Technical Specification

ISO/TS 7815-1

First edition
2025-01

Intelligent transport systems — Telematics applications for regulated commercial freight vehicles (TARV) using ITS stations —

Part 1: Secure vehicle interface framework and architecture

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

Partie 1: Cadre et architecture de l'interface sécurisée du véhicule

Reference number
ISO/TS 7815-1:2025(en)

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

Published in Switzerland

Contents

Page

Foreword

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

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

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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

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

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

A list of all parts in the ISO 7815 series can be found on the ISO website.

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

Introduction

Many intelligent transport system (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. Such regulatory services in use or under consideration vary from region to region, but include electronic on-board recorders, vehicle charging, digital tachograph, on-board mass monitoring, emissions monitoring, vehicle access monitoring, hazardous goods tracking and eCall. Additional applications with a regulatory impact currently under development include fatigue management, speed monitoring and heavy vehicle charging based on mass, location, distance and time.

In this emerging environment of regulatory and commercial applications, between 2008 and 2012, ISO 15638-1 was developed and approved, enabling on-board equipment and back-office systems to be commercially designed in an open market, meeting the common requirements of jurisdictions.

Although the concept of co-operative ITS (C-ITS) was well advanced at this time, its implementation was not. In particular, provisions for achieving the "bounded secure managed domain," required by ISO 21217, were still in their early stages of development. Security (i.e. "cybersecurity") was a significant concern, given that the communications means themselves were not necessarily very secure. Telematics applications for regulated commercial freight vehicles (TARV), designed to work with whatever wireless communications interface are available in the vehicle, offered a solution to this problem: the enquirer would provide a requested destination address and reference for the data. The vehicle response would then be to send the data (along with the requested destination address and reference) directly and only to its landside "application service provider" (ASP), a contracted secure provider. As a trusted party approved by the jurisdiction, the ASP would validate the request and destination address before forwarding the information to that address. TARV was flexible in concept, and could be adapted to different jurisdictional arrangements.

ISO 15638-2 provided a migration path to C-ITS enabled vehicles, but remained devoid of the necessary security parameters, so the passage to data to the jurisdiction remained via the secure and trusted ASP.

In the decade since 2010, with the publication of ISO 21177, the necessary security and data exchange protocols have been finalized to provide a "secure vehicle interface" (SVI) in which two devices can cooperate in a trusted way, i.e. exchange information in secure application sessions with optional explicit bi-directional protection. The devices can thus only access data or request data for which they have the appropriate access credentials. The trust relation between two devices is illustrated in Figure 1.

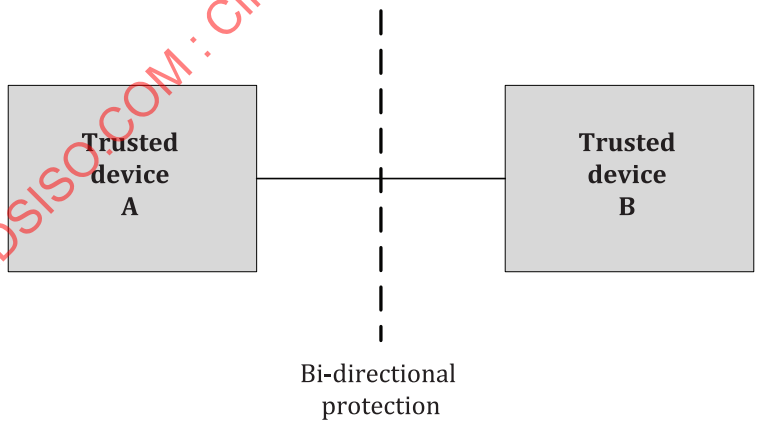


Figure 1 — Interconnection of trusted devices (ISO 21177)

Taking these developments into account, while the ISO 15638 series remains valid and appropriate in many cases, it is also appropriate to provide specifications for the direct transfer of data using a secure vehicle interface. This document provides the specification of the architecture and framework within which such transactions can be undertaken.

Intelligent transport systems — Telematics applications for regulated commercial freight vehicles (TARV) using ITS stations —

Part 1: Secure vehicle interface framework and architecture

1 Scope

This document specifies the following elements for cooperative telematics applications for regulated commercial freight vehicles directly communicating via a secure vehicle interface:

a) a framework for the provision of cooperative telematics application services for regulated commercial freight vehicles;

b) a description of the concept of operation, regulatory aspects and options and the role models;

c) a conceptual architecture using an on-board platform and wireless communications to a regulator or their agent;

d) references for the key documents on which the architecture is based;

e) the architecture of the facilities layer;

f) a taxonomy of the organization of generic procedures.

This document does not replace, but is complementary to ISO 15638-1. It provides an alternative communication architecture for achieving similar service provision by means of a standardized secure vehicle interface.

2 Normative references

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

ISO/TS 7815-2, *Intelligent transport systems — Telematics applications for regulated commercial freight vehicles (TARV) using ITS stations — Part 2: Specification of the secure interface*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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

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

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

3.1
application service
service provided by a service provider accessing data from the in-vehicle system (IVS) of a regulated commercial freight vehicle via a wireless communications network

3.2
appoint
assign officially to take responsibility for a role

3.3
architecture
formalized description of the design of the structure of the telematics applications for regulated commercial freight vehicles secure vehicle interface (TARV-SVI) and its framework

3.4
controller area networking bus
CAN bus
network designed for use in automotives

Note 1 to entry: See ISO 11898-1, ISO 11898-2 and ISO 11898-3 for further information.

Note 2 to entry: CAN uses a single terminated twisted pair cable and is multi-master. The maximum signal frequency used is 1 Mbit/s, with a typical length of 40 m at 1 Mbit/s up to 10 km at 5 Kbit/s.

Note 3 to entry: CAN has high reliability with extensive error checking. The typical maximum data rate achievable is 40 KB/s. The maximum latency of a high priority message < 120 µs at 1 Mbit/s.

Note 4 to entry: CAN is unusual in that the entities on the network, called nodes, are not given specific addresses. Instead, it is the messages themselves that have an identifier which also determines the messages' priority. For this reason there is no theoretical limit to the number of nodes, although in practice it is approximately 63.

3.5
certificate authority
<digital> organization which issues digital certificates for use by other parties, specifically in the context of communications security

3.6
commercial application
intelligent transport systems (ITS) application in regulated commercial freight vehicles for commercial (non-regulated) purposes

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

3.7
framework
particular set of beliefs or ideas referred to in order to describe a scenario or solve a problem

3.8
global navigation satellite system
GNSS
several networks of satellites that transmit radio signals containing time and distance data that can be picked up by a receiver, allowing the user to identify the location of its receiver anywhere around the globe

[SOURCE: ISO 15638-1:2012, 4.21, modified — "comprises" has been removed from the beginning of the definition.]

3.9
in-vehicle system
IVS
intelligent transport system (ITS) station and connected equipment on board a vehicle

3.10
jurisdiction
government, road or traffic authority which owns the regulatory applications

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

3.11
map
spatial dataset that defines the road system

3.12
on-board unit
OBU
integrated telematics unit installed on board which provides the specified telematics functionality required for the in-vehicle system (IVS)

3.13
regulated application
regulatory application approval arrangement utilized by jurisdictions for granting certain categories of commercial vehicle rights to operate in regulated circumstances subject to certain conditions

Note 1 to entry: Each jurisdiction may use their own terminology including, but not limited to, "permit", "application", "scheme", "concession", "exemption", "gazettal" and "notice".

3.14
regulated application service
telematics applications for regulated commercial freight vehicles (TARV) application service that is mandated by a regulation imposed by a jurisdiction, or an option supported by a jurisdiction

3.15
regulated commercial freight vehicle
vehicle (often but not always designed to haul commercial freight) that is subject to regulations determined by the jurisdiction as to its use on the road system of the jurisdiction in regulated circumstances, subject to certain conditions, and in compliance with specific regulations for that class of vehicle

Note 1 to entry: Jurisdictions can choose to require the provision of information via telematics applications for regulated commercial freight vehicles (TARV) or provide operators with the option to do so.

3.16
specification
explicit and detailed description of the nature and functional requirements and minimum performance of equipment, service or a combination of both

3.17
Unified Modeling Language
UML
graphical language for visualizing, specifying, constructing and documenting the artifacts of a software-intensive system

Note 1 to entry: UML offers a standard way to write a system's blueprints, including conceptual elements such as business processes and system functions as well as concrete elements such as programming language statements, database schemas, and reusable software components, and is standardized as ISO/IEC 19501.

3.19
user
party that makes use of the vehicle

EXAMPLE Driver, transport operator, freight owner, etc.

4 Abbreviated terms

For the purposes of this document, the following abbreviated terms apply.

app	application programme
CAN	controller area network
C-ITS	cooperative intelligent transport systems
CONOPS	concept of operations
ExVe	extended vehicle (ISO 20077-1)
GNSS	global navigation satellite system
ITS	intelligent transport system
IVS	in-vehicle system
OBU	on-board unit
OEM	original equipment manufacturer
PKI	public key infrastructure
PKC	public key certificate
RAM	random access memory
TARV	telematics applications for regulated commercial freight vehicles
SCMS	security credential management system
SSP	secure service provider
SVI	secure vehicle interface
UML	Unified Modeling Language (ISO)) 19501)
V2I	vehicle to infrastructure (communication)
V2V	vehicle to vehicle communication
VRU	vulnerable road user

5 Conformance

This document specifies an adaptation of the TARV general architecture. It contains no specific conformance tests. It is possible that some aspects defined within will have conformance tests defined in other parts of the ISO 7815 series, or in the ISO 15638 series.

Conformance declarations for the various parts of the SVI shall be based on the relevant referenced SVI International Standards.

Conformance to any other International Standard or specification referenced in this document shall be ascertained according to the requirements of the referenced document.

Conformance to this document can therefore be attained by self-declaration of conformance, or submission to a test house to ascertain adherence to the provisions of the clauses of this document.

6 General overview and framework

6.1 Objective

This clause describes a generic framework for the provision of cooperative telematics application services for regulated commercial freight vehicles. Clause 7 provides the general concept of operations for which this architecture is designed. Clause 8 provides a framework, role definition and elaboration of the architecture at a conceptual level. Clause 9 defines the communications architecture. The objectives regarding service provision in this document are the same as those defined in ISO 15638-1, but are delivered by different means.

6.2 National variations

6.2.1 As stated in the scope of ISO 15638-1, the definition of what comprises a "regulated" vehicle is regarded as an issue for national decision and can vary from region to region.

6.2.2 It is likely that the instantiation of interoperable on-board platforms for regulated commercial freight vehicles with common features will vary from region to region, as will the provision of regulated, or supported, services.

6.2.3 It is possible that some regions will mandate the use of such a platform, whereas others will offer it as an option to meet the requirements of a given regulation with minimum administration and paperwork (thereby providing a good business case for operators to fit and use the equipment).

6.2.4 It is possible that some regions will choose to implement a single, government-operated, controlled, or contracted service provider, which will be the single communication manager between the vehicle and the service. Other regions will potentially provide a market-based solution with multiple service providers competing for the business of vehicle operators.

6.3 Mandatory, optional and cooperative issues

6.3.1 As stated in 6.2.1, the definition of what comprises a "regulated" service is regarded as an issue for national decision, and can vary from region to region. Furthermore, services can be required by a regulator, or alternatively, they can be supported by a regulator, but not required.

EXAMPLE The choice can be provided to use electronic means to plan, approve and monitor the movement of a hazardous cargo journey, or to use a traditional paper request, approval and monitoring option.

6.3.2 The IVS may also support the provision of other commercial application services that are not required by the regulator.

6.3.3 No requirements are imposed by the ISO 7815 series and the ISO 15638 series regarding which services for regulated commercial freight vehicles a given region will require, or which they will support as an option. Instead, the ISO 7815 series and the ISO 15638 series provide a generic common architecture within which regions can achieve their own objectives regarding application services for regulated commercial freight vehicles. The ISO 7815 series and the ISO 15638 series also provide standardized sets of requirements descriptions for identified services to enable consistent and cost-efficient implementations where instantiated.

6.3.4 Within the context of this document, cooperative ITS applications refer to the use of a common on-board platform to meet both regulated and commercial service provision.

6.4 Specification of service provision

Cooperative ITS applications for regulated commercial freight vehicles (both regulated services and commercial services) are specified in terms of service provision, and not in terms of hardware and software.

6.5 Architecture options

Architecturally, it is necessary for a vehicle operator to be able to use the services of different service providers. The in-vehicle system can be a vehicle original equipment specification option, inbuilt at the time of manufacture of the vehicle, with the service provider selection being a subsequent user choice, or it can be aftermarket equipment that has access rights to the required data. Other options are possible and should be able to be supported within the conceptual architecture.

7 Concept of operations

7.1 General

A "concept of operations" (CONOPS) generally evolves from a concept and is a description of how a set of capabilities can be employed to achieve desired objectives. This clause describes the characteristics of a proposed system from the viewpoint of an individual who will use that system. Its objective is to communicate the quantitative and qualitative system characteristics to all stakeholders.

This document describes the roles and responsibilities of the classes and actors involved in the provision of regulated services for regulated commercial freight vehicles using a secure vehicle interface.

This document recognizes that there will be variations between jurisdictions. It does not attempt, nor recommend, homogeneity between jurisdictions. Rather, it is designed to provide common standard features in order to make it possible to have equipment of common specification, which supports a standardized SVI and common features of service provision. The intention is to enable referencing by a jurisdiction within its regulatory or legislative regime by way of a simple reference to an International Standard, meaning that only the additional requirements of that jurisdiction will need to be further specified.

7.2 Statement of the goals and objectives of the system

The overall objective of TARV is the assessment, monitoring, management, and in some cases control, of regulated commercial freight vehicles to meet the requirements of the jurisdiction within it is operating domain, using telematics.

This is achieved by the provision of application services for specific aspects of the control and management of regulated commercial freight vehicles (for examples, see ISO 15638-9 to ISO 15638-25). These services are required by regulation of the jurisdiction or are provided by agreement with the user, to meet the requirements of the jurisdiction using an in-vehicle system with an SVI communications capability between the vehicle and the jurisdiction and access to relevant data from the regulated commercial freight vehicle.

NOTE ISO/TS 5616 includes a specification of an SVI.

7.3 Strategies, tactics, policies and constraints affecting the system

Strategies, tactics, policies, constraints and even the services that are regulated as mandatory or optionally supported can vary from jurisdiction to jurisdiction. Clause 6 provides detail of the options for such aspects.

7.4 Organizations, activities and interactions among participants and stakeholders

The classes, attributes and key relationships are described in Clause 8.

7.5 Responsibilities and authorities delegated

Clause 6 describes the high-level options and issues. The actors involved, their responsibilities and authorities are described in Clause 8. The roles are described in Clause 8 and in this clause (Clause 7).

7.6 Operational processes for the system

7.6.1 General

The following description of operational processes is at a high abstracted level (above that of any particular application service). Specific services can have additional requirements not described herein. Guidance and specification for additional aspects can be obtained from ISO 15638-6 and ISO 15638-7.

7.6.2 Definition of service requirements

A jurisdiction passes legislation or regulations to require or support the provision of a particular application service. The legislation or regulation needs to provide a clear and unambiguous definition of what is required.

7.7 Appointment of an approval authority (regulatory)

The jurisdiction creates or appoints an authority to approve and audit the process. The structure of that authority is a matter for the jurisdiction and it can be a separate appointed organization, or a department of the jurisdiction. Within the context of this document, it is the actor (role) of "approval authority" that is important, not its structure, ownership or business model.

An approval authority (regulatory) may preside over only the instantiation and operation of one particular application service, or may preside over the instantiation and operation of some or all application services for regulated commercial freight vehicles (at the discretion of the jurisdiction).

The approval authority (regulatory) will, where appropriate, approve service providers, IVS, and will provide an audit as described in Clause 6, in accordance with the requirements of the jurisdiction.

NOTE The TARV approval authority is described throughout as the "approval authority (regulatory)" to clearly distinguish it from a certificate authority which issues digital certificates (particularly in the context of communications security).

7.8 In-vehicle system

In TARV-SVI, the in-vehicle system (IVS) that provides the application service is an ITS trusted device that meets the requirements of ISO/TS 7815-2.

7.9 User

The user is usually the operator of the regulated commercial freight vehicle, but in some cases it can be the driver.

It is the responsibility of the operator of the vehicle to have its vehicle equipped to enable it to provide the service (regardless of whether the user of the service is the vehicle operator or the driver of the vehicle).

7.10 Application service

In the TARV-SVI paradigm, the vehicle IVS is designed to provide the requested data, either cyclically, or on request.

In a cyclical implementation, the IVS is pre-programmed to provide the information at predetermined times, or in the event of pre-defined parameters being exceeded, to an address predetermined by the jurisdiction, with that address offering the appropriate credentials to the SVI.

In an "on request" implementation, an ITS trusted device of the jurisdiction, offering the appropriate credentials via the SVI will request pre-specified information from the IVS, which, on confirmation of the credentials of the requestor for the requested information will provide this requested information via the SVI.

An IVS can be, but is not necessarily, set up to deal with one or both cyclical and on request demands for information.

The nature and definition of the information supplied shall be the subject of a regulation, formal notification or shall be defined in a standard.

8 Conceptual architecture framework

8.1 General

Clause 7 provided the generic concept of operations which actors and classes enact in order to provide application service(s). In order to specify a generic framework standard of the ITS service platform, this document identifies core actors and classes in 8.2 to 8.4, which are described as elements which are independent of any specific application.

8.2 Actors

This document defines a role model where the roles and responsibilities of three key actor classes are defined to provide an entity known as an "application service":

a) the "Jurisdiction(s)";

b) the "Users";

c) the "Service provider(s)";

Figure 2 provides the general attributes and the responsibilities of these parties, illustrating a conceptual role model architecture for TARV-SVI.

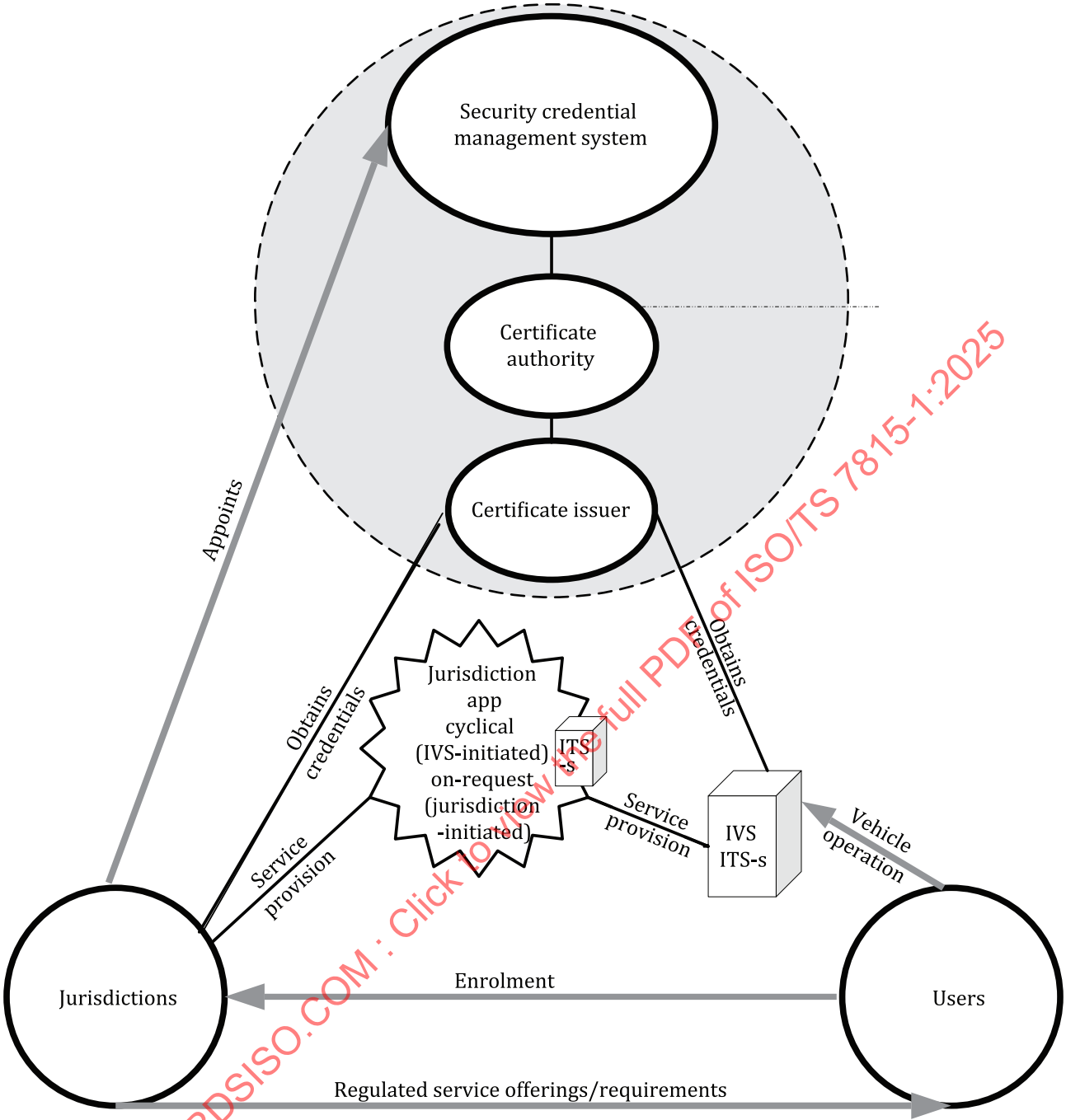


Figure 2 — Role model conceptual architecture

Using a UML approach, the relationships between the classes can be represented as shown in Figure 3.

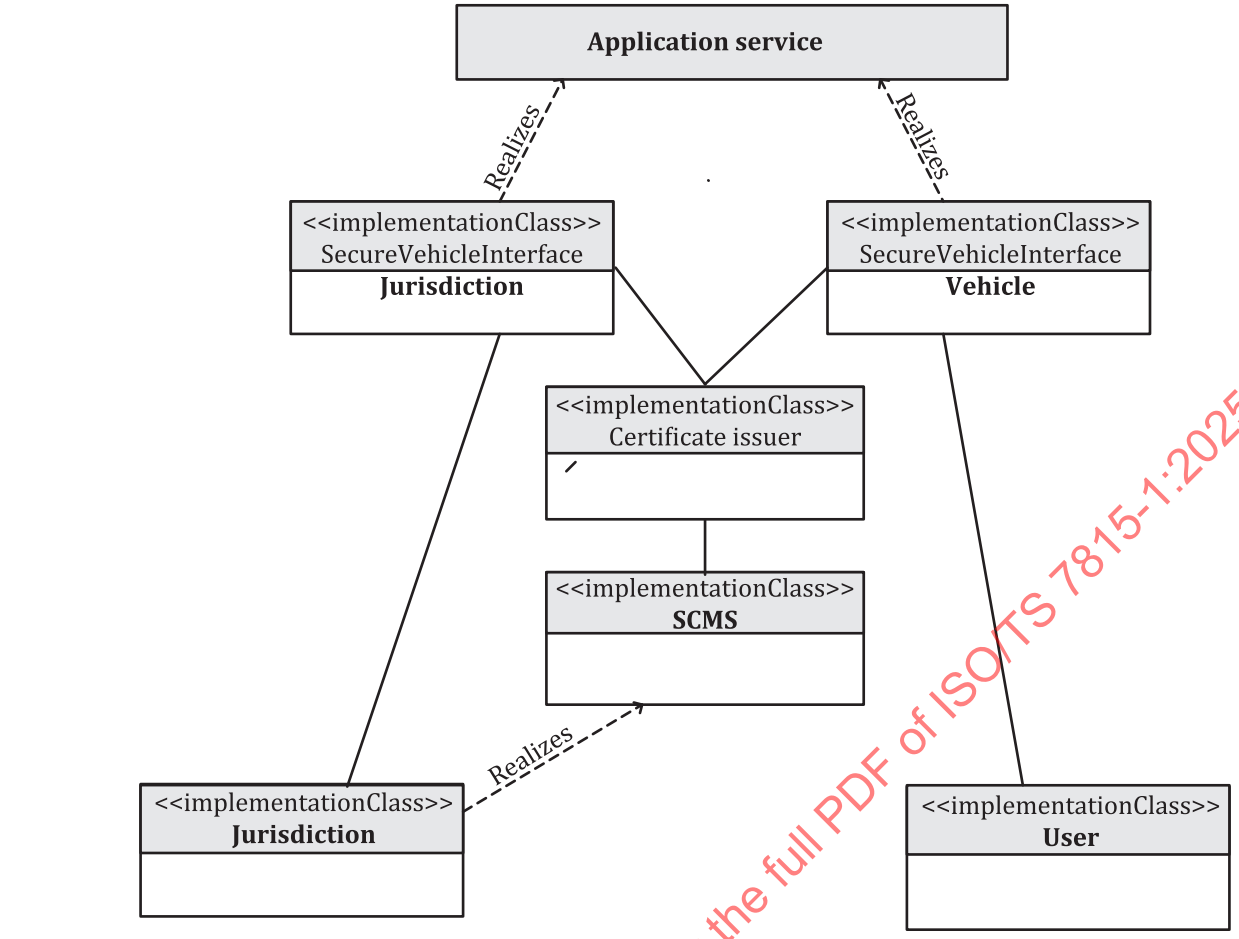


Figure 3 — UML model overview of the classes

8.3 Service definition

The service definition for each application service comprises:

a) a clear description of the service provided and its inputs, outputs and results;

b) basic vehicle data content and quality that an IVS is required to deliver;

c) core application data content to meet the requirements of the jurisdiction;

d) any additional application-specific data content for the provision of that particular service;

e) service elements (such as “retrieve data from IVS”, “map data to a map with access conditions”, “report non-compliance”, etc.);

f) rules for the approval of IVSs and application services.

8.4 Role model architecture

8.4.1 General

This subclause considers the roles of the actors defined in 8.2 and their interrelationship in greater detail, and their relationship to the provision of the applications service(s).

8.4.2 Jurisdictions

The jurisdiction is the body that has official power to make legal decisions and impose regulations. How this operates will vary from region according to the relevant constitution or legal structure. Regions can have a single jurisdiction, or can delegate such authorities to their constituent states, or, as in the case in Europe, independent states can concede part of their independent national jurisdiction to a common jurisdiction union (e.g. European Union) to achieve common goals and interoperability within common conditions, while retaining independent jurisdiction in other matters.

Regardless of the differences between jurisdictions, what is common for the purposes of this document, is the concept that at any specific location and time, there is a single jurisdiction that has official power to make legal decisions and impose regulations in respect of the regulation of commercial freight transport.

While the specific regulated application services that are offered or imposed on regulated commercial freight vehicles will vary from jurisdiction to jurisdiction, the generic requirements to offer or impose such regulated application services are largely similar.

The jurisdictions are the owners of the regulated applications. These can be required by regulation, or can be offered by a jurisdiction as an option to demonstrate compliance to a regulation, according to the choice of the jurisdiction and the regulations that it enforces.

Within the context of this document the role of the jurisdiction is to:

— define the regulated application services;

— determine if they are mandatory or optional;

— pass legislation to determine and regulate;

— manage and regulate the provision of the regulated application services.

Without prescribing the domestic arrangements within any jurisdiction, the management and regulation of the provision of the regulated application services can be architecturally described as:

— laws and regulations;

— adopted standards;

— adjudication and mediation;

— auditing;

— approval of equipment;

— approval of service providers (where appropriate);

— approval of application services;

— trusted third party (or third parties).

This involves seven further classes/subclasses of actors in addition to the jurisdiction:

— the jurisdiction;

— the security credential management system (SCMS);

— the certificate issuer;

— the IVS;

— the equipment installer (subclass);

— the IVS equipment maintainer (subclass);

— the approval authority (regulatory);

— the user.

Single entities may perform the roles of multiple classes of actor. For example, the SCMS and the certificate authority may be the same actor. Other actors will also be embraced within these key roles (such as a communications provider), but these can be regarded as additional subclasses that support one of the key actor roles.

At the specific jurisdiction level, this architecture can be elaborated in greater detail, and specifically to the instantiation of TARV-SVI within that jurisdiction. For the purposes of this document, however, abstracting to the level of Figure 1 and Figure 2 provides a generic common framework that can be instantiated with variations from jurisdiction to jurisdiction, yet remain a generic common framework according to which equipment can be built and application services can be specified.

8.4.3 Application services

Application services, whether regulated or commercial, need clear definition in terms of the requirements on the IVS.

As there is no application service provider (ASP) in the TARV-SVI model, it is necessary for the jurisdiction to develop the application service which, in the case of cyclical provision of data, receives and processes data, and in the case of a request-based service, requests then processes the received data.

It is also necessary for the jurisdiction to provide sufficiently accurate specification of what is required from the vehicle to enable the original equipment manufacturer (OEM), or aftermarket provider to design the IVS. In this circumstance, responsibilities for any deficiencies in that specification will lie with the jurisdiction. Part of that specification will normally prohibit any intermediary processing of the data on board the vehicle or via an ExVe cloud or similar.

8.4.4 The IVS equipment installer

This is the actor who installs the IVS into the vehicle and connects it to additional equipment that is required, so that it is able to perform the application service.

If this is part of the original equipment specification for the vehicle, the IVS equipment installer will be the vehicle manufacturer or its agent.

In all circumstances where the IVS is not part of the original equipment, it is expected that in most jurisdictions these equipment installers will have to be registered with, and approved by, the approval authority (regulatory).

The IVS equipment installer has the role of installing the IVS communications equipment and also connecting it to other equipment required in order to deliver the application service. For example, in the case of remotely monitoring an electronic tachograph, the tachograph is required to be connected into the IVS. The IVS equipment installer also has the role of testing the functionality of the installed equipment, and ensuring that where multiple equipment is connected, all regulated services can be provided without detriment of one because of another.

In order to maintain control of the regime, the IVS equipment installer is held accountable by the approval authority (regulatory) for providing the data to the application service(s) of the required quality. Therefore, the installers of any other equipment have to ensure for the IVS equipment installer that their equipment functions properly.

8.4.5 The IVS equipment maintainer

Once installed, the IVS equipment shall be maintained. Functionality and capabilities shall be checked periodically, and it can be necessary for the equipment to be recalibrated and recertified periodically in accordance with the regime imposed by the jurisdiction.

A number of business models for this can be envisaged. Maintenance may be a service provided by the service provider; it may be provided by the equipment installer; it may be provided by the vehicle maintainer; it may be provided by the vehicle inspector used for vehicle safety test approval; etc.

The regime allowed will depend on how the jurisdiction best believes that its regime can be implemented and maintained, and will vary from jurisdiction to jurisdiction.

Regardless of the business model operating within a particular jurisdiction, the IVS equipment maintainer can also architecturally be considered as a sub-class of the equipment installer.

8.4.6 Approval authority (regulatory)

An approval authority (regulatory) is appointed by the jurisdiction and it can be a separate appointed organization, or a department of the jurisdiction. Within the context of this document, it is the actor (role) of “approval authority" that is important, not its structure, ownership or business model.

An approval authority (regulatory) may preside over only the instantiation and operation of one particular application service, or may preside over the instantiation and operation of some or all application services for regulated commercial freight vehicles (at the discretion of the jurisdiction).

Approval refers to the confirmation of certain characteristics of an object, person or organization. In this context, approval applies to both the application(s) behind the service provision and the IVS for which requirements need to be formulated. These requirements need be described as tests to be passed. Each requirement leads to a verdict (passed or failed) on which the approval is based. The ISO 7815 series does not prescribe the specific requirements to achieve approval, nor its procedures nor pass criteria, nor evaluation methods, which are deemed to be within the provenance of each jurisdiction.

8.4.7 Security credential management system/public key infrastructure

The security credential management system (SCMS) is a central part of the SVI. The SCMS, and public key infrastructure (PKI) in particular, encode the trust relationships and governance structures for identity and authority management, and thus lie at the technical heart of the TARV-SVI. In this document, when referring to the management of asymmetric keys, the term SCMS is synonymous with the term PKI.

The SCMS itself plays no part in the message security solution for vehicle-to-vehicle (V2V) and vehicle-to infrastructure (V2I) communication. Rather, it facilitates the secure communication by ensuring that all participants in the system have access to the message-specific, or application-specific, cryptographic key material. The PKI approach ensures public key certificate (PKC) management to facilitate trusted communication. A PKC carries the public key and an attestation by the issuing party that the public key is bound to an attribute of the holder of the matching private (secret) key. In C-ITS/TARV-SVI the attribute is most often the secure service provider (SSP). Authorized system participants use digital certificates issued by authorities within the SCMS to obtain public keys used to validate the content of signed messages. To protect privacy, these certificates contain no personal or equipment-identifying information but serve as attribute certificates attesting that the holder is authorized to make the claim of the attribute (e.g. the specific value of an SSP) and that other users in the system can trust the attestation from the source of each message. The SCMS also plays a key function in protecting the integrity of the system by ensuring that keys and their associated certificates are revoked. The rules for revocation may include acting on reports of misbehaving devices. See Figure 4.

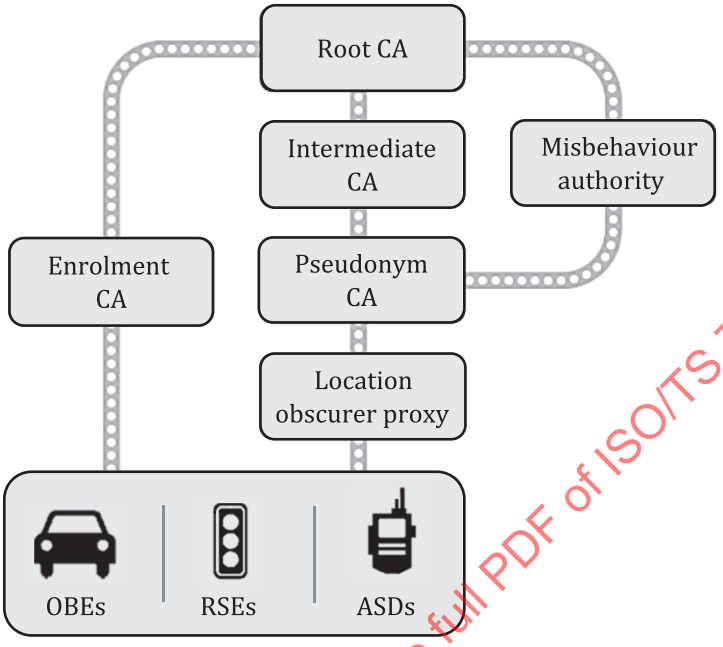
Principal components of the SCMS are:

— a certificate authority (CA) that stores, issues and signs the digital certificates (CAs may be ordered in a hierarchy, with the top of the hierarchy termed the Root CA);

— a registration authority (RA) which verifies the identity of entities requesting their digital certificates to be stored at the CA (RAs are not mandated but may be used to relieve the processing burden on CAs);

— a key and certificate repository, i.e. a secure location in which keys are stored and indexed;

— a certificate management system managing elements like the access to stored certificates or the delivery of the certificates to be issued.



SOURCE US Department of Transportation, reproduced with the permission of the authors.

Figure 4 — Simplified SCMS architecture

NOTE The European C-ITS paradigm uses the term "EU CCMS" (EU C-ITS security credential management system) to refer to SCMS.[16]

8.4.8 Certificate authority (digital)

Part of the SCMS (see 8.4.7), the certificate authority is the user-facing organization which issues digital certificates for use by both the IVS and the TARV-SVI application service.

8.4.9 Application service approval

Each application service, whether regulated, or unregulated, shall need to be tested and certified by the approval authority (regulatory) to ensure that:

a) the system provides the application service and data consistent with its specification and documentation;

b) the documentation is adequate;

c) the provision of the application service does not adversely impact the provision of other regulated application services.

8.4.10 In-vehicle system (IVS) approval

8.4.10.1 General

Having ensured that the service provider is capable of providing and is certified to provide the application services, the approval authority (regulatory) shall also:

— type approve the IVS, or if performance-based requirements are in place, perform tests to ensure conformance with those requirements;

— provide a regime to test and provide assurance that IVS equipment is capable and properly installed in order to provide the application services.

These should be treated as two functionally separate tasks.

Where an IVS takes the form of a discrete OBU, it can be "type approved" using an independent test house. This is more complex in the case of OEM installed equipment, which will have to be certified as part of the vehicle type approval tests.

The jurisdiction or approval authority can confirm that approved equipment has been installed correctly by either designing specific installation tests directly, or by assigning this role as a responsibility of a service provider. This decision is made by the jurisdiction and is not defined in this document.

8.4.10.2 IVS type approval

In terms of in-vehicle platform approval, IVS type approval refers to processes intended to determine if the IVS meets minimum standards to ensure the required quality.

8.4.10.3 IVS instantiated as an OBU

In the case where the IVS is an independent functioning on-board unit (OBU), it may be viewed as a single product, independent of the vehicle into which it is fitted. It shall be tested in a testable environment where its functionality can be tested separately from the functionality and performance of any equipment connected to it in order to provide data for the performance of an application service.

8.4.10.4 IVS instantiated not as an OBU

If the IVS is part of the original equipment of the vehicle, it is likely that there will not be a single OBU, but that the functionality will be provided, at least in part via the controller area networking bus (CAN bus) or from similar equipment disbursed around the vehicle, or both. For example, the GNSS data and compass function will probably be obtained from the vehicles satellite navigation system; accelerometer data and multi-axis gyroscope from the electronic drive/stability control, etc.

In this event, the IVS approval will have to be integrated into the overall vehicle approval.

8.4.10.5 IVS attributes

The functionality of the IVS is a computing device with six key attributes:

— central processing unit;

— data storage means;

— data input means;

— connectivity means to/from auxiliary equipment;

— communications means;

— power supply.

Each function needs specific tests as to fitness of purpose.

8.4.10.6 Central processing unit

The IVS shall be able to prove that it is able to perform the program of operations required in order to fulfil regulated service provision. This normally implies the combination of:

— a processor;

— volatile memory (RAM/DRAM/SRAM etc.);

— recognized operating system (e.g. LINUX®).[1)]

Functionality tests for such systems are widely available and easily devised. The speed of the processor shall be sufficiently adequate to perform the regulated application service. By today's typical computer performance standards, these demands are not high and can be easily demonstrated to be satisfied.

NOTE Providers of in-vehicle platforms that can perform multiple functions in the vehicle in addition to regulated services can be advised to use high performance processors, but this is not a requirement for the provision of currently envisaged regulated services.

Volatile memory shall be adequate to handle data processing of multiple regulated applications. Since non-volatile memory will also be present, by standards of typical computer performance at the time of the development of this document, these demands are not high and can be easily demonstrated to be satisfied.

The testing of the central processing unit shall be completely independent of any envisaged application service.

8.4.10.7 Data storage means

The IVS shall have a means of non-volatile bistable data storage that can retain the stored information even when not powered (such as hard disc, flash memory, etc.).

8.4.10.8 Data input means

The IVS shall have a means to receive inputs both from auxiliary equipment, and from its communications capability.

8.4.10.9 Connectivity means to/from auxiliary equipment

The IVS shall have multiple interfaces to connect with auxiliary equipment using standard physical interfaces (USB2, RS232, RS422, OBD2, etc.), or in the case of OEM installation, access to the CAN bus.

In the case of OEM installation, the IVS shall be provided with access to the vehicle generic data as specified in ISO 15638-5 (i.e. from GNSS, accelerometer, multi-axis gyroscope, altimeter, clock, compass, etc., and potentially a megapixel camera/video) or shall provide such functionalities as defined in ISO 15638-5 that are not available to it elsewhere.

8.4.10.10 Communications means

The IVS shall have, or have access to, one or more wireless means to communicate with the application of the jurisdiction. The interface(s) shall conform to ISO/TS 7815-2.

1) This trademark is provided for reasons of public interest. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO.