TECHNICAL SPECIFICATION

ISO/TS 21177

First edition
2019-08

Intelligent transport systems — ITS station security services for secure session establishment and authentication between trusted devices

Reference number
ISO/TS 21177:2019(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

This document is about ITS station security services required to ensure the authenticity of the source and confidentiality and integrity of application activities taking place between ***trusted devices***.

The trust relation between two devices is illustrated in Figure 1. Two devices cooperate in a trusted way, i.e. exchange information with optional explicit bi-directional protection.

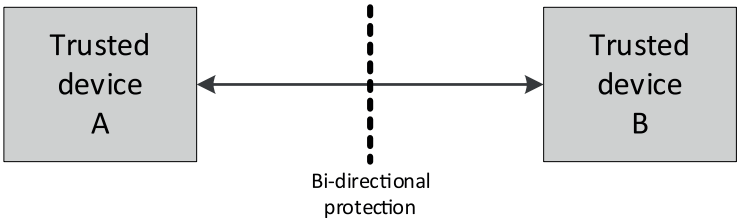

Figure 1 — Interconnection of trusted devices

According to ISO 21217, an ITS station unit (ITS-SU), i.e. the physical implementation of the ITS station (ITS-S) functionality, is a trusted device, and an ITS-SU may be composed of ITS station communication units (ITS-SCU) that are interconnected via an ITS station-internal network. Thus an ITS-SCU is the smallest physical entity of an ITS-SU that is referred to as a trusted device.

NOTE 1 ISO 21217 fully covers the functionality of EN 302 665[15], which is a predecessor of ISO 21217.

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[5] and ISO 17419. Station-internal management communications between ITS-SCUs of the same ITS-SU is specified in ISO 24102-4[7]. 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 can 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.

Four implementation contexts of communication nodes in ITS communications networks are identified in the ITS station and communication architecture ISO 21217, each comprised of ITS-station units (ITS-SU) taking on a particular role; personal, vehicular, roadside, or central. These ITS-SUs are ITS-secured communication nodes as required in ISO 21217 that participate in a wide variety of ITS services related to, e.g. sustainability, road safety and transportation efficiency.

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 (IVN) and from Infrastructure/Roadside Networks (IRN), some of which require secure local access to time-critical information; see Figures 2 and 3.

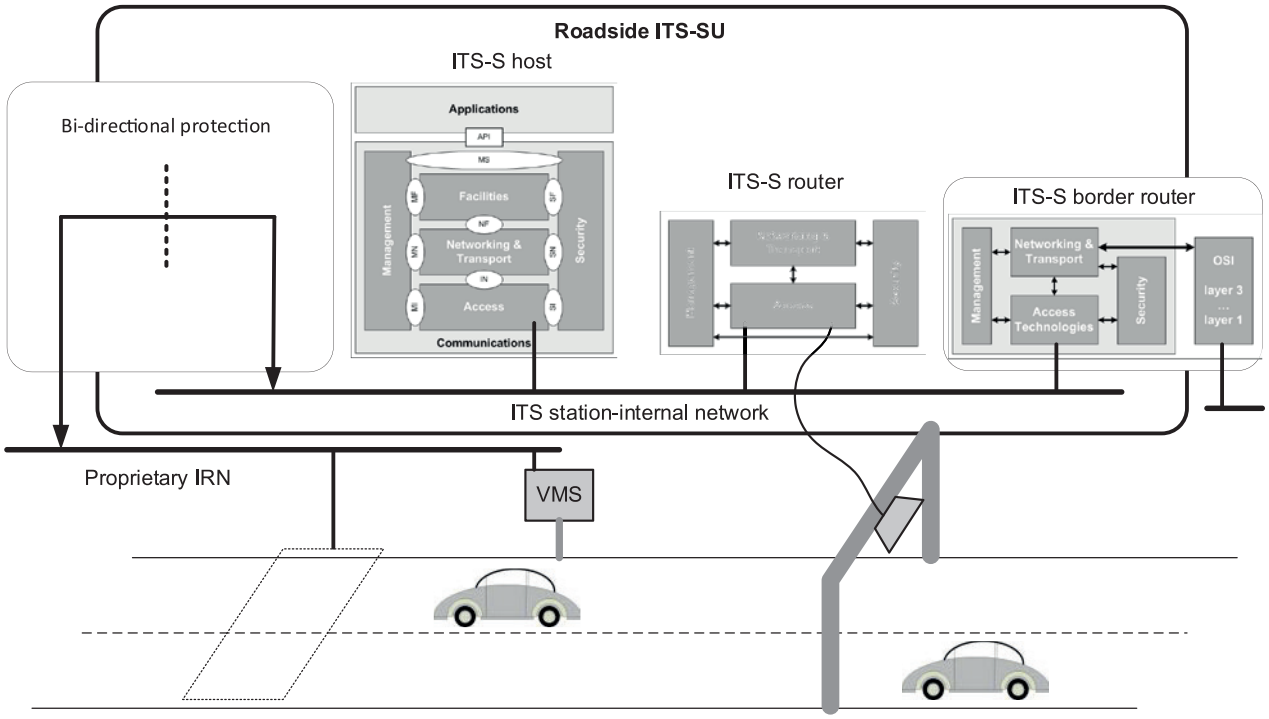

Figure 2 — Example of a roadside ITS-SU connected with proprietary IRN

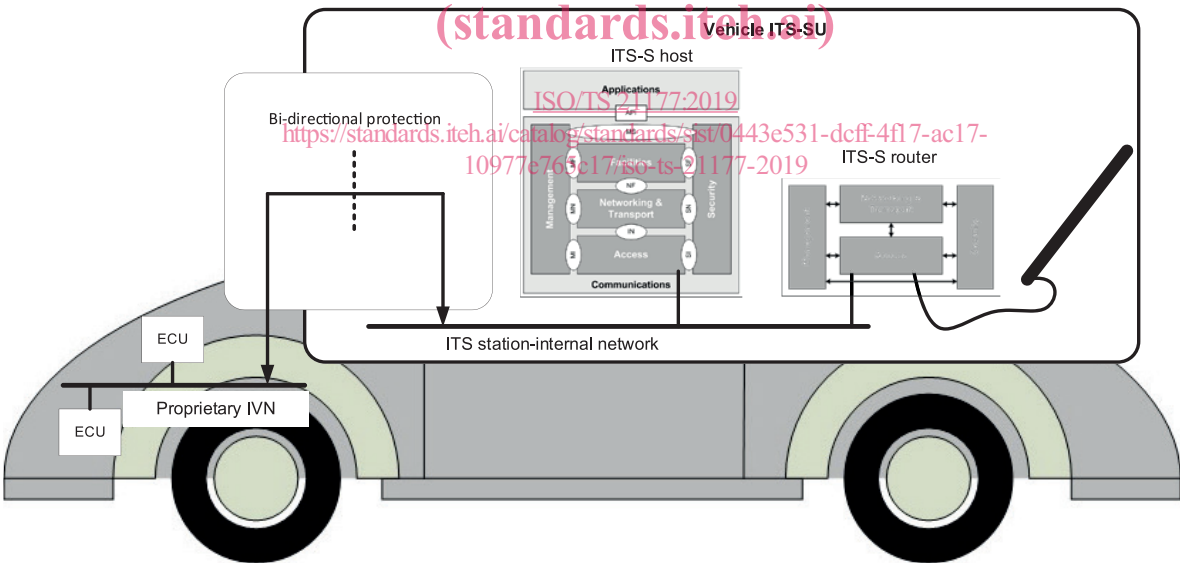

Figure 3 — Example of a vehicle ITS-SU connected with proprietary IRN

Trust in the ITS domain primarily is between ITS Station Communication Units (ITS-SCUs) introduced in ISO 21217; see Figure 4.

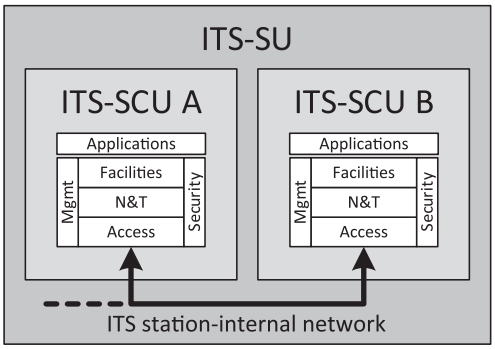

Figure 4 — Interconnection of ITS-SCUs in an ITS-SU

ITS-SCUs are interconnected via an ITS station-internal network. Applying basic security means specified in this document, the ITS-SCUs trust each other. Additionally, protocol data units exchanged between ITS-SCUs may be further protected by additional means, e.g. applying encryption. Major application domains of secure communications between ITS-SCUs of the same ITS-SU are local station management specified in ISO 24102-1[4] using station-internal management communications specified in ISO 24102-4[7].

Trust in the ITS domain further is between ITS-SUs introduced in ISO 21217; see Figure 5.

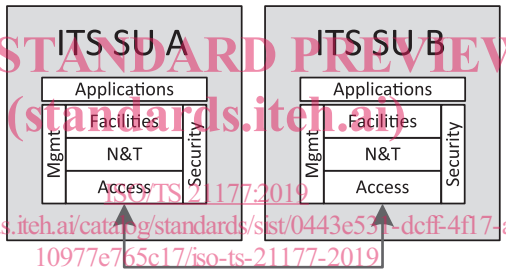

Figure 5 — Interconnection of ITS-SUs

Applying basic security means specified in this document, the ITS-SUs can establish secure application sessions. Establishment of sessions either needs a-priori knowledge about a session partner or can be achieved by means of service announcement specified in ISO 22418[3]. Further on, broadcast of messages is secured by means of authenticating the sender of such a message, applicable for the service advertisement message (SAM) specified in ISO/TS 16460[1] and used in ISO 22418[3]. Additionally, other security means may be applied, e.g. encryption of messages.

A further trust relation in the ITS domain is between an ITS-SU consisting of one or several ITS-SCUs and a sensor and control network (SCN). Trust is achieved by applying security means in an interface as illustrated in Figure 6 with details specified in this document.

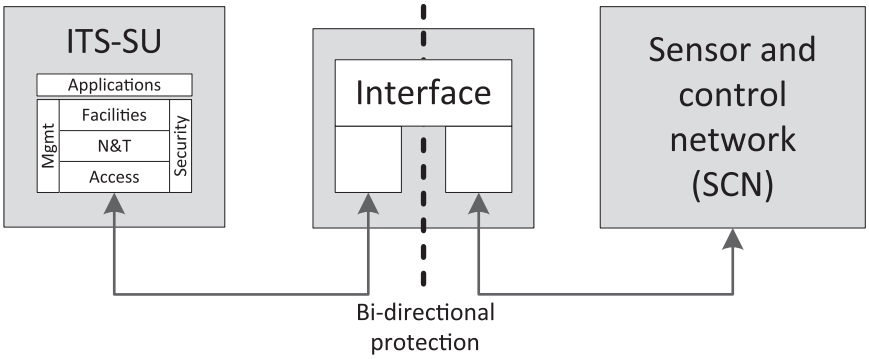

Figure 6 — Interface between ITS-SU and sensor and control network

The interface presented in Figure 6 may be a stand-alone device, or may be integrated in the ITS-SU, or may be part of the SCN. Examples of SCNs are "In-Vehicle Networks" (IVN) and "Infrastructure/ Roadside Networks" (IRN).

Related use cases of these ITS services have largely been derived from regulatory requirements and ITS 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;

— protection of private data, e.g. in compliance with the European "General Data Protection Regulation" (GDPR)[16];

— 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 PT 1705 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[17]. 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. All ITS-SUs need being capable of secure software updates.

According to ISO 21217, an ITS-SCU of an ITS-SU can communicate with devices that, in a strict sense, are not compliant with the architecture specified in ISO 21217. However, in order to have trusted communications, a certain minimum level of security measures must be shared between an ITS-SCU and such an external device. Examples of such external devices are a node in the Internet, or a node in a sensor and control network. In this document, the assumption is made that ITS-S application processes operating on ITS-SUs are issued with *certificates* by a Certificate Authority (CA), and that the CA is a trusted third party in the sense that before issuing the certificate to the ITS-S application process, it ensures that the ITS-SU on which the ITS-S application process is resident meets the minimum security requirements for that application. This allows peer ITS-S application processes which observe that an ITS-S application process possesses a valid certificate to have a level of assurance that the ITS-S application process is in fact secure and trustworthy.

The subject of this document thus is three-fold:

1) Specify ITS station security services for enabling trust between ITS-S application processes running on different ITS-SCUs of the same ITS-SU, i.e. establishing a trusted processing platform, considering also trust inside an ITS-SCU:

   — protection of applications from the actions of other applications;

   — protection of shared information;

   — protection of shared processing resources such as communications software and hardware, which includes methods of prioritisation and restricted access.

2) Specify ITS station security services for enabling trust between ITS-S application processes running on the same ITS-SU.

3) Extend these ITS security services for enabling trust between an ITS-SCU and devices being part of a sensor and control network.

NOTE 3 It is intended to extend the subject of this document in future editions.

Such security services include e.g. the basic security features of:

a) authentication and authorisation;

b) confidentiality and privacy;

c) data integrity;

d) non-repudiation.

Tasks related to communications are:

a) establishing secure sessions for bi-directional communications, e.g. based on service advertisement specified in ISO 22418[3];

b) authenticating a sender of broadcast messages, e.g. CAM, DENM, BSM, SPaT, MAP, FSAM, WSA;

c) encrypting messages.

NOTE 4 Tasks b) and c) above related to communications are already specified in other standards, see e.g. IEEE Std. 1609.2™ and several related standards from ETSI TC ITS.

Intelligent transport systems — ITS station security services for secure session establishment and authentication between trusted devices

1 Scope

This document contains specifications for a set of ITS station security services required to ensure the authenticity of the source and integrity of information exchanged between trusted entities:

— devices operated as bounded secured managed entities, i.e. "ITS Station Communication Units" (ITS-SCU) and "ITS station units" (ITS-SU) specified in ISO 21217, and

— between ITS-SUs (composed of one or several ITS-SCUs) and external trusted entities such as sensor and control networks.

These services include authentication and secure session establishment which are required to exchange information in a trusted and secure manner.

These services are essential for many ITS applications and services including time-critical safety applications, automated driving, remote management of ITS stations (ISO 24102-2[5]), and roadside/infrastructure related services.

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

IEEE Std 1609.2™, *IEEE Standard for Wireless Access in Vehicular Environments — Security Services for Applications and Management Messages*

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
Access Control PDU
PDU generated by the Security Subsystem for purposes of establishing the authorisation status of a peer ITS-S application process

3.2
Access Control Policy
data source governing what access to resources is permissible by peer Applications

3.3
application
functional entity, i.e. an ITS-S application process

3.4
security subsystem
functional entity providing security functionality for use by an ITS-S application process

3.5
Security Adaptor Layer
functional entity providing multiplexing and demultiplexing functionality for data and session control commands

3.6
Secure Session
functional entity providing confidentiality, integrity, authentication, guaranteed in-order delivery, and replay protection on the datagrams that are passed over it

3.7
resources
functional entity constituting endpoints of ITS-S application process activity

3.8
Cryptomaterial Handle
reference to Cryptomaterial allowing that Cryptomaterial to be used in cryptographic operations, i.e. sign, verify, encrypt, decrypt

3.9
Cryptomaterial
cryptographic keys and associated material, either a secret key for a symmetric algorithm, or a private key for an asymmetric algorithm, and the associated public key or certificate

3.10
Secure Session Service
functional entity responsible for establishing secure communications sessions with its peer instances

4 Symbols and abbreviated terms

ACK	acknowledge
ALPDU	adaptor layer PDU
APDU	application protocol data unit
DTLS	datagram TLS
ID	identifier
IRN	infrastructure/roadside network
ITS	intelligent transport systems
ITS-S	ITS station [SOURCE: ISO 21217:2014]
ITS-SCP	ITS station communication profile Note to entry: From ISO 21217

ITS-SU	ITS station unit [SOURCE: ISO 21217:2014]
IVN	in-vehicle network
OSI	open system interconnection
OTP	one time password
PDU	protocol data unit
PDU	protocol data unit
PSID	provider service identifier
SAM	service advertisement message [SOURCE: ISO/TS 16460]
SCN	sensor and control network
SDEE	secure data exchange entity
SPAKE2	secure password authenticated key exchange 2
SRM	service response message [SOURCE: ISO/TS 16460]
SSP	service specific permission
SSTD	secure session between trusted devices
TLS	transport layer security

5 Overview

5.1 Goals

Clause 5 presents the logical architecture followed in this document. The logical architecture is designed to accomplish the following goals:

— Two peer ITS-S application processes can communicate securely, i.e. in an authorized, integrity protected and confidential manner.

— The ITS-S application processes can authenticate to each other using role- or attribute-based access control.

— Each individual incoming application protocol data unit (APDU) can be subject to individual access control processes.

— The security state of the connection (i.e. the authentication status of one ITS-S application process with respect to access to the other connection) can be updated within the secure session as follows.

— An ITS-S application process can prove to the other that it knows a shared secret (Enhanced Authentication, see 7.3) — the intended use of this is to allow the owner or other legitimate operator of one ITS-S application process to permit access by a specific peer ITS-S application process, see Clause 6 for further discussion.