TECHNICAL SPECIFICATION

ISO/TS 21185

First edition
2019-10

Intelligent transport systems — Communication profiles for secure connections between trusted devices

Reference number
ISO/TS 21185:2019(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*.

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

ITS Station Communication Profiles (ITS-SCP) used in communications between trusted devices enable

— interoperability between ITS-SUs,

— and portability of ITS applications (that provide the ITS services).

Examples of trusted devices, i.e. ITS-secured communication nodes, are ITS-station units (ITS-SU) specified in ISO 21217:2014. Four implementation contexts of communication nodes in ITS communications networks are identified in ISO 21217:2014, each comprised of ITS-station units (ITS-SU) taking on a particular role: personal, vehicular, roadside, or central. Such ITS-SUs participate in a wide variety of ITS services related to, e.g. sustainability, road safety and transportation efficiency.

NOTE 1 ISO 21217:2014 fully covers the functionality of EN 302 665[27], which is a predecessor of ISO 21217:2014.

NOTE 2 An ITS-SU can be composed of ITS-SCUs from different vendors where each ITS-SCU is linked to a different ITS-SCU configuration and management centre specified in ISO 24102-2[16] and ISO 17419. Station-internal management communications between ITS-SCUs of the same ITS-SU are specified in ISO 24102-4[17]. European C-ITS regulation refers to the "ITS-SCU configuration and management centre" as "C-ITS station operator" meaning the entity responsible for the operation of a C-ITS station. The C-ITS station operator may be responsible for the operation of one single C-ITS station (fixed or mobile), or a C-ITS infrastructure composed of a number of fixed C-ITS stations, or a number of mobile ITS-Stations.

Such ITS-SCPs are essential for many ITS applications and services including time-critical safety applications, automated driving, remote management of ITS-SUs (ISO 24102-2[16]), and roadside/infrastructure related services.

Over the last decade, ITS services have arisen that require secure access to data from Sensor and Control Networks (SCN), e.g. from In-Vehicle Networks (IVNs) and from Infrastructure/Roadside Networks (IRNs), some of which require secure local access to time-critical information, see Figures 1 and 2.

NOTE 3 Figures 1 and 2 are functional illustrations not describing or specifying a specific implementation.

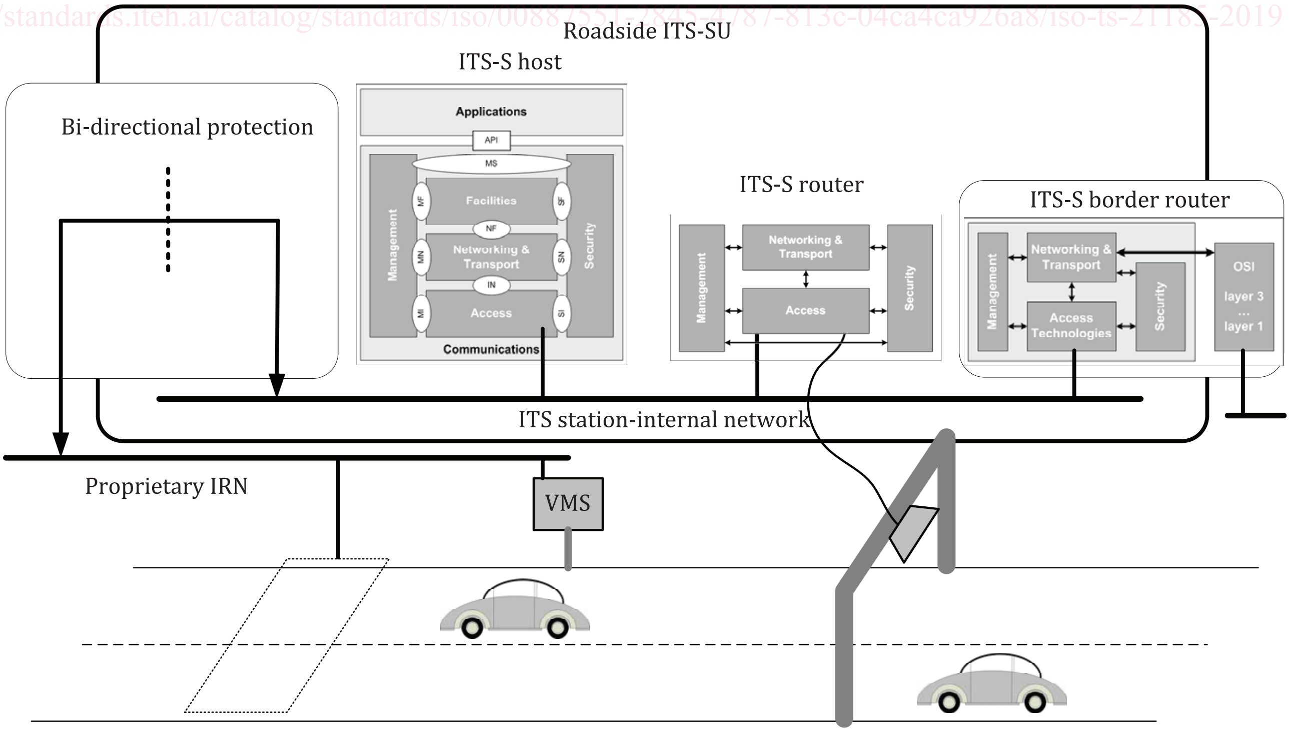

Figure 1 — Example of a roadside ITS-SU connected to a secure proprietary IRN

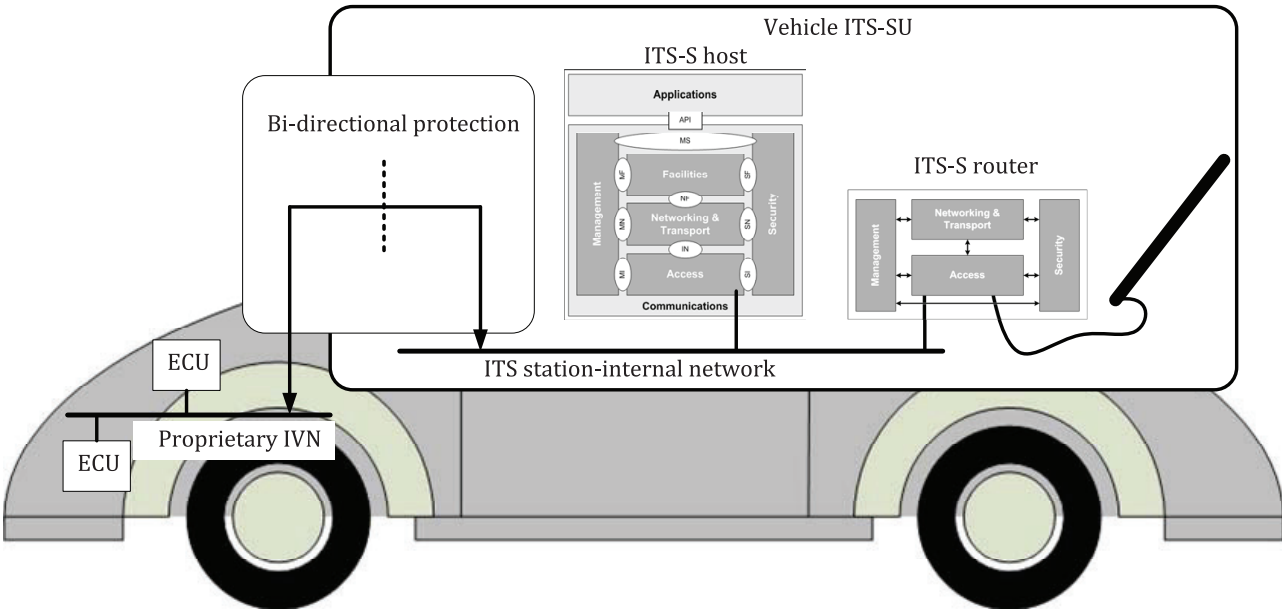

Figure 2 — Example of a vehicle ITS-SU connected to a secure proprietary IVN

Related use cases of these ITS services have largely been derived from regulatory requirements and urban operational needs, and they include:

— secure real-time access to time-critical vehicle-related data for safety of life and property applications, e.g. collision avoidance, emergency electronic brake light and event determination;

— secure local access to detailed real-time data for efficiency applications (traffic management), e.g. intersection interaction, congestion avoidance, dynamic priorities;

— local access to certified real-time data for sustainability applications, e.g. dynamic emission zones (controlled zones as currently standardized in CEN TC 278 within the Project Team PT1705 funded by the European Commission), intersection priorities based on emissions, interactive optimum vehicle settings to minimize fuel consumption.

There are many use cases of ITS services currently identified where real-time exchange of time-critical information between ITS-SUs in close proximity is essential, and the number will grow (see, e.g. the US National ITS Reference Architecture[30]). It is critical that ultimately all ITS-SUs in a given area are able to be engaged in these distributed services. This, in turn, requires vehicle ITS-SUs to have real-time access to vehicle data, and roadside ITS-SUs to have real-time access to infrastructure data, and to be capable of secure software updates.

Another use case involving connectivity between ITS-Ss involves access to ITS-secure SCNs by ITS-SUs over the Internet, i.e. cloud connectivity. Functions and services described in this document and accompanying standards for creating secure communication links can be used to implement such connectivity. Examples include secure communications between a server in a cloud-based ITS-SU and an ITS-SU in a vehicle using a cellular modem, and secure communications between server in an ITS-SU in a traffic control center and a client in an ITS-SU in the roadside “furniture” which it controls using a fibre optic and/or microwave link.

Data and message specifications related to SCNs are provided in ISO/TS 21184[9].

Cyber security means related to "Secure Sessions between Trusted Devices" (SSTD) in general, and particularly to SCNs, are specified in ISO/TS 21177[8].

Cyber security means related to information dissemination (broadcast of messages) are specified in IEEE Std. 1609.2™[21].

Intelligent transport systems — Communication profiles for secure connections between trusted devices

1 Scope

This document specifies a methodology to define ITS-S communication profiles (ITS-SCPs) based on standardized communication protocols to interconnect trusted devices. These profiles enable secure information exchange between such trusted devices, including secure low-latency information exchange, in different configurations. The present document also normatively specifies some ITS-SCPs based on the methodology, yet without the intent of covering all possible cases, in order to exemplify the methodology.

Configurations of trusted devices for which this document defines ITS-SCPs include:

a) ITS station communication units (ITS-SCU) of the same ITS station unit (ITS-SU), i.e. station-internal communications;

b) an ITS-SU and an external entity such as a sensor and control network (SCN), or a service in the Internet;

c) ITS-SUs.

Other ITS-SCPs can be specified at a later stage.

The specifications given in this document can also be applied to unsecured communications and can be applied to groupcast communications as well.

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/IEC 8825-1, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) — Part 1*

ISO 17419, *Intelligent transport systems — Cooperative systems — Globally unique identification*

ISO 17423:2018, *Intelligent transport systems — Cooperative systems — Application requirements and objectives*

ISO 21217:2014, *Intelligent transport systems — Communications access for land mobiles (CALM) — Architecture*

3 Terms and definitions

For the purposes of this document, the following terms and definitions 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
ITS-S communication profile
parameterized ITS-S communication protocol stack

[SOURCE: ISO 17423:2018, 3.6]

3.2
ITS communication protocol
communication protocol applicable in ITS

3.3
ITS-S communication protocol stack
consistent set of ITS-S communication protocols enabling communications between an ITS-SCU and other nodes which may be identified by a registered globally unique reference number

[SOURCE: ISO 17423:2018, 3.7]

4 Symbols and abbreviated terms

CSP	communication service parameter [SOURCE: ISO 17423:2018]
ITS-CP	ITS communication protocol
ITS-SCP	ITS station communication profile [SOURCE: ISO 17423:2018]
ITS-SCPS	ITS station communication protocol stack [SOURCE: ISO 17423:2018]
ITS-SCU	ITS station communication unit [SOURCE: ISO 21217:2014]
ITS-SU	ITS station unit [SOURCE: ISO 21217:2014]
IRN	infrastructure/roadside network
IVN	in-vehicle network
SCN	sensor and control network
SSTD	secure session between trusted devices
OID	object identifier

5 OID conventions

The following OIDs are specified and used in this document:

1) Identifying this document:

   { iso (1) standard (0) cptd21185 (21185) }

2) Identifying ASN.1 module specifications of this document:

   { iso (1) standard (0) cptd21185 (21185) asn1 (1) }

3) Identifying an ITS communications protocol:

{ iso (1) standard (0) cptd21185 (21185) commProtocol (2) }

4) Identifying an ITS-S communication protocol stack (ITS-SCPS):

{ iso (1) standard (0) cptd21185 (21185) its-scps (3) }

5) Identifying an ITS-S communications profile (ITS-SCP):

{ iso (1) standard (0) cptd21185 (21185) its-scp (4) }

6 Architecture

This document considers the ITS station and communication architecture specified in ISO 21217:2014 and specifies globally unique identifiers of ITS-S communication profiles (ITS-SCPs) for e.g.

— interconnecting ITS-SCUs in an ITS-SU,

— interconnecting ITS-SUs, and for,

— interconnecting an ITS-SU with a SCN,

using OIDs identifying

— ITS communication protocols,

— ITS-S communication protocol stacks (ITS-SCPS),

— ITS-S communication profiles (ITS-SCP),

also specified in this document. The approach is based on the methodology for protocol parameters CSP_Protocol and CSP_SpecificCommsProts specified in ISO 17423:2018 and illustrated in 7.1.

7 Communication profiles and protocol stacks — Overview

7.1 Definitions and methodology

An ITS-SCP is defined in ISO 17423:2018 as a "parameterized ITS-S communication protocol stack". ISO 17423:2018 further specifies how ITS-S application processes can present their communication needs by means of "Communication Service Parameters" (CSP) to the ITS-S management, and how the ITS-S management selects applicable ITS-S communication profiles. This document uses the following two CSPs for specifying ITS-SCPs:

a) CSP_Protocol:

Identification of a complete non-parameterized communication protocol stack by means of a globally unique registered communication protocol stack identifier of ASN.1 type `ProtocolReq::=ITSprotocolStackID`, with `ITSprotocolStackID` specified in ISO 17419; see Clause 8.2.6.

NOTE 1 ISO 17419 specifies ITSprotocolStackID as an INTEGER.

b) CSP_SpecificCommsProts:

Identification of selected non-parameterized communications protocol stack elements by means of a sequence of protocol identifiers of ASN.1 type `SpecCommProts::=SEQUENCE OF ITSprotID`, with `ITSprotID` specified in ISO 17419 as a sequence of a ITS-S protocol location of ASN.1 type `ItssProtocolLocation` followed by an ITS protocol identifier of ASN.1 type `ItsProtocolIdentifier`; see Table 1 and Clause 8.

NOTE 2 ISO 17419 specifies ItsProtocolIdentifier as an INTEGER.

NOTE 3 `ITSprotID` is used in Service Announcement specified in ISO 22418[14].

Table 1 — Named Integer values of `ItsProtocolLocation` as specified in ISO 17419

ITS-S layer or entity (ISO 21217:2014)	ItsProtocolLocation[a]	
	Acronym	Value
ITS-S access layer	"acLayer"	1
ITS-S networking & transport layer	"ntLayer"	2
ITS-S facilities layer	"fcLayer"	4
ITS-S management entity	"mgEntity"	8
ITS-S security entity	"scEntity"	16
Other location	"other"	32

[a] For ITS protocols residing in more than one layer or entity, the acronym to be used in the context of this document is "several" with a value given by the sum of the values of the respective layers and entities. Alternatively, the parts of such an ITS protocol may be identified separately.

The methodology for specifying ITS-SCPs in this document is given by the following steps:

1) Identify ITS communication protocols (ITS-CPs) by means of an "Object Identifier" (OID) reference to the standard or specification of the protocol based on the methodology for CSP_SpecificCommsProts specified in ISO 17423:2018; see 8.1.

2) Identify ITS-SCPSs by means of an "Object Identifier" (OID) reference to a set of ITS-CPs based on the methodology for CSP_Protocol specified in ISO 17423:2018; see 9.1.

3) Identify ITS-SCPs by means of an "Object Identifier" (OID) reference to an ITS-SCPS and parameterization information, see 10.1.

7.2 Contexts

7.2.1 ITS-SCPs related to communications between ITS-SCUs

An example of an ITS-SCP for the links between ITS-SCUs of the same ITS-SU (see Figure 3) is presented in 10.2.1.

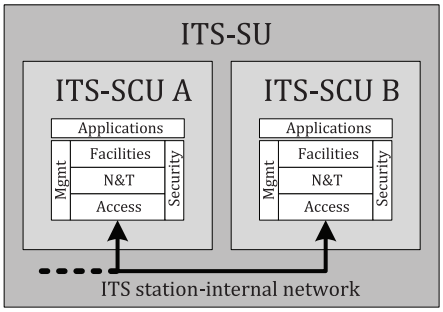

Figure 3 — Interconnection of ITS-SCUs in an ITS-SU

7.2.2 ITS-SCPs related communications between ITS-SUs

An example of an ITS-SCP for the link between ITS-SUs (see Figure 4) is presented in 10.2.3.