TECHNICAL SPECIFICATION

ISO/TS 15638-4

First edition
2020-02

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

Part 4: System security requirements

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

Partie 4: Exigences des systèmes de sécurité

Reference number
ISO/TS 15638-4:2020(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

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

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

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

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

A list of all parts in the ISO 15638 series can be found on the ISO website.

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

Introduction

Many ITS technologies have been embraced by commercial transport operators and freight owners, in the areas of fleet management, safety and security. 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.

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. The ISO 15638-4 series of standards describes and defines the framework and requirements so that the on-board equipment can be commercially designed in an open market to meet common requirements.

The ISO 15638 series of standards:

- provides the basis for future development of cooperative telematics applications for regulated commercial freight vehicles. Many elements to accomplish this are already available. Existing relevant standards will be referenced, and the specifications will use existing standards (such as published CALM documents) wherever practicable.
- allows for a powerful platform for highly cost-effective delivery of a range of telematics applications for regulated commercial freight vehicles.
- is a business architecture based on a (multiple) service provider oriented approach.
- addresses legal and regulatory aspects for the approval and auditing of service providers.

The ISO 15638 series of standards is timely as many governments (Europe, North America, Asia and Australia/New Zealand) are considering the use of telematics for a range of regulatory purposes. 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 document provides general specifications for security for communications and data exchange aspects of candidate regulated applications which are specified in ISO 15638-8 (and Parts 8 to 21 at the time of developing this document, but further parts may be added later if a requirement for additional regulated applications to be standardised are identified), the selection and implementation for all or any of which remain a decision for the implementing jurisdiction.

NOTE 1 The definition of what comprises a ‘regulated’ vehicle is regarded as an issue for National decision, and can vary from jurisdiction to jurisdiction. The ISO 15638 series of standards does not impose any requirements on nations in respect of how they define a regulated vehicle.

NOTE 2 The definition of what comprises a ‘regulated’ service is regarded as an issue for National decision, and may vary from jurisdiction to jurisdiction. The ISO 15638 series of standards does not impose any requirements on nations in respect of which services for regulated vehicles jurisdictions 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.

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

Part 4: System security requirements

1 Scope

Security requirements address both hardware and software aspects.

This document addresses the security requirements for:

- the transfer of TARV data from an IVS to an application service provider across a wireless communications interface;
- the receipt of instructions from an application service provider to a TARV IVS;
- the communications aspects of handling of software updates for the IVS over wireless communications.

This document defines the requirements for telematics applications for regulated commercial vehicles for:

a) threat, vulnerability and risk analysis;

b) security services and architecture;

c) identity management;

d) security architecture and management;

e) identity-trust and privacy management;

f) security-access control;

g) security-confidentiality services.

This document provides:

- general specifications for the security of TARV;
- specifications for the security of TARV transactions and data within an ITS-station “bounded secure managed domain” (BSMD);
- specifications for the security of TARV transactions and data transacted with a predetermined address outside of a BSMD.

IVS security requirements are dealt with by the prime service provider and application service provider (See ISO 15638-1).

Application service provision security is dealt with by the application service provider (and could be the subject of a separate TARV standards deliverable).

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

ISO/IEC 15408-1, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

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

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

ISO 17423, *Intelligent transport systems — Cooperative systems — Application requirements and objectives*

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

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

ISO 24102-3, *Intelligent transport systems — ITS station management — Part 3: Service access points*

ETSI TS 102 940, *Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management*

3 Terms and definitions

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

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

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

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

3.1
access
admittance, entry, permit to use the road network and/or associated infrastructure, e.g. bridges, tunnels

3.2
access monitoring
observation and recording of vehicle related data when using the road network and/or associated infrastructure, e.g. bridges, tunnels

3.3
application service
service provided by a *service provider* (3.24) enabled by accessing data from the *in-vehicle system* (*IVS*) (3.14) of a regulated vehicle via a wireless communications network

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

3.5
architecture
formalised description of the design of the structure of TARV and its *framework* (3.13)

3.6
authentication
function intended to establish and verify a claimed identity

3.7
bounded secure managed domain
BSMD
secure peer-to-peer communications between entities (*ITS-stations* (3.16)) that are themselves capable of being secured and remotely managed;

Note 1 to entry: The bounded nature is derived from the requirement for ITS-stations to be able to communicate amongst themselves, i.e. peer-to-peer, as well as with devices that are not secured (referred to as 'other ITS-stations'), and realizing that to achieve this in a secure manner often requires distribution and storage of security-related material that must be protected within the boundaries of the *ITS-stations,* leads to the secured nature of the entity, as there is great flexibility to achieve desired communication goals, there is a requirement that this flexibility be managed; within C-ITS and ISO 21217 such *ITS-stations* are defined as operating within BSMD, or outside of the BSMD.

3.8
communications access for land mobiles
CALM
layered solution that enables continuous or quasi continuous communications between vehicles and the infrastructure, or between vehicles, using such (multiple) wireless telecommunications media that are available in any particular location, and which have the ability to migrate to a different available media where required and where media selection is at the discretion of *user* (3.27) determined parameters by using a suite of standards based on ISO 21217 (*CALM* architecture) and ISO 21210 (*CALM* networking) that provide a common platform for a number of standardised media using *ITS-stations* (3.16) to provide wireless support for applications, such that the application is independent of any particular wireless medium

3.9
commercial application(s)
ITS applications in regulated vehicles for commercial (non-regulated) purposes

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

3.10
cooperative ITS
C-ITS
ITS applications for both regulatory and commercial purposes that require the exchange of data between uncontracted parties using multiple *ITS-stations* (3.16) communicating with each other and sharing data with other parties with whom they have no direct contractual relationship to provide one or more *ITS services* (3.15)

3.11
data pantry
secure area of memory in *IVS* (3.14) where data values are stored

Note 1 to entry: See ISO 15638-1.

3.12
facilities
layer that sits on top of the communication stack and helps to provide data interoperability and reuse, and to manage applications and enable dynamic real time loading of new applications

3.13
framework
particular set of beliefs and ideas referred to in order to describe a scenario or solve a problem

3.14
in-vehicle system
IVS
ITS-station (3.16) and connected equipment on board a vehicle

3.15
ITS service
communication functionality offered by an *ITS-station* (3.16) to an *ITS-station* application

3.16
ITS-station
ITS-s
entity in a communication network, comprised of application, *facilities* (3.12), networking and access layer components specified in ISO 21217 that operate within a bounded secure management domain

3.17
jurisdiction
government, road or traffic authority which owns the r*egulatory applications* (3.21)

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

3.18
jurisdiction regulator
agent of the *jurisdiction* (3.17) appointed to regulate and manage TARV within the domain of the *jurisdiction*, which may or may not be the *approval authority (regulatory)*

3.19
operator
fleet manager of a regulated vehicle

3.20
prime service provider
service provider (3.24) who is the first contractor to provide *regulated application services* (3.22) to the regulated vehicle, or a nominated successor on termination of that initial contract, and who is responsible to maintain the installed *IVS* (3.14) and if the *IVS* was not installed during the manufacture of the vehicle, the *prime service provider* (3.20) is also responsible to install and commission the *IVS*

3.21
regulated application
regulatory application
application arrangement using TARV utilised by *jurisdictions* (3.17) for granting certain categories of commercial vehicles rights to operate in regulated circumstances subject to certain conditions, or indeed to permit a vehicle to operate within the *jurisdiction* and which may be mandatory or voluntary at the discretion of the *jurisdiction*

3.22
regulated application service
TARV application service (3.3) to meet the requirements of a *regulated application* (3.21) that is mandated by a regulation imposed by a *jurisdiction* (3.17), or is an option supported by a *jurisdiction*

3.23
regulated commercial freight vehicle
regulated commercial regulated vehicle
vehicle that is subject to regulations determined by the *jurisdiction* (3.17) as to its use on the road system of the *jurisdiction* in regulated circumstances, subject to certain conditions, and in compliance with specific regulations for that class of regulated vehicle and which at the option of *jurisdictions* may require the provision of information via TARV or provide the option to do so

3.24
service provider
party which is approved by an approval authority (regulatory) as suitable to provide regulated or commercial ITS *application services* (3.3)

3.25
specification
explicit and detailed description of the nature and functional requirements and minimum performance of equipment, service or a combination of both

3.26
telematics
use of wireless media to obtain and transmit (data) from a distant source

3.27
user
individual or party that enrols in and operates within a regulated or *commercial application* (3.9) service

EXAMPLE *Driver,* transport *operator* (3.19)*,* freight owner.

4 Abbreviated terms

ADR	European Agreement concerning the international carriage of Dangerous goods by Road/Accord européen relatif au transport international des marchandises Dangereuses par Route
ASP	application service provider (3.4)
BSMD	bounded secure managed domain
CALM	communications access for land mobiles (3.8)
C-ITS	cooperative intelligent transport systems (3.10)
ID	identity
IP	internet protocol
ITS-s	ITS-station (3.16)
IVS	In-vehicle system (3.14)
TARV	telematics (3.26) applications for regulated vehicles
UNECE	United Nations Economic Commission for Europe

5 General overview and framework

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

To understand clearly the TARV framework the reader is referred to ISO 15638-1.

Clause 6 contains security related requirements for the roles in the framework. The three-step security evaluation process outlined in ISO/IEC 15408-1 is used. In many cases security functions are inherited from a specific referenced ISO document, in particular, the security functions inherited from ITS-station. Security requirements for non-ITS-station compliant IVS are also described.

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

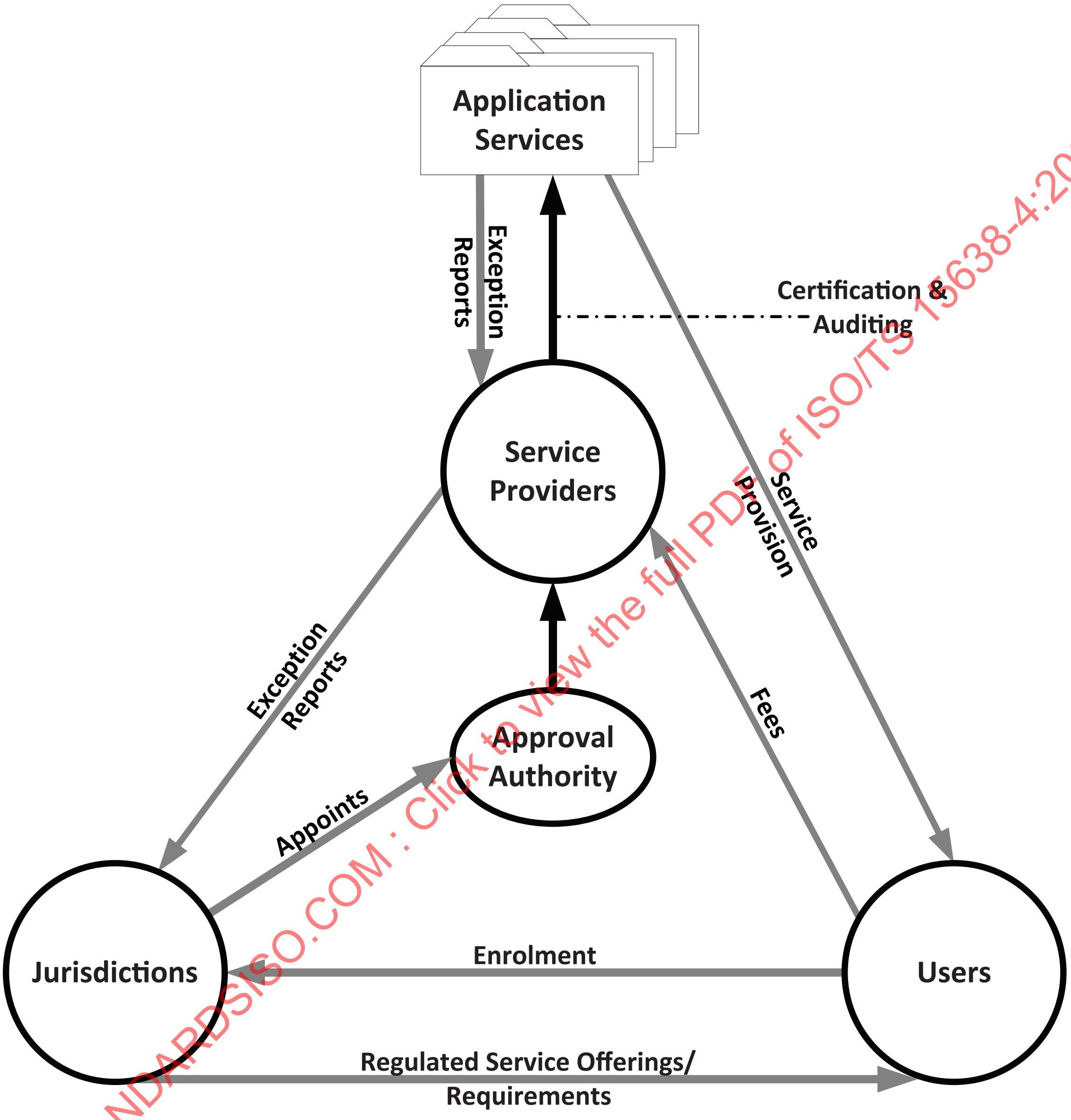

Figure 1 — Role model conceptual architecture (Source: ISO 15638-1)

The ISO 15638 series of standards addresses and defines the framework for a range of cooperative telematics applications for regulated commercial freight vehicles (e.g. access monitoring, driver fatigue management, speed monitoring, on-board mass monitoring). The overall scope includes the concept of operation, legal and regulatory issues, and the generic cooperative ITS service platform (ITS-station). The framework is based on a (multiple) service provider-oriented approach provision for the certification and auditing of service providers.

— ISO 15638-1:2012, *TARV — Framework and architecture*

— ISO 15638-2:2013, *TARV — Common platform parameters using CALM*

- ISO 15638-3:2013, *TARV — Operating requirements, 'Approval Authority' procedures, and enforcement provisions for the providers of regulated services*
- ISO/TS 15638-4:2020, *TARV — System security requirements* (this document)
- ISO 15638-5:2013, *TARV — Generic vehicle information*
- ISO 15638-6:2014, *TARV — Regulated applications*
- ISO 15638-7:2013, *TARV — Other applications*
- ISO 15638-8:2014, *TARV — Vehicle access management*
- ISO 15638-9:—[1], *TARV — Remote digital tachograph monitoring*
- ISO 15638-10:2017, *TARV — Emergency messaging system/eCall*
- ISO 15638-11:2014, *TARV — Driver work records*
- ISO 15638-12:2014, *TARV — Vehicle mass monitoring*
- ISO 15638-13:2015, *TARV — "Mass" information for jurisdictional control and enforcement*
- ISO 15638-14:2014, *TARV — Vehicle access control*
- ISO 15638-15:2014, *TARV — Vehicle location monitoring*
- ISO 15638-16:2014, *TARV — Vehicle speed monitoring*
- ISO 15638-17:2014, *TARV — Consignment and location monitoring*
- ISO 15638-18:2017, *TARV — ADR (Dangerous Goods)*
- ISO 15638-19:2013, *TARV — Vehicle parking facilities (VPF)*
- ISO 15638-20:—[2], *TARV — Weigh-in-motion monitoring*
- ISO 15638-21:2018, *TARV — Monitoring of regulated vehicles using roadside sensors and data collected from the vehicle for enforcement and other purposes*
- ISO 15638-22:2019, *TARV — Freight vehicle stability monitoring*

Further information and assistance on aspects of security and risk in ITS and C-ITS systems can be found in the following publications:

- ISO TR 17427-6, *Intelligent transport systems — Cooperative ITS — 'Core system' risk assessment methodology*
- ISO TR 17427-7, *Intelligent transport systems — Cooperative ITS — Privacy aspects*
- ISO TR 17427-8, *Intelligent transport systems — Cooperative ITS — Liability aspects*
- ISO TR 17427-9, *Intelligent transport systems — Cooperative ITS — Compliance and enforcement aspects*

This document defines the system security requirements for the wireless transfer of TARV data and other related support services within the framework of the ISO 15638 series of standards.

[1] Under preparation. Stage at the time of publication: ISO/FDIS 15638-9:2020.

[2] Under preparation. Stage at the time of publication: ISO/PRF 15638-20:2020.

6 Requirements

6.1 Threat, vulnerability and risk analysis

The ISO/IEC 15408 series provides a means of security evaluation.

ISO/IEC 15408-1, *Introduction and general model*, is the introduction to the ISO/IEC 15408 series. It defines general concepts and principles of IT security evaluation and presents a general model of evaluation. It also presents constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems. In addition, the usefulness of each part of the ISO/IEC 15408 series is described in terms of each of the target audiences.

ISO/IEC 15408-2, *Security functional components*, establishes a set of functional components as a standard way of expressing the functional requirements for TOEs (Targets Of Evaluation). It catalogues the set of functional components, families, and classes.

ISO/IEC 15408-3, *Security assurance components*, establishes a set of assurance components as a standard way of expressing the assurance requirements for TOEs. It catalogues the set of assurance components, families and classes. It also defines evaluation criteria for 'Protection Profiles' and 'Security Targets' and presents evaluation assurance levels that define the predefined ISO/IEC 15408 scale for rating assurance for TOEs, which is called Evaluation Assurance Levels (EALs).

In respect of the overall TARV system concept described in the previous Clause, the security objective for TARV communications is assessed as follows:

a) The objective of TARV is to collect and collate relevant data on-board a vehicle, and to pass that data to a landside "Application service provider" who will deliver the application service to the service recipient. In respect of actors in a TARV environment, refer to ISO 15638-1 (TARV framework and architecture). In respect of actors in the general cooperative ITS paradigm, see ISO 17427-1 (Cooperative ITS Roles and responsibilities in the context of co-operative ITS architecture(s)).

b) The on-board security of the function and performance of the on-board equipment is essential, but, save for the general requirements of 6.1 above and 6.2 below, is in general an IVS design issue and outside the scope of the ISO 15638 TARV series of International Standards.

c) The security of the TARV 'Application Service', once the data is delivered is essential but, save for the general requirement in 6.2 and 6.3.1 below, is a function of the landside application service provider and outside the scope of the ISO 15638 TARV series of International Standards.

The functional requirements for security are defined in the following clauses. The assurance components are by requirement defined to conform to the referenced standards.

6.2 Functional requirements for security of targets of evaluation (TOEs)

6.2.1 TOE — In-vehicle systems

All in-vehicle equipment and in vehicle systems used for TARV shall be assessed in accordance with ISO/IEC 15408-1.

The detail of how this is assessed is outside the scope of this document and may be the subject of (future) application service specific standards deliverables.

6.2.2 TOE — Application service provider systems

All application service provider systems that are the destination of TARV data transfers shall be assessed in accordance with the appropriate part of ISO/IEC 15408.

The detail of how this is assessed is outside the scope of this document and may be the subject of (future) application service specific standards deliverables.

6.2.3 TOE — TARV data transfer

The security of the transfer of TARV data (regardless of the specific application service) from the IVS to the application service provider, is assessed herein, at a high level, in the context of ISO/IEC 15408 (all parts) and in a detailed level by reference to ITS and C-ITS security standards and specifications referenced herein.

6.2.4 Means of TARV data transfer

To understand the security issues concerning the transfer of TARV data it is first necessary to specify the means by which TARV data can be transferred.

At an architectural level, TARV data transfer can be effected by means of:

a) An ITS-station to ITS-station communication in accordance with ISO 21217 and its associated International Standards (for example as part of a cooperative ITS data exchange). Such data exchanges shall be compliant to ISO 21217 and its associated standards and shall normally be effected within a “Bounded Secure Managed Domain” as defined in ISO 21217 and its associated Standards.

b) A system specific non-ITS-station compliant (not ISO 21217 or not peer-to-peer) IVS, using a specified wireless communication media (e.g. GSM/UMTS/E-UTRAN), or a master/slave wireless media such as 5,8 GHz CEN DSRC, etc. where data is transferred only to a predetermined IP address or known short range interrogator.

6.2.5 TARV data security requirements

TARV data may, at the discretion of the application service provider, be subjected to different security requirements, according to the sensitivity of the data, as assessed by the application service provider, and/or privacy requirements.

Nonetheless, all data that may be described as ‘personal’ data shall be sent by means that ensure that the data receives the protection required by all regional, national and international privacy protection requirements and data protection requirements to which the jurisdiction has acceded or subscribed or itself regulated.

This document provides general specifications for the security of TARV (regardless of specific communications provisions), and provides

a) Specifications for the security of TARV transactions and data within an ITS-station “bounded secure managed domain” (BSMD);

b) Specifications for the security of TARV transactions and data outside of a BSMD where data is transferred to a predetermined address or identified short range interrogator.

The application service provider shall ensure that TARV data exception reports are not modified or tampered with when reporting to the jurisdiction.

6.3 General specifications for the security of TARV

6.3.1 Destined to a predetermined IPv6 address (URI)

It is a basic tenet of all TARV data transfers that they are made to a predetermined address of an “application service provider” (commercial, or agency of a jurisdiction). This is most typically an IPv6 (or IPv4) address (URL) that has been predetermined and programmed into the IVS. However, other regulatory transactions are possible (such as interrogation via a short range 5,8 GHz DSRC link for regulatory compliance inspections using predetermined security provisions), or data may be transferred in either direction within a “bounded secure managed domain” as specified in ISO 21217.

With the exception of the case of a secured short range communication, or a data exchange within a BSMD, whenever contact is made using an ITS-station to request data from the IVS, the IVS shall always send the requested data to the predetermined IP address (previously) provided by the application service provider, (together with a reference provided by the interrogating party, and the required end destination address [URI] for the data), even where the request is made by a known or believed to be legitimate interrogator (e.g. police, inspector appointed by the jurisdiction).

It shall be the responsibility of the application service provider, and therefore outside the specifications of the ISO/IEC 15408 TARV series of standards, to assess the validity of the interrogator and interrogation, to determine whether or not to provide the data, and if assessed as a valid request, to forward the data to the requested destination address together with the reference.

6.3.2 ASP or jurisdiction determines security requirements

Within the privacy requirements (if applicable) of 6.10, and data destination requirements of 6.3.1, the application service provider shall predetermine the level of security required for the transfer of TARV data for specific applications, unless the jurisdiction has imposed specific security requirements as part of their regulation. In the case where the jurisdiction has imposed security requirements for data transfer, it shall be the responsibility of the application service provider to ensure that such security requirements of the jurisdiction are accorded with, and it is recommended that jurisdictions use the provisions of 6.5 or 6.6 in order to achieve a secure transaction.

6.4 Low security data transfers via an ITS-station

Where the application service provider determines that the data and security requirements are low because of the non-sensitive nature of the data, and security of the communications media over which it will be sent (e.g. GSM/UMTS/E-UTRAN), the data may be sent using an ISO 21217 compliant ITS-station via an ISO 21212/ISO 21213 communications medium provided that the communication is in accordance with ISO 21210.

6.5 TARV Data transfers via an ITS-station with C-ITS security (BSMD)

ITS-station to ITS-station data transfers in a cooperative ITS environment (contracted or uncontracted) shall take place within a BSMD as defined in ISO 21217 and its associated standards.

6.5.1 Within ISO 21217 ITS-station environment

TARV data transfer via an ITS-station with C-ITS security shall be effected within, and compliant to, the ITS-station architecture environment specified in ISO 21217.

6.5.2 Within ISO 21210 networking environment

TARV data transfer via an ITS-station with C-ITS security shall be effected within, and compliant to the networking environment specified in ISO 21210.

6.5.3 Within ISO 17423 selection of communications profile requirements

TARV data transfer via an ITS-station with C-ITS security shall be effected within, and compliant to the communications profile requirements specified in ISO 17423.

6.5.4 When accessing specific wireless media

Where TARV data transfer is made via an ITS-station with C-ITS security using a specified wireless communications media it shall be effected within, and compliant to the ITS-station management service access points specified in ISO 24102-3.

6.6 TARV data transfers including defined security, but outside a BSMD

6.6.1 General

There are circumstances where security is required, but not within the strict time managed environment of the ITS-station BSMD (see 6.5). This may simply be for convenience or because the security risk is lower, but may be because of the requirements of a regulation of a jurisdiction, etc. Such services are deemed to be between two ‘contracted’ parties (albeit that the ‘contract’ may be a regulation of the jurisdiction that the vehicle and/or its driver are bound by).

In these circumstances, data integrity and security may be obtained by securing the data within the IVS and by passing only the secured payload data and security related data across the wireless communication medium, to a predetermined IP address, meaning that only authorised persons have the means to understand the data passed across the communication, and to verify its authenticity.

It is assumed that data will normally be cryptographically protected before it reaches the IVS, or within the IVS, before it is sent across the wireless medium. This encryption process is application specific and outside of the scope of this document. For the purposes of this document, it is assumed that

a) the payload data is available in the data pantry of the IVS in an already protected form;

b) a field of security data is always associated with each field of payload data and is made available alongside the payload data in the data pantry of the IVS.

It is also assumed that cryptographic techniques will change over time, and that the mechanisms described in 6.6 enable change and update of security provisions without the need to revise this document. These techniques are therefore not defined within this document.

In this scenario, each field data shall therefore comprise 5 elements. See Table 1.

Table 1 — Structure of TARV data

A	B	C	D	E
Number of octets of payload data	Number of octets of security data	Payload data	Security data	10101010 end of field identifier octet
2 octets	2 octets	(A) Octets of payload data	(B) Octets of security data	1 octet
Example: 3	2	111111110000000011111111	0000000011111111	10101010

Payload data shall comprise the information content to be transferred across the air interface. Other than the overall field size constraint of A (65 535 octets), the number of octets of payload data is not limited per se by the standard but may be limited by the physical and practical constraints of the communication medium (for example when using CEN 5,8 GHz DSRC) or by a regulation of the jurisdiction.

Security data shall comprise the security ‘keys’ or links to keys or other security mechanisms provided to enable the payload data to be decrypted. Other than the overall field size constraint of B (65 535 octets), the number of octets of security data is not limited per se by the standard, but may be limited by the physical and practical constraints of the communication medium.

The ‘payload’ shall consist of a structured record (ASN.1 SEQUENCE) of five fields:

```
TARVData ::=   SEQUENCE {

               payloadLength      PayloadLength,

               securityLength     SecurityLength,
                TARVPayload         TARVPayload,

                securityData        SecurityData,

                endData             EndData

}
```

The content of the security data shall be known only to and within the control of a competent control authority (e.g. a jurisdiction), and those parties with whom they share this information and is outside the provisions of the communication that is the subject of this document, save that the communication makes provision to transfer a packet of security data with every packet of payload data.

6.6.2 Security data

Security data (securityData), comprising the data required by the interrogating party to complete its ability to decrypt the data (not only the cryptographic information, but also a protocol how and when to exchange said information) shall be supplied as defined elsewhere by the competent control authority, or as provided for within provisions of a regulation, part of which is presented as a data concept value, for temporary storage in the data pantry of the IVS, as the current version of securityData, in the form defined by the competent control authority.

6.6.3 IVS TARV security module

In order to use this security option, a TARV security module function shall be present in the IVS and is responsible for securing the data which is to be transmitted from the IVS data pantry to the requirements of the competent control authorities. The secured data is stored in the TARV IVS memory (data pantry). At intervals determined by the competent control authorities, the IVS replenishes and encrypts the TARV data concept (which comprises encrypted payload data and security data, concept values) held in the data pantry of the TARV-IVS. The operation of the security module is to be defined by the competent control authorities and is outside the scope of this document, save that it shall be required to provide updates to the VU Communication facility each time the TARV-IVS data changes.

6.7 Identity management

As required in ETSI TS 102 940 or equivalent of local jurisdiction. No other requirements are determined in this document.

6.8 Trust and privacy management

As required in ETSI TS 102 940 or equivalent of local jurisdiction. No other requirements are determined in this document.

6.9 Access control

As required in ETSI TS 102 940 or equivalent of local jurisdiction. No other requirements are determined in this document.

6.10 Confidentiality services

As required in ETSI TS 102 940 or equivalent of local jurisdiction. No other requirements are determined in this document.

6.11 Data privacy

All TARV applications shall operate within the guidelines of ISO TR 12859 as it affects the region in which the system is being operated.

All TARV applications shall operate within the provisions of privacy regulations of the jurisdiction in which the system is being operated.

6.12 Integrity of trailer identification

As required in ISO 15638-3:2013, 9.19.3 regarding integrity of trailer identification, the transmission of trailer identification data from the trailer identification device (TID) to the IVS shall support a form of Trailer ID data authentication subject to the approval of the certification authority, that can verify the origin and integrity of the Trailer ID data.

The application service provider shall document, to the satisfaction of the jurisdiction regulator, the Trailer ID data authentication mechanism.

6.13 Exception handling

No provision for exception handling is made in this document, but it may be specified in a later version.

6.14 Cross-border operations and harmonization

No provision for cross-border operations is made in this document, but it may be specified in a later version.

7 Quality of service requirements

This document contains no specific requirements concerning quality of service. Such aspects may be determined by a jurisdiction as part of its specification for any particular regulated application service.

8 Test requirements

This document contains no specific requirements concerning test requirements. Such aspects may be determined by a jurisdiction as part of its specification for any particular regulated application service.

9 Marking, labelling and packaging

This document has no specific requirements for marking, labelling or packaging.

However, where the privacy of an individual may potentially or actually be compromised by any instantiation based on the ISO 15638 series of standards, the contracting parties shall make such risk explicitly known to the implementing jurisdiction and shall abide by the privacy and data requirements of the implementing jurisdiction and shall mark up or label any contracts specifically and explicitly drawing attention to any loss of privacy and precautions taken to protect privacy. Attention is drawn to ISO TR 12859 in this respect.