicle’ in that it must always be provided to all *jurisdictions* [4.9]/applications, but may be frequently required by multiple applications/*jurisdictions*. This is the data that fills the information gap between ‘basic vehicle’ (provided to all applications) data and the *core application data* [4.5] required by a *jurisdiction*, or for a class of *TARV* within a *jurisdiction*, in order for the *jurisdiction* to achieve its regulation of *TARVs*.

Whether to service the provision of an *application service* [4.2] or to meet the requirements of a *jurisdiction* [4.9], where a data concept is to be used by multiple applications, it is logical and judicious, in order to maximise interoperability and reuse, that such data concepts, while not required for all applications, have common definition.

Populating that side-branch and or individual data concepts in the data pantry shall be ordered and effected by the app provided or approved by the *jurisdiction* [4.9] requiring that:

- The local *jurisdiction* shall specify its data requirements in an ‘*App’* that is normally downloaded as the vehicle enters the *jurisdiction* (or may be provided by the *jurisdiction* in advance of the journey);
- The *jurisdiction* shall be responsible to ensure that the ‘*App’* is both achievable and up to date;
- The ‘*App’* shall draw the *basic vehicle data* [4.4] from the *TARV LDT* [4.10]; and
- The ‘*App’* shall obtain the additional data to be added to the *core application data* [4.5] from the data pantry

thus providing the *jurisdiction* [4.9] with the information that it requires.

Figure 9 (above) shows a hypothetical example of *core application data* [4.5].

It is important to understand that the app provided by the *jurisdiction* [4.9] only demands the data. A separate on-board app usually provided by the *application service* [4.2] provider, and not shared with the *jurisdiction*, is responsible to calculate the data (although in some circumstances the *jurisdiction* may provide such a ‘standard’ app to the *application service* provider). Thus, for example, in obtaining data on direction of travel, the *jurisdiction* only receives the result of the calculation. The calculation will probably be made from data collected from several recent vehicle locations, but the *jurisdiction* does not receive the ‘raw’ data behind the calculation, and is therefore not able to use that data for another purpose (for example calculating vehicle speed from several time and location combinations). If the *jurisdiction* requires speed data it must request it directly.

It is also important to understand that instigating the command ‘`GETCoreData`’ results in that data being sent only to a previously determined IPv6 address. For security, it is never returned to the enquirer.

The use of all or any of the candidates in 9.2 below in additional to the *basic vehicle data* [4.4] to form the *core application data* [4.5] is at the election of the *jurisdiction* [4.9].

The purpose of defining these additional data concepts is to provide international interoperability so that where used, they are used consistently.

9.2 provides some candidates for such data concepts that are likely to occur/recur.

9.2 Additional data options for 'core application data'

9.2.1 Accelerometer data

An accelerometer measures acceleration. A 3-axis accelerometer provides the orientation of a stationary platform relative to earth's surface.

This part of ISO 15638 does not determine any application or interpretation of accelerometer data, solely the architecture of the data and message.

Data from an accelerometer shall follow the following architecture:

```
struct input_event {
struct timeval time;
__u16 type;
__u16 code;
__s32 value;
};
```

The data shall be written to the stream message by message and stored in the *RAM* or volatile bistable data storage of the *IVS*. The minimal blocksize is 128 bit (16 byte). The data may be stored as relative data or absolute data.

Relative values:

```
|----- time ------| |type| |code| |-value-|
8c66 4819 721c 0006 0002 0002 03a8 0000
8c66 4819 7222 0006 0000 0000 0000 0000
8c66 4819 99e6 0006 0002 0000 0048 0000
8c66 4819 9a36 0006 0002 0001 0024 0000
8c66 4819 9a50 0006 0002 0002 0396 0000
8c66 4819 9a57 0006 0000 0000 0000 0000
```

Absolute values:

```
|----- time ------| |type| |code| |-value-|
8163 49da 6d62 000d 0000 0000 0000 0000
8163 49da 91d8 000d 0003 0000 0048 0000
8163 49da 9231 000d 0003 0001 0012 0000
8163 49da 9251 000d 0003 0002 03ba 0000
8163 49da 9270 000d 0000 0000 0000 0000
8163 49da b6cf 000d 0003 0000 0036 0000
```

Typical message block

A typical message block consists of 3 messages containing the acceleration data for each of the three axis followed by a synchronization message to signal the end of the block.

The following example is such a message block with detailed explanation of its different messages and data sections:

```
8c66 4819 99e6 0006 0002 0000 0048 0000
|------Time-------| EV_REL REL_X |-Value-|
```

(Explanation: Measured acceleration in x axis direction of 72)

```
8c66 4819 9a36 0006 0002 0001 0024 0000
|------Time-------| EV_REL REL_Y |-Value-|
```

(Explanation: Measured acceleration in y axis direction of 36)

```
8c66 4819 9a50 0006 0002 0002 0396 0000
```

```
|------Time-------| EV_REL REL_Z |-Value-|
```

(Explanation: Measured acceleration in z axis direction of 918)

```
8c66 4819 9a57 0006 0000 0000 0000 0000
|------Time-------| EV_SYN SYN_REPORT |-Value-|
```

(Explanation: The transmitted data block is complete you may process the given data)

9.2.2 Gyroscope data

This part of ISO 15638 does not determine any application or interpretation of gyroscope data, solely the architecture of the data and message.

This part of ISO 15638 does not determine any application or interpretation of a combination of gyroscope and accelerometer data, solely the architecture of the data and messages.

The output data shall be stored in the following format.

Data engineering unit	**Format**	**Voltage (raw) format**
Angular Rate X (10 bits)	deg/sec	*A/D voltage* [4.1]
Angular Rate Y (10 bits)	deg/sec	*A/D voltage* [4.1]
Angular Rate Z (10 bits)	deg/sec	*A/D voltage* [4.1]
Acceleration X (10 bits)	*G's* [4.6]	*A/D voltage* [4.1]
Acceleration Y (10 bits)	*G's* [4.6]	*A/D voltage* [4.1]
Acceleration Z (10 bits)	*G's* [4.6]	*A/D voltage* [4.1]

9.2.3 Camera/video data

9.2.3.1 Still camera data

Still camera images shall be stored and transmitted as JPEG (.jpg) in accordance with ISO 10918-1 (Information technology — Digital compression and coding of continuous-tone still images: Requirements and guidelines). Recognised standard data compression techniques may be used in transmission of the data.

9.2.3.2 Video data

Video images shall be stored and transmitted in accordance with ISO 21000 (Information technology — Multimedia framework (MPEG-21) — Part 1: Vision, Technologies and Strategy). Recognised standard data compression techniques may be used in transmission of the data.

9.2.4 Vehicle speed data

Where required by the *jurisdiction* [4.9], or in support of an *application service* [4.2] elected by the user, vehicle speeds and vehicle speed histories may be calculated and stored.

Where such data is required the vehicle speed shall be measured by a *GNSS* doppler derived method, or provided by equipment, ancillary to the *TARV IVS*, to an 'app' provided in the applications library of the *IVS*, and resultant data stored in the *IVS* data pantry, as specified by the *jurisdiction* [4.9].

The *GNSS* reported vehicle speed between 60 km/h and 150 km/h shall be accurate to within 3.0 km/h when using at least four satellites and a 'Horizontal Dilution of Precision' of < 4 (at lower or higher speeds there may be a greater degree of error).

The resolution of the vehicle speed data recorded by the *IVS* shall be to 0.1 km/h or better (or 0.1 mph if so specified by the *jurisdiction* [4.9]).

Each instance of recording the speed of the vehicle shall be stored in the semantic format:

S serial number between 0-999 Timestamp k/m value where k=kph and m=mph

The timestamp shall be in the format defined in 8.3.10 above

When recording or providing a speed record a location record shall always be recorded/provided as defined in 8.3.11.

As:

S(serial number) timestamp k/m speed location direction of travel

Example *s0123 1297339499 k 53 0x0A5D3770 0x027E2938 >0123*

The serial number shall increment by 1 for each record and shall revert to 000 after reaching 999.

The data records of vehicle speed, where recorded, shall be stored in the non-volatile bistable data storage of the *IVS*.

In the event that vehicle speeds are being recorded to support an application service, at the time that the service is installed or point where the driver is contracted (whichever is later), the user shall advise the driver in writing that the speed of the vehicle is being monitored and passed to the *application service* [4.2].

9.2.5 Alarm status data and records

Where required as *basic vehicle data* [4.4] the *IVS* shall generate and store alarm records in its non-volatile bistable non-volatile data storage for each of the following events:

Alarm Code	**Alarm type description**
A1	external power supply is disconnected from the *IVS*;
A2	external power supply is reconnected to the *IVS*;
A3	movement is indicated by the ignition while the external power supply is disconnected from the *IVS*, using two different features independent from the *GNSS* signal. (see 8.13.4)
A4	movement is detected by the other independent movement sensor while the external power supply is disconnected from the *IVS*, using two different features independent from the *GNSS* signal.(see 8.13.4)
A5	ignition is disconnected from the *IVS* (with and without external power being connected);
A6	ignition is reconnected to the *IVS* (with and without external power being connected);
A7	other independent movement sensor is disconnected from the *IVS* (with and without external power being connected);
A8	other independent movement sensor is reconnected to the *IVS* (with and without external power being connected);
A9	unauthorised access to data in the *IVS* is detected;
A10	unauthorised access to *IVS* software is detected;
A11	*GNSS* antenna is disconnected from the *IVS*; and
A12	*GNSS* antenna is reconnected to the *IVS*.
A13	after a period of non-operation, the distance between the position record before and the position record after that period exceeds 500 metres
A14	zero satellites used for a continuous period of operation of at least five minutes while the vehicle was moving
A15	after a period where zero satellites were used for a continuous period of operation of at least five minutes, the distance between the position record before and the position record after the cessation of signal, exceeds 500 metres

A16 less than four satellites used for a continuous period of operation of at least 20 minutes, while the vehicle was moving

An alarm record counter of 0000-9999 shall be created and incremented with each alarm instance and shall revert to 0000 for the event after 9999 is reached.

An alarm record shall consist of at least the following data:

a. record number;

b. date / time of generation (*UTC* elapsed secondsformat as defined in 8.9.10 above)

c. the event that triggered the generation of the Alarm Record as per A1-A17 above.

Represented semantically as:
Example

A01234	1297339499	A1
A01235	1297339799	A3
A01236	1297334003	A4
A01237	1297334223	A2
A01238	1297334227	A6

9.3 Distributed directory service (DDS) requirements

The function of the distributed directory service is to enable data to be exchanged between vehicle *ITS*-station subsystems.

The distributed directory service shall operate in compliance with the basic Java bundle that includes a distributed directory service. See:

http://www.osgi.org/javadoc/r4v42/org/osgi/service/provisioning/ProvisioningService.html

together with the process devised by CVIS, to automate and secure this process. These extra additional JAVA™ classes are found in:

http://www.itscommunity.eu/cvisproject/download/Deliverables/DEL_CVIS_3.4_Final_Architecture_and_System_Specifications_v1.0.pdf

(Chapter 3.1). - See Annex B.

10 Test requirements

No specific conformance tests are included in this version of this part of ISO 15638, but the minimum requirements that shall constitute any conformance tests shall include:

CT01: Test that: the generic information known within the ISO 15638 suite of standards deliverables as *basic vehicle data* [4.4], shall be supported by all *IVSs*. (for example, shall have a unique identifier, collect time and location data, etc.)

C02: Test that: Certification procedures and enforcement provisions for the providers of regulated services conform to ISO 15638-3 Clause 12.

CT03: Test that: *IVS* requirements are as defined in clause 9 of ISO 15638-3.

CT04: Test that: TARV-ROAM communications layers conform to ISO 15638-2.

CT05: Test that: TARV-ROAM security aspects conform to ISO 15638-4.

CT06: Test that: Host management centre (HMC) requirements operate in compliance with the basic Java bundle that includes a management agent

CT07: Test that: Additional *apps* in the library have been provided by the prime *service provider* [4.15] that collate the data into two collated data concepts:

a) TARV LDT values
b) C-ITS LDT values

(as defined in the Clauses of this part of ISO 15638).

CT08: Test that: A further app has been provided by the prime *service provider* [4.15] that creates an archive of the history and values of data, stored in a file called ‘RecentArchive’.

CT09: Test that: On receipt of the command ‘GETTARVLDT’ the system shall provide the values of the *TARV LDT* [4.10] data concept (specified in this part of ISO 15638) to the previously advised destination address of the requesting *application service* [4.2] provider or *jurisdiction* [4.9]**.** Test that the system sends an ACK to the requesting address and closes the communication with that address immediately.

CT09: Test that: On receipt of the command ‘CREATECoreData’ the system runs the previously provided ‘app’ which bears the same name as the destination IPv6 address (see 8.1.2 above) which populates the *core application data* [4.5] data concept with the current values of the *TARV LDT* [4.10] together with any additional data concept values specified in the ‘app’.

CT10: Test that: on request ‘GETCoreData’ the system provides the values to the previously advised destination address of the requesting *application service* [4.2] provider or *jurisdiction* [4.9], as determined in the previously uploaded ‘app’. Test that the system sends an ACK to the requesting address and closes the communication with that address immediately.

CT11: Test that: On receipt of the command ‘GETC-ITSLDT’ the system makes the values of the *C-ITS LDT* [4.10] data concept available to authorised users and provides the values to the previously advised destination address of the *application service* [4.2] provider

CT12: Test that: On receipt of the command ‘GETArchive’ the system provides the contents of the ‘RecentArchive’ file stored in the non volatile memory of the *IVS* to the IPv6 address previously provided by the prime *service provider* [4.15].

CT13: Test that: On successful receipt of the receipt of the ‘RecentArchive’ data, the prime *service provider* [4.15] sends an ACK to the *IVS* acknowledging, in the form prescribed in ISO 15638-3, that it has received the data.

CT14: Test that: On receipt of the ACK by the *IVS*, the *IVS* clears the data in the ‘RecentArchive’ file and commences to repopulate that file with a record of the clearance of the file in the format yyyymmddhhmmss.

CT15: Test that: Data has been formatted as defined in 8.3 and 8.4

CT16: Test that: Any additional data concepts conform to definitions in Clause 9 wherever the concept is defined in Clause 9.

11 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 may potentially or actually compromised by any instantiation based on the ISO 15638 family of Standards, the contracting parties shall make such risk explicitly known to the implementing *jurisdiction* [4.9] 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.

12 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 specified within ISO 15638-6 – ISO 15638-19 contain no direct patents nor intellectual property other than the copyright of ISO. However, national, regional or local instantiations of any the applications services defined in ISO 15638-6 – ISO 15638-19, or of the *Basic vehicle data* [4.4] defined in this part of ISO 5638, the security requirements contained in ISO 15638-4, or the requirements of ISO 15638-3, may have additional requirements which may have patent or intellectual property implications. The reader is referred to the regulation regime of the *jurisdiction* [4.9] and its regulations for instantiation in this respect.

Annex A
(informative)

Registration provisions of ISO 14816

This Annex contains example of the usage by this part of ISO 15638 of the registration requirements of ISO 14816 at the time of publication of this part of ISO 15638, in respect of its CS1 and CS2 coding schemes. Those intending to use these procedures should consult the current version of ISO 14816.

Management & general rules for the administration of Coding Structure CS 1, and CS 2

A.1 General rules

This Annex describes the administration procedure for numbers issued under the coding structure for **CS1, CS2 and CS8.**

In order to ensure interoperability it is essential that the coding structures defined in this International Standard (ISO 14816), which this Annex supports, be applied in a consistent manner. The structures of this International Standard (ISO 14816) are so constructed that they may be administered at a local level without danger of ambiguity of number series. In general terms this allows the (political) principles of subsidiarity to be followed. However there is a requirement for central maintenance of 'Issuer Identifiers'. It is up to Nation States to determine which *issuers* shall be authorised in respect of nationally determined schemes, and the role of the CRA shall be limited to registering such decisions.

Management procedures for the structures shall be minimised and shall be restricted to simple recording and registration of local systems.

The central and all National registration authorities shall conform to all regional and national legislative requirements with respect to data protection and privacy within the domain of the scheme.

A.1.1 Registration hierarchy

Figure A.1 depicts the layout of the registration hierarchy.

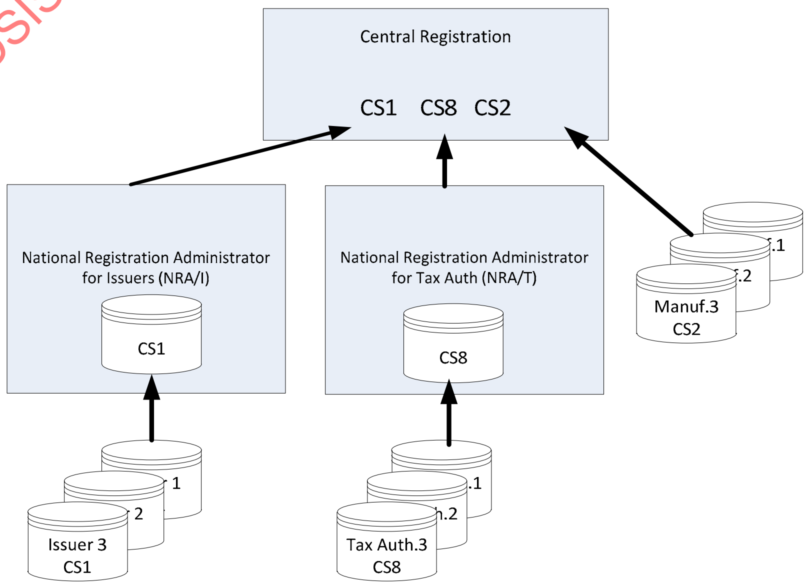
Central Registration
CS1 CS8 CS2
National Registration Administrator for Issuers (NRA/I)
CS1
National Registration Administrator for Tax Auth (NRA/T)
CS8
.1
.2
Manuf.3
CS2
1
2
Issuer 3
CS1
.1
h.2
Tax Auth.3
CS8

Figure A.1 — Layout of the registration hierarchy

A.1.2 Definition of actors

A.1.2.1 Central registration administrator (CRA):

A body, which maintains the registers of' National Registration Administrators' (NRA/I and NRA/T), and the register of Manufacturers. See A.1.3.(of ISO 14816).

Note: At the date of publication of this International Standard (ISO 14816), the EN ISO 14816 CRA is: Nederlands Normalisatie-instituut (NNI)

P.O. Box 5059
NL-2600 GB Delft
The Netherlands

A.1.2.2 National registration administrator for Issuers (NRA/I):

A body appointed by the Nation State to authorize CS1 issuers and to issue **CS1 issuer identifiers** at Nation State level. NRA/I is registered by the **CRA,** and it is expected that this will normally be the National Standardisation body or its appointee.

12.1.1 Issuer:

A body authorised by the **NRA/I** to issue a '**CS1 Service Code/Unambiguous Number'** and identified by a unique identifier (**issuer identifier**) within a country in accordance with this Standard (ISO 14816).

12.1.2 Issuer register:

The **NRA/I** shall maintain a register of all Issuers and structure details on a National level. The **NRA/I** shall provide a copy of their **register of issuers** at agreed intervals to the **CRA** who shall maintain and make available a copy of the full **register of issuers**. The issuer register shall not contain any personal information.

A.1.3 Central registration administrator (CRA)

12.1.3 General

The 'Central Registration Administrator' has been appointed in the first place by agreement of the plenary of the technical committees (ISO TC204 and CEN TC278) and any replacement shall be managed by the ISO Central Secretariat according to the ISO rules.

12.1.4 Responsibilities

The responsibilities of the CRA shall be:

1. to maintain a register of NRA/I's and NRA/T's.
2. to compile, collate and issue a Register of all NRA/I registers and to circulate a copy of this register to all NRA/I's in an agreed format.
3. to compile collate and issue a register of all NRA/T registers and to circulate a copy of this register to all NRA/T's in an agreed format.
4. to maintain a register of manufacturers according to the rules in A.4;
5. to keep CS1, CS2 and cs8 registers on a central level, and to make these registers available to the public. The preferred method would be free public Internet access.

   NOTE: the home page of the cra is:

   http://www.nni.nl/cen278/14816main.html

   At this web-site more information and application forms can be downloaded

A.2 Application and registration procedures FOR CS1: Issuers

A.2.1 Issuer

A.2.1.1 Application procedure for assignment of an issuer identifier

The ‘applicant’ **issuer** shall apply in writing to its **National registration administrator for issuers (NRA/I)** for the assignment of an **issuer identifier**. The **NRA/I** shall satisfy itself of the status of the applicant and shall assign an unused **issuer identifier**.

In unforeseen cases an issuer may wish to appeal against the decision of its NRA/I. In this case the Issuer should lodge a written appeal with the CRA. The CRA will immediately notify ISO/TC 204 of any appeal lodged. In cases where the CRA cannot solve the issue, it may request guidance from CEN/TC 278 or ISO/TC 204.

An **issuer** may request several **issuer identifiers**. This may be granted by the **NRA/I**. Each **issuer identifier** shall then be handled as belonging to a separate **issuer.**

The reuse of issued **identifiers** should be avoided, and in any case expired **identifiers** shall not be reused until 3 years after its expiration period.

A.2.1.2 Criteria for approval of an application for a CS1 issuer identifier

Applications for an **issuer identifier** shall meet the criteria for approval below:

1. the applicant shall be a single entity with a legal status.
2. the applicant shall use the **issuer identifier** for an agreed use within the intended scope.
3. the applicant shall pay any fees required by the **NRA/I** based on the guidelines in A.5.
4. The **issuer identifier** shall only be issued by the **NRA/I** when there is expected to be an immediate use, or when the **NRA/I** considers that such requirement is imminent.
5. The **NRA/I** may request a national service code/ unambiguous coding structure. The details that the **NRA/I** may request shall be the details of his local numbering sub structures within his service code/unambiguous number structure, but the unambiguous identification codes shall not be revealed to the **NRA/I**.

Note Multinational companies or similarly a group of mutually independent **issuers** in several member countries may agree to form an alliance under a single entity to use a single **issuer** Identification (CS1). Where such companies already hold an **issuer identifier** in one country, they may apply for the issue of a similar number in another country, which may be issued out of sequence, so long as that number is not already in use. where the number is already in use, the applicant may request a new number in the first country, which may be granted at the discretion of the **NRA/I.**

A.2.1.3 Responsibilities of the issuer

1. To comply fully with the numbering system and the requirements of this International Standard (ISO 14816) and its Annexes

   Note An **issuer** can not issue a number that has not been formally allocated to it by the relevant **NRA/I.**
2. To retain the letter of authorisation of its **issuer identifier** by the **NRA/I.**
3. To issue **service codes/unambiguous numbers** using the *issuer* **identifier** number assigned to them by the **NRA/I,** and in accordance with the requirements of this International Standard (ISO 14816).
4. To communicate to the **registration administrator** any proposed changes that would alter material facts contained within the original registration,

5. To keep a register of issued **service codes/unambiguous numbers** within the limits of its intended use, and to maintain such records in a secure place and in accordance with the requirements for data protection in the country/countries of their sphere of operation.
6. Where the **issuer** is required to provide an anonymous mode, to maintain a service code/unambiguous coding structure that will enable this in an efficient manner.
7. To pay fees in accordance with agreements with the **NRA/I** based on the guidelines in A.5.
8. Where the **issuer** wants to terminate the issuing operation, to give 3 months notice to the **NRA/I.**

   Note All privacy related materials shall be destructed in accordance with the requirements for data protection in the country/countries of their sphere of operation.

A.2.2 National registration administrator (NRA/I)

A.2.2.1 Eligibility to become a National registration administrator (NRA/I)

The **NRA/I** shall be a single entity designated in each country by the Nation State authorities, usually the National Standards authorities.

A.2.2.2 Resignation

If a **NRA/I,** which is not a standardisation member body, finds it necessary to resign, six month's notice in writing shall be given to the National Standards authorities.

A.2.2.3 Non compliance

If the **CRA** has reasonable cause to believe that a **NRA/I** is not complying properly with the structure as defined in this International Standard (ISO 14816), it shall provide formal notice in writing to the **NRA/I** and National authorities.

A.2.2.4 Responsibilities

The responsibilities of a **NRA/I** shall be:

1. To ensure that the application fully complies with the procedures for application for *Issuer* in this International Standard (ISO 14816);
2. To verify that the applicant's use and **service codes/unambiguous number** structures comply with the scope of this International Standard (ISO 14816);
3. To process, within 60 days of receipt of the applications, the applications for **issuers** from within their areas of responsibility;
4. To send notification to the applicant in writing, within the same period of 60 days of receipt of the application, as to the disposition of their application;
5. To assign a unambiguous **issuer identifier** to each approved **issuer**;
6. To maintain a **register** providing details of all registered '**issuers'** together with their '**issuer identifier'** and summary of their structures.
7. To retain a copy of each application;
8. To provide an annual report of activity to the *CRA*. The report shall include an up to date copy of their **issuer register**, and the number of applications for **issuer**, together with the number granted in the period;
9. To respond to general enquiries covering this International Standard (ISO 14816).

A.2.2.5 National register of issuers

A.2.2.5.1 Publication and availability

The **NRA/I** shall publish an **issuer register**. The **register** shall be published in both numerical (**issuer identifier**) and alphabetical (issuer name) order.

Note: The final issue of unambiguous numbers shall remain private and shall not be declared to the NRA/I, and shall therefore not appear on any published register whatsoever.

The **National register of issuers** shall be a publicly available document. The register may be available at the cost of reproduction, or the NRA/I may choose to publish it on the Internet according to the provisions in A.5.

A.2.2.5.2 Contents

The **CS1 issuer register** shall contain the following information

- name of **Issuer**;
- address and communication address (e.g. tel., fax., E-mail) of *Issuer* and principal contacts within organisation as indicated in the application;
- **Issuer identifier** number assigned to the **Issuer** by the *NRA/I;*
- date of issuing and date of end of issuing, if any;
- for each issuer a summary of its SC/UNs and substructures if applicable.

A.3 Application and registration procedures for CS8: Tax codes

(Not relevant for ISO 15638).

A.4 Application and registration procedures for CS2: Manufacturers

A.4.1 Application procedure for assignment of a manufacturer Identifier

1. The ‘applicant’ Manufacturer shall apply in writing to the **CRA** for the assignment of a **manufacturer identifier**.
2. The **CRA** shall assign an unused **manufacturer identifier** to any company or organisation that fulfils the criteria in A.4.2.
3. In unforeseen cases there may be a need for a **manufacturer** to consult the *TC* as an appeal procedure against the decision of the CRA. In this case the consulting party shall make a written request for clarification to the TC Chairman, with copy to the Secretariat. The TC Chairman may then delegate the resolution of this request to the relevant Working Group.
4. A **manufacturer** may request several **manufacturer identifiers**. This may be granted by the **CRA**. each **manufacturer identifier** shall then be handled as belonging to a separate **manufacturer**.
5. The reuse of issued **manufacturer identifiers** should be avoided, and in any case expired **manufacturer identifiers** shall not be reused until 3 years after their expiration period.

A.4.2 Criteria for approval of an application for an manufacturer identifier

Applications for a **manufacturer identifier** shall meet the criteria for approval below:

1. The applicant shall be a single entity with a legal status.
2. The applicant shall use the **manufacturer identifier** for an agreed use within the intended scope.
3. The applicant shall pay any fees required by the CRA according to the rules in A.5.

A.4.3 Responsibilities of the manufacturer

1. To comply fully with the numbering system and the requirements of this International Standard and its Annexes, a manufacturer may **NOT** issue a number that has not been formally allocated to it by the **CRA**
2. To retain the letter of authorisation of its **manufacturer identifier** by the **CRA**.
3. To issue **service codes/unambiguous numbers** using the **manufacturer identifier** number assigned to them by the **CRA**, and in accordance with the requirements of the Standard which this Annex supports.
4. To communicate to the **central registration administrator** any proposed changes that would alter material facts contained within the original registration.
5. To keep a register of issued **service codes/unambiguous numbers** within the limits of its intended use, and to maintain such records in a secure place and in accordance with the requirements for data protection in the country/countries where the register is maintained.
6. To pay fees in accordance with agreements with the **CRA** based on the guidelines in A.5.

A.4.4 Responsibilities CRA for manufacturer register

The responsibilities of a CRA shall be:

1. To ensure that the application fully complies with the procedures for application for **manufacturer identifier** in this International Standard.
2. To verify that the applicant's use of service codes/unambiguous coding structures comply with the scope of this International Standard.
3. To process, within 60 days of receipt of the applications, the applications for a **manufacturer identifier**.
4. To send notification to the applicant in writing, within the same period of 60 days of receipt of the application, as to the disposition of their application.
5. To assign a unambiguous **manufacturer identifiers** to each approved manufacturer.
6. To maintain a *register* providing details of all registered manufacturers together with their **manufacturer identifier'**.
7. To retain a copy of each application.
8. To respond to general enquiries covering this International Standard.

A.4.5 Register of manufacturers

A.4.5.1 Publication and availability

The CRA shall publish a manufacturer **register**. the **register** shall be published in both numerical (**manufacturer identifier**) and alphabetical (manufacturer name) order.

Note The final issue of service codes/ unambiguous numbers shall remain private and shall not be declared to the CRA and shall therefore not appear on any published register whatsoever.

the **register of manufacturers** shall be a publicly available document. the register may be available at the cost of reproduction, or the CRA may choose to publish it on the internet according to the provisions in a.3. (of ISO 14816).

A.4.5.2 Contents

The **manufacturer register** shall contain the following information

- name of manufacturer;

- address and communication address (e.g. tel., fax., E-mail) of manufacturer and principal contacts within organisation:
- **Manufacturer Identifier** assigned to the manufacturer by the CRA;
- date of issuing and date of end of issuing, if any.

A.5 Costs aspects

The costs of the entire registration procedure will be recovered on the basis of nominal cost. An **issuer** will pay a registration fee and an annual renewal fee to its **NRA** *(*or **CRA**, in case of **CS2***)*. The **NRA** will pay a fee to the **CRA**. The fee structure to be determined locally. The registration fees may be set to cover a free public Internet access to the **NRA/CRA** registry. The charges for issuing of documents shall be at the cost recovery basis.

A.6 Disclaimer

The following declaration by the registration administrator should be used to protect its position against possible misuse of the coding structure by bodies outside their control.

A similar declaration replacing **issuer** with **manufacturer** or **tax authority** should be made for **CS2** and **CS8**

"IMPORTANT INFORMATION REGARDING YOUR NUMBER ASSIGNMENT"

This number is issued with the understanding that this **issuer identifier** will be used in accordance with the requirements in ENV 12314-1 and ENV ISO 14816. It should be understood that in assigning an *issuer* **identifier** in response to your application, the **National registration Administrator** is designating the assigned number as identifying the organisation specified as an '**issuer'** as described in ENV ISO 14816.

Tthe use of this number or any other number by a party that chooses not to comply with the provisions of this International Standard (ISO 14816) with or without the knowledge of the **national registration administrator** is beyond the control of the **national registration administrator.** therefore, the **national registration administrator** cannot guarantee the sole and unambiguous use of this identifier to your organisation.

The operation of the **national registration administrator** is a voluntary non-profit service to **issuers** complying with ENV ISO 14816 and its success depends, in part, on the co-operation of **issuers**. The **national registration administrator** will not be held financially liable for errors in the registration, reservation or assignment of **issuer identifier** or the publication of those identifiers and the names and addresses

Annex B
(normative)

CVIS 3.4 System Specifications

CVIS 3.4 System specifications sections;

CVIS 3.1 OSGi™framework & lifecycle management and

CVIS3.2 Distributed directory service

B.1 CVIS Architecture and system specifications Section 3.1

Abbreviations and definitions

Abbreviation	**Definition**
API	Application Programming Interface
Application	Software bundle providing "End User Services"
CALM	Communication Access for Land Mobiles - this is the work title of a basic set of CEN/ISO communication standards for cooperative ITS
CVIS	Cooperative Vehicle-Infrastructure Systems
DDS	Distributed Directory Service
FOAM	Framework for Open Application Management. A CVIS sub-project
HMC	Host management centre
OSGi	Open Services Gateway initiative
SOAP	Simple Object Access Protocol
URI	Uniform Resource Identifier

B.1.1 CVIS 3.1 OSGi™framework & lifecycle management

The *OSGi*™framework provides a comprehensive set of functions to provide and deploy software bundles. This allows the addition, change or removal of applications software or facility software during the runtime of the system. CVIS will implement *JAVA*™/*OSGi*™in such a way, that these runtime system changes can be done from remote through the "Host Management Centre" (*HMC*) and the corresponding *HMC* on the associated hosts.

A more detailed introduction into *JAVA*™/*OSGi*™and the application run time environment of CVIS is given in chapter 6 of D.FOAM.3.2.

http://www.cvisproject.org/download/Deliverables/DEL_CVIS_3.3_Architecture_and_System_Specification

*JAVA™/OSGi™*specifications are available on www.osgi.org. e.g.

OSGi™service Platform - Core Specification, Release 4, Version 4.1, the *OSGi*™Alliance, April 2007

OSGi™service Platform - service Compendium, Release 4, Version 4.1, the OSGi Alliance, April 2007

B.1.1.1 CVIS 3.1.1 Overview

The functionality of the *OSGi*™framework is divided in the following layers [Core]:

1. Security layer
2. Module layer
3. Lifecycle layer
4. Service layer
5. Actual services

This layering is described in more detail in section 5. Here we introduce the layers that are of special relevance for the concepts in CVIS:

The ***security layer*** is based on Java 2 security but adds a number of constraints and fills in some of the blanks that standard Java leaves open. It defines a secure packaging format as well as the runtime interaction with the Java 2 security layer.

The ***lifecycle layer*** provides a lifecycle *API* to bundles. This *API* provides a runtime model for bundles. It defines how bundles are started and stopped as well as how bundles are installed, updated and uninstalled. Additionally, it provides a comprehensive event *API* to allow a management bundle to control the operations of the service platform. The lifecycle layer requires the module layer but the security layer is optional.

The ***service layer*** provides a dynamic, concise and consistent programming model for Java bundle developers, simplifying the development and deployment of service bundles by de- coupling the service's specification (Java interface) from its implementations. This model allows bundle developers to bind to services only using their interface specifications. The selection of a specific implementation, optimized for a specific need or from a specific vendor, can thus be deferred to run-time.

Deployment and provisioning

Related to the lifecycle management is the deployment and provisioning features:

Deployment should be interpreted as the process of making a *service application* available at an *HMC*. This includes the packaging and transport of the application and all its components from the service centre to the *HMC*.

Provisioning should be interpreted as the process of enabling a *service application* for use on a *CVIS unit.* This includes packaging, transport of the application and all of its components and activation of the application on the CVIS unit.

In CVIS the host platform will be equipped with the *management agent*. The management agent will support the lifecycle management.

Figure B.1 (Figure 16 in CVIS Section 3.1) illustrates the two different steps "deployment" and "provisioning".

- New software applications (A1, …) are issued by suppliers (or by service centres acting as software supplier) and need to be "deployed" to the *HMC* entities.

All CVIS hosts belong to exactly one *HMC* (myHMC). There may be numerous *HMCs* run by different organisations.

- A "Management Agent" (MA) on a host contains the necessary functionality for managing the download of new applications. This "provisioning" is based on an *OMA*-DM protocol which has already been demonstrated in the GST project.

After the provisioning is concluded applications (A1, A2) can run on the host. In the example figure they communicate with the service centre.

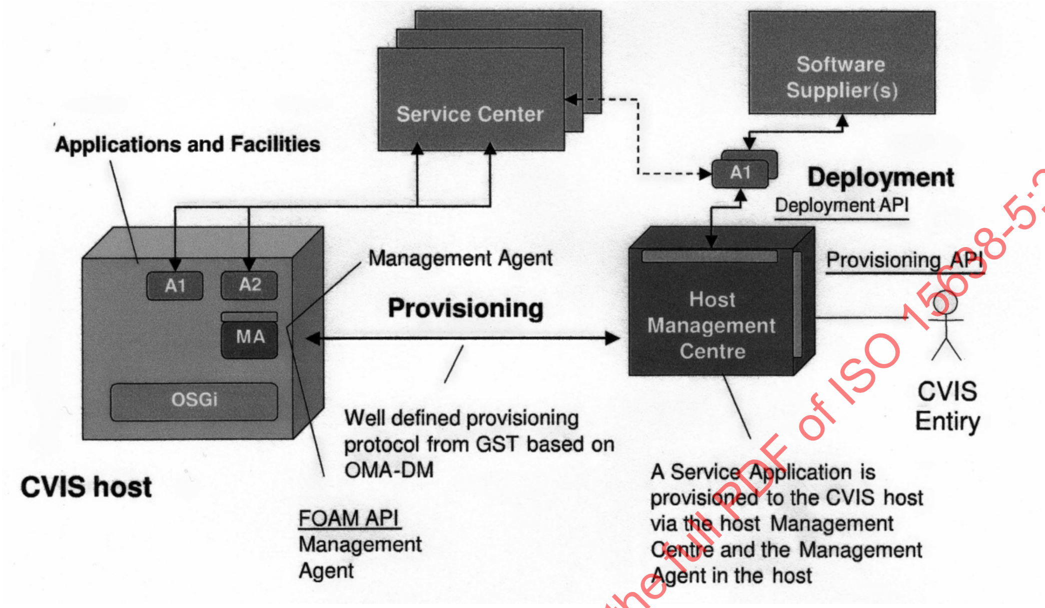
Service Center
Software Supplier(s)
Applications and Facilities
A1
Deployment
Deployment API
Management Agent
Provisioning API
A1
A2
MA
Provisioning
Host Management Centre
OSGi
CVIS Entiry
Well defined provisioning protocol from GST based on OMA-DM
CVIS host
A Service Application is provisioned to the CVIS host via the host Management Centre and the Management Agent in the host
FOAM API
Management Agent

Figure B.1 — CVIS Fig 16 System overview for deployment and provisioning

B.2 CVIS 3.1.2 Application programming interface

For the actions of deployment and provisioning, CVIS defines the following Java *OSGi™APIs*:

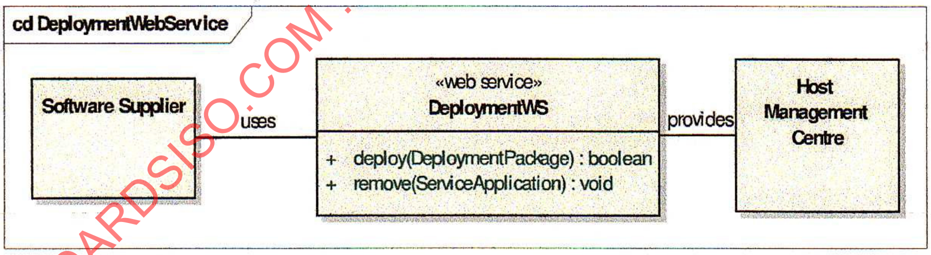

Figure B.2 — CVIS Figure 17 – Deployment API

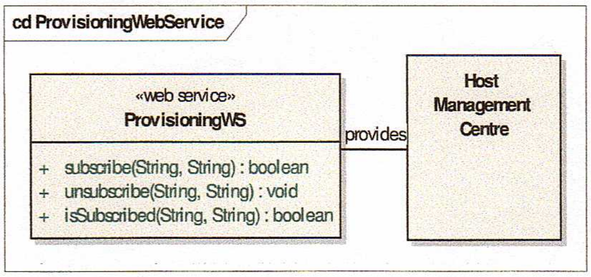
cd ProvisioningWebService
«web service»
ProvisioningWS
+ subscribe(String, String) : boolean
+ unsubscribe(String, String) : void
+ isSubscribed(String, String) : boolean
provides
Host Management Centre

Figure B.3 — CVIS Figure 18 – Provisioning API

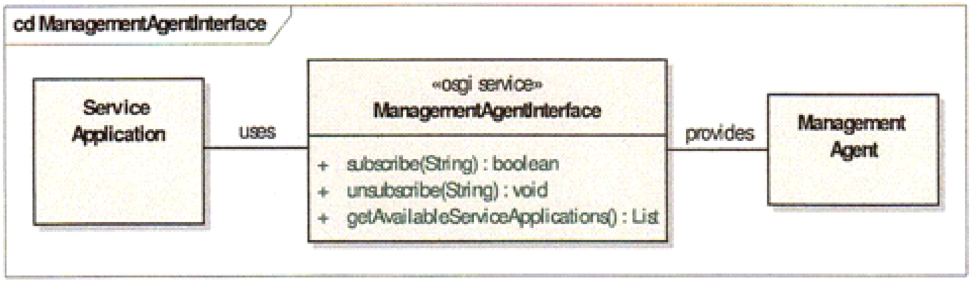
cd ManagementAgentInterface
Service Application
uses
«osgi service»
ManagementAgentInterface
+ subscribe(String) : boolean
+ unsubscribe(String) : void
+ getAvailableServiceApplications() : List
provides
Management Agent

Figure B.4 — CVIS Figure 19: Provisioning API of the CVIS host

In principle here all the *OSGi*™functionality would be right to be quoted as "the" *API*. As this is not the intention of this part of ISO 15638, the following figure is just an example illustrating the lifecycle layer.

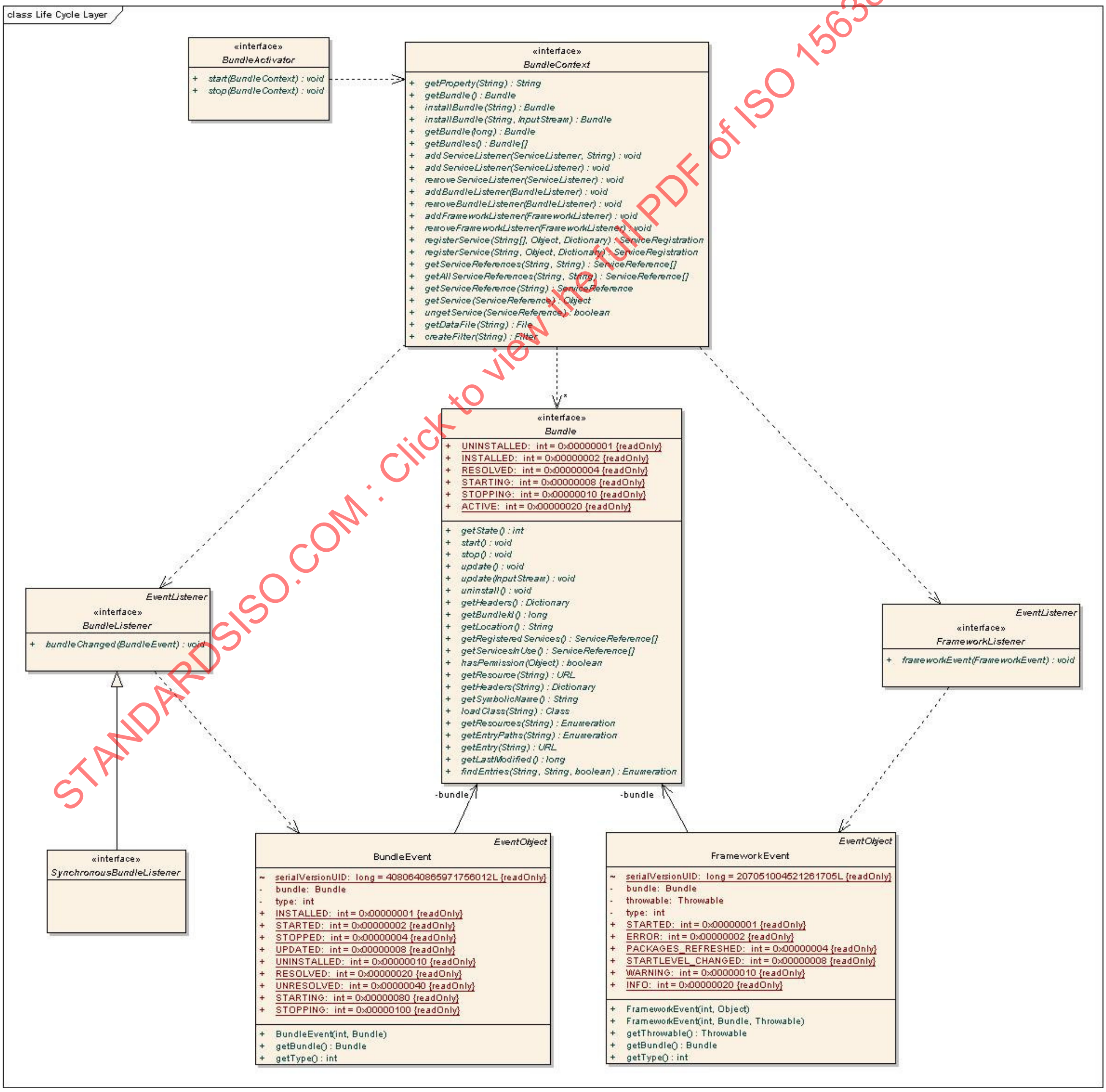
class Life Cycle Layer
«interface»
BundleActivator
+ start(BundleContext) : void
+ stop(BundleContext) : void
«interface»
BundleContext
+ getProperty(String) : String
+ getBundle() : Bundle
+ installBundle(String) : Bundle
+ installBundle(String, InputStream) : Bundle
+ getBundle(long) : Bundle
+ getBundles() : Bundle[]
+ addServiceListener(ServiceListener, String) : void
+ addServiceListener(ServiceListener) : void
+ removeServiceListener(ServiceListener) : void
+ addBundleListener(BundleListener) : void
+ removeBundleListener(BundleListener) : void
+ addFrameworkListener(FrameworkListener) : void
+ removeFrameworkListener(FrameworkListener) : void
+ registerService(String[], Object, Dictionary) : ServiceRegistration
+ registerService(String, Object, Dictionary) : ServiceRegistration
+ getServiceReferences(String, String) : ServiceReference[]
+ getAllServiceReferences(String, String) : ServiceReference[]
+ getServiceReference(String) : ServiceReference
+ getService(ServiceReference) : Object
+ ungetService(ServiceReference) : boolean
+ getDataFile(String) : File
+ createFilter(String) : Filter
*
«interface»
Bundle
+ UNINSTALLED: int = 0x00000001 {readOnly}
+ INSTALLED: int = 0x00000002 {readOnly}
+ RESOLVED: int = 0x00000004 {readOnly}
+ STARTING: int = 0x00000008 {readOnly}
+ STOPPING: int = 0x00000010 {readOnly}
+ ACTIVE: int = 0x00000020 {readOnly}
+ getState() : int
+ start() : void
+ stop() : void
+ update() : void
+ update(InputStream) : void
+ uninstall() : void
+ getHeaders() : Dictionary
+ getBundleId() : long
+ getLocation() : String
+ getRegisteredServices() : ServiceReference[]
+ getServicesInUse() : ServiceReference[]
+ hasPermission(Object) : boolean
+ getResource(String) : URL
+ getHeaders(String) : Dictionary
+ getSymbolicName() : String
+ loadClass(String) : Class
+ getResources(String) : Enumeration
+ getEntryPaths(String) : Enumeration
+ getEntry(String) : URL
+ getLastModified() : long
+ findEntries(String, String, boolean) : Enumeration
EventListener
«interface»
BundleListener
+ bundleChanged(BundleEvent) : void
EventListener
«interface»
FrameworkListener
+ frameworkEvent(FrameworkEvent) : void
«interface»
SynchronousBundleListener
-bundle
-bundle
EventObject
BundleEvent
~ serialVersionUID: long = 4080640865971756012L {readOnly}
- bundle: Bundle
- type: int
+ INSTALLED: int = 0x00000001 {readOnly}
+ STARTED: int = 0x00000002 {readOnly}
+ STOPPED: int = 0x00000004 {readOnly}
+ UPDATED: int = 0x00000008 {readOnly}
+ UNINSTALLED: int = 0x00000010 {readOnly}
+ RESOLVED: int = 0x00000020 {readOnly}
+ UNRESOLVED: int = 0x00000040 {readOnly}
+ STARTING: int = 0x00000080 {readOnly}
+ STOPPING: int = 0x00000100 {readOnly}
+ BundleEvent(int, Bundle)
+ getBundle() : Bundle
+ getType() : int
EventObject
FrameworkEvent
~ serialVersionUID: long = 207051004521261705L {readOnly}
- bundle: Bundle
- throwable: Throwable
- type: int
+ STARTED: int = 0x00000001 {readOnly}
+ ERROR: int = 0x00000002 {readOnly}
+ PACKAGES_REFRESHED: int = 0x00000004 {readOnly}
+ STARTLEVEL_CHANGED: int = 0x00000008 {readOnly}
+ WARNING: int = 0x00000010 {readOnly}
+ INFO: int = 0x00000020 {readOnly}
+ FrameworkEvent(int, Object)
+ FrameworkEvent(int, Bundle, Throwable)
+ getThrowable() : Throwable
+ getBundle() : Bundle
+ getType() : int

Figure B.5 — CVIS Figure 20: OSGi™lifecycle API

B.2.1 VIS3.1.3 Interaction model

To illustrate what the term "lifecycle" means, the state diagram of a service bundle is shown in Figure B.6 (CVIS Figure 21). As can be seen, during its lifecycle the bundle passes through 6 states:

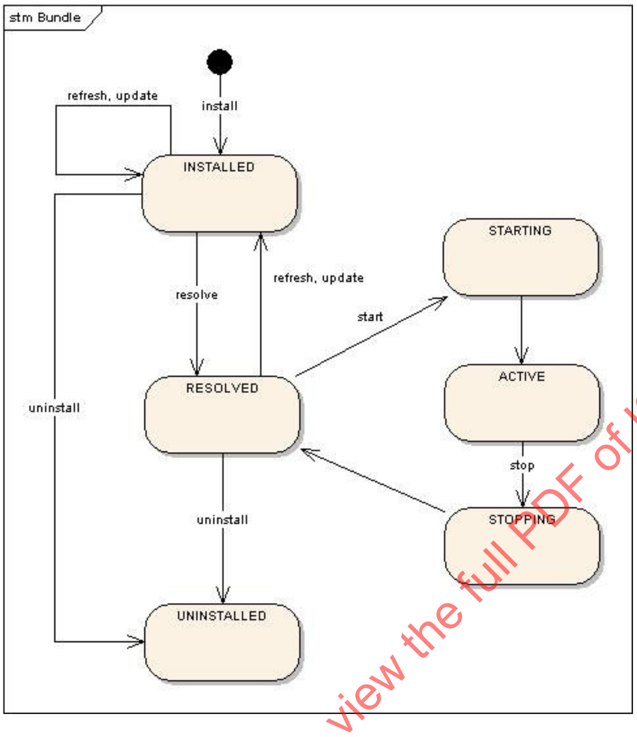

Figure B.6 — CVIS Figure 21: Lifecycle states of JAVA OSGi™bundles

B.3 CVIS 3.2 Distributed directory service

This sub-section is based on the "Distributed Directory Service" (*DDS*) section of the D.FOAM.3.2 specification document. In this document (the D.CVIS.3.4) the focus is on the external interface of the *DDS* and how these services are accomplished through interactions between different parts of the CVIS system. For discussions of the internal architecture of the *DDS* we refer to the D.FOAM.3.2 specification document.

B.3.1 CVIS 3.2.1 Overview

DDS provides mechanisms for looking up deployed applications and facilities in a CVIS distributed peer to peer network, enabling ad hoc communication between CVIS sub-systems and applications. The *DDS* basically provides two discovery mechanisms:

A CVIS peer can look up another peer using some search criteria. The peers' unique identification can be used as the search criteria to look up a specific peer.

A CVIS peer can subscribe to and be notified when a particular service provided by a facility or an application is within reach. To accomplish this, the *DDS* provides facilities for broadcasting service announcements and to subscribe announcements of particular services. Thus, if a broadcasted service announcement reaches a particular CVIS peer that has subscribed to this particular service, the peer gets notified and they can start to interact.

Context

The CVIS system will consist of many applications and facilities (implemented as OSGi™bundles) running on different CVIS hosts. A CVIS host can be a mobile unit (in-vehicle or nomadic), a road-side unit, or a centre-side system. In order to achieve their goals, applications and facilities typically need to form ad-hoc collaborations with other applications and facilities. Due to the dynamic and distributed nature of the CVIS system, the lifecycle of each application and facility will be independent from other applications and facilities. This implies that the formation of collaborations will be a dynamic process as well.

In order to establish collaboration, an application has to find the peers with which to communicate. Within a particular CVIS host, the OSGi™framework offers a local service discovery mechanism. However, this mechanism is not designed for operation in a distributed, dynamic environment. For this reason CVIS offers an additional discovery mechanism, the "Distributed Directory Service" (DDS). In essence, the DDS offers a yellow pages service across the CVIS network. This mechanism allows an application to search for applications running on other CVIS hosts based on a set of specific selection criteria. Examples of specific selection criteria are:

Applications in vehicles in a particular area;

Applications in vehicles travelling via a particular junction;

Applications in vehicles carrying (a particular class of) dangerous goods;

Applications in road-side systems in a particular area;

Applications in road-side systems along a particular road segment.

The result of the search is a set of communication handles that are returned to the searching application. Each communication handle enables the searching application to set up a communication channel to another application that satisfies the search criteria.

B.3.2 CVIS 3.2.2 Application programming interface

DDS basic facility is provided as single Java bundle running on the local CVIS host and provides the services defined in the *DDS API*. The *DDS API* is shown in B.7 (CVIS Figure 22).

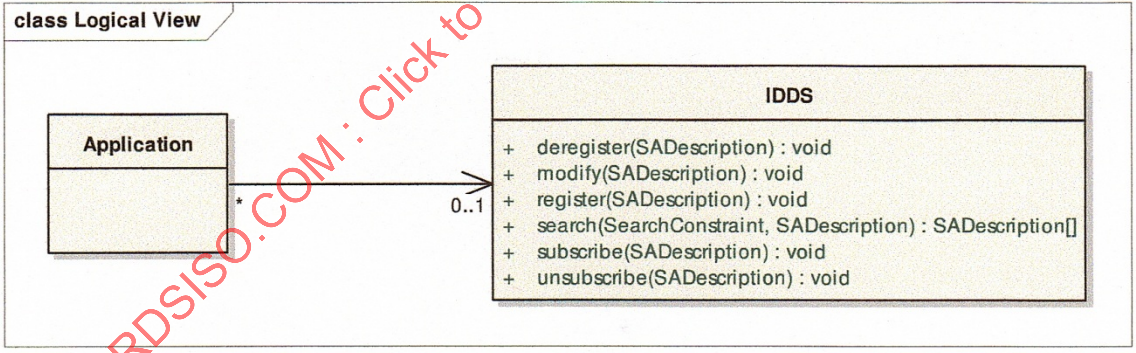
class Logical View
Application
*
0..1
IDDS
+ deregister(SADescription) : void
+ modify(SADescription) : void
+ register(SADescription) : void
+ search(SearchConstraint, SADescription) : SADescription[]
+ subscribe(SADescription) : void
+ unsubscribe(SADescription) : void

Figure B.7 — CVIS Figure 22: The DDS API

An application or a facility uses the register operation to register themselves with the local *DDS* facility when they are deployed. This is accomplished by submitting a description object. The specification of the description object is shown in Figure B.8 (CVIS Figure 23) includes an identifier which is unique within the local CVIS host, a "Universal Resource Identifier" (*URI*), which acts as a communications handle, some flags and an optional set of properties (encoded as key-value pairs) such as the area and direction where the vehicle is currently travelling, its cargo etc. An application can modify these registered properties with the *DDS* when their values have changed. It is also possible for the application to deregister itself.

The search operation is used to look up available services and applications. As part of the search an application submits a set of selection criteria by defining a number of properties. The application can also define a search constraint, which contains a timeout period (defining the maximum amount of time a query may take), the maximum number of resulting communication handles, of the maximum depth of the search. If successful, the *DDS* will return a set of description objects including the *URIs* of the matching peers. The

URIs acts as communication handles. The description objects also include the last known values of the properties.

Based on the query result, the application can perform a number of actions. For instance, it can initiate a separate communication session with one or each of the matched peers, e.g. in order to perform some kind of negotiation, or it can perform a multicast to the set of peers. It could also choose not to initiate a communication session at all, but instead take an action based on the received values of the properties of the selected peers.

In the case that there is only a limited amount of discovery time available, e.g. with vehicles entering the local communication range of a road-side unit at high speed, the performance of the above *DDS* mechanism might not be sufficient. In that case, the publish/subscribe mechanism offered by the *DDS* can be used. An application can register itself with its local *DDS* instance by submitting a description object, where the "*isPublish*" flag is set to 'true' (its default value is 'false'). This particular form of registration implies a publish action. The *DDS* will initiate a continuous broadcast of the presence of the service provided by the registered application, i.e., the identifier and the *URI* are broadcasted within the transmission range of the corresponding CVIS unit, e.g. a road-side unit.

An application executing on a mobile host, e.g. in a vehicle, that wants to discover and initiate a communication session with providers of particular service subscribes its interest of this service. This is accomplished by calling the subscribe operation and submit a description object describing the service of interest. From this moment on, its local *DDS* instance will monitor all available communication channels for the presence of this service. At a certain moment, the mobile CVIS unit enters the communication range of the broadcasting CVIS unit. The local *DDS* will directly be made aware of the broadcasted service, and forward the description object with the corresponding *URI* to the matching subscribed entities. Upon reception of the description object, the recipient can directly set up a communication session.

When the application does not wish to make its services available anymore, it deregisters itself with the *DDS*.

Table B.1 — Method, types and parameters

Method	Type	Parameters
register(sad)	void	Sad: SADescription - in
deregister(sad)	void	Sad: SADescription - in
modify(sad)	void	Sad: SADescription - in
search(sad, sc)	SADescription[*]	Sad: SADescription - in Sc: SearchConstraint - in
subscribe(sad)	Void	Sad: SADescription - in
unsubscribe(sad)	Void	Sad: SADescription - in

B.3.3 CVIS 3.2.3 Information model

The *DDS* information model is depicted in Figure B.8 (CVIS Figure 23).

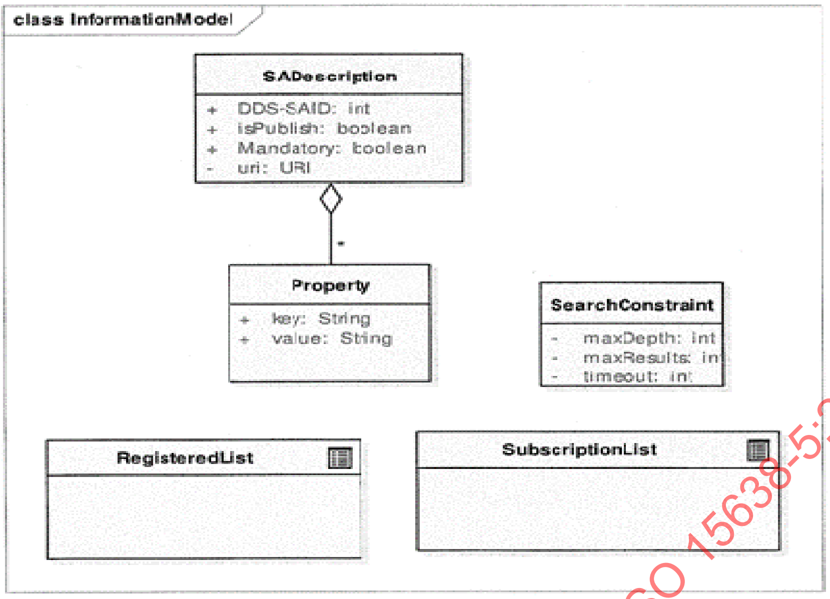

Figure B.8 — CVIS Figure 23: DDS information model

It specifies four information objects:

The description object *SADescription* contains the following attributes:

- The identifier *DDS SAID* which is defined according to element AID of the CEN DSRC standard EN 12834. This identification includes identification of the application type.
- The service announcement broadcast flag *isPublish*. Setting this flag to true implies regular broadcasts of the provided service of the registered application or facility. The default value is false.
- The "*Mandatory*" flag. Setting this flag implies that the provided service is mandatory. For instance vehicles may be required to install a particular tolling application before entering a particular city.
- The communication handle in the form of a *URI*.

Properties (encoded as key-value pairs) may include information such as the area and direction where the vehicle is currently travelling, its cargo etc. The properties are used as baseline for setting search criteria when looking up particular services. Care must be taken by application designers to ensure that the property facility is used in the right way. For instance, if the application were to register the actual position as a *DDS* property, then a periodic update of this value (say each second) would most probably incur a huge performance cost. Therefore, properties must change its value only slowly over time.

The *SearchConstraint* defines constraints on the search. It contains the following attributes

- *maxDepth,*
- *maxResults,*
- *timeout.*

RegisteredList contains the list of registered applications and facilities

SubscriptionList contains a list specifying which local applications and facilities that have subscribed to what services.

B.3.4 CVIS 3.2.4 Interaction model

The *DDS* provides two discovery mechanisms; *search* and *publish-subscribe* as presented in section 3.2.(of CVIS deliverable)

The behavioural model related to the search mechanism is specified in Figure B.9 (CVIS Figure 24). The scenario includes a provider side (provider application, *DDS*, connection manager and communication infrastructure (CommInfr)) that resides on one particular node, e.g. a vehicle, and a consumer side (consumer application, *DDS*, connection manager and CommInfr) residing on another node, e.g. a road-side unit.

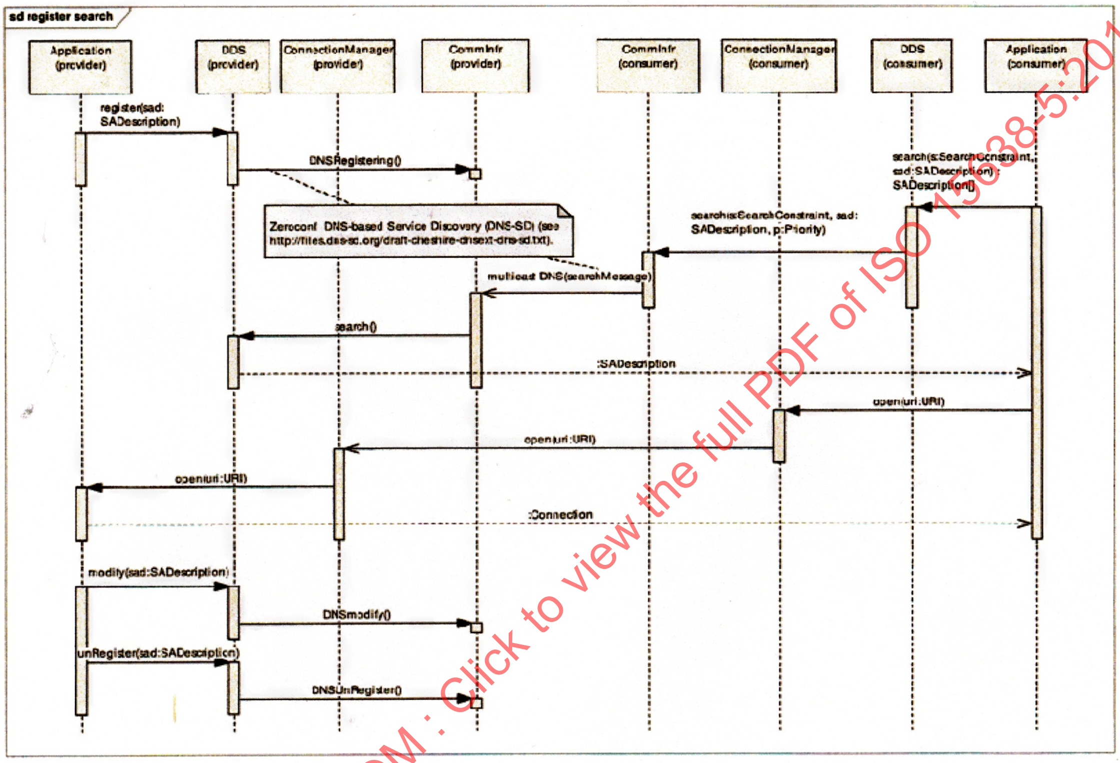
sd register search
Application (provider)
DDS (provider)
ConnectionManager (provider)
CommInfr (provider)
CommInfr (consumer)
ConnectionManager (consumer)
DDS (consumer)
Application (consumer)
register(sad: SADescription)
DNSRegistering()
Zeroconf DNS-based Service Discovery (DNS-SD) (see http://files.dns-sd.org/draft-cheshire-dnsext-dns-sd.txt).
search(s:SearchConstraint, sad:SADescription) : SADescription[]
search(s:SearchConstraint, sad: SADescription, p:Priority)
multicast DNS(searchMessage)
search()
:SADescription
open(uri:URI)
open(uri:URI)
open(uri:URI)
:Connection
modify(sad:SADescription)
DNSmodify()
unRegister(sad:SADescription)
DNSUnRegister()

Figure B.9 — CVIS Figure 24: The search sequence model

After the consumer application has discovered the presence of provider application, it sets up a communication session through the communication handle (the **URI**) it has received from the provider *DDS*.

The usage scenario above depends on an active search to be performed by the application that wishes to initiate a communication session. Depending on the search criteria used, this search can require a considerable period of time. Since CVIS in-vehicle hosts may be travelling with speeds in excess of 40 m/s, i.e. 144 km/h, the typical dwell time within the communication range of a road-side unit with a potential communication partner may be very short (less then a few seconds).

For this reason, the *DDS* also offers a "publish-subscribe" mechanism. An application can subscribe to (and de-subscribe from) applications of a particular type. The *DDS* will then 'listen' for applications of this type, on behalf of the subscribing application. As soon as the *DDS* discovers, through the usage of its underlying infrastructure, e.g. *CALM* FAST service advertisement (ISO 24102 and ISO 29281), that there is such an application within reach, it will immediately provide a communication channel between the publisher and subscriber applications that can be used to fulfil the applications' communication needs. This is illustrated in Figure B.10 (CVIS Figure 25).

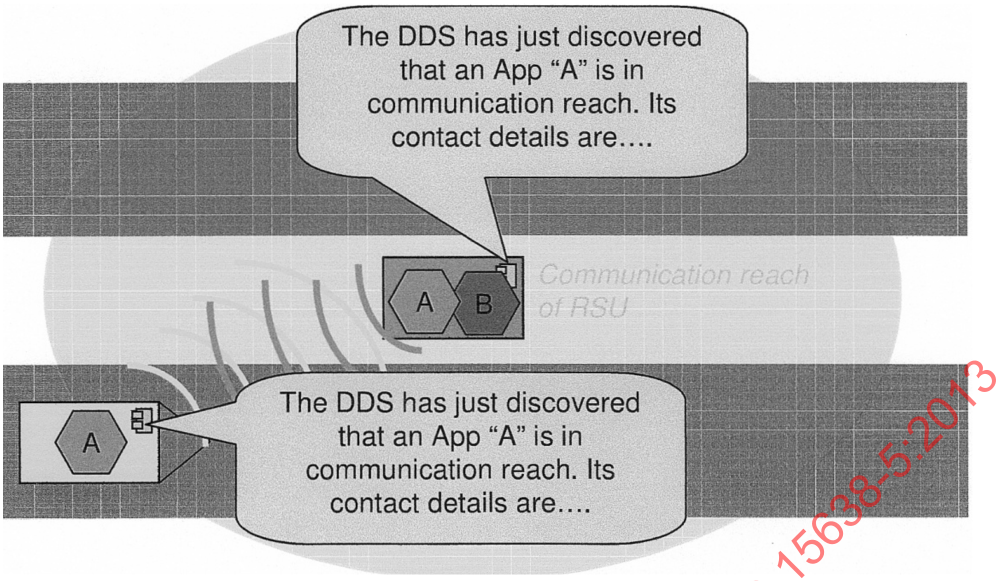
The DDS has just discovered that an App "A" is in communication reach. Its contact details are….
A
B
Communication reach of RSU
A
The DDS has just discovered that an App "A" is in communication reach. Its contact details are….

Figure B.10 — CVIS Figure 25: Illustration of publish subscribe scenario

The "publish-subscribe" sequence diagram is shown in Figure B.11 (CVIS Figure 26) Once again, the scenario includes a provider and a consumer side. After registration with the *DDS*, with the "*isPublish*" flag set to 'true', the *DDS* start continuous broadcasting of service announcements based on the information in the description object. As soon as a consumer comes within the transmission range, the consumer *DDS* picks up this broadcast and relays it directly to the actual application that has subscribed to this particular service. The *DDS* relies on services provided by the underlying communication infrastructure to provide this broadcast-and-detect facility. The connection is set up by the connection manager similarly as for the search scenario. Thus the interaction with the connection manager is not shown in Figure B.11 (CVIS Figure 26).

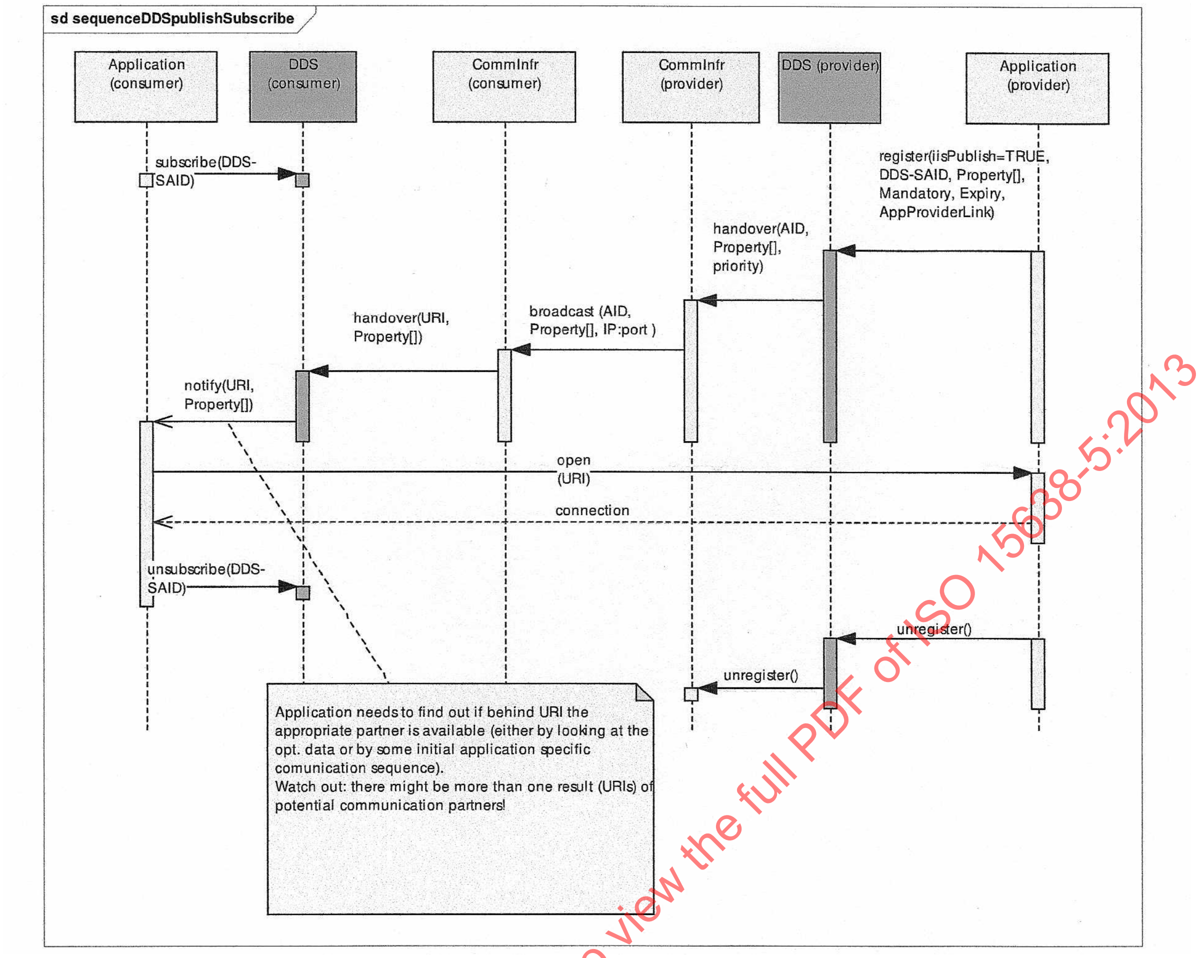
sd sequenceDDSpublishSubscribe
Application (consumer)
DDS (consumer)
CommInfr (consumer)
CommInfr (provider)
DDS (provider)
Application (provider)
subscribe(DDS-SAID)
register(iisPublish=TRUE, DDS-SAID, Property[], Mandatory, Expiry, AppProviderLink)
handover(AID, Property[], priority)
broadcast (AID, Property[], IP:port)
handover(URI, Property[])
notify(URI, Property[])
open (URI)
connection
unsubscribe(DDS-SAID)
unregister()
unregister()
Application needs to find out if behind URI the appropriate partner is available (either by looking at the opt. data or by some initial application specific comunication sequence).
Watch out: there might be more than one result (URIs) of potential communication partners!

Figure B.11 — CVIS: Sequence DDS Publish/Subscribe

In some cases applications can be mandatory. For instance authorities of regions, e.g. a city authority, can require some applications, e.g. a particular tolling application, to be present to allow entrance into the region. When registering such an application both the "*isPublish*" flag and the "*Mandatory*" flag need to be set. The "*isPublish*" flag ensures broadcasting of service announcements and the "*Mandatory*" flag ensures that if the application is not available a download action is triggered. This scenario is a special case of the above "Publish-Subscribe" scenario. The sequence diagram is shown in Figure B.12 (CVIS Figure 27).

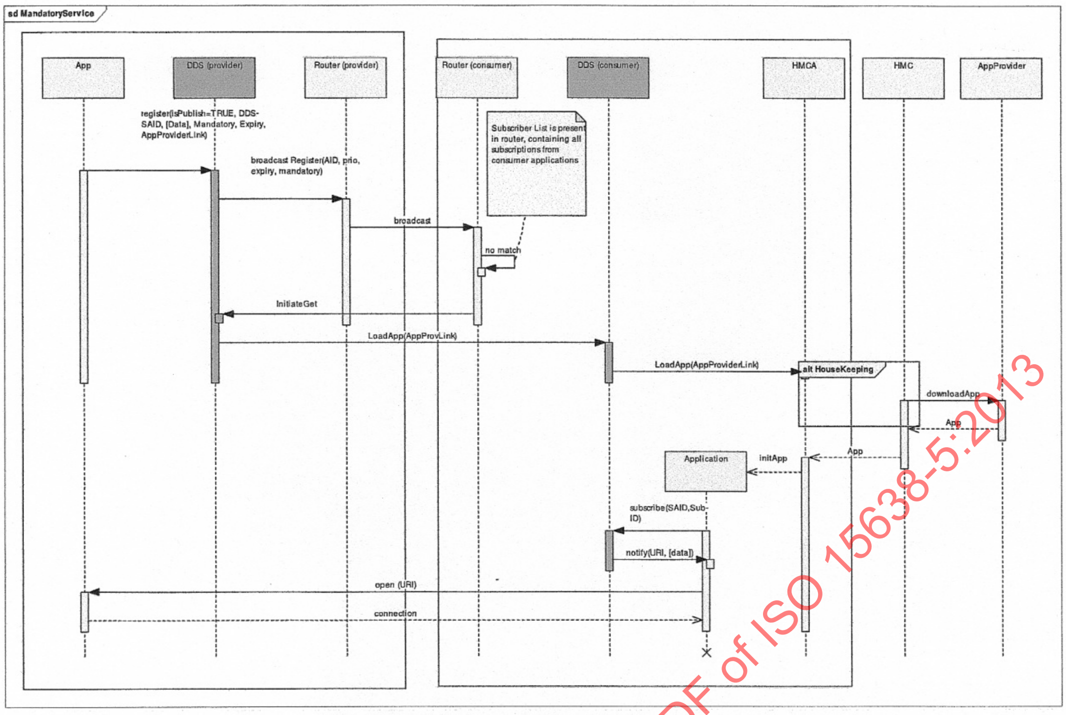

Figure B.12 — CVIS Figure 27: Mandatory service

Annex C
(informative)

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

C.1 Objectives

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

Instigation

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

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

The vehicle sends the datafile to the predetermined destination IPv6 (internet) address

Recipient address sends acknowledgement

IVS closes the communication on receipt of acknowledgement

Interrogation

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

The IVS of a vehicle is switched on but is not connected

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

On receipt it acknowledges the request (ACK)

It closes the communication

Opens a new communication session using one of (and must be tested for each of) several wireless media defined below.

Sends the datafile to a predetermined destination IPv6 (internet) address

Recipient address sends acknowledgement

IVS Closes the communication on receipt of acknowledgement

These scenarios need to be tested using each of 2G, 3G, WiFi, 5.9GHz (IEEE802.11) using the same data

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

In respect of ‘interrogation’ scenarios the ability to receive the interrogation on one medium (esp. 5.9GHz) and to instigate the subsequent message using a different medium needs to be tested

Preconditions, Assumptions and Simulations

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

CALM and media choice are assumed, and not s.u.t.

The vehicle is equipped with wireless communications that enable it to make communications using 2G, 3G, Mesh WiFi, 5.9GHz (IEEE 802.11p)

The means to trigger the sending of a message from the vehicle is a function of IVS design, not s.u.t., therefore may be simulated

The destination address is intended to be an IPv6 address, but may be simulated with an IPv4 address as this is an internet issue, not s.u.t.

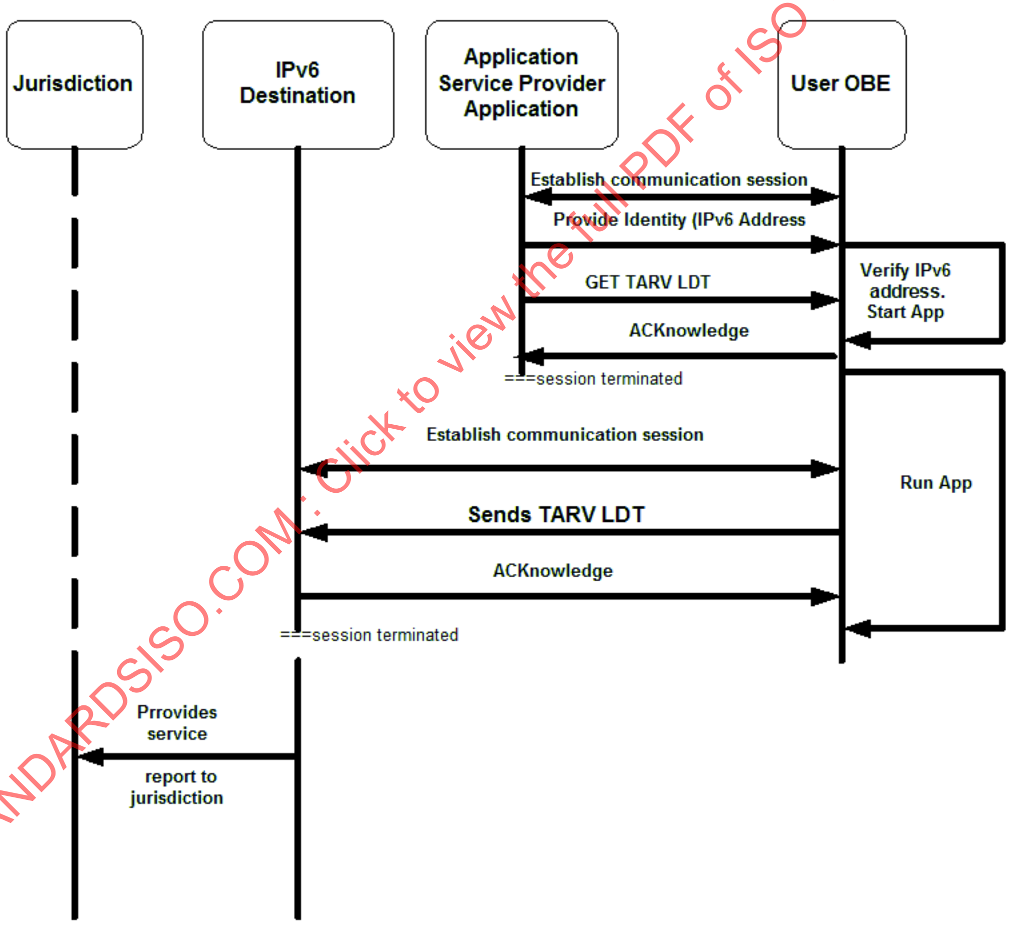

Figure C.1 — Communications sequences to obtain TARV LDT

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

VAM	*vehicle access monitoring*
RTM	*remote electronic tachograph monitoring*
EMS	*emergency messaging system*

DWR	*driver work records* (work and rest hours compliance)
VMM	*vehicle mass monitoring*
VMC	*vehicle mass charging (no test - data as VMM)*
VAC	*vehicle access control (no test - data as VAM)*
VLM	*vehicle location monitoring*
VSM	*vehicle speed monitoring*
CLM	*consignment and location monitoring*
ADR	*Accord Dangereuses par Route (Dangerous Goods) monitoring*
VPF	*vehicle parking facilities*

C.2 Test script 1 LDT Service : Local Data Tree

CTP 1.1.1 Instigated LDT using 2G

SUT Reference	**Instigated send of LDT data using 2G**
CTP/1.1.1	
.	
SUT Test Objective	The IVS of a vehicle establishes a new communication using one of (and must be tested for each of) several wireless media defined below. The IVS of a vehicle internally triggers a requirement to send a packet of data to a predetermined destination IPv6 (internet) address The vehicle sends the datafile to the predetermined destination IPv6 (internet) address Recipient address sends acknowledgement IVS closes the communication on receipt of acknowledgement
CTP Origin	CSI
Reference requirement	**ISO 15638-8 and ISO 15638-6 Clause 8.3.4.2**
Initial Conditions	The s.u.t concerns only the communication between the IVS and the application service provider address. No other part of the system specifications are to be tested (they appear in the figures below for context, and because there are copied from the base standards.) CALM and media choice are assumed and not s.u.t. The vehicle is equipped with wireless communications that enable it to make communications using 2G, 3G, WiFi, 5.9GHz (IEEE802.11p)

	The means to trigger the sending of a message from the vehicle is a function of IVS design, not s.u.t., therefore may be simulated The destination address is intended to be an IPv6 address, but may be simulated with an IPv4 address as this is an internet issue, not s.u.t.

Stimulus and expected behaviour

Test point		**Tester action**	**Pass Condition**
1.1.1.1	1	IVS instigates a communication session using selected media (2G) to predetermined destination IP address	Session established
1.1.1.2	2	IVS sends file named <44EMV03WRRLDT> <START> <AaaSs0,,0,xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx,128..165 11,1G1JF27W8GJ178227,000000,1297339499,0x0A5D3770, 0x027E2938,0000,Sat8,0,123,Ign 1,000,000,010326 UKPeter Jones,01,02,03a,h1,120325,010326 124538, Peter Jones 01,02,h1120325> <END>	File sent and arrives correctly at destination
1.1.1.3	3	Destination address sends ACK <LDX>	
1.1.1.4	4	IVS receives ACK <LDX>	File received and ACK <LDX> sent
1.1.1.5	5	IVS closes communication session	Communication session closed

			If ALL individual pass conditions listed in this column above have been met
			THEN CTP PASS
			ELSE CTP FAIL

.

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

CTP 1.1.2 Interrogated LDT using 2G

SUT Reference	Interrogated send of LDT data using 2G
CTP/1.1.2	
.	
SUT Test Objective	The IVS of a vehicle receives a wireless interrogation requesting a packet of data. The IVS of a vehicle is switched on but is not connected The IVS of a vehicle receives a 2G wireless interrogation requesting a packet of data. On receipt it acknowledges the request (ACK) It closes the communication Opens a new communication session using one of (and must be tested for each of) several wireless media defined below. Sends the datafile to a predetermined destination IPv6 (internet) address Recipient address sends acknowledgement IVS Closes the communication on receipt of acknowledgement
CTP Origin	CEN
Reference requirement	ISO 15638-8 and ISO 15638-6 Clause 8.3.4.2
Initial Conditions	The s.u.t concerns only the communication between the IVS and the application service provider address. No other part of the system specifications are to be tested (they appear in the figures below for context, and because there are copied from the base standards.) CALM and media choice are assumed and not s.u.t. The vehicle is equipped with wireless communications that enable it to make communications using 2G, 3G, WiFi, 5.9GHz (IEEE802.11p) The means to trigger the sending of a message from the vehicle is a function of IVS design, not s.u.t., therefore may be simulated The destination address is intended to be an IPv6 address, but may be simulated with an IPv4 address as this is an internet issue, not s.u.t.

Stimulus and expected behaviour

Test point		**Tester action**	**Pass Condition**
1.1.2.1	1	session connected (incoming call)	Call in progress
1.1.2.2	2	Caller sends data request command (GPRS, EDGE etc) GET VAM	Data request sent
1.1.2.3	3	IVS acknowledges request by returning ACKnowledgement <A>	ACK <A> received
1.1.2.4	4	IVS closes communication session	Communication session closed
1.1.2.5	5	IVS instigates a communication session using selected media to predetermined destination IP address	Communication session successfully opened
1.1.2.5	6	IVS sends file named <44EMV0 <START> <AaaSs0,,0,xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx,128..16511, 1G1JF27W8GJ178227,000000,1297339499,0x0A5D3770,0x027 E2938,0000,Sat8,0,123,Ign 1,000,000,010326 UKPeter Jones,01,02,03a,h1,120325,010326 124538, Peter Jones 01,02,h1120325><END>	File sent and arrives correctly at destination
1.1.2.6	7	Destination address sends ACK <LDX>	
1.1.2.7	8	IVS receives ACK <LDX>	File received and ACK <LDX> sent
1.1.2.8	9	IVS closes communication session	Communication session closed

			If ALL individual pass conditions listed in this column above have been met
			THEN CTP PASS
			ELSE CTP FAIL

.

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

CTP 1.1.3 Interrogated LDT using 5.9GHz and responding using 2G or 3G

SUT Reference	**Interrogated LDT using 5.9 GHz and send of LDT data using 2G or 3G**
CTP/1.1.3	
.	
SUT Test Objective	The IVS of a vehicle receives a wireless interrogation requesting a packet of data. The IVS of a vehicle is switched on but is not connected The IVS of a vehicle receives a 5.9GHz (IEEE 802.11p) wireless interrogation requesting a packet of data. On receipt it acknowledges the request (ACK) It closes the communication Opens a new communication session using 2G or 3G. Sends the datafile to a predetermined destination IPv6 (internet) address Recipient address sends acknowledgement IVS Closes the communication on receipt of acknowledgement
CTP Origin	CEN
Reference requirement	**ISO 15638-8 and ISO 15638-6 Clause 8.3.4.2**
Initial Conditions	The s.u.t concerns only the communication between the IVS and the application service provider address. No other part of the system specifications are to be tested (they appear in the figures below for context, and because there are copied from the base standards.) CALM and media choice are assumed and not s.u.t. The vehicle is equipped with wireless communications that enable it to make communications using 2G, 3G, WiFi, 5.9GHz (IEEE802.11p) The means to trigger the sending of a message from the vehicle is a function of IVS design, not s.u.t., therefore may be simulated The destination address is intended to be an IPv6 address, but may be simulated with an IPv4 address as this is an internet issue, not s.u.t.

Stimulus and expected behaviour

Test point		Tester action	Pass Condition
1.1.3.1	1	session connected (incoming call) using 5.9 Ghz (IEEE 802.11p)	Call in progress
1.1.3.2	2	Caller sends data request command GET LDT	Data request sent
1.1.3.3	3	IVS acknowledges request by returning ACKnowledgement <A>	ACK <L> received
1.1.3.4	4	IVS closes communication session	Communication session closed
1.1.3.5	5	IVS instigates a communication session using 2G or 3G	Communication session successfully opened
1.1.3.5	6	IVS sends file named <44EMV03WRRLDT> <START> <AaaSs0,,0,xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx,128..16511, 1G1JF27W8GJ178227,000000,1297339499,0x0A5D3770,0x027 E2938,0000,Sat8,0,123,Ign 1,000,000,010326 UKPeter Jones,01,02,03a,h1,120325,010326 124538, Peter Jones 01,02,h1120325><END>	File sent and arrives correctly at destination
1.1.3.6	7	Destination address sends ACK <LDX>	
1.1.3.7	8	IVS receives ACK <LDX>	File received and ACK <LDX> sent
1.1.3.8	9	IVS closes communication session	Communication session closed

			If ALL individual pass conditions listed in this column above have been met
			THEN CTP PASS
			ELSE CTP FAIL

.

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

CTP 1.2.1 Instigated LDT using 3G

SUT Reference	**Instigated send of LDT data using 3G**
CTP/1.2.1	
SUT Test Objective	The IVS of a vehicle establishes a new communication using one of (and must be tested for each of) several wireless media defined below. The IVS of a vehicle internally triggers a requirement to send a packet of data to a predetermined destination IPv6 (internet) address The vehicle sends the datafile to the predetermined destination IPv6 (internet) address Recipient address sends acknowledgement IVS closes the communication on receipt of acknowledgement
CTP Origin	CSI
Reference requirement	**ISO 15638-8 and ISO 15638-6 Clause 8.3.4.2**
Initial Conditions	The s.u.t concerns only the communication between the IVS and the application service provider address. No other part of the system specifications are to be tested (they appear in the figures below for context, and because there are copied from the base standards.) CALM and media choice are assumed and not s.u.t. The vehicle is equipped with wireless communications that enable it to make communications using 2G, 3G, WiFi, 5.9GHz (IEEE802.11p) The means to trigger the sending of a message from the vehicle is a function of IVS design, not s.u.t., therefore may be simulated The destination address is intended to be an IPv6 address, but may be simulated with an IPv4 address as this is an internet issue, not s.u.t.

Stimulus and expected behaviour

Test point		**Tester action**	**Pass Condition**
1.2.1.1	1	IVS instigates a communication session using selected media (3G) to predetermined destination IP address	Session established
1.2.1.2	2	IVS sends file named <44EMV03WRRLDT> <START> <AaaSs0,,0,xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx,128..16511,1G1JF27W8GJ178227,000000,1297339499,0x0A5D3770,0x027E2938,0000,Sat8,0,123,Ign	File sent and arrives correctly at destination

		1,000,000,010326 UKPeter Jones,01,02,03a,h1,120325,010326 124538, Peter Jones 01,02,h1120325> <END>	
1.2.1.3	3	Destination address sends ACK <LDX>	
1.2.1.4	4	IVS receives ACK <LDX>	File received and ACK <LDX> sent
1.2.1.5	5	IVS closes communication session	Communication session closed

			If ALL individual pass conditions listed in this column above have been met
			THEN CTP PASS
			ELSE CTP FAIL

.

TEST RESULT: CTP 1.2.1	PASS / FAIL	Date: 28th June 2102
Signature/initials	**PASS**	innovITS ADVANCE k4, MIRA, Watling St, Nuneaton, Warwickshire, CV10 0TU, UK **Tel: +44 (0)7730 922 810** Web: www.innovits.com/advance

CTP 1.2.2 Interrogated at 5.9 GHz and send of LDT using 3G

SUT Reference	**5.8GHz Interrogated and send of LDT data using 3G**
CTP/1.2.2	
SUT Test Objective	The IVS of a vehicle receives a wireless interrogation requesting a packet of data. The IVS of a vehicle is switched on but is not connected The IVS of a vehicle receives a wireless interrogation requesting a packet of data. On receipt it acknowledges the request (ACK) It closes the communication Opens a new communication session using one of (and must be tested for each of) several wireless media defined below. Sends the datafile to a predetermined destination IPv6 (internet) address Recipient address sends acknowledgement IVS Closes the communication on receipt of acknowledgement
CTP Origin	CEN
Reference requirement	**ISO 15638-8 and ISO 15638-6 Clause 8.3.4.2**
Initial Conditions	The s.u.t concerns only the communication between the IVS and the application service provider address. No other part of the system specifications are to be tested (they appear in the figures below for context, and because there are copied from the base standards.) CALM and media choice are assumed and not s.u.t. The vehicle is equipped with wireless communications that enable it to make communications using 2G, 3G, WiFi, 5.9GHz (IEEE802.11p) The means to trigger the sending of a message from the vehicle is a function of IVS design, not s.u.t., therefore may be simulated The destination address is intended to be an IPv6 address, but may be simulated with an IPv4 address as this is an internet issue, not s.u.t.

Stimulus and expected behaviour

Test point		Tester action	Pass Condition
1.2.2.1	1	session connected (incoming call) using 5.9 Ghz (IEEE 802.11p)	Call in progress
1.2.2.2	2	Caller sends data request command GET LDT	Data request sent
1.2.2.3	3	IVS acknowledges request by returning ACKnowledgement <L>	ACK <L> received
1.2.2.4	4	IVS closes communication session	Communication session closed

1.2.2.5	5	IVS instigates a communication session using selected media (2G or 3G) to predetermined destination IP address	Communication session successfully opened
1.2.2.5	6	IVS sends file named <44EMV03WRRLDT> <START> <AaaSs0,,0,xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx,128..16511,1G1JF27W8GJ178227,000000,1297339499,0x0A5D3770,0x027E2938,0000,Sat8,0,123,Ign 1,000,000,010326 UKPeter Jones,01,02,03a,h1,120325,010326 124538, Peter Jones 01,02,h1120325>	File sent and arrives correctly at destination
1.2.2.6	7	Destination address sends ACK <LDX>	
1.2.2.7	8	IVS receives ACK <LDX>	File received and ACK <LDX> sent
1.2.2.8	9	IVS closes communication session	Communication session closed

			If ALL individual pass conditions listed in this column above have been met
			THEN CTP PASS
			ELSE CTP FAIL

.

TEST RESULT: CTP 1.2.2	**PASS / FAIL**	**Date: 28th June 2102**
Signature/initials	**PASS**	innovITS ADVANCE k4, MIRA, Watling St, Nuneaton, Warwickshire, CV10 0TU, UK **Tel: +44 (0)7730 922 810** Web: www.innovits.com/advance

CTP 1.3.1 Instigated LDT using 802.11p (WAVE) 5.9 GHz

SUT Reference	**Instigated LDT using 802.11p (WAVE) 5.9 GHz**
CTP/1.3.1	
.	
SUT Test Objective	The IVS of a vehicle establishes a new communication using one of (and must be tested for each of) several wireless media defined below. The IVS of a vehicle internally triggers a requirement to send a packet of data to a predetermined destination IPv6 (internet) address The vehicle sends the datafile to the predetermined destination IPv6 (internet) address Recipient address sends acknowledgement IVS closes the communication on receipt of acknowledgement
CTP Origin	CSI
Reference requirement	**ISO 15638-8 and ISO 15638-6 Clause 8.3.4.2**
Initial Conditions	The s.u.t concerns only the communication between the IVS and the application service provider address. No other part of the system specifications are to be tested (they appear in the figures below for context, and because there are copied from the base standards.) CALM and media choice are assumed and not s.u.t. The vehicle is equipped with wireless communications that enable it to make communications using 2G, 3G, WiFi, 5.9GHz (IEEE802.11p) The means to trigger the sending of a message from the vehicle is a function of IVS design, not s.u.t., therefore may be simulated The destination address is intended to be an IPv6 address, but may be simulated with an IPv4 address as this is an internet issue, not s.u.t.

Stimulus and expected behaviour

Test point		**Tester action**	**Pass Condition**
1.3.1.1	1	IVS instigates a communication session using selected media (5.9G) to predetermined destination IP address	Session established
1.3.1.2	2	IVS sends file named <44EMV03WRRLDT> <START> <AaaSs0,,0,xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx,128..16511,1G1JF27W8GJ178227,000000,1297339499,0x0A5D3770,0x027E2938,0000,Sat8,0,123,Ign 1,000,000,010326 UKPeter	File sent and arrives correctly at destination

		Jones,01,02,03a,h1,120325,010326 124538, Peter Jones 01,02,h1120325> <END>	
1.3.1.3	3	Destination address sends ACK <LDX>	
1.3.1.4	4	IVS receives ACK <LDX>	File received and ACK <LDX> sent
1.3.1.5	5	IVS closes communication session	Communication session closed

			If ALL individual pass conditions listed in this column above have been met
			THEN CTP PASS
			ELSE CTP FAIL

.

TEST RESULT: CTP 1.3.1	**PASS / FAIL**	**Date: 28th June 2102**
Signature/initials	**PASS**	innovITS ADVANCE k4, MIRA, Watling St, Nuneaton, Warwickshire, CV10 0TU, UK **Tel: +44 (0)7730 922 810** Web: www.innovits.com/advance

CTP 1.3.2 Interrogated LDT using 802.11p (WAVE) 5.9 GHz

SUT Reference	**Interrogated send of LDT using 802.11p (WAVE) 5.9 GHz**
CTP/1.3.2	
.	
SUT Test Objective	The IVS of a vehicle receives a wireless interrogation requesting a packet of data. The IVS of a vehicle is switched on but is not connected The IVS of a vehicle receives a wireless interrogation requesting a packet of data. On receipt it acknowledges the request (ACK) It closes the communication Opens a new communication session using one of (and must be tested for each of) several wireless media defined below. Sends the datafile to a predetermined destination IPv6 (internet) address Recipient address sends acknowledgement IVS Closes the communication on receipt of acknowledgement
CTP Origin	CEN
Reference requirement	**ISO 15638-8 and ISO 15638-6 Clause 8.3.4.2**
Initial Conditions	The s.u.t concerns only the communication between the IVS and the application service provider address. No other part of the system specifications are to be tested (they appear in the figures below for context, and because there are copied from the base standards.) CALM and media choice are assumed and not s.u.t. The vehicle is equipped with wireless communications that enable it to make communications using 2G, 3G, WiFi, 5.9GHz (IEEE802.11p) The means to trigger the sending of a message from the vehicle is a function of IVS design, not s.u.t., therefore may be simulated The destination address is intended to be an IPv6 address, but may be simulated with an IPv4 address as this is an internet issue, not s.u.t.

Stimulus and expected behaviour

Test point		**Tester action**	**Pass Condition**
1.3.2.1	1	session connected (incoming call) using 5.9 Ghz (IEEE 802.11p)	Call in progress
1.3.2.2	2	Caller sends data request command GET LDT	Data request sent
1.3.2.3	3	IVS acknowledges request by returning ACKnowledgement <L>	ACK <L> received
1.3.2.4	4	IVS closes communication session	Communication session closed
1.3.2.5	5	IVS instigates a communication session using 5.9GHz selected media to predetermined destination IP address	Communication session successfully opened
1.3.2.5	6	IVS sends file named <44EMV03WRRLDT> <START> <AaaSs0,,0,xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx,128..16511,1G 1JF27W8GJ178227,000000,1297339499,0x0A5D3770,0x027E2938, 0000,Sat8,0,123,Ign 1,000,000,010326 UKPeter Jones,01,02,03a,h1,120325,010326 124538, Peter Jones 01,02,h1120325><END>	File sent and arrives correctly at destination
1.3.2.6	7	Destination address sends ACK <LDX>	
1.3.2.7	8	IVS receives ACK <LDX>	File received and ACK <LDX> sent
1.3.2.8	9	IVS closes communication session	Communication session closed

			If ALL individual pass conditions listed in this column above have been met
			THEN CTP PASS
			ELSE CTP FAIL

.

TEST RESULT: CTP 1.3.2	**PASS / FAIL**	**Date: 28th June 2102**
Signature/initials	**PASS**	innovITS ADVANCE k4, MIRA, Watling St, Nuneaton, Warwickshire, CV10 0TU, UK **Tel: +44 (0)7730 922 810** Web: www.innovits.com/advance

CTP 1.4.1 Instigated LDT using Mesh WiFi

SUT Reference	**Instigated send of LDT data using Mesh WiFi**
CTP/1.4.1	
SUT Test Objective	The IVS of a vehicle establishes a new communication using one of (and must be tested for each of) several wireless media defined below. The IVS of a vehicle internally triggers a requirement to send a packet of data to a predetermined destination IPv6 (internet) address The vehicle sends the datafile to the predetermined destination IPv6 (internet) address Recipient address sends acknowledgement IVS closes the communication on receipt of acknowledgement
CTP Origin	CSI
Reference requirement	**ISO 15638-8 and ISO 15638-6 Clause 8.3.4.2**
Initial Conditions	The s.u.t concerns only the communication between the IVS and the application service provider address. No other part of the system specifications are to be tested (they appear in the figures below for context, and because there are copied from the base standards.) CALM and media choice are assumed and not s.u.t. The vehicle is equipped with wireless communications that enable it to make communications using 2G, 3G, WiFi, 5.9GHz (IEEE802.11p) The means to trigger the sending of a message from the vehicle is a function of IVS design, not s.u.t., therefore may be simulated The destination address is intended to be an IPv6 address, but may be simulated with an IPv4 address as this is an internet issue, not s.u.t.

Stimulus and expected behaviour

Test point		**Tester action**	**Pass Condition**
1.4.1.1	1	IVS instigates a communication session using selected media (Mesh WiFi) to predetermined destination IP address	Session established
1.4.1.2	2	IVS sends file named <44EMV03WRRLDT> <START> <AaaSs0,,0,xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx,128..165 11,1G1JF27W8GJ178227,000000,1297339499,0x0A5D3770,	File sent and arrives correctly at destination

		0x027E2938,0000,Sat8,0,123,Ign 1,000,000,010326 UKPeter Jones,01,02,03a,h1,120325,010326 124538, Peter Jones 01,02,h1120325> <END>	
1.4.1.3	3	Destination address sends ACK <LDX>	
1.4.1.4	4	IVS receives ACK <LDX>	File received and ACK <LDX> sent
1.4.1.5	5	IVS closes communication session	Communication session closed

			If ALL individual pass conditions listed in this column above have been met
			THEN CTP PASS
			ELSE CTP FAIL

.

TEST RESULT: CTP 1.4.1	**PASS / FAIL**	**Date: 28th June 2102**
Signature/initials	**PASS**	innovITS ADVANCE k4, MIRA, Watling St, Nuneaton, Warwickshire, CV10 0TU, UK **Tel: +44 (0)7730 922 810** Web: www.innovits.com/advance