SLOVENSKI STANDARD
SIST-TS CEN ISO/TS 21177:2019

01-december-2019

Inteligentni transportni sistemi - Storitve varovanja postaj ITS za varno vzpostavitev sej in preverjanje pristnosti med zaupanja vrednimi napravami (ISO/TS 21177:2019)

Intelligent transport systems - ITS station security services for secure session establishment and authentication between trusted devices (ISO/TS 21177:2019)

Intelligente Verkehrssysteme - Sicherheitsdienste für eine ITS-Station zum sicheren Aufbau und Authentizierung einer Sitzung zwischen zuverlässigen Geräten (ISO/TS 21177:2019)

Systèmes intelligents de transport - Interface véhicule sécurisée - Services de sécurité de la station ITS pour l'établissement et l'authentification des sessions sécurisées (ISO/TS 21177:2019)

Ta slovenski standard je istoveten z: **CEN ISO/TS 21177:2019**

ICS:

03.220.01	Transport na splošno	Transport in general
35.030	Informacijska varnost	IT Security
35.240.60	Uporabniške rešitve IT v prometu	IT applications in transport

SIST-TS CEN ISO/TS 21177:2019 **en,fr,de**

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN ISO/TS 21177

October 2019

ICS 03.220.01; 35.030; 35.240.60

English Version

Intelligent transport systems - ITS station security services for secure session establishment and authentication between trusted devices (ISO/TS 21177:2019)

Systèmes intelligents de transport - Interface véhicule sécurisée - Services de sécurité de la station ITS pour l'établissement et l'authentification des sessions sécurisées (ISO/TS 21177:2019)

Intelligente Verkehrssysteme - Sicherheitsdienste für eine ITS-Station zum sicheren Aufbau und Authentizierung einer Sitzung zwischen zuverlässigen Geräten (ISO/TS 21177:2019)

This Technical Specification (CEN/TS) was approved by CEN on 13 August 2019 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Contents

Page

European foreword

This document (CEN ISO/TS 21177:2019) has been prepared by Technical Committee ISO/TC 204 "Intelligent transport systems" in collaboration with Technical Committee CEN/TC 278 “Intelligent transport systems” the secretariat of which is held by NEN.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO/TS 21177:2019 has been approved by CEN as CEN ISO/TS 21177:2019 without any modification.

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

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.

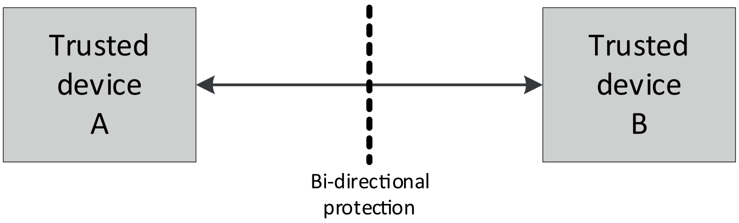

Figure 1 — Interconnection of trusted devices

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.

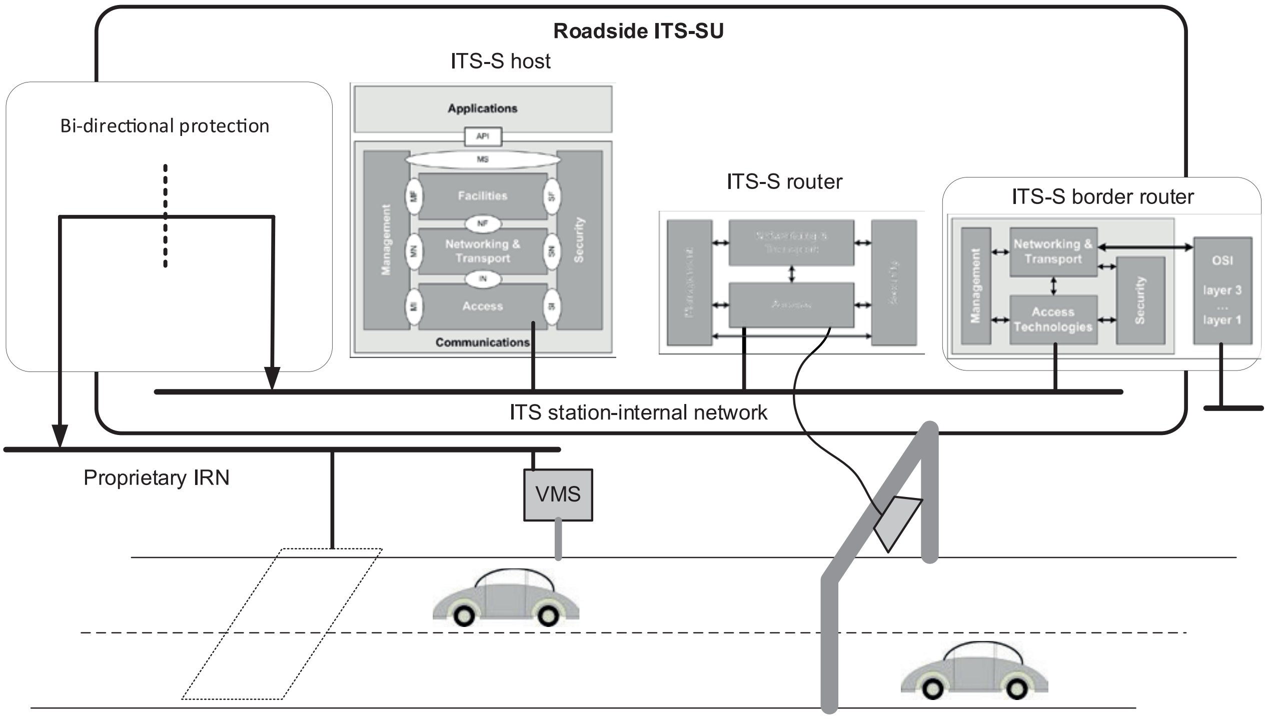

Figure 2 — Example of a roadside ITS-SU connected with proprietary IRN

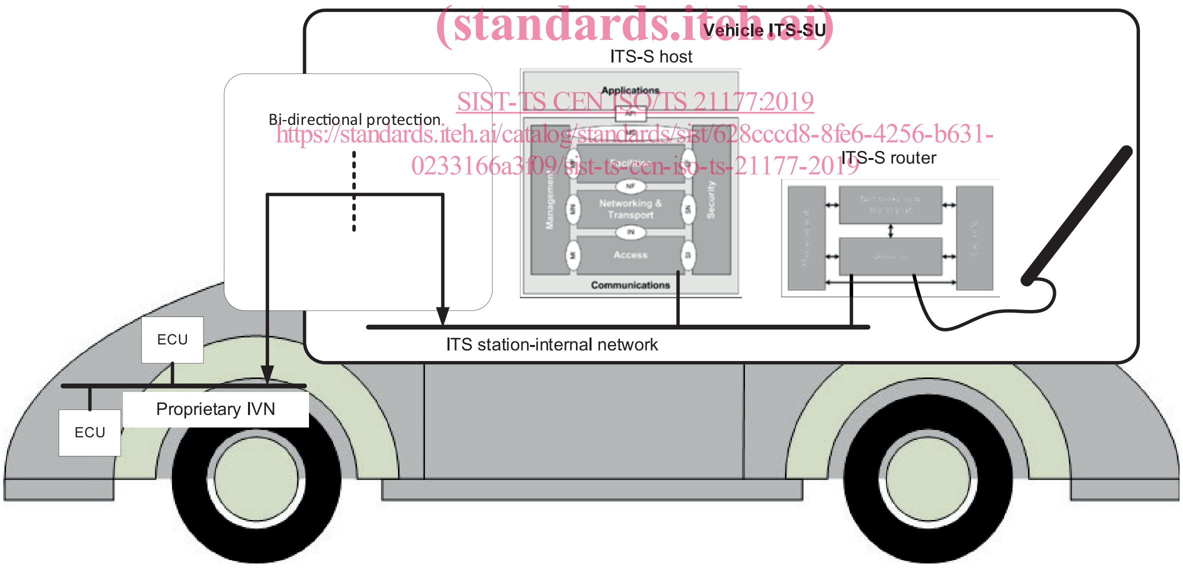

Figure 3 — Example of a vehicle ITS-SU connected with proprietary IRN

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

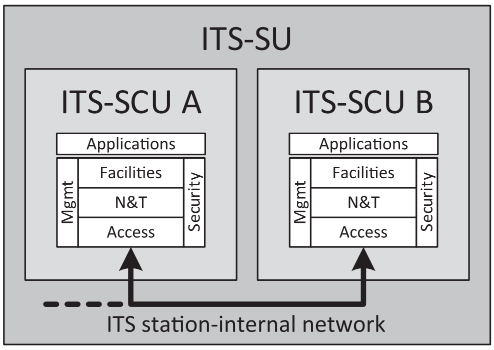

Figure 4 — Interconnection of ITS-SCUs in an ITS-SU

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.

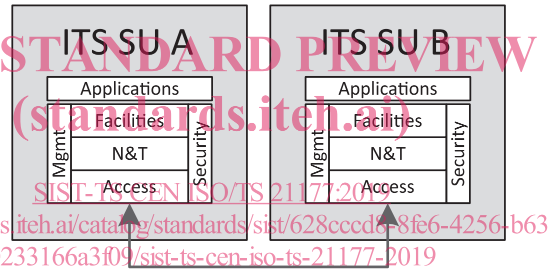

Figure 5 — Interconnection of ITS-SUs

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.