FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/FDIS
21177**

ISO/TC **204**

Secretariat: **ANSI**

Voting begins on:
2023-11-13

Voting terminates on:
2024-02-05

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

Systèmes de transport intelligents — Services de sécurité des stations ITS pour l'établissement et l'authentification des sessions sécurisées entre dispositifs de confiance

ISO/CEN PARALLEL PROCESSING

Reference number
ISO/FDIS 21177:2023(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 document 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/TC 278, *Intelligent transport systems,* in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This second edition cancels and replaces the first edition (ISO 21177:2023), of which it constitutes a minor revision. The changes are as follows:

— cross-references to RFC 8942 have been updated to RFC 8902 throughout the document;

— information concerning patent(s) required for the implementation of this document has been moved from the Introduction to the Foreword.

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 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, states 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 needs to include an access control policy, indicating which properties are required to 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.

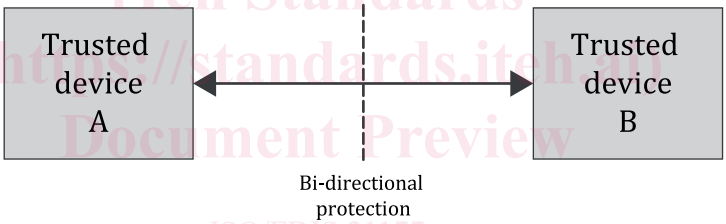


Figure 1 — Interconnection of trusted devices

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-SCUs) 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.

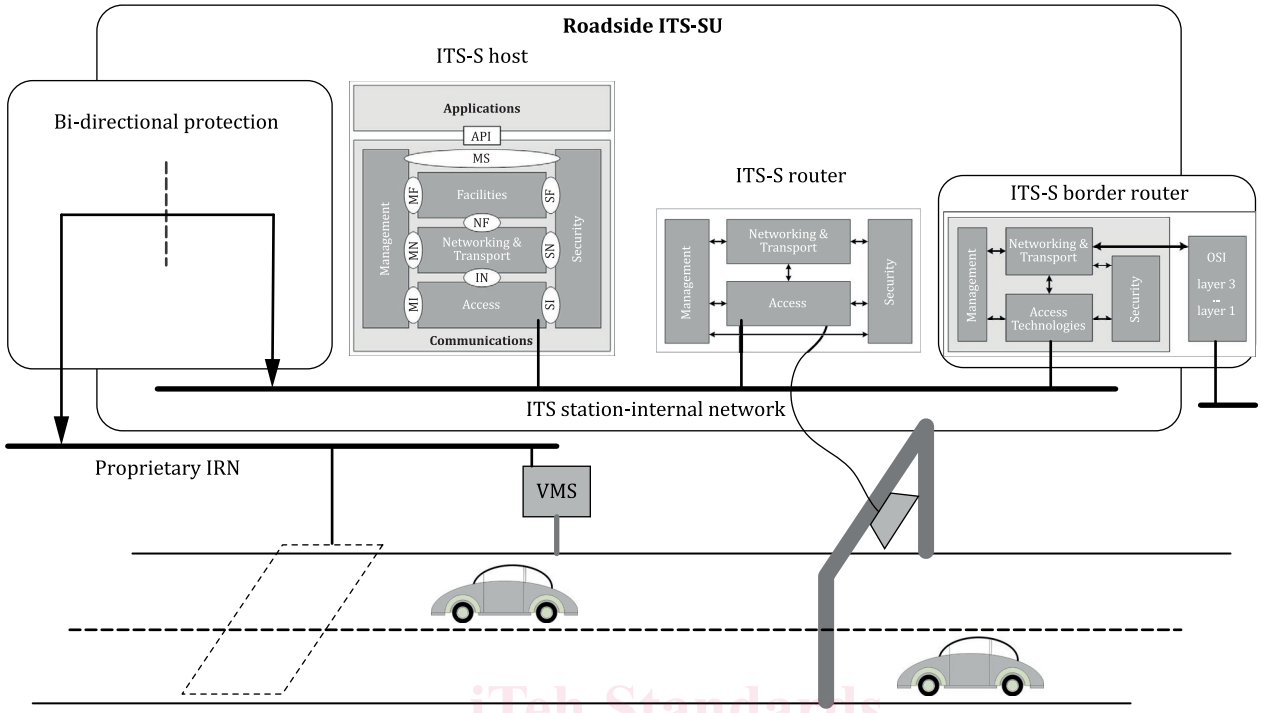
NOTE 1 ISO 21217 fully covers the functionality of EN 302 665,[16] which is a predecessor of ISO 21217.

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 and ISO 17419. Station-internal management communications between ITS-SCUs of the same ITS-SU are specified in ISO 24102-4. The 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 of ISO 21217, each comprised of ITS-SUs 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, for example, 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), for example, from in-vehicle networks (IVN) and from infrastructure/roadside

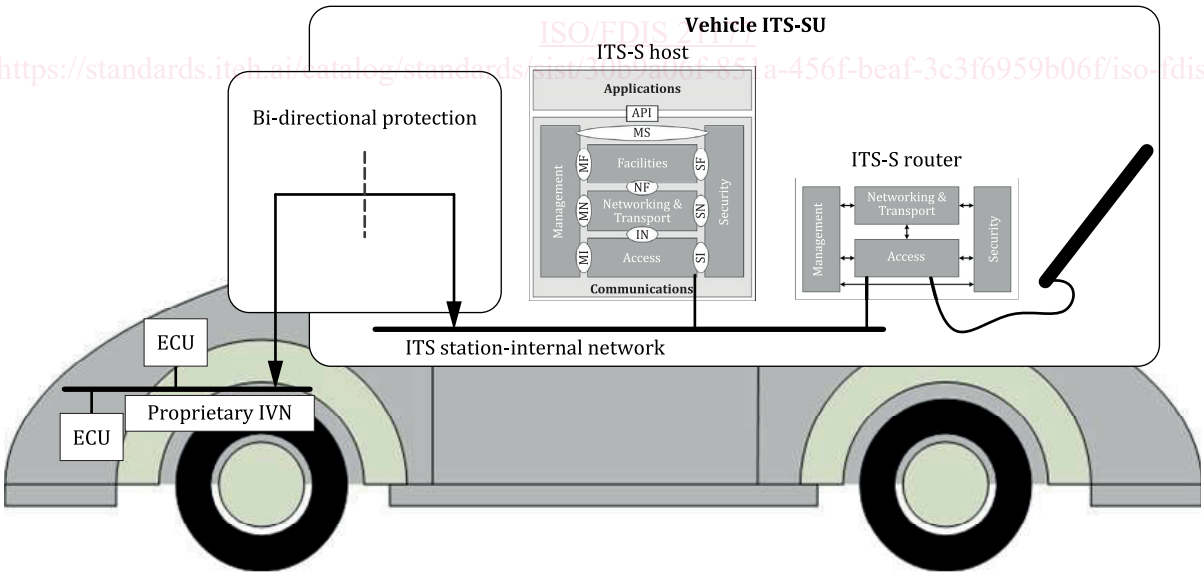
networks (IRN), some of which require secure local access to time-critical information; see Figure 2 and Figure 3.



Key

VMS variable message sign

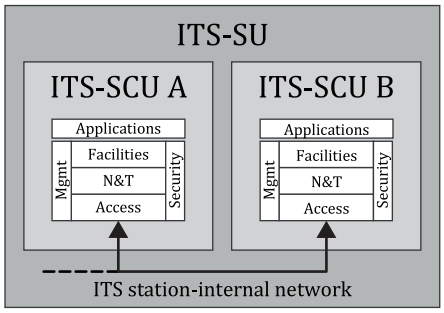
Figure 2 — Example of a roadside ITS-SU connected with proprietary IRN



Key

ECU electronic control unit

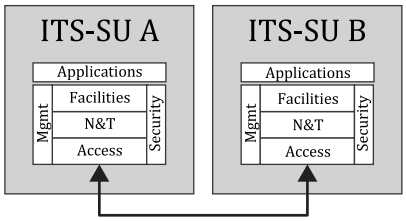
Figure 3 — Example of a vehicle ITS-SU connected with proprietary IVN



Key

N&T Networking & Transport

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



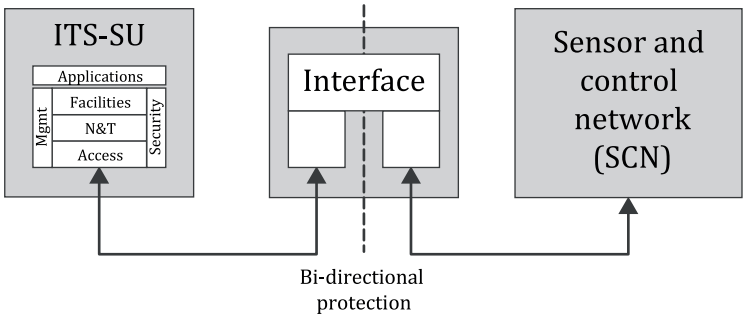
Key

N&T Networking & Transport

Figure 5 — Interconnection of ITS-SUs

By applying basic security means specified in this document, the ITS-SUs can establish secure application sessions. Establishment of sessions either requires prior knowledge about a session partner or can be achieved by means of a service announcement as specified in ISO 22418. Further on, the broadcasting 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 and used in ISO 22418. 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.



Key

N&T Networking & Transport

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 and dynamic priorities;

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

— local access to certified real-time data for sustainability applications, e.g. dynamic emission zones (controlled zones as currently standardized by CEN/TC 278), intersection priorities based on emissions, and 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 this number will grow (see the US National ITS Reference Architecture,[19] for example). It is critical that ultimately all ITS-SUs in a given area be 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 to be 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 need to 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) Specification of 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 prioritization and restricted access.

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

3) Extension of 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, for example, the basic security features of:

a) authentication and authorization;

b) confidentiality and privacy;

c) data integrity;

d) non-repudiation.

Tasks related to communications are:

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

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

g) encrypting messages.

NOTE 3 Tasks f) and g) above related to communications are already specified in other standards: see IEEE 1609.2 and several related standards from ETSI, for example.

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, i.e.:

— between devices operated as bounded secured managed entities, i.e. "ITS Station Communication Units" (ITS-SCU) and "ITS station units" (ITS-SU) as 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 the authentication and secure session establishment which are required to exchange information in a trusted and secure manner.

These services are essential for many intelligent transport system (ITS) applications and services, including time-critical safety applications, automated driving, remote management of ITS stations (ISO 24102-2), 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.

ETSI TS 102 941, *Intelligent Transport Systems (ITS); Security; Trust and privacy management*

ETSI TS 103 097, *Intelligent Transport Systems (ITS); Security; Security header and certificate formats*

IEEE 1609.2, *including Amendment 1, IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages*

IEEE 1003.1:2017, *IEEE Standard for Information Technology--Portable Operating System Interface (POSIX(R)) Base Specifications, Issue 7*

3 Terms and definitions

For the purposes of this document, the following terms and definitions 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 https://www.electropedia.org/

3.1
access control PDU
protocol data unit (PDU) generated by the security subsystem for purposes of establishing the authorization 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

Note 1 to entry: The natural language term "application" is used in this document as a synonym to the term "ITS-S application process" specified in ISO 21217.

3.4
cryptomaterial
cryptographic keys and associated material

Note 1 to entry: Cryptomaterial refers to either a secret key for a symmetric algorithm, or a private key for an asymmetric algorithm and the associated public key or certificate.

3.5
cryptomaterial handle
reference to cryptomaterial allowing that cryptomaterial to be used in cryptographic operations (sign, verify, encrypt, decrypt)

3.6
handshake ITS-AID
ITS application identifier (ITS-AID) that appeared in the SignedData HeaderInfo in the signed transport layer security (TLS) messages within the TLS handshake that started a secure session

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

3.8
security subsystem
functional entity providing security functionality for use by an ITS-S application process

3.9
security adaptor layer
functional entity providing multiplexing and demultiplexing functionality for data and session control commands

3.10
secure session service
functional entity providing confidentiality, integrity, authentication, guaranteed in-order delivery and replay protection on the datagrams that are passed over it

4 Abbreviated terms

ACK	acknowledge
ALPDU	adaptor layer protocol data unit
APDU	application protocol data unit
ASD	aftermarket safety device
ASN.1	abstract syntax notation 1
BSM	basic safety message