INTERNATIONAL STANDARD

ISO 21177:~~2022~~2023(E)

ISO TC 204/WG 18

Date: ~~2022-06-17~~2023-02

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

Style Definition: List Bullet: Indent: Left: 0 cm, Hanging: 0.63 cm, No bullets or numbering, Tab stops: 0.63 cm, List tab

Style Definition: List Bullet 3: Indent: Left: 1 cm, Hanging: 0.63 cm, No bullets or numbering, Tab stops: 1.63 cm, List tab

Style Definition: List Bullet 4: Indent: Left: 1.5 cm, Hanging: 0.63 cm, No bullets or numbering, Tab stops: 2.13 cm, List tab

Style Definition: List Bullet 5: Indent: Left: 2 cm, Hanging: 0.63 cm, No bullets or numbering, Tab stops: 2.63 cm, List tab

Style Definition: List Number 5: Indent: Left: 2 cm, Hanging: 0.63 cm, No bullets or numbering, Tab stops: 2.63 cm, List tab

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted

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*, 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 first edition cancels and replaces the first edition (ISO/TS 21177:2019), which has been technically revised.

The main changes are as follows:

— change proposals presented in ISO/TR 21186-3:2021 have been incorporated, including:

  — CRL request functionality added;

  — session extension functionality added;

— editorial improvements to improve readability and clarity have been made, including:

  — revision of Figure 7, renumbered to Figure 8;

  — insertion of new Figure 7.

Formatted: English (United Kingdom)
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: Font: Not Italic, English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: Font: Not Italic, English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: std_publisher, English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: std_documentType, English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: std_docNumber, English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: std_year, English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: Don't keep with next, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Font: Cambria, English (United Kingdom)
Formatted: Default Paragraph Font

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.

Formatted: English (United Kingdom)

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: English (United Kingdom)

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 mustneeds to include an access control policy, indicating whatwhich properties mustare 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.

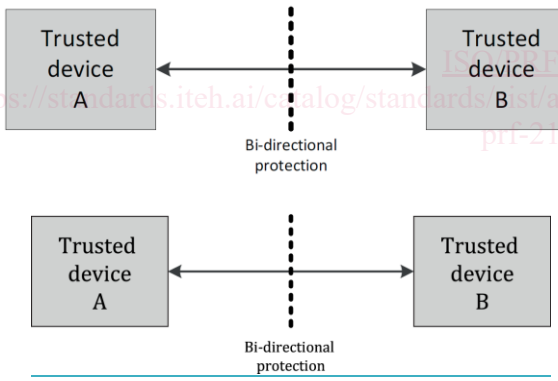


Figure 1— — Interconnection of trusted devices

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.

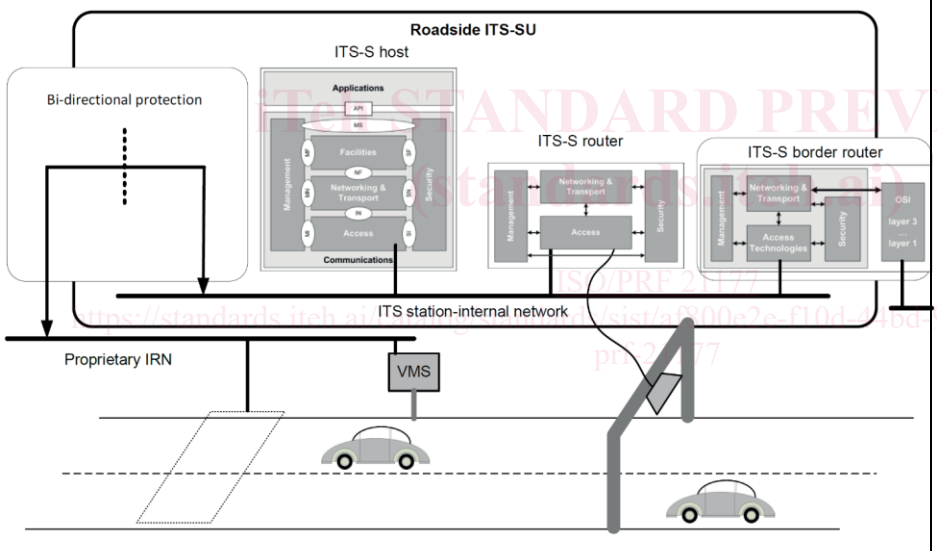
Formatted: std_docPartNumber

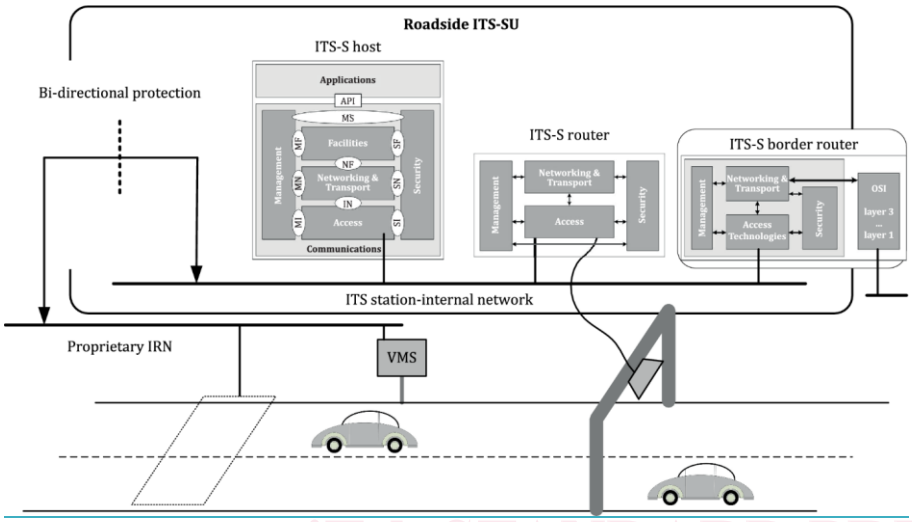
NOTE 2 An ITS-SU can be composed of ITS-SCUs from different vendors where each ITS-SCU is linked to a different ITS-SCU configuration and management centre specified in ISO 24102-2 and ISO 17419. Station-internal

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 ITSstations.

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 station units (ITS-SU) 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

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left

Formatted Table