SLOVENSKI STANDARD
oSIST prEN ISO 21177:2022

01-junij-2022

Inteligentni transportni sistemi - Storitve varovanja postaj ITS za varno vzpostavitev sej in preverjanje pristnosti med zaupanja vrednimi napravami (ISO/DIS 21177:2022)

Intelligent transport systems - ITS station security services for secure session establishment and authentication between trusted devices (ISO/DIS 21177:2022)

Intelligente Verkehrssysteme - Sicherheitsdienste für eine ITS-Station zum sicheren Aufbau von Sitzungen und zur Authentisierung zwischen vertrauenswürdigen Geräten (ISO/DIS 21177:2022)

Systèmes de transport intelligents - Services de sécurité de la station ITS pour l'établissement et l'authentification des sessions sécurisées (ISO/DIS 21177:2022)

Ta slovenski standard je istoveten z: **prEN ISO 21177**

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

oSIST prEN ISO 21177:2022 **en,fr,de**

DRAFT INTERNATIONAL STANDARD

ISO/DIS 21177

ISO/TC **204**

Secretariat: **ANSI**

Voting begins on:
2022-04-11

Voting terminates on:
2022-07-04

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

ICS: 35.030; 03.220.01; 35.240.60

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

Reference number
ISO/DIS 21177:2022(E)

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

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.

This second edition cancels and replaces the first edition (ISO/TS 21177:2019), which has been editorially and slightly technically improved.

The main changes are as follows:

— implement change proposals presented in ISO/TR 21186-3:2021 including:

  — add CRL request functionality;
  — add session extension functionality;
— editorial improvements to improve readability and clarity including
  — revised Figure 7; renumbered to Figure 8
  — new Figure 7 inserted.

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

The document specifies ITS station security services that provide authenticity of the source and confidentiality and integrity of application activities taking place between trusted devices. The two devices taking part in a data exchange establish a cryptographically secure session; as part of establishing this session, each device (or, more precisely, each end entity (EE), which is an application on the device) is sent one or more digital certificates that are cryptographically bound to the other EE and contain statements, made by a trusted third party, about the EE's capabilities, properties, and permissions. This allows each EE to have assurance about the properties of the other EE in the session, and this in turn allows each EE to make trust and access control decisions about data that the other EE can access, commands that the other EE can execute, state that the other EE can change, and other types of access that the other EE can request. In other words, the two EEs establish a trust relationship where each EE is trusted by the other EE to carry out specific actions, without requiring one EE to allow the other EE to have arbitrary access.

The mechanisms specified in this document allow each EE to establish trusted facts about the other EE. For these mechanisms to be used, the EE specification must include an access control policy, indicating what properties must be known to be true about the other EE for that other EE to be allowed to carry out particular actions. In other words, this document provides a means to obtain security-relevant information, but the use of that security-relevant information is to be specified in the specification of the EE.

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.

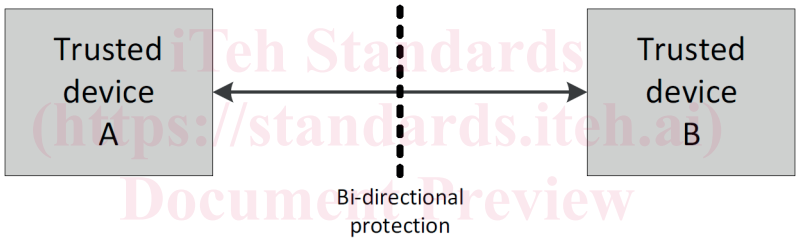

Figure 1 — Interconnection of trusted devices

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,[16] 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[6] and ISO 17419. Station-internal management communications between ITS-SCUs of the same ITS-SU is specified in ISO 24102-4.[8] 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.

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. See also Figure 2, Figure 3, Figure 4 and Figure 5.

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 Figure 2 and Figure 3.

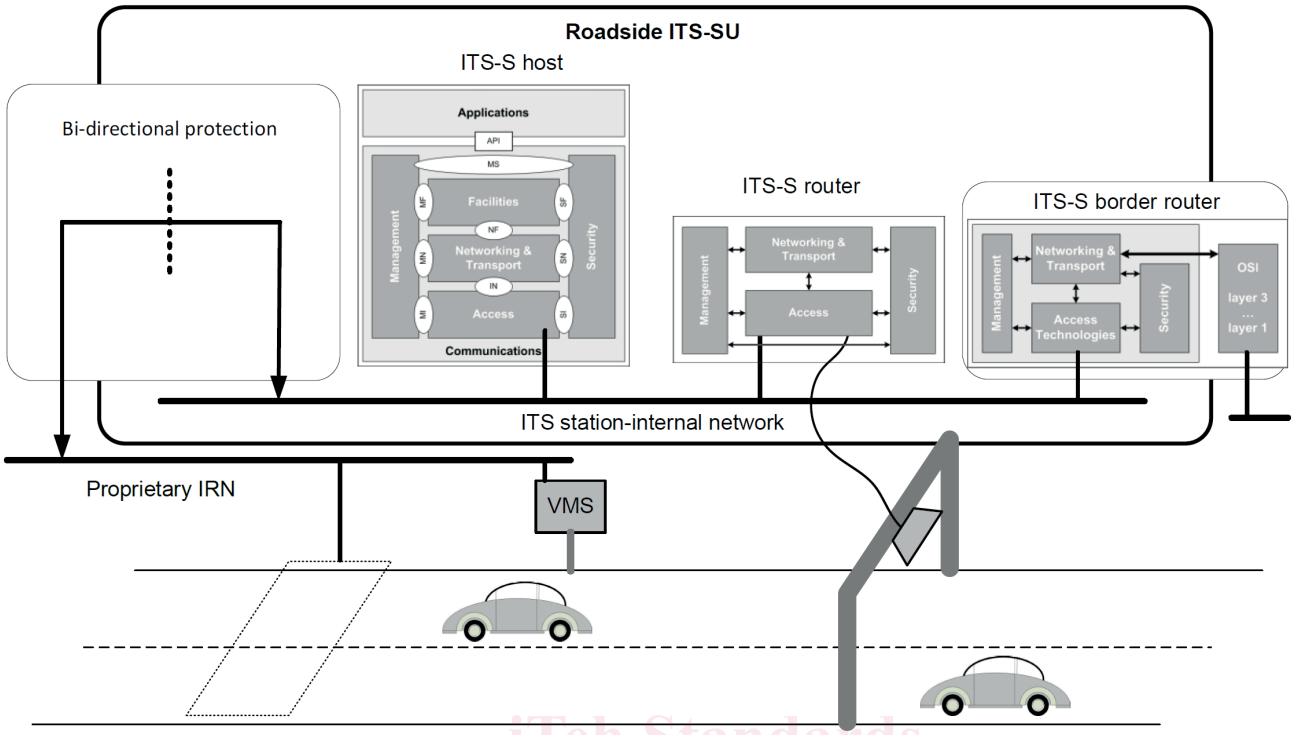

Figure 2 — Example of a roadside ITS-SU connected with proprietary IRN

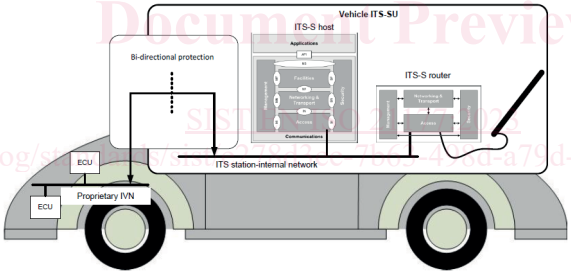

Figure 3 — Example of a vehicle ITS-SU connected with proprietary IVN

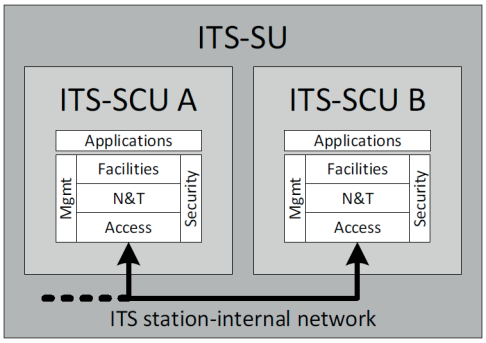

Figure 4 — Interconnection of ITS-SCUs in an ITS-SU

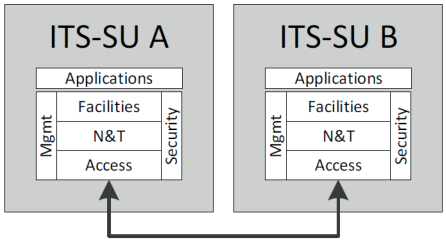

Figure 5 — Interconnection of ITS-SUs

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.[4] 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 16460[1] and used in ISO 22418.[4] 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.

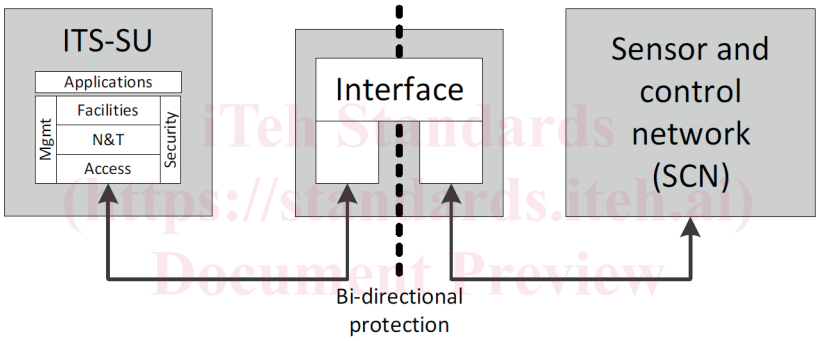

Figure 6 — Interface between ITS-SU and sensor and control network

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, .eg., collision avoidance, emergency electronic brake light and event determination;

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

— protection of private data, .eg., in compliance with the European "General Data Protection Regulation" (GDPR)[18];

— local access to certified real-time data for sustainability applications, .eg., dynamic emission zones (controlled zones as currently standardized in CEN TC278 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.[18] 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.

Such security services include .eg., 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, .eg., 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 3 Tasks b) and c) above related to communications are already specified in other standards, see .eg., IEEE Std. 1609.2™ and several related standards from ETSI TC ITS.

Identification of patent holders: the following text shall be included if patent rights have been identified.

The International Organization for Standardization (ISO) draws attention to the fact that it is claimed that compliance with this document may involve the use of a patent.

ISO takes no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured ISO that he/she is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with ISO. Information may be obtained from the patent database available at www.iso.org/patents.

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