TECHNICAL REPORT

ISO/TR 4445

First edition
2021-09

Intelligent transport systems — Mobility integration — Role model of ITS service application in smart cities

Systèmes de transport intelligents - Intégration de la mobilité - Schéma d'application des services ITS

Reference number
ISO/TR 4445:2021(E)

COPYRIGHT PROTECTED DOCUMENT

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

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*.

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

Currently, more than 70 % of the world's people live in cities. The proportion of people living in cities is rising around the world as civilisations develop and congregate around cities where there are more employment opportunities. Societies develop more innovatively and rapidly in cities, and they present better entertainment opportunities, adding to their attraction. *The Economist* magazine recently forecast that by 2045, an extra 2 billion people will live in urban areas[16]. The resulting concentration of population creates various issues such as road congestion due to an increase in vehicle population and environmental pollution due to exhaust gas and tyre erosion. These issues have been attributed to increases in the number of delivery trucks, taxis and town centre traffic and are further exacerbated by obstacles to the effective use of urban space due to the private ownership of cars (parking lots, street parking).

The pressures caused by scientific advice that significant action and change of behaviour is needed to ameliorate the adverse effects of climate change require a more environmentally friendly use of the transport system.

It is recognized that there is also road infrastructure deterioration, a lack of provision of information on the use of public transportation, driver shortages due to the increase in the number of elderly people and the inconvenience of multimodal fare payments, and action to improve the situation is urgently needed.

The International Data Corporation forecasts that of the USD 81 billion that will be spent on smart city technology in 2020, nearly a quarter will go into fixed visual surveillance, smart outdoor lighting and advanced public transit[17].

Eventually, this is likely to mean high speed trains and driverless cars. Consultancy McKinsey forecasts that up to 15 % of passenger vehicles sold globally in 2030 will be fully automated, while revenues in the automotive sector could nearly double to USD 6.7 trillion thanks to shared mobility (car-sharing, e-hailing) and data connectivity services (including apps and car software upgrades)[18].

Changing consumer tastes are also calling for new types of infrastructure. Today's city dwellers, for example, increasingly shop online and expect ever faster delivery times. To meet their needs, modern urban areas need the support of last-minute distribution centres, backed by out-of-town warehouses.

Therefore, in recent years, in Europe, studies on the development of mobility integration standards have been active to solve urban problems. There are various movements around the world making efforts to address these issues. In the United States, ITS technology is used to try to solve these urban problems, as in the Smart City Pilot Project. Columbus, Ohio has been selected as a smart city pilot project which is currently being designed in detail. Important key factors here are the core architectural elements of smart cities, and urban ITS sharing of probe data (also called sensor data), connected cars and automated driving. In addition, new issues have been recognized with the introduction of the connected car to the real world in respect of privacy protection, the need to strengthen security measures, big data collection and processing measures, which are becoming important considerations.

In terms of the effective use of urban space, it is hoped that the introduction of connected cars and automated driving can significantly reduce the requirements for urban parking lots (redistribution of road space). If technology can eliminate congestion, the city road area usage can also be minimized and reallocated (space utilization improvement) to improve the living environment of, and quality of life in, the city. In addition, the environment around the road will be improved by improving enforcement (e.g. overloaded vehicles). On the other hand, even in rural areas, it is possible to introduce automated driving robot taxis and other shared mobility that saves labour (and is therefore more affordable) and improves the mobility of elderly people.

To achieve this requires the realization of various issues, for example:

— cooperation with harmonization of de-jure standards such as ISO and industry de facto standards;

— recognition of the significance of international standardization (e.g. to reduce implementation costs);

- recognition of the significance of harmonization activities by countries around the world;
- cooperation and contribution between ISO/TC 22 for in-vehicle systems and ISO/TC 204 for ITS technology.

As mentioned above, automated driving mobility is expected to play an important role both in cities and in rural areas. The main effects are, as described above, the reduction of traffic accidents, reduction of environmental burden, elimination of traffic congestion, realization of effective use of urban space, etc.

ITS technology is an important element for realizing smart cities, and it is important to clearly understand the role model of ITS service applications when developing standards to achieve these objectives.

This document gives an important overview of the options for this objective. Considering the emerging direction of mobility electrification, automated driving and the direction of an environmentally friendly society, incorporating other urban data such as traffic management into the city management will improve the mobility of urban society. It is important to consider the creation of a common open role model for smart city data platforms (such as the ISO 15638 series service framework). Similar platforms will be necessary for the realization of the future mobility such as automated driving and electrification of vehicles. A common role model will be developed for all modes of vehicle, including public transport, general passenger vehicles and heavy vehicles. The incorporation of electronic regulation is especially important for automated vehicles and it is essential to incorporate it as a core element of urban ITS.

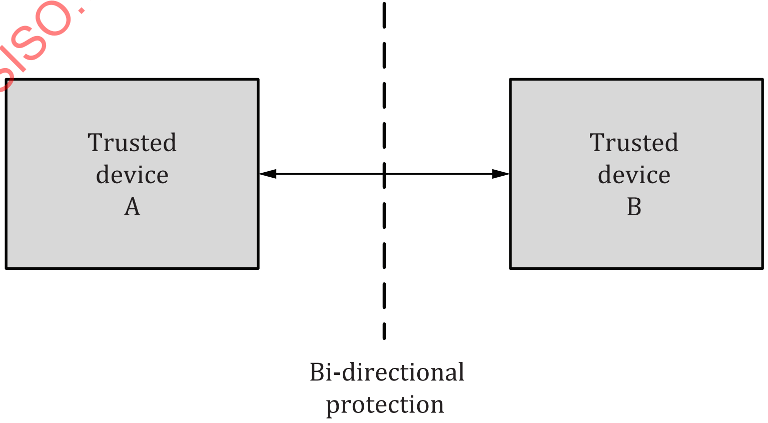
This document describes how ITS data can be presented, interchanged and used by smart cities. This document does not describe smart city use cases for ITS data in any detail nor does it describe in detail any specific ITS use cases. It is focused on the generic role model for data exchange between ITS and smart cities.

The necessary security and data exchange protocols have now been finalized to provide a secure ITS interface, with the approval of ISO/TS 21177[5], i.e. exchange information with bi-directional protection.

The trust relation between two devices is illustrated in Figure 1.

The relation enables two devices to cooperate in a trusted way, i.e. to exchange information in secure application sessions, and thus only access data or request data that they have the appropriate credentials to access.

This document provides the framework within which these transactions can be undertaken.



NOTE Source: ISO/TS 21177:2019[5], Figure 1.

Figure 1 — Interconnection of trusted devices

Intelligent transport systems — Mobility integration — Role model of ITS service application in smart cities

1 Scope

This document describes a basic role model of smart city intelligent transport systems (ITS) service applications as a common platform for smart city instantiation, directly communicating via secure ITS interfaces. It provides a paradigm describing:

a) a framework for the provision of a cooperative ITS service application;

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

c) a conceptual architecture between actors involved in the provision/receipt of ITS service applications;

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

e) a taxonomy of the organization of generic procedures.

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 14812,[1)]*Intelligent transport systems — Vocabulary*

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/TS 15638-4, *Intelligent transport systems — Framework for cooperative telematics applications for regulated commercial freight vehicles (TARV) — Part 4: System security requirements*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/TS 14812, ISO 15638-1, ISO 15638-3 and ISO/TS 15638-4 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 http://www.electropedia.org/

[1)] Under preparation. Stage at the time of publication: ISO/DTS 14812:2020.

4 Abbreviated terms

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

API	application programming interface
app	application programme
APDU	application protocol data unit
ASD	alcohol screening device
CA	certificate authority
CAN	controller area network
CCAM	cooperative, connected and automated mobility
C-ITS	cooperative intelligent transport system
CONOPS	concept of operations
ECU	engine control unit
ExVe	extended vehicle (see the ISO 20078 series[4])
GNSS	global navigation satellite system
ITS	intelligent transport system
ITS-S	intelligent transport system station
ITS-SCU	intelligent transport system station communication unit
ITS-SU	intelligent transport system station unit
MaaS	mobility as a service
OBE	on-board equipment
OEM	original equipment manufacturer
PKC	public key certificate
PKI	public key infrastructure
RA	registration authority
RAM	random access memory
RSE	road-side equipment
RV	road vehicle
RVU	road vehicle user
Rx	receive
SAPDU	service access point data unit
SCMS	security credential management system

SSP	secure service provider
TARV	telematics applications for ITS service applications
Tx	transmit
TLS	transport layer security
UML	Unified Modelling Language (see ISO/IEC 19501[3])
V2I	vehicle-to-infrastructure (communication)
V2V	vehicle-to-vehicle (communication)
VRU	vulnerable road user

5 General overview and framework

5.1 Objective

This clause describes a generic framework for the provision of cooperative telematics application services for ITS service applications.

Clause 6 provides the general CONOPS for which this architecture is designed. Clause 7 provides a framework, role definition and summary of the architecture at a conceptual level. Clause 8 describes the communications architecture.

5.2 National variations

The instantiation of interoperable on-board platforms for ITS service applications with common features is expected to vary from country to country, as will the provision of regulated, or supported, services.

5.3 Mandatory, optional and cooperative issues

5.3.1 This document does not impose any requirements on nations in respect of which services for ITS service applications countries will require, or which they will support as an option, but provides a generic common framework architecture within which countries can achieve their own objectives in respect of application services for ITS-supported service applications in cities, and provide standardized sets of requirements descriptions for the exchange of data to enable consistent and cost-efficient implementations where instantiated.

5.3.2 Cooperative ITS application, in this context, is the use of a common platform to meet both regulated and commercial service provision, providing collaboration between transport systems and smart cities.

5.4 Specification of service provision

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

5.5 Architecture options

Architecturally, it needs to be possible for a vehicle user/OBE to use the services of different application services. The in-vehicle system is a vehicle original equipment specification option, inbuilt at the time of manufacture of the vehicle, with service provider selection being a subsequent service-user choice (e.g. like selecting an internet service provider) or is aftermarket equipment that has access rights to the required data. An ITS application service is based in the infrastructure. Other options are possible and can be supported within the conceptual architecture. The objective of this role model is the accessibility of the use of ITS data generated in ITS application services in smart city application services.

6 Concept of operations

6.1 General

This clause describes the characteristics of a proposed system from the viewpoint of an individual who uses 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 ITS services for ITS service applications using a secure vehicle interface.

This document recognizes that there are variations between jurisdictions. It does not attempt, nor recommend, homogeneity between jurisdictions. It is designed to provide common standard features to enable equipment of common specification, that supports a standardized secure ITS interface to be used, and the common features of service provision to be able to be referenced simply by reference to an International Standard (requiring it to specify in detail only the additional requirements of a jurisdiction).

A CONOPS generally evolves from a concept and is a description of how a set of capabilities is employed to achieve desired objectives.

6.2 Statement of the goals and objectives of the system

The overall objective of the ITS service application in smart cities is the seamless exchange of data between transport applications and smart city service applications.

These services are provided to meet the smart city requirements using common secure ITS interface communications between ITS systems (including in-vehicle systems, infrastructure-based systems and personal ITS stations) and smart city applications.

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

Strategies, tactics, policies and constraints, and indeed the services that are regulated as mandatory or optionally supported, vary from jurisdiction to jurisdiction. Clause 7 provides details of the options of such aspects.

6.4 Organizations, activities and interactions among participants and stakeholders

The classes, attributes and key relationships are described in this clause. Some high-level conceptual architectural details are elaborated in Clause 7. Clause 8 provides the taxonomy of the architecture. Clause 9 defines the communications architecture. Clause 10 defines the facilities layer and its interoperability.

6.5 Clear statement of responsibilities and authorities delegated

Clause 5 describes the high-level options and issues. The actors, their responsibilities and authorities are described in Clause 7. The roles are described in this clause and in Clause 7.

6.6 Operational processes for the system

6.6.1 General

The description given in 6.6.2 of operational processes is at a high abstracted level (above that of any application service). Specific services have additional requirements not described herein.

6.6.2 Service requirements definition

A smart city application service provides a “service” (a benefit that a service user receives or a duty that a service user provides) to a service user using exchanges of data, in this case using a secure ITS interface. (Smart cities also use other communications means appropriate to the context of their use.) The interface is wired or wireless, but is likely to be the latter, in which case the latency of the system limits the ability to provide/capabilities of the application service.

An ITS application service provides an ITS “service” (a benefit that a service user receives or a duty that a user provides) to a service user using a secure ITS interface. The interface is wired or wireless, but is likely to be the latter, in which case the latency of the system limits the ability to provide/capabilities of the application service.

Wireless communications between a vehicle and its OEM (commonly known as “ExVe”) are separate and complementary to, and out of the scope of, this document.

6.7 Appointment of an approval authority (regulatory)

This document is based on the premise that a smart city develops its own regulation base (in consort with national government and other smart cities). The term used in this document to describe this organization and its regulation base is the “jurisdiction”, and this body creates or appoints an authority to approve and audit the process. The “process” in this context is a smart city application service, and the assumption is made that there is some form of approval process to control smart city application services and their cybersecurity (at a minimum to protect privacy and avoid fraud, and to minimize risks of terrorism or other disruption). The structure of that authority or authorities is a matter for the jurisdiction, and it is a separate appointed organization or a department of the jurisdiction. Within the context of this document, it is the actor role of the approval authority that is important, not its structure, ownership or business model.

An approval authority (regulatory) only presides over the instantiation and operation of one application service or presides over the instantiation and operation of many application services (at the discretion of the jurisdiction).

The approval authority (regulatory), where appropriate, approves service providers (or delegate the approval of service providers), and provides an audit as described in Clause 5, in accordance with the requirements of the jurisdiction.

6.8 In-vehicle system

In ITS service applications, the OBE that provides the application service is an ITS trusted device that meets the requirements of ISO/TS 5616[1].

6.9 User

An ITS application service provides a service to a service user using a secure ITS interface. Within the context of mobility integration, while most of ITS services are being provided to/from a road vehicle/road vehicle user (RV/RVU) to another RV/RVU, or between an RV/RVU and a service provider or service receiver, the application service is also between the RV/RVU and another transport system using entity, such as a VRU, micro mobility user, public transport service provider, MaaS service provider, etc.

6.10 Application service

An application service is provided on request or is cyclical to a pre-agreed cycle.

In an "on request" implementation, an ITS trusted device, offering the appropriate credentials via the secure ITS interface requests pre-specified information from the client OBE, which on confirmation of the credentials of the requestor for the requested information provides it via the secure ITS interface.

An OBE is or is not set up to deal with one or both cyclical and on request demands for information.

The nature and definition of the information supplied is the subject of a specification or regulation.

6.11 Big data management entity

The big data are connected to other smart city data entities and share the data for the efficient smart city operation in a manner approved and authorized by the jurisdiction. This role is required to support privacy requirements and to fairly manage any business case issues.

6.12 Data aggregator

The data aggregator provides timely and value-added data to the service provider for its ITS service application provisioning. Data collected for sharing are generally not forwarded in the same formats or data timing so there is a need to have an entity that can provide standardized data to the service provider in a standard data format and data timing. This role is similar to the ISO/TS 21184[6] role between ITS entities, but in this case is between ITS entities and smart city entities. Artificial intelligence (AI) can be deployed to create such structured value-added data for service providers.

The role of big data/data aggregation in smart cities is out of the scope of this document.

7 Conceptual architecture framework

7.1 General

Clause 6 provides the generic CONOPS which these actors and classes enact to provide the application service(s). To specify a generic framework standard of the ITS service platform exchange of data with smart cities, this framework standardization deliverable identifies core actors and classes as described in 7.2 to 7.4, which are described as elements independent of any specific application.

7.2 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":

- the service users;
- the service provider(s);
- for any regulated applications: the jurisdiction(s).

The role model provides the general attributes and the responsibilities of the parties. These aspects are described in this document. Figure 2 illustrates a conceptual role model architecture for application service provision.

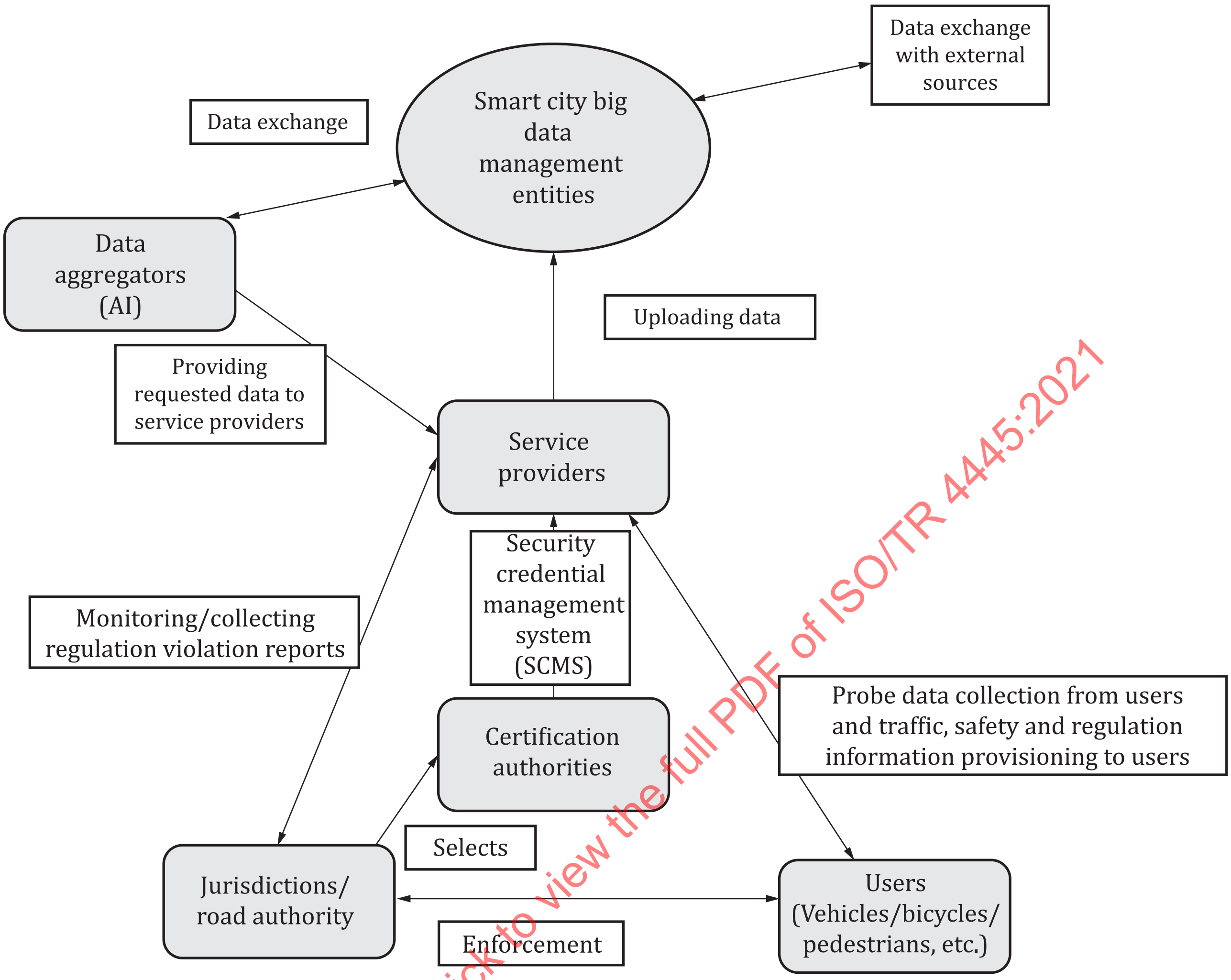

Data exchange with external sources
Smart city big data management entities
Data exchange
Data aggregators (AI)
Uploading data
Providing requested data to service providers
Service providers
Security credential management system (SCMS)
Monitoring/collecting regulation violation reports
Certification authorities
Probe data collection from users and traffic, safety and regulation information provisioning to users
Selects
Jurisdictions/ road authority
Users (Vehicles/bicycles/ pedestrians, etc.)
Enforcement

Figure 2 — Role model conceptual architecture — Smart city ITS application service

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

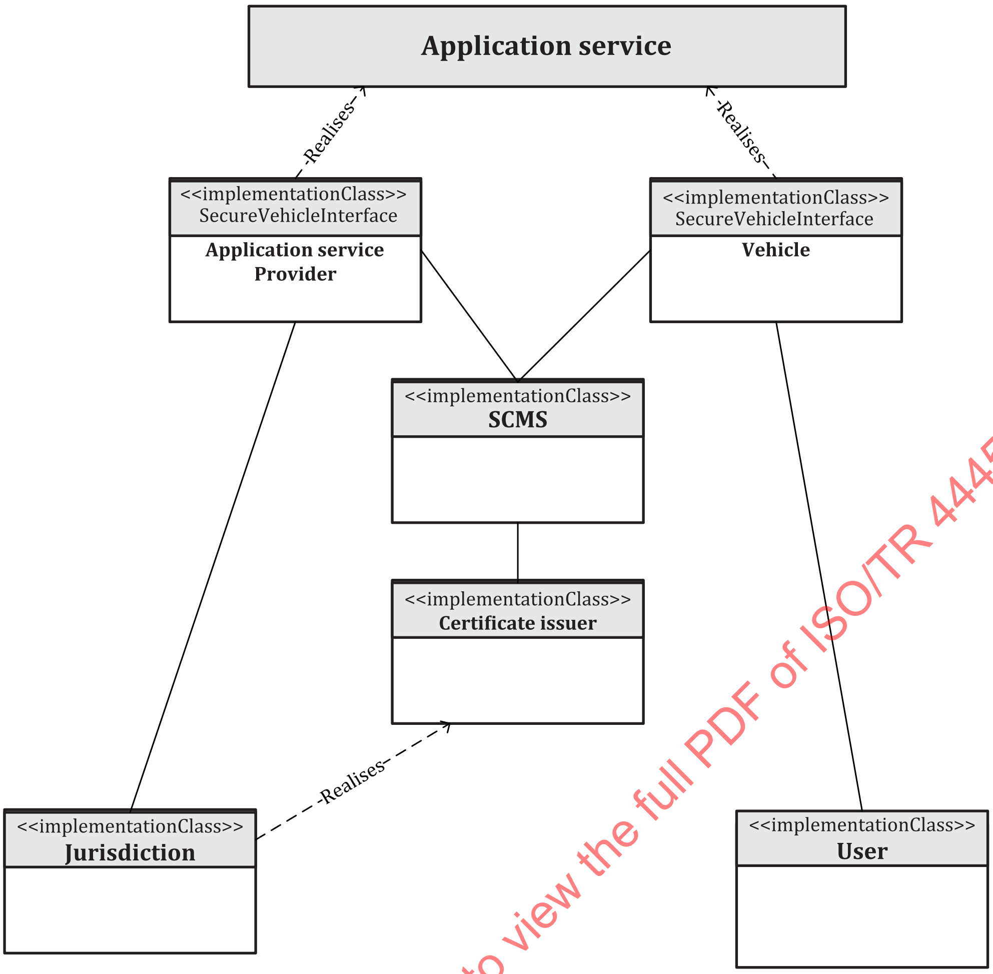


Figure 3 — UML model overview of the classes

7.3 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 OBE must deliver;

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

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

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

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

7.4 Role model architecture

7.4.1 General

This subclause considers the roles of the actors defined in 7.2 and their interrelationship in greater detail, and their relationship to the provision of the applications service(s).

7.4.2 Jurisdictions

The jurisdiction is the body that has official power to make legal decisions and impose regulations. How this operates varies from country to country according to their constitution or legal structure. Countries have a single jurisdiction or delegate such authorities to their constituent states or, as in the case of Europe, independent states 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 where it deems applicable to impose regulations in respect of the regulation of ITS service applications.

ITS service applications and smart city applications vary. In some jurisdictions, some application services are mandatory or voluntary (but if implemented are implemented in a specific way). Most services envisaged are safety services, mobility-related services or commercial services.

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

- determine which application services are mandatory, which are optional and which are prohibited;
- define any regulated application services;
- 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.

At the specific jurisdiction level, this architecture can be elaborated in greater detail, and specifically to the instantiation of an ITS or smart city application service within that jurisdiction. For the purposes of this document, however, abstracting to the level of Figures 2 and 3 provides a generic common framework that can be instantiated with variations from jurisdiction to jurisdiction, yet remains a generic common framework to which equipment can be built and application services specified.

7.4.3 Application service actors

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

It also falls to the service provider to provide an accurate enough specification of what is required from the vehicle to enable the OEM, or aftermarket provider, to design the OBE.

Application services can be architecturally described as involving seven further classes/subclasses of actors in addition to the jurisdiction:

- the jurisdiction;
- the SCMS;
- the certificate issuer;
- the OBE;
- the equipment installer (subclass);
- the OBE equipment maintainer (subclass);
- the approval authority (regulatory);
- the service user.

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

7.4.4 Service provider(s)

A service provider, within the context of this deliverable, can be described as a party which is providing safety, commercial or regulated ITS or smart city services. Application services are certified by the certification authority (regulatory) as suitable.

7.4.5 The OBE equipment installer

This is the actor which installs the OBE into the vehicle and connects it to additional equipment that is required, so that it can perform the application service.

If this is part of the original equipment specification for the vehicle, the OBE equipment installer is the vehicle manufacturer or his/her agent.

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

The OBE equipment installer has the role not only to install the OBE communications equipment but to connect it to other equipment required to deliver the application service.

7.4.6 The OBE equipment maintainer

Once installed, the OBE equipment is maintained. Functionality and capabilities are checked from time to time, and the equipment is recalibrated and recertified from time to time in accordance with the regime imposed by the jurisdiction or to conform to International Standards, to enable interoperability.

Several business models for this can be envisaged. Maintenance is a service provided by:

- the service provider;
- the equipment installer;
- the vehicle maintainer;
- the vehicle inspector used for vehicle safety test approval, etc.

Regardless of the business model operating within a particular jurisdiction, the OBE equipment maintainer can also architecturally be considered as a subclass of the equipment installer.

7.4.7 Approval authority (regulatory)

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

An approval authority (regulatory) presides over the instantiation and operation of one application service or presides over the instantiation and operation of many application services for ITS or smart city service applications (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 OBE 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. This document 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.

7.4.8 Security credential management system/public key infrastructure

The SCMS is a central part of the secure vehicle interface. The SCMS, and PKI, encode the trust relationships and governance structures for identity and authority management, and thus lie at the technical heart of this secure ITS interface. In this document when referring to the management of asymmetric keys, the term "SCMS" is synonymous with the term "PKI".

The SCMS of 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 a C-ITS/ITS service application–secure ITS interface 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 service 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 include acting on reports of misbehaving devices.

The principal components of the SCMS are:

- a certificate authority (CA) that stores, issues and signs the digital certificates;

  NOTE 1 CAs are ordered in a hierarchy, with the top of the hierarchy termed the "root CA".

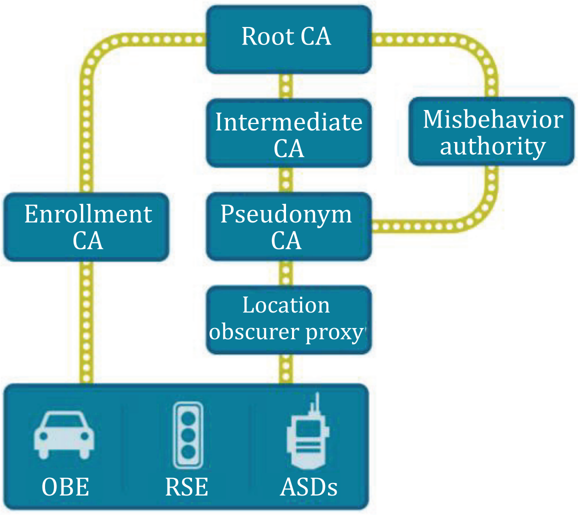
- a registration authority (RA) which verifies the identity of entities requesting their digital certificates to be stored at the CA;

  NOTE 2 RAs are not mandated but are 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 things such as the access to stored certificates or the delivery of the certificates to be issued.

NOTE 3 In the European C-ITS paradigm (C-ITS Delegated Act and its annexes), SCMS are referred to as the "EU CCMS" (EU C-ITS security credential management system).

A simplified SCMS architecture is shown in Figure 4.



NOTE Source: US Department of Transportation.

Figure 4 — Simplified SCMS architecture

7.4.9 Certification authority (digital)

Part of the SCMS (see 7.4.8), the certificate authority is the service user facing organization which issues digital certificates for use by both the OBE and the ITS service application-secure ITS-interface application service.

7.4.10 Application service approval

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

a) the system provides the application service and its 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 application services and especially any regulated application services.

7.4.11 Onboard equipment OBE approval

7.4.11.1 General

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

- type approve the OBE or, if performance-based requirements are in place, perform tests to ensure compliance with those standards;
- provide a regime to test and provide assurance that OBE is capable and professionally installed to provide the application services.

These are two functionally separate tasks.

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

In respect of approving that approved equipment has been installed correctly, the jurisdiction/approval authority (regulatory) has several ways that it can do this, either by designing specific installation tests directly or assigning that role as a responsibility of a service provider. That decision is made by the jurisdiction and is not defined in this document.

7.4.11.2 OBE type approval

OBE approval refers to processes intended to determine if the OBE meets minimum standards to ensure the required quality.

7.4.11.3 OBE instantiated as an OBE

In cases where the OBE is independent functioning OBE, it is viewed as a single product, independent of the vehicle into which it is fitted. It is tested in a testable environment where its functionality can be tested separately from the functionality and performance of any equipment connected to it to provide data for the performance of an application service.

7.4.11.4 OBE instantiated not as an OBE

If the OBE is part of the original equipment of the vehicle, it is likely that there is not a single OBE, but that the functionality is provided, at least in part, via the CAN bus and/or from similar equipment disbursed around the vehicle. For example, the GNSS data and compass function are most probably obtained from the vehicles satellite navigation system, accelerometer data and multi-axis gyroscope from the electronic drive/stability control, etc.

In this event, the OBE approval has to be integrated into the overall vehicle approval.

7.4.11.5 OBE attributes

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

- central processing unit;
- data storage means;
- data input means;
- connectivity means to/from auxiliary equipment;
- communications mean;
- power supply.

Each function needs specific tests as to fitness of purpose.

7.4.11.6 Central processing unit

The OBE is able to prove that it is able to perform the programme of operations required to fulfil regulated service provision. This normally implies the combination of:

- a processor;
- a volatile memory (RAM, DRAM, SRAM, etc.);
- a recognized operating system (e.g. LINUX®[2]).

Functionality tests for such systems are widely available and easily devised.

[2] LINUX® is an example of a suitable product available commercially. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of this product.

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

7.4.11.7 Data storage means

The OBE has a means of non-volatile bi-stable data storage that can retain the stored information even when not powered (such as a hard disc, flash memory, etc.).

7.4.11.8 Data input means

The OBE has a means to receive inputs both from auxiliary equipment and from its communications capability.

7.4.11.9 Connectivity means to/from auxiliary equipment

The OBE has 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 OBE is provided with access to the CAN bus.

7.4.11.10 Communications means

The OBE has access to one or more wireless means to communicate with the application of the jurisdiction. The interface(s) complies to a defined specification of the secure ITS interface.

7.4.11.11 Power supply

Normally, an OBE draws its electricity from the vehicle power supply. However, systems need one or several physically protected independent power supplies in the event of the disconnection of the vehicle power supply (e.g. in the event of an accident), a combination of independent power supply and non-volatile memory to prevent attempts to overcome/outwit the system, and, where required, to obtain information from the vehicle where the vehicle power supply has been intentionally removed (such as during service or vehicle lay-up, or in the event of a collision disconnected automatically as a safety measure).

The means of achieving the power supply requirements are a matter of system design. However, the minimum requirements are specified by the jurisdiction. Aspects specified by the jurisdiction are easy to demonstrate and include:

- the availability of power to the OBE when the vehicle is in operation (normally this requirement is 100 %);
- the number of hours the OBE can actively function when the vehicle power supply is not available;
- the number of hours the OBE can remain in a stand-by state.

7.4.12 Vehicle user

It is important to understand clearly who is the vehicle user as defined in this document. The vehicle user is not to be confused with the user of the application service (which is the vehicle user but is also a smart city user.

While this appears to be a simple clarification, it is in practice more complex.

There are four possibilities as to who is the user of the vehicle:

- the owner/keeper of the vehicle;
- the operator of the vehicle;

- the driver;
- the owner of the freight.

The owner of the vehicle is usually the person or organization that has registered the vehicle with the jurisdiction's vehicle registration system. But depending on the regulations of the jurisdiction, which vary around the world, the person/organization registering the vehicle is or is not the actual owner, and can also be a lessee or the vehicle keeper.

A further complication is that the owner of the vehicle is not the operator of the vehicle since the owner can lease or rent out the vehicle or leave the operation of the vehicle to a third party (as in the case of commercial freight vehicles).

The operator of the vehicle is the party who has the direct interest in the movement of the vehicle, both economically and physically. It is the operator who has given the instruction for the vehicle to take to the road, who has determined the destination, who has determined the route and who has obtained any permits that are required. The operator can therefore be the vehicle user.

In a connected vehicle, the operator/vehicle user is usually also the driver. In an automated vehicle, this is not the case.

In many cases, the driver is not the owner of the vehicle but an employee of the vehicle operator. Various drivers drive one vehicle during a period, and it is not uncommon for long-haul trucks to have two drivers on board who take it in turns to drive while the other rests. Further, in general, the individual driver is not the economic beneficiary of the transport service.

The owner of the freight benefits from the transport service, but normally has no influence on the transport service itself. The owner of the freight usually has no influence on the choice of vehicle configuration or on the detailed route taken.

Architecturally, this can be very messy. Therefore, some simplification and clarity are introduced.

The vehicle user is in most circumstances the operator of the vehicle, but in other circumstances, is the driver of the vehicle. ITS application system specifications are therefore required to specify and define who the user of the vehicle is deemed to be.

It is true to say that the vehicle user is most commonly the operator of the regulated commercial freight vehicle.

Users of the vehicle choose to enrol into a voluntary application or are required to enrol in a mandatory application, as determined by the jurisdiction, and this varies from jurisdiction to jurisdiction.

7.4.13 Application service provision

Within the ITS service application–secure ITS interface paradigm, application services are how the service user obtains the information it requires.

8 Communications architecture

Communications are defined in a specification of the secure ITS interface (see ISO/TS 5616[1]). An example is given in Annex A.

9 Quality of service requirements

This document contains no specific requirements concerning quality of service. Such aspects are determined by a jurisdiction.

10 Test requirements

There are no test requirements in this document.

11 Marking, labelling and packaging

There are no test requirements in this document.

Attention is drawn to ISO/TR 12859[2] in this respect. Regulation EU 2016/679[15] applies to implementers in Europe.

12 Declaration of patents and intellectual property

This document contains no known patents or intellectual property other than that which is implicit in the media standards referenced.

Annex A
(informative)

ITS data management architecture

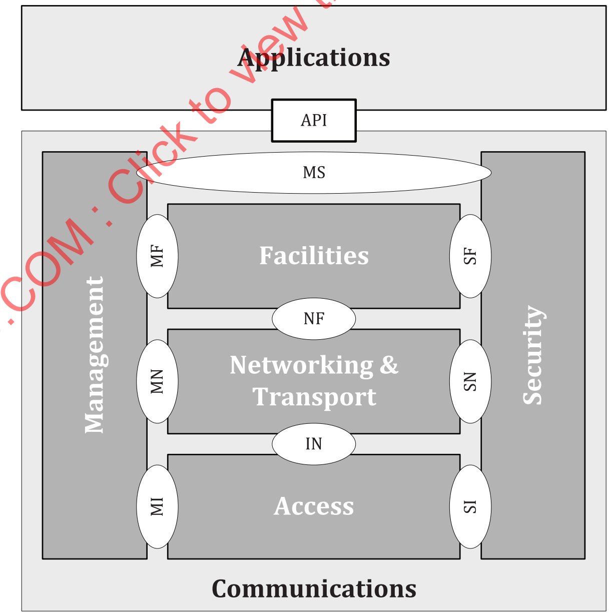
A.1 Background

The organizational structure of the governance process is described in ISO/TS 5616[1]. This annex shows the process flow of typical transactions to obtain or provide ITS data as advocated in this document and specified in ISO/TS 5616[1] using the secure ITS data management and access interface (SI) in accordance with ISO/TS 5616[1], ISO/TS 21177[5], ISO 21217[8], ISO 24102-1[9], ISO 24102-2[10], ISO 24102-3[11], ISO 24102-4[12] and ISO 24102-6[13], with the support of ISO/TS 21184[6] and ISO/TS 21185[7], in order to instantiate ITS service application in smart cities.

This annex describes the architecture of a secure process flow between a source ITS system and a destination ITS system.

A.2 Architectural foundation of the secure ITS data management and access interface

At the foundation of the process is the ISO 21217[8] ITS-station architecture, see Figure A.1.



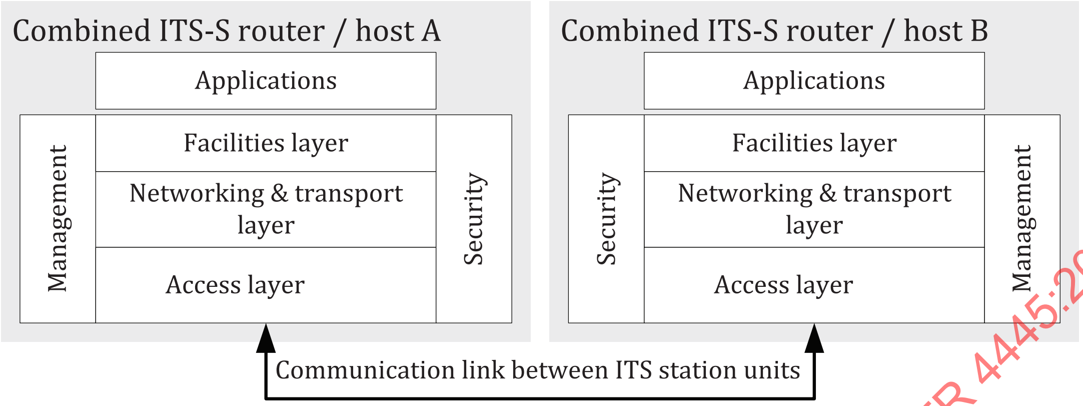
NOTE Source: ISO 21217:2020, Figure 13.

Figure A.1 — Simplified ITS-station reference architecture

The ITS-station communications stack is consistent with the OSI communications stack and its levels, and that each level is paired and that the same technical solution is used (paired) by both the originating and destination system at each level of the stack.

For simplicity of representation, in terms of the OSI communications stack, the facilities layer relates to the OSI presentation and session layers, and the access layer represents the combined communication interfaces layers, i.e. the data link layer (LLC, MAC) and the physical layer (802.11; 3GPP Release 8, 3GPP Release 14, 3GPP Release 21; i/r; I430/431; 802.3, etc.).

Figure A.2 shows a high-level view of the communication between two ITS stations.

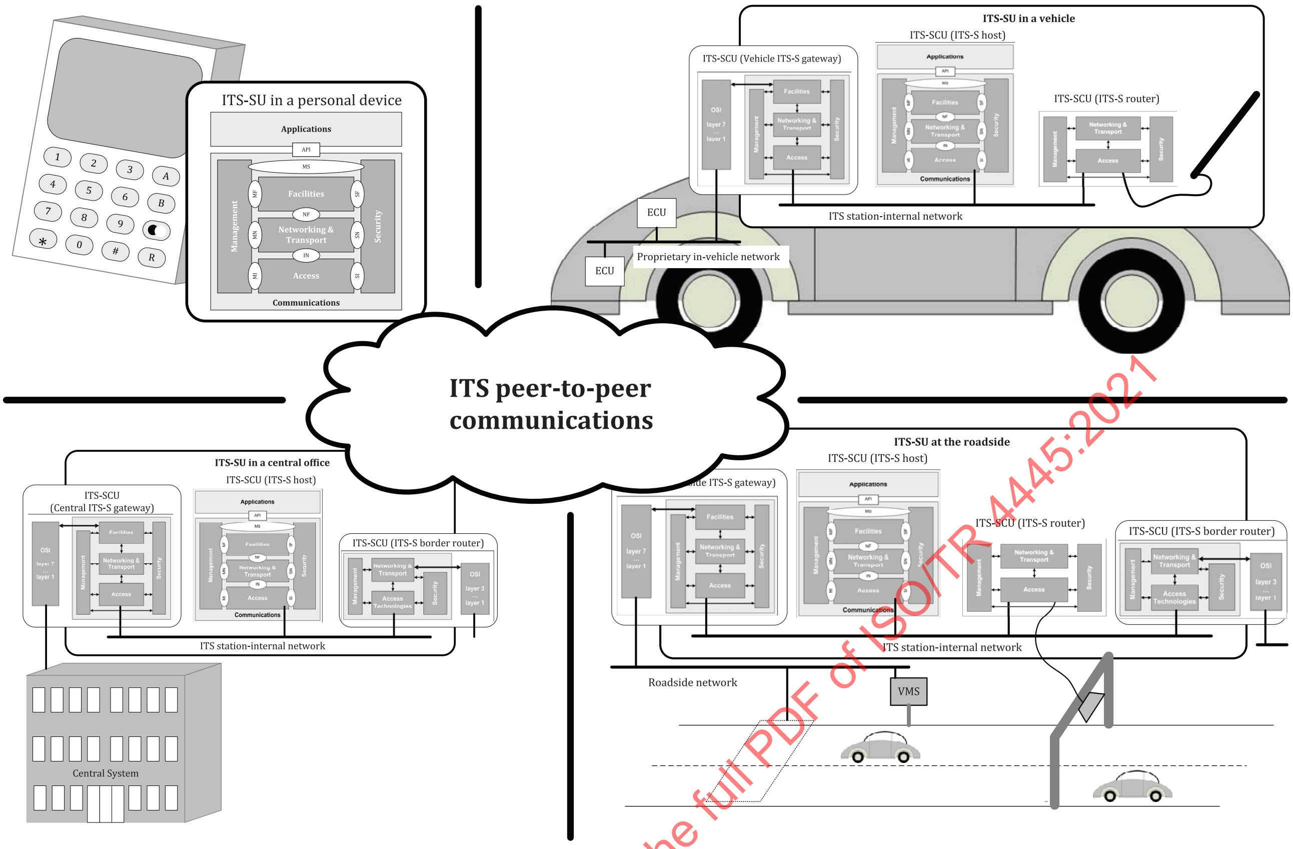

Combined ITS-S router / host A
Applications
Facilities layer
Networking & transport layer
Access layer
Management
Security
Combined ITS-S router / host B
Applications
Facilities layer
Networking & transport layer
Access layer
Security
Management
Communication link between ITS station units

NOTE Source: CSi UK.

Figure A.2 — Implementation architecture

An ITS station is situated in a vehicle, at the roadside, at a communications or service centre. The purpose of the transaction is not material to the concept, and the concept is agnostic to the communications technology so long as it can support the security requirements and required data rates. However, some applications have low latency requirements, which limits their choice of communications media.

The secure ITS data management and access interface is a peer-to-peer communication between any two ITS stations, regardless of its use case. ISO 21217[8] provides the illustration given in Figure A.3 to show that an ITS station is a vehicle, roadside, centre or personal device.


ITS-SU in a personal device
Applications
API
Facilities
Networking & Transport
Access
Management
Security
Communications
1
2
3
A
4
5
6
B
7
8
9
*
0
#
R
ITS-SU in a vehicle
ITS-SCU (ITS-S host)
ITS-SCU (Vehicle ITS-S gateway)
ITS-SCU (ITS-S router)
OSI layer 7 ... layer 1
ECU
ECU
Proprietary in-vehicle network
ITS station-internal network
ITS peer-to-peer communications
ITS-SU in a central office
ITS-SCU (ITS-S host)
ITS-SCU (Central ITS-S gateway)
ITS-SCU (ITS-S border router)
Access Technologies
ITS station-internal network
Central System
ITS-SU at the roadside
ITS-SCU (ITS-S host)
ITS-SCU (Roadside ITS-S gateway)
ITS-SCU (ITS-S router)
ITS-SCU (ITS-S border router)
OSI layer 3 ... layer 1
ITS station-internal network
Roadside network
VMS

NOTE Source: ISO 21217:2020, Figure 29[8].

Figure A.3 — Typical implementations of ITS station units

The secure ITS data management and access interface is based on the ISO 21217[8] concept of communications between ITS stations. The use case of an eSafety incident support information service (ISIS) is used in Figure A.4 as an example. This service is a support service for emergency responders following an eCall or other emergency call that has been triggered and completed. The source is the originating application, which in this use case is an emergency responder (fire brigade, paramedic, police). The connecting application is the destination, which is a vehicle affected by a crash (one of the vehicles that has crashed or a nearby vehicle). The objective of the service used in this example is to obtain data from the vehicle sensors or cameras, or to make voice over internet protocol (VOIP) contact with the occupants of the vehicle. As part of a preceding eCall that set the incident response in motion, the destination vehicle has already indicated its consent to participate in this service.

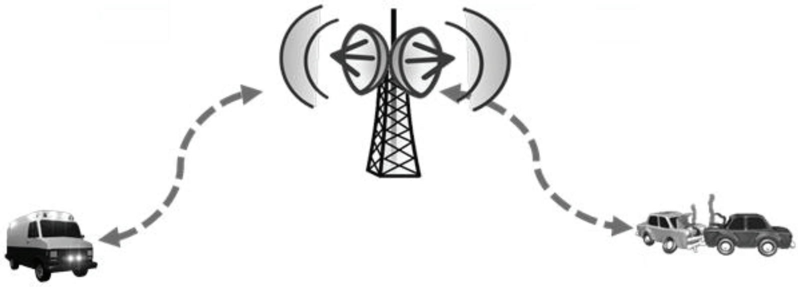


Figure A.4 — Example use case of an ISIS architecture objective

The objective, using the ITS-station implementation architecture, is illustrated in Figure A.5.

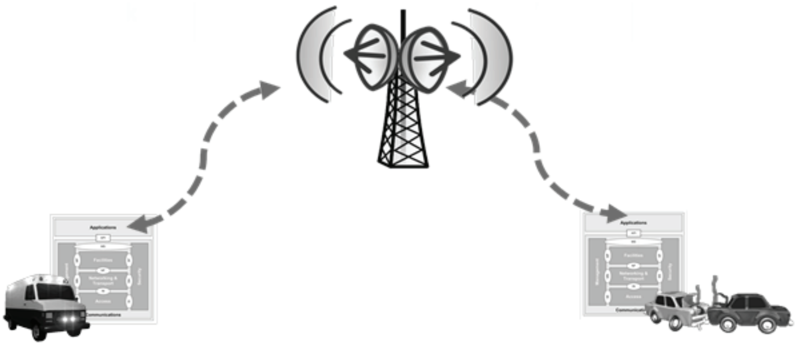


Figure A.5 — ISIS architecture using ISO 21217[8] ITS stations

To abstract this away from any particular use case, it can be illustrated as given in Figure A.6.

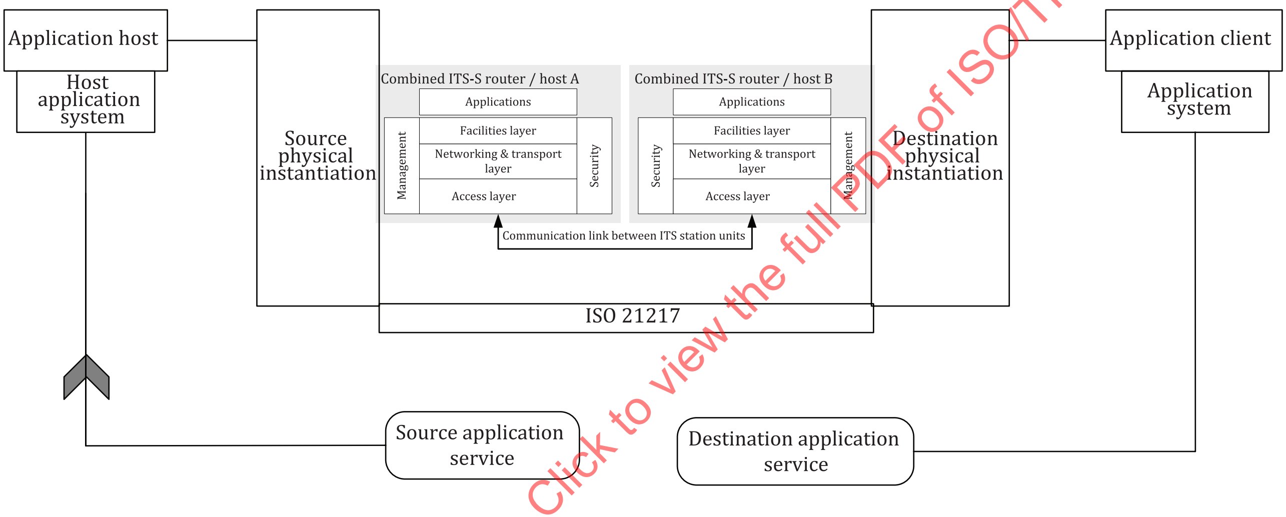

Application host
Host application system
Source physical instantiation
Combined ITS-S router / host A
Applications
Facilities layer
Networking & transport layer
Access layer
Management
Security
Combined ITS-S router / host B
Applications
Facilities layer
Networking & transport layer
Access layer
Security
Management
Communication link between ITS station units
Destination physical instantiation
Application client
Application system
ISO 21217
Source application service
Destination application service

Figure A.6 — Generic architecture using ITS stations

In addition, there are national and international regulations to apply, and the regulations for the source instantiation are different than those for the destination instantiation. The host instantiation operates within its regulatory environment and the destination instantiation operates within its regulatory environment.

Further, the application, whatever it is (e.g. eSafety ISIS as in the example used above), is probably defined in international or regional standard(s) in order that both source and destination instantiations have a common understanding, common sequences and common data concepts. These requirements are dealt with outside of the ISO 21217[8] architecture, affecting the host application or the destination client application. See Figure A.7.

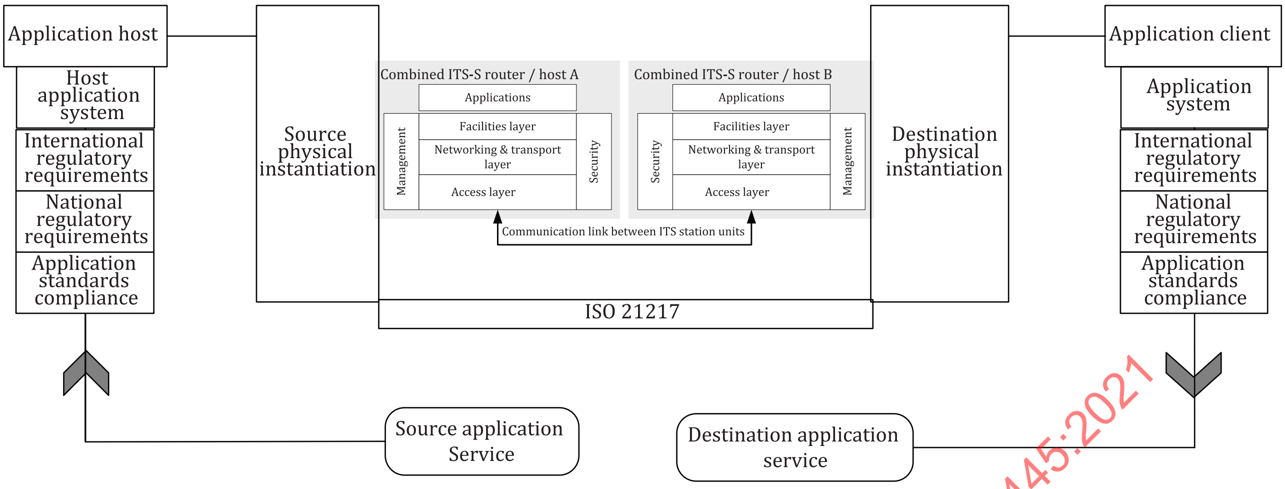

Application host
Host application system
International regulatory requirements
National regulatory requirements
Application standards compliance
Source physical instantiation
Combined ITS-S router / host A
Applications
Facilities layer
Networking & transport layer
Access layer
Management
Security
Combined ITS-S router / host B
Applications
Facilities layer
Networking & transport layer
Access layer
Security
Management
Communication link between ITS station units
ISO 21217
Destination physical instantiation
Application client
Application system
International regulatory requirements
National regulatory requirements
Application standards compliance
Source application Service
Destination application service

Figure A.7 — Generic architecture taking into account regulations and application standards

ISO 21217:2020[8] specifies what it calls a “bounded secured managed domain”, setting the overall cybersecurity requirements and providing basic communications security across the network, but leaving access details to the application-level systems. However, in a paradigm where the host system and the application system have different functionalities, different actors have different rights of access.

In the ISIS example used above, the fire brigade responders and police need access to the information concerning the cargo load of a crashed large goods vehicle, but that information cannot be available to other parties (since it is commercially sensitive). If there is medical information available that occupants of the vehicle have made available from wearable technology to the vehicle, using a Bluetooth link, it is only available to paramedic emergency responders. If the emergency responders have created an incident event and linked in several vehicles to obtain their camera feeds, the other vehicles do not have access to any of the information above.

In other domains, e.g. tuning and maintenance, only qualified and/or authorized actors can alter the operating parameters of the vehicle: fleet operators to fleet operational data, and insurers to pre-agreed data relevant to insurance. Bearing in mind the wide gamut of application systems in a connected vehicle, there has to be a system of selective access that is cybersecure and tailorable between any two parties so that they can access only authorized relevant data.

ISO 21217:2020[8] introduces ISO/TS 21177[5]. At this stage of the architecture elaboration, ISO/TS 21177[5] is the gatekeeper and controller of access to the ISO 21217-bounded secure managed domain and uses IEEE 1609.2[14] certificates to control what transactions are allowed between any two parties across the ITS station >< ITS-station interface.

ISO/TS 21185[7] additionally provides profiles at all layers of the communications stack.

See Figure A.8.

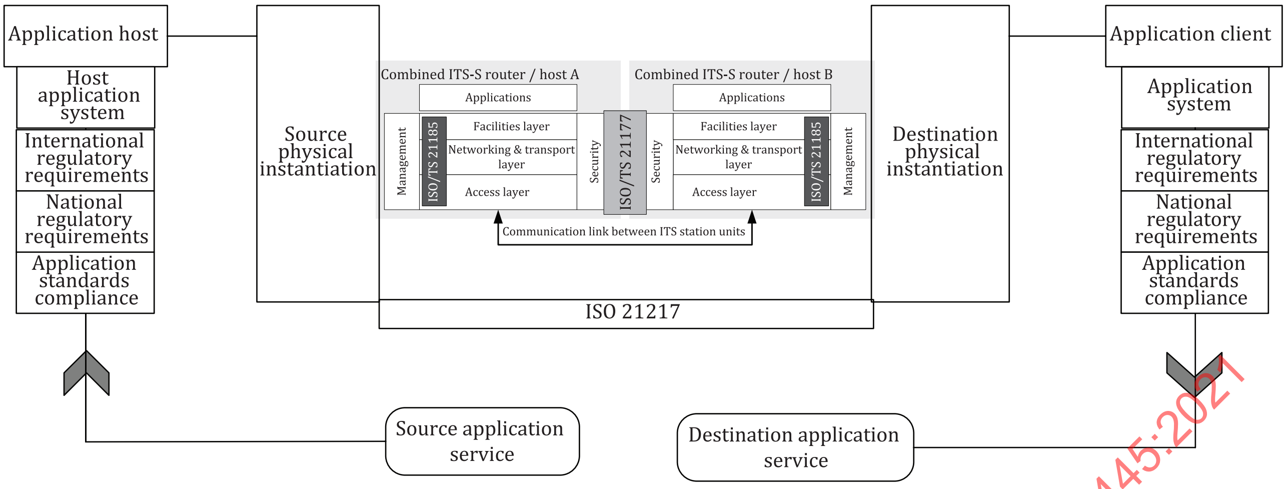

Application host
Host application system
International regulatory requirements
National regulatory requirements
Application standards compliance
Source physical instantiation
Combined ITS-S router / host A
Applications
Management
ISO/TS 21185
Facilities layer
Networking & transport layer
Access layer
Security
ISO/TS 21177
Security
Combined ITS-S router / host B
Applications
Facilities layer
Networking & transport layer
Access layer
ISO/TS 21185
Management
Communication link between ITS station units
ISO 21217
Destination physical instantiation
Application client
Application system
International regulatory requirements
National regulatory requirements
Application standards compliance
Source application service
Destination application service

Figure A.8 — Generic architecture with ISO 21217[8] and ISO/TS 21177[5] selective access and cybersecurity

Ideally, the same data presentation and data formats would be used by everyone. However, systems are designed by different system specialists and evolve (and often carry historical baggage) over many years or decades (and in some cases centuries). Often, they are developed within a specialized domain with its own defined requirements, and with no need to look beyond this domain. The result is that apparently identical systems and sub-systems are defined differently, and, most importantly, transactions and data are defined in different nomenclatures, different structures and in different definition formats. Sometimes the differences are between different applications. But differences also occur, sometimes with good reason, within the same application. For example, a vehicle manufacturer employs different access protocols to its sensors in a vehicle in comparison with a different manufacturer, it has its own unique set of CAN bus IDs and uses its own unique cybersecurity on its internal networks.

Although it could be ideal to harmonize all these things, this is impracticable and in some cases undesirable. However, the requirements of connectivity and interdependencies of the connected ITS paradigm mean that it is necessary to exchange data with other actors, and to understand those data. Without it, the connected and automated vehicle (CAV) is not safe and is not allowed by regulators in mixed traffic.

ISO/TS 21184[6] defines the standardized data classes in a global transport data format (GTDF) and the means to manage them. Data exchange between ITS stations is based on messages and content composed of pre-configured information including conditional handling. Each message uses a global unique identifier and the associated data element. The format of the data element is specified by the global unique identifier pointing to configuration information including instructions for correct interpretation of the data element; thus, providing intelligible data transfer between actors without either actor having to fundamentally change/redesign its (often proprietary) system.

ISO/TS 21184[6] is applicable both outside and within the bounded secure managed domain. See Figure A.9.

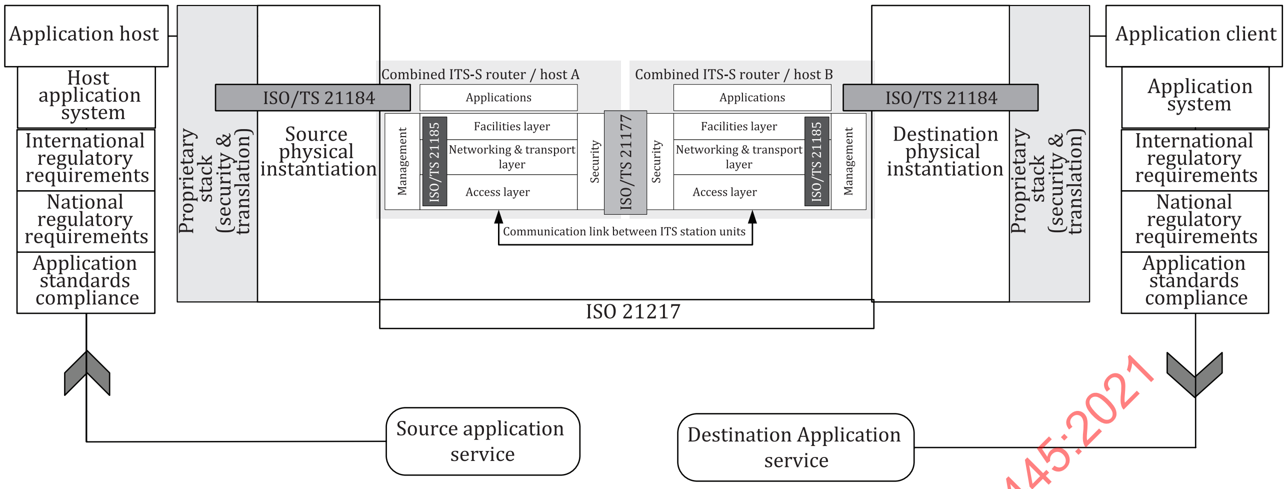

Application host
Host application system
International regulatory requirements
National regulatory requirements
Application standards compliance
Proprietary stack (security & translation)
ISO/TS 21184
Source physical instantiation
Combined ITS-S router / host A
Applications
Facilities layer
Networking & transport layer
Access layer
Management
ISO/TS 21185
Security
ISO/TS 21177
Combined ITS-S router / host B
Communication link between ITS station units
ISO 21217
Destination physical instantiation
Application client
Application system
Source application service
Destination Application service

Figure A.9 — Generic architecture with ISO 21217[8] and ISO/TS 21177[5] selective access and ISO/TS 21184[6] translation

In practice, the examples given in Figure A.10 can therefore be seen.

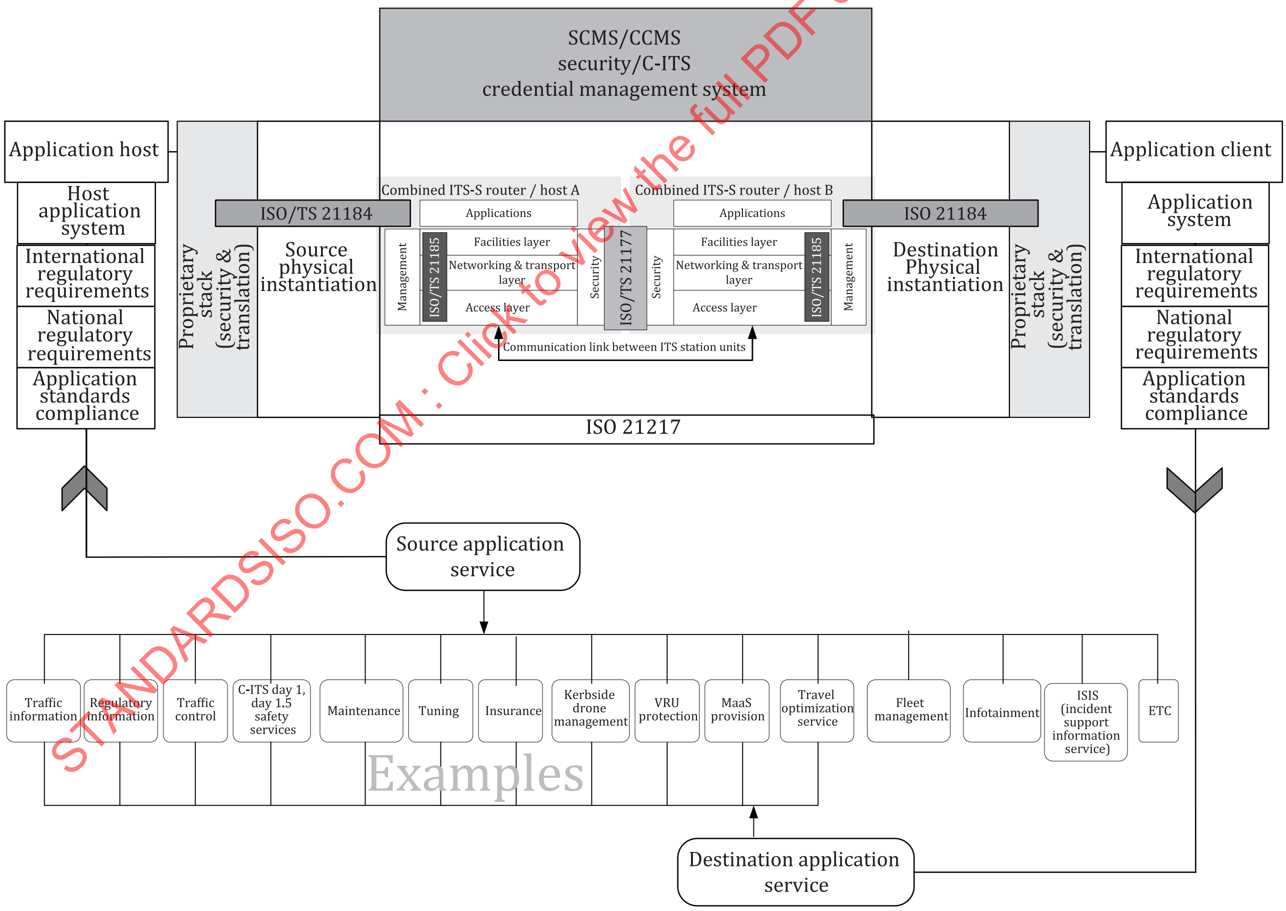

SCMS/CCMS security/C-ITS credential management system
Application host
Host application system
International regulatory requirements
National regulatory requirements
Application standards compliance
Proprietary stack (security & translation)
ISO/TS 21184
Source physical instantiation
Combined ITS-S router / host A
Applications
Facilities layer
Networking & transport layer
Access layer
Management
ISO/TS 21185
Security
ISO/TS 21177
Combined ITS-S router / host B
Communication link between ITS station units
ISO 21217
ISO 21184
Destination Physical instantiation
Application client
Application system
Source application service
Traffic information
Regulatory information
Traffic control
C-ITS day 1, day 1.5 safety services
Maintenance
Tuning
Insurance
Kerbside drone management
VRU protection
MaaS provision
Travel optimization service
Fleet management
Infotainment
ISIS (incident support information service)
ETC
Examples
Destination application service

Figure A.10 — Generic secure ITS data management and access interface architecture

A.3 Functional architecture of the secure ITS data management and access interface

Figures A.8 and A.9 show that the inclusion of ISO/TS 21177[5] provides selective access and security, but they do not explain how it achieves this and how this aspect of the architecture works. Figure A.11 zooms in on the central bounded secure managed domain section of Figures A.8 and A.9 and shows where ISO/TS 21177[5], as well as ISO/TS 21184[6] and ISO/TS 21185[7], impact.

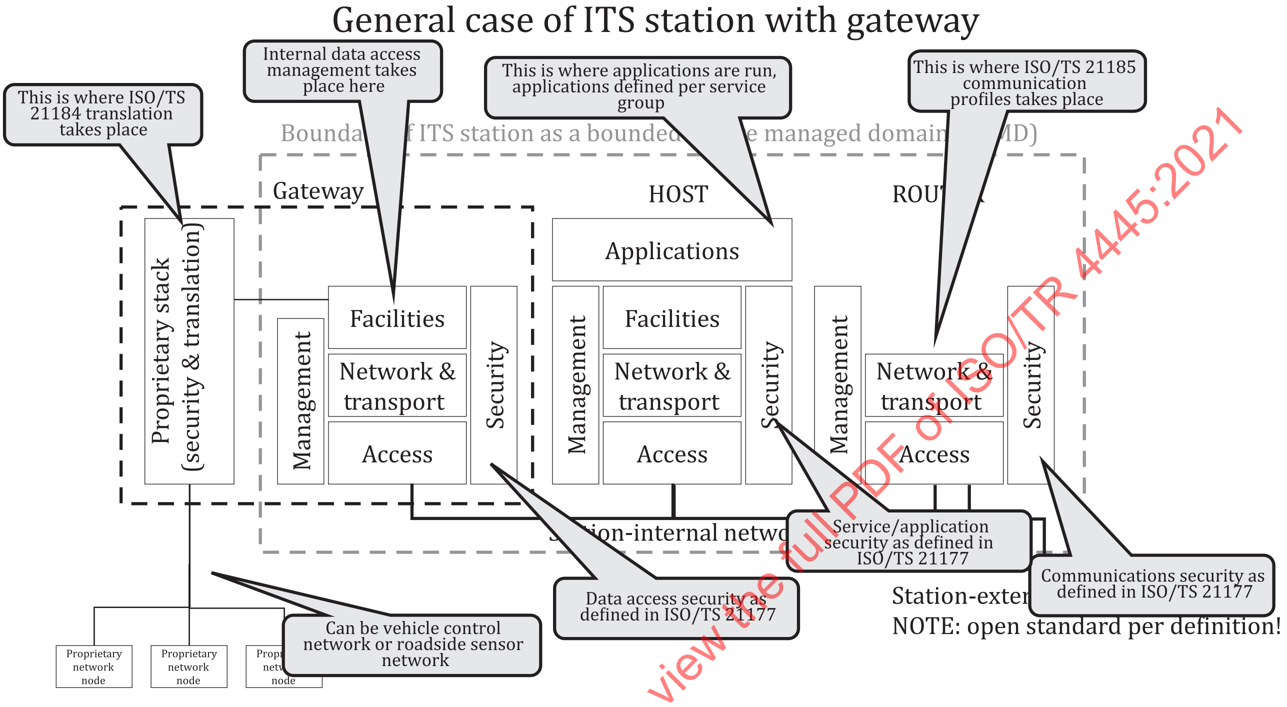

General case of ITS station with gateway
This is where ISO/TS 21184 translation takes place
Internal data access management takes place here
This is where applications are run, applications defined per service group
This is where ISO/TS 21185 communication profiles takes place
Bounda f ITS station as a bounded e managed domain MD)
Gateway
HOST
ROU
Proprietary stack (security & translation)
Management
Facilities
Network & transport
Access
Security
Applications
Facilities
Network & transport
Access
Management
Security
Management
Network & transport
Access
Security
ion-internal netwo
Service/application security as defined in ISO/TS 21177
Communications security as defined in ISO/TS 21177
Data access security as defined in ISO/TS 21177
Station-exter
NOTE: open standard per definition!
Can be vehicle control network or roadside sensor network
Proprietary network node
Proprietary network node
Prop netv node

Figure A.11 — Where ISO/TS 21177[5], ISO/TS 21184[6] and ISO/TS 21185[7] impact

The central characteristic for how ISO/TS 21177[5] achieves selective access and cybersecurity is that two devices cooperate in a trusted way, i.e. exchange information in secure application sessions (see Figure A.12)

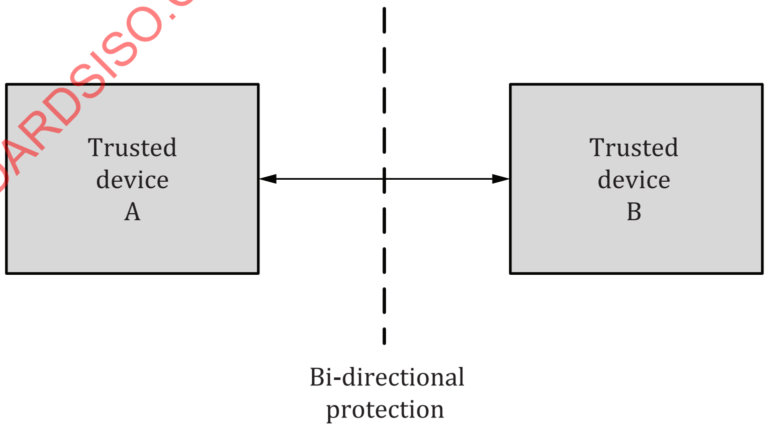


Figure A.12 — The basic transaction paradigm

Figure A.13 shows an example of an on-board device supporting multiple applications.

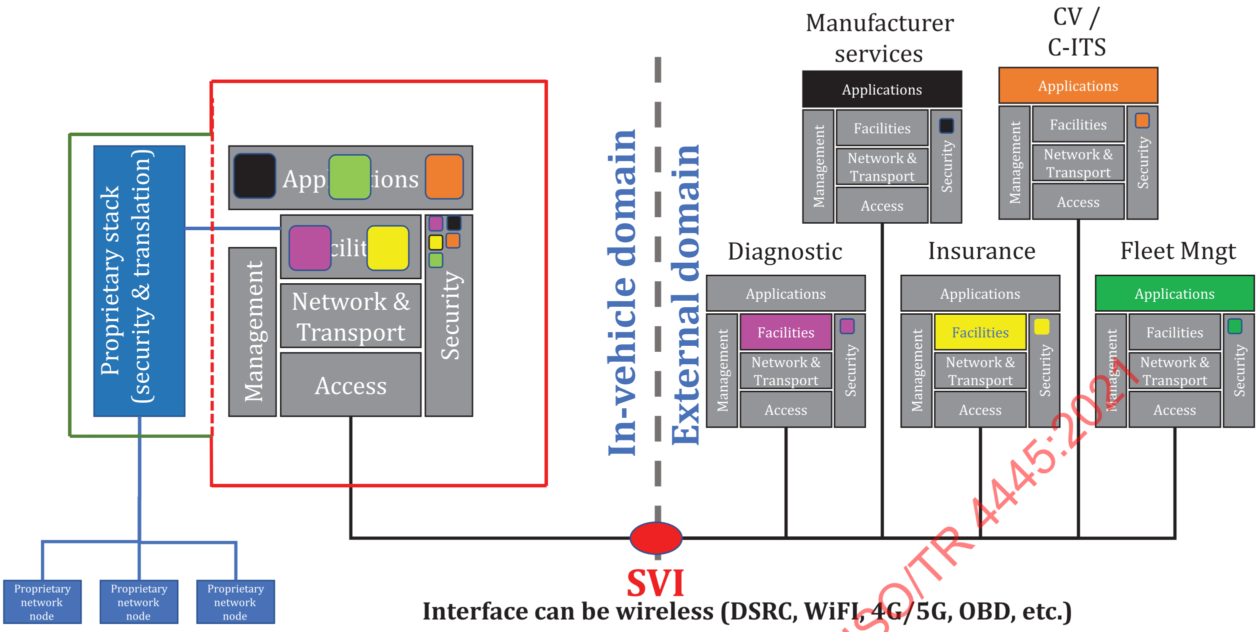


Figure A.13 — Example of an on-board unit supporting multiple applications

The first step is to obtain an access certificate. The ISIS example is shown in Figures A.14, A.15, A.16, A.17 and A.18. Access to a connected vehicle, so called "C-ITS", is shown in Figures A.19 and A.20. Diagnostic services are shown in Figures A.21, A.22, A.23, and A.24.

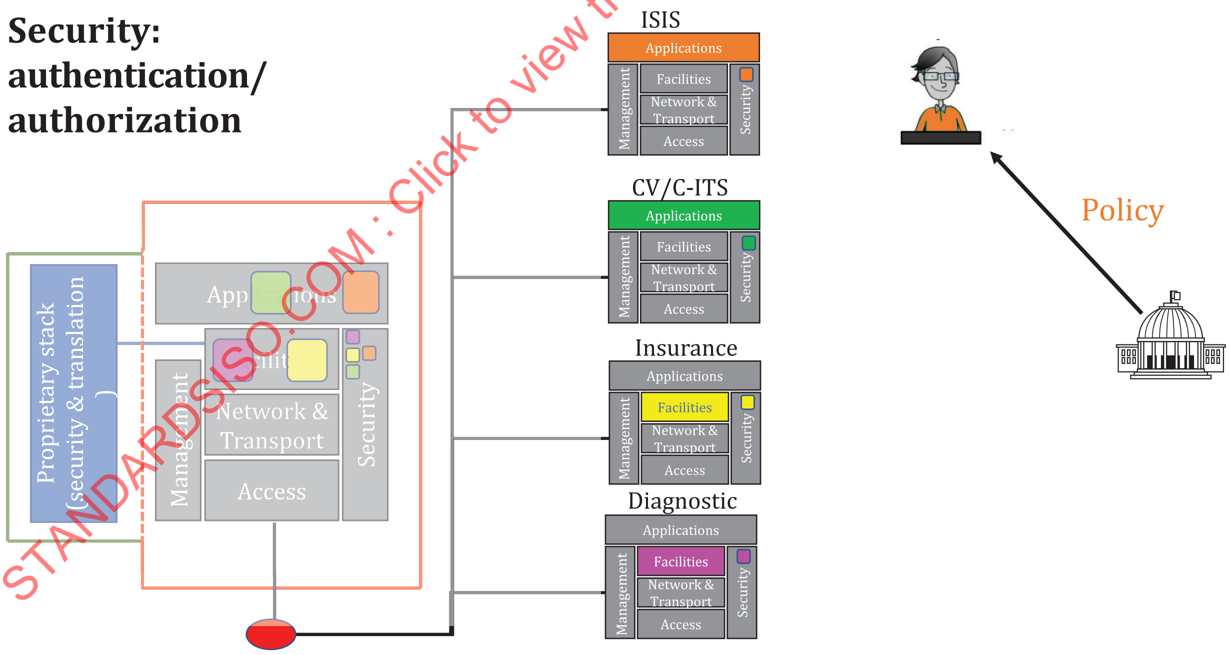


Figure A.14 — Example of a governance asserts policy (ISIS)

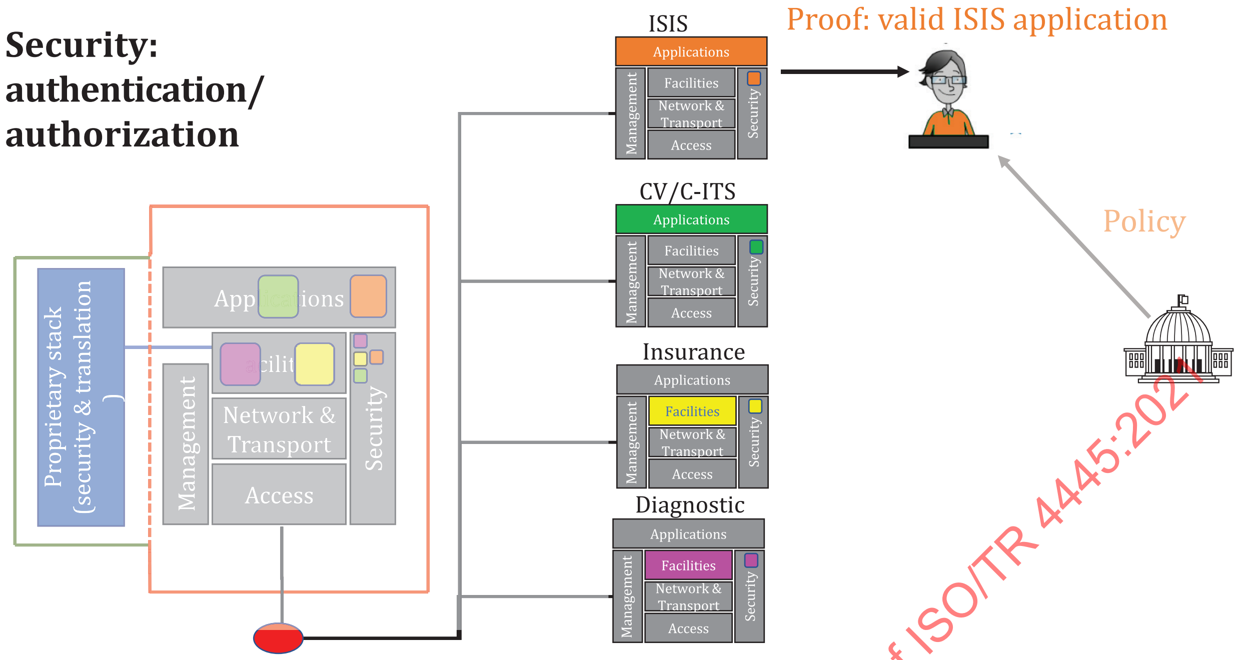


Figure A.15 — Example of an application (ISIS)

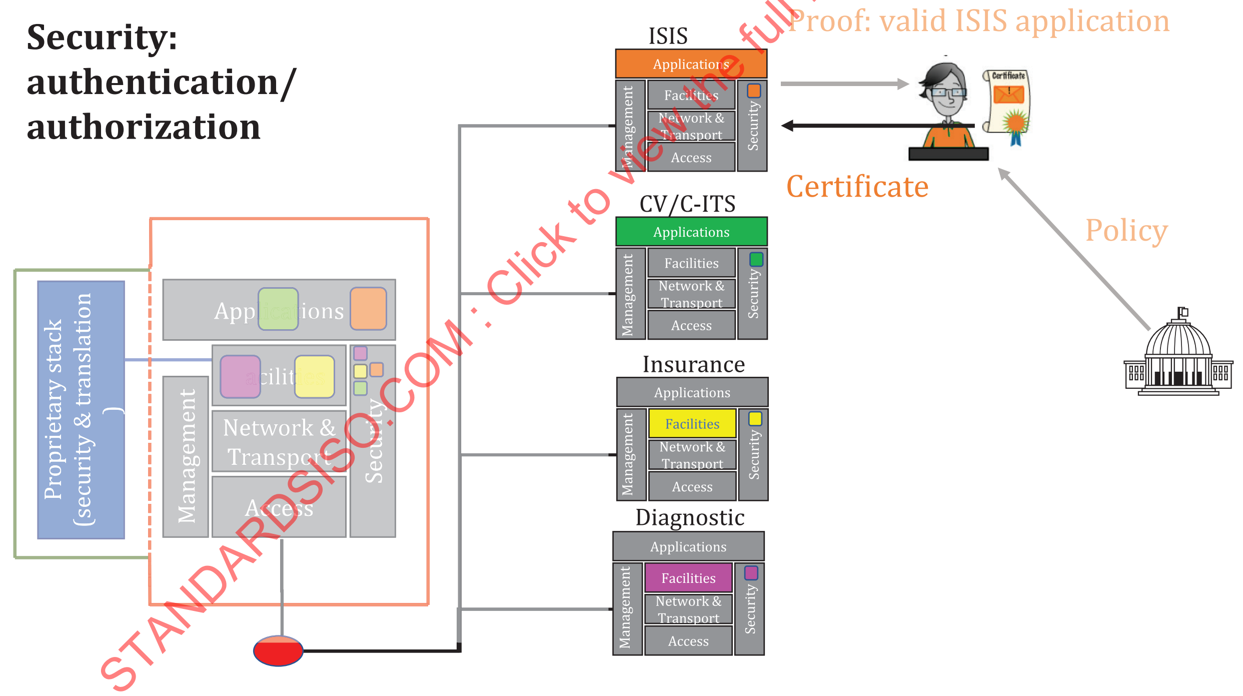


Figure A.16 — Example of an issue certificate (ISIS)

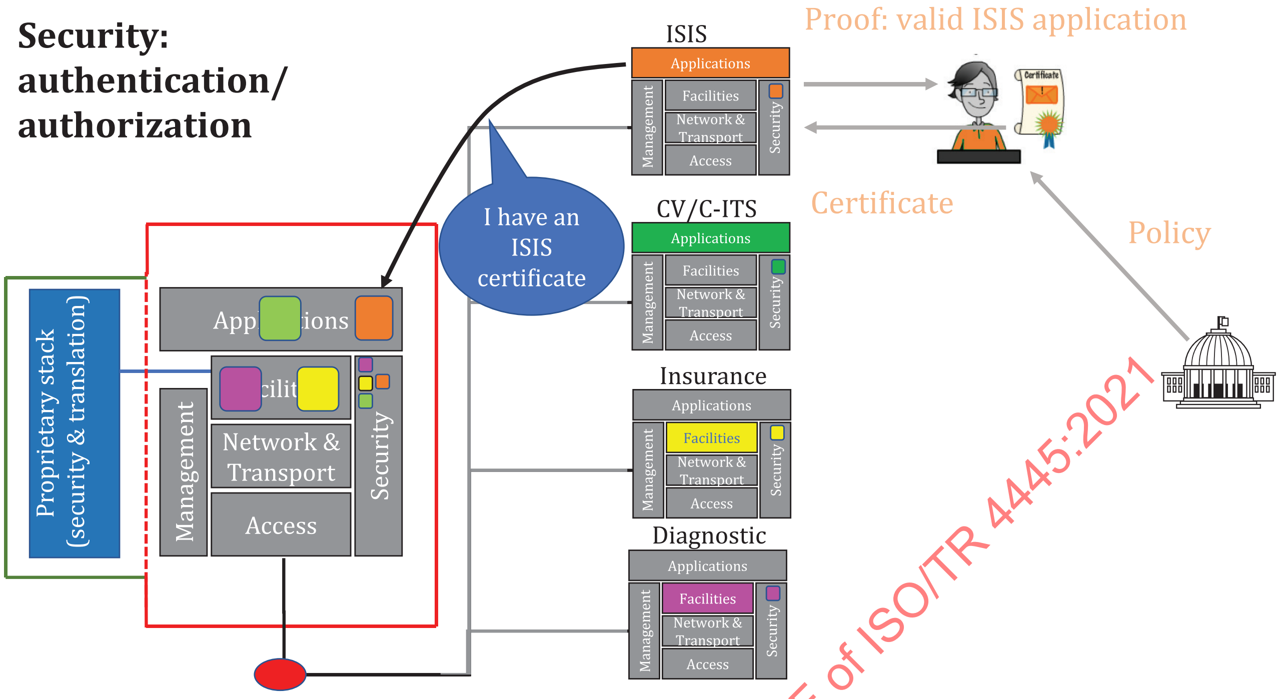


Figure A.17 — Example of a declaration (ISIS)

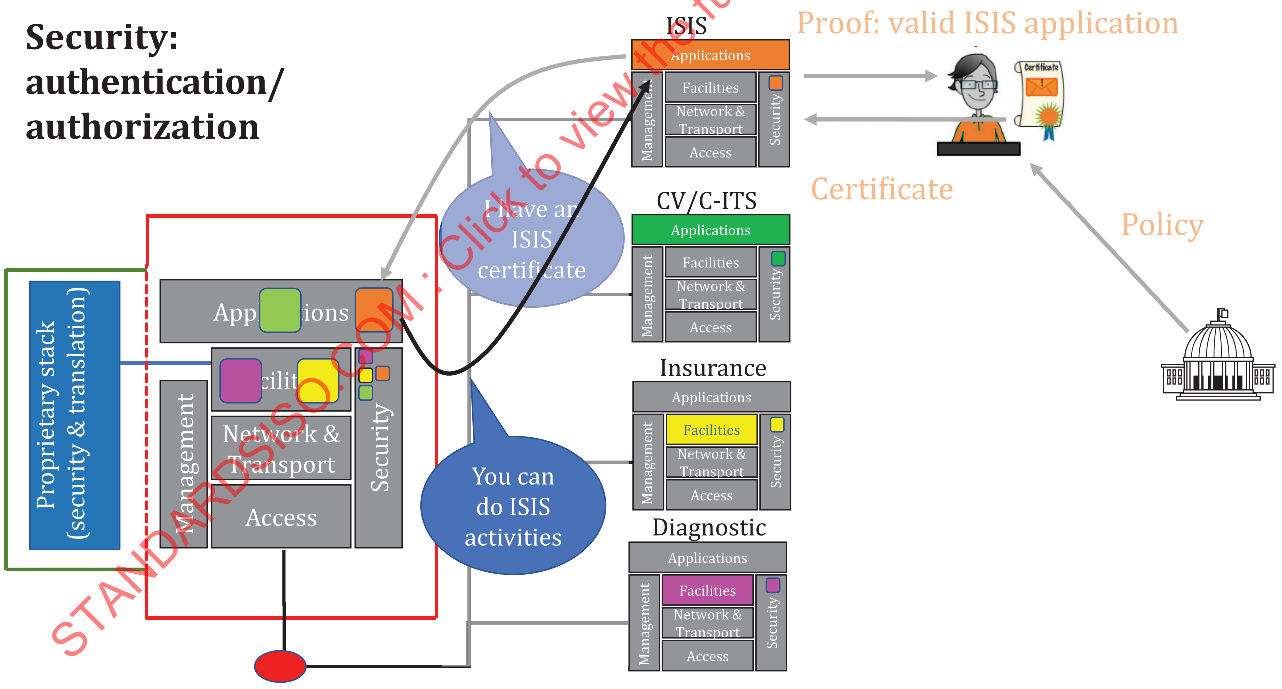


Figure A.18 — Example of an authentication (ISIS)

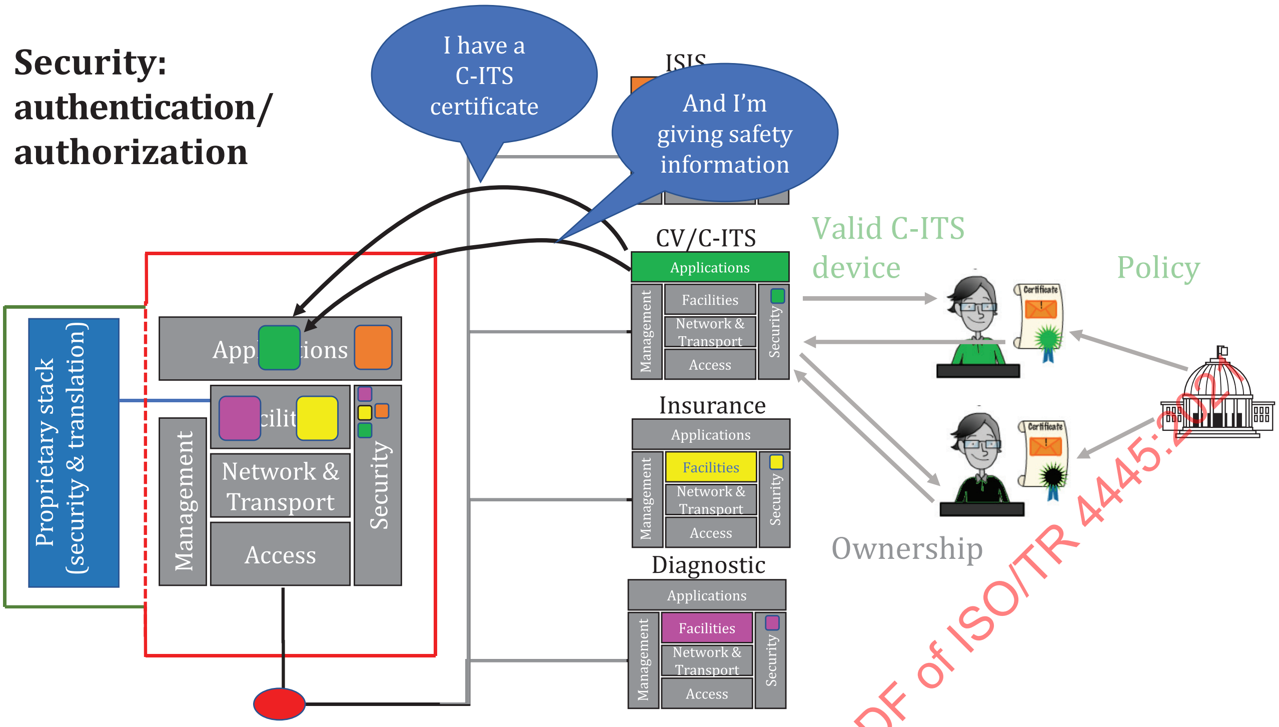


Figure A.19 — Example of a declaration (connected vehicle/CCAM/C-ITS)

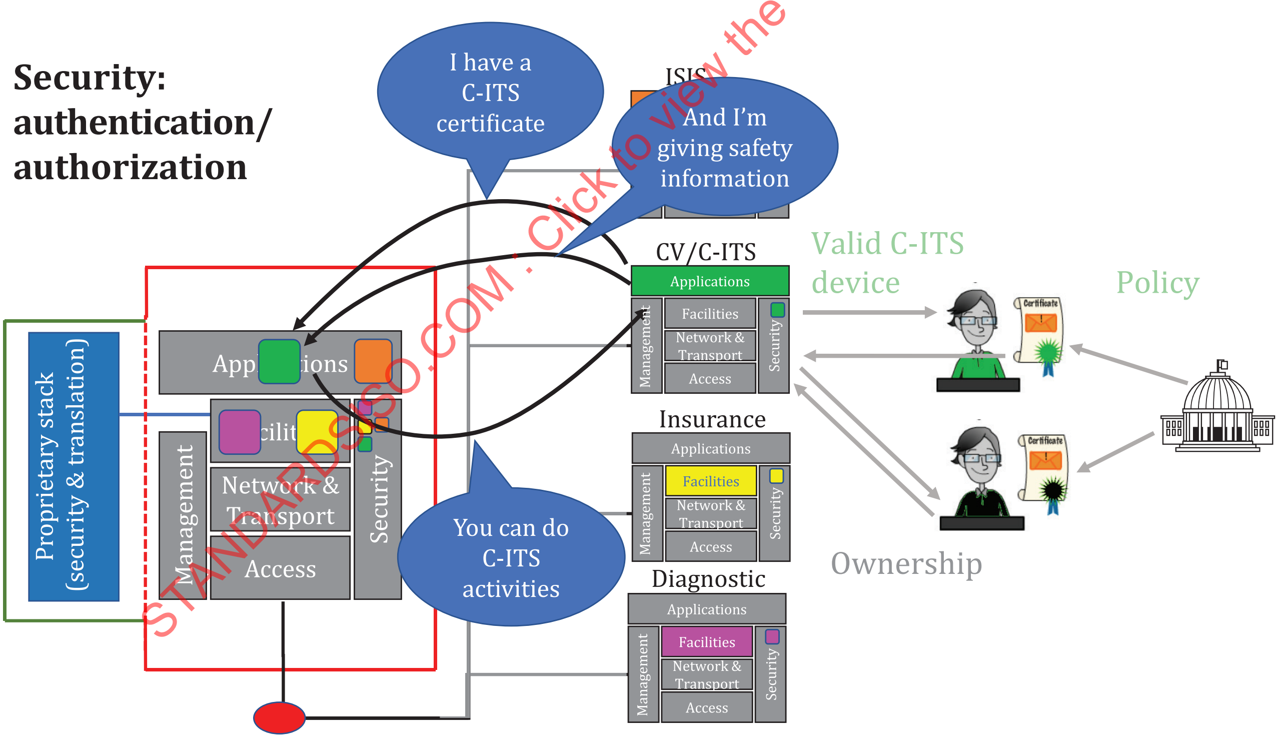

Security: authentication/ authorization
I have a C-ITS certificate
And I'm giving safety information
You can do C-ITS activities
ISIS
CV/C-ITS
Applications
Facilities
Network & Transport
Access
Management
Security
Insurance
Diagnostic
Valid C-ITS device
Policy
Ownership
Proprietary stack (security & translation)
Certificate

Figure A.20 — Example of an authentication (connected vehicle/CCAM/C-ITS)