



# SLOVENSKI STANDARD SIST EN ISO 21177:2023

01-julij-2023

Nadomešča:

SIST-TS CEN ISO/TS 21177:2019

---

**Inteligentni transportni sistemi - Storitve varovanja postaj ITS za varno vzpostavitev sej in preverjanje pristnosti med zaupanja vrednimi napravami (ISO 21177:2023)**

Intelligent transport systems - ITS station security services for secure session establishment and authentication between trusted devices (ISO 21177:2023)

Intelligente Verkehrssysteme - Sicherheitsdienste für eine ITS-Station zum sicheren Aufbau von Sitzungen und zur Authentisierung zwischen vertrauenswürdigen Geräten (ISO 21177:2023)

Systèmes de transport intelligents - Services de sécurité de la station ITS pour l'établissement et l'authentification des sessions sécurisées (ISO 21177:2023)

**Ta slovenski standard je istoveten z: EN ISO 21177:2023**

---

**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 EN ISO 21177:2023**

**en,fr,de**



EUROPEAN STANDARD

EN ISO 21177

NORME EUROPÉENNE

EUROPÄISCHE NORM

April 2023

ICS 03.220.01; 35.030; 35.240.60

Supersedes CEN ISO/TS 21177:2019

English Version

## Intelligent transport systems - ITS station security services for secure session establishment and authentication between trusted devices (ISO 21177:2023)

Systèmes de transport intelligents - Services de sécurité des stations ITS pour l'établissement et l'authentification des sessions sécurisées entre dispositifs de confiance (ISO 21177:2023)

Intelligente Verkehrssysteme - Sicherheitsdienste für eine ITS-Station zum sicheren Aufbau von Sitzungen und zur Authentisierung zwischen vertrauenswürdigen Geräten (ISO 21177:2023)

This European Standard was approved by CEN on 20 February 2023.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

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, Türkiye 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.....	3

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST EN ISO 21177:2023](https://standards.iteh.ai/catalog/standards/sist/e278d3ee-7b63-498d-a79d-0b224171d5d2/sist-en-iso-21177-2023)

<https://standards.iteh.ai/catalog/standards/sist/e278d3ee-7b63-498d-a79d-0b224171d5d2/sist-en-iso-21177-2023>

## European foreword

This document (EN ISO 21177:2023) 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.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by October 2023, and conflicting national standards shall be withdrawn at the latest by October 2023.

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 supersedes CEN ISO/TS 21177:2019.

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

Any feedback and questions on this document should be directed to the users' national standards body/national committee. A complete listing of these bodies can be found on the CEN website.

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, Türkiye and the United Kingdom.

[SIST EN ISO 21177:2023](https://standards.iteh.ai/catalog/standards/sist/e278d3ee-7b63-498d-a79d-0b224171e23)

[https://standards.iteh.ai/catalog/standards/sist/e278d3ee-7b63-498d-a79d-](https://standards.iteh.ai/catalog/standards/sist/e278d3ee-7b63-498d-a79d-0b224171e23)

[0b224171e23](https://standards.iteh.ai/catalog/standards/sist/e278d3ee-7b63-498d-a79d-0b224171e23) **Endorsement notice**

The text of ISO 21177:2023 has been approved by CEN as EN ISO 21177:2023 without any modification.



INTERNATIONAL  
STANDARD

ISO  
21177

First edition  
2023-04

---

---

**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*

iTeh STA (standards.iteh.ai)

SIST EN ISO 21177:2023

<https://standards.iteh.ai/catalog/standards/sist/e278d3ee-7b63-498d-a79d-0b224171d5d2/sist-en-iso-21177-2023>



Reference number  
ISO 21177:2023(E)

© ISO 2023

# iTeh STANDARD PREVIEW (standards.iteh.ai)

SIST EN ISO 21177:2023

<https://standards.iteh.ai/catalog/standards/sist/e278d3ee-7b63-498d-a79d-0b224171d5d2/sist-en-iso-21177-2023>



## **COPYRIGHT PROTECTED DOCUMENT**

© ISO 2023

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
CP 401 • Ch. de Blandonnet 8  
CH-1214 Vernier, Geneva  
Phone: +41 22 749 01 11  
Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland



# Contents

Page

<b>Foreword</b> .....	<b>vi</b>
<b>Introduction</b> .....	<b>vii</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Abbreviated terms</b> .....	<b>2</b>
<b>5 Overview</b> .....	<b>4</b>
5.1 General description, relationship to transport layer security (TLS) and relationship to application specifications.....	4
5.2 Goals.....	5
5.3 Architecture and functional entities.....	5
5.4 Cryptomaterial handles.....	10
5.5 Session IDs and state.....	10
5.6 Access control and authorization state.....	11
5.7 Application level non-repudiation.....	11
5.8 Service primitive conventions.....	11
<b>6 Process flows and sequence diagrams</b> .....	<b>12</b>
6.1 General.....	12
6.2 Overview of process flows.....	12
6.3 Sequence diagram conventions.....	13
6.4 Configure.....	14
6.5 Start session.....	15
6.6 Send data.....	18
6.7 Send access control PDU.....	21
6.8 Receive PDU.....	22
6.9 Extend session.....	27
6.9.1 Goals.....	27
6.9.2 Processing.....	28
6.10 Secure connection brokering.....	28
6.10.1 Goals.....	28
6.10.2 Prerequisites.....	28
6.10.3 Overview.....	29
6.10.4 Detailed specification.....	30
6.11 Force end session.....	38
6.12 Session terminated at session layer.....	40
6.13 Deactivate.....	40
6.14 Secure session example.....	41
<b>7 Security subsystem: interfaces and data types</b> .....	<b>43</b>
7.1 General.....	43
7.2 Access control policy and state.....	44
7.3 Enhanced authentication.....	45
7.3.1 Definition and possible states.....	45
7.3.2 States for owner role enhanced authentication.....	45
7.3.3 State for accessor role enhanced authentication.....	47
7.3.4 Use by access control.....	47
7.3.5 Methods for providing enhanced authentication.....	47
7.3.6 Enhanced authentication using SPAKE2.....	47
7.4 Extended authentication.....	48
7.5 Security Management Information Request.....	49
7.5.1 Rationale.....	49
7.5.2 General.....	50
7.6 Data types.....	51

## ISO 21177:2023(E)

7.6.1	General	51
7.6.2	Imports	51
7.6.3	“Helper” data types	51
7.6.4	Iso21177AccessControlPdu	52
7.6.5	AccessControlResult	52
7.6.6	ExtendedAuthPdu	52
7.6.7	ExtendedAuthRequest	53
7.6.8	InnerExtendedAuthRequest	53
7.6.9	AtomicExtendedAuthRequest	53
7.6.10	ExtendedAuthResponse	54
7.6.11	ExtendedAuthResponsePayload	54
7.6.12	EnhancedAuthPdu	54
7.6.13	SpakeRequest	55
7.6.14	SpakeResponse	55
7.6.15	SpakeRequesterResponse	55
7.6.16	SecurityMgmtInfoPdu	55
7.6.17	SecurityMgmtInfoRequest	55
7.6.18	EtsiCrlRequest	56
7.6.19	CertChainRequest	56
7.6.20	SecurityMgmtInfoResponse	56
7.6.21	SecurityMgmtInfoErrorResponse	57
7.6.22	EtsiCrlResponse	57
7.6.23	EtsiCtlResponse	57
7.6.24	IeeeCrlResponse	57
7.6.25	CertChainResponse	58
7.6.26	SessionExtensionPdu	58
7.7	App-Sec Interface	60
7.7.1	App-Sec-Configure.request	60
7.7.2	App-Sec-Configure.confirm	61
7.7.3	App-Sec-StartSession.indication	61
7.7.4	App-Sec-Data.request	61
7.7.5	App-Sec-Data.confirm	62
7.7.6	App-Sec-Incoming.request	62
7.7.7	App-Sec-Incoming.confirm	63
7.7.8	App-Sec-EndSession.request	64
7.7.9	App-Sec-EndSession.indication	64
7.7.10	App-Sec-Deactivate.request	65
7.7.11	App-Sec-Deactivate.confirm	65
7.7.12	App-Sec-Deactivate.indication	65
7.8	Security subsystem internal interface	66
7.8.1	General	66
7.8.2	Sec-AuthState.request	66
7.8.3	Sec-AuthState.confirm	66
<b>8</b>	<b>Adaptor layer: interfaces and data types</b>	<b>67</b>
8.1	General	67
8.2	Data types	68
8.2.1	General	68
8.2.2	Iso21177AdaptorLayerPDU	68
8.2.3	Apdu	69
8.2.4	AccessControl	69
8.2.5	TlsClientMsg1	69
8.2.6	TlsServerMsg1	69
8.3	App-AL Interface	69
8.3.1	App-AL-Data.request	69
8.3.2	App-AL-Data.confirm	70
8.3.3	App-AL-Data.indication	70
8.3.4	App-AL-EnableProxy.request	71
8.4	Sec-AL Interface	73

8.4.1	Sec-AL-AccessControl.request	73
8.4.2	Sec-AL-AccessControl.confirm	73
8.4.3	Sec-AL-AccessControl.indication	73
8.4.4	Sec-AL-EndSession.request	74
8.4.5	Sec-AL-EndSession.confirm	74
<b>9</b>	<b>Secure session Services</b>	<b>74</b>
9.1	General	74
9.2	App-Sess interfaces	74
9.2.1	App-Sess-EnableProxy.request	74
9.3	Sec-Sess interface	75
9.3.1	Sec-Sess-Configure.request	75
9.3.2	Sec-Sess-Configure.confirm	77
9.3.3	Sec-Sess-Start.indication	77
9.3.4	Sec-Sess-EndSession.indication	78
9.3.5	Sec-Sess-Deactivate.request	78
9.3.6	Sec-Sess-Deactivate.confirm	79
9.4	AL-Sess interface	79
9.4.1	AL-Sess-Data.request	79
9.4.2	AL-Sess-Data.confirm	79
9.4.3	AL-Sess-Data.indication	80
9.4.4	AL-Sess-EndSession.request	80
9.4.5	AL-Sess-EndSession.confirm	80
9.4.6	AL-Sess-ClientHelloProxy.request	81
9.4.7	AL-Sess-ClientHelloProxy.indication	81
9.4.8	AL-Sess-ServerHelloProxy.request	82
9.4.9	AL-Sess-ServerHelloProxy.indication	82
9.5	Permitted mechanisms	83
9.5.1	TLS 1.3	83
9.5.2	DTLS 1.3	84
<b>Annex A</b>	<b>(informative) Usage scenarios</b>	<b>85</b>
<b>Annex B</b>	<b>(normative) ASN.1 module</b>	<b>93</b>
<b>Annex C</b>	<b>(normative) Session extension PDU functional type</b>	<b>94</b>
<b>Annex D</b>	<b>(normative) Owner authorization</b>	<b>95</b>
	<b>Bibliography</b>	<b>99</b>

## ISO 21177:2023(E)

## 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](http://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](http://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](http://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 of ISO 21177 cancels and replaces 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](#).

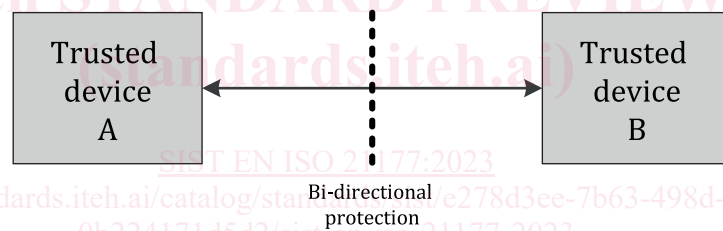
Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at [www.iso.org/members.html](http://www.iso.org/members.html).

## 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,<sup>[16]</sup> which is a predecessor of ISO 21217.

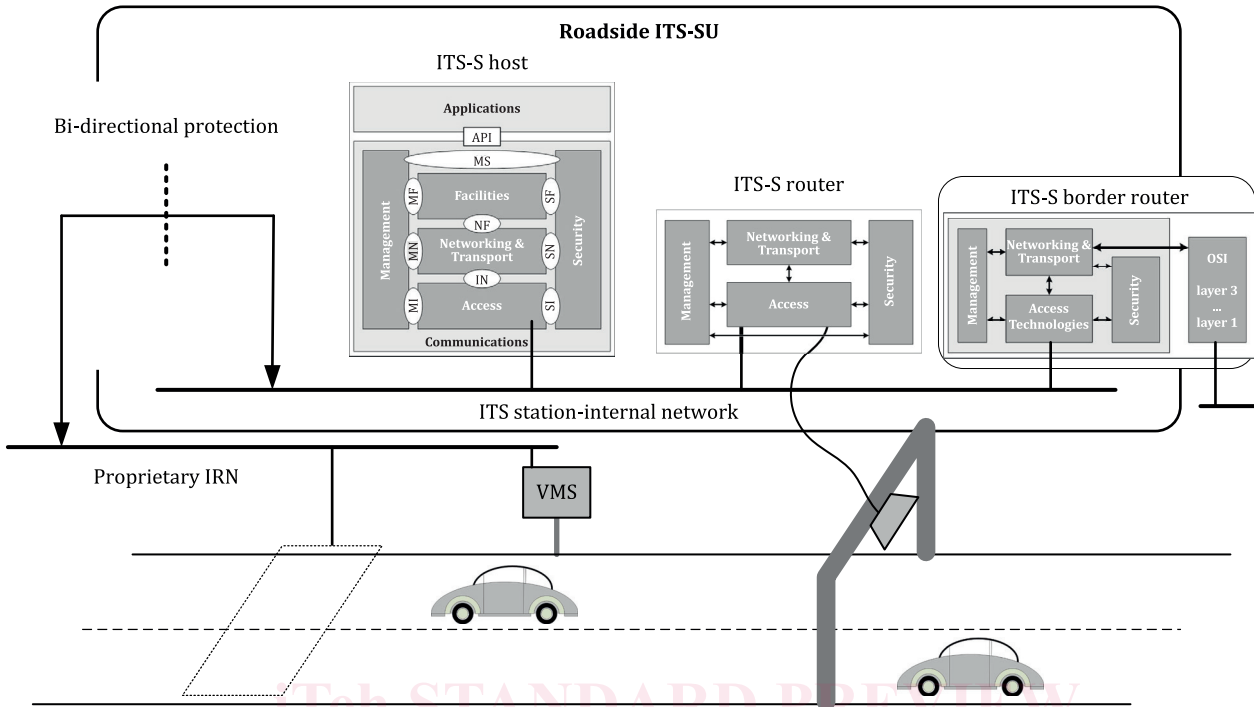
NOTE 2 An ITS-SU can be composed of ITS-SCUs from different vendors where each ITS-SCU is linked to a different ITS-SCU configuration and management centre specified in ISO 24102-2 and ISO 17419. Station-internal management communications between ITS-SCUs of the same ITS-SU are specified in ISO 24102-4. 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

ISO 21177:2023(E)

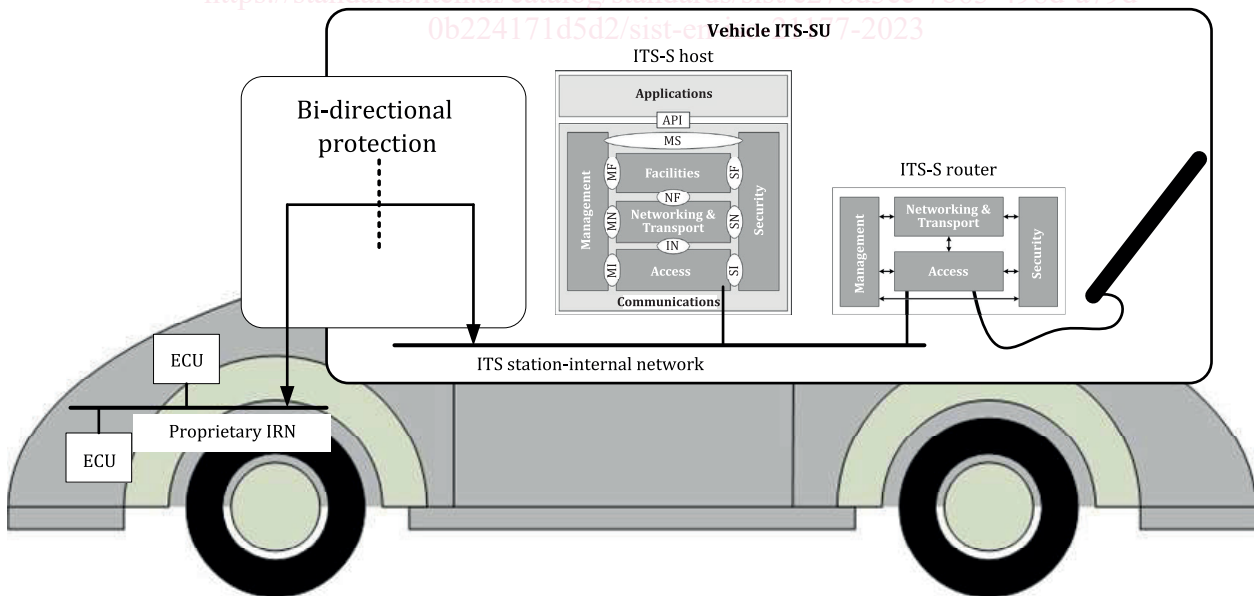
networks (IRN), some of which require secure local access to time-critical information; see [Figure 2](#) and [Figure 3](#).



**Key**  
VMS Variable Message Sign

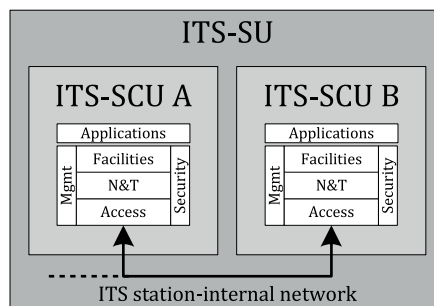
**Figure 2 — Example of a roadside ITS-SU connected with proprietary IRN**

<https://standards.iteh.ai/catalog/standards/sist/e278d3ee-7b63-498d-a79d-0b224171d5d2/sist-en-21177-2023>

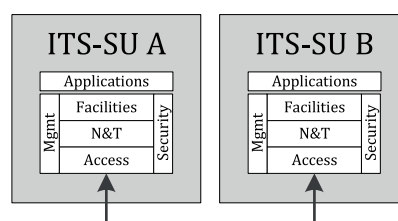


**Key**  
ECU Electronic control unit

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

**Key**

N&amp;T Networking &amp; Transport

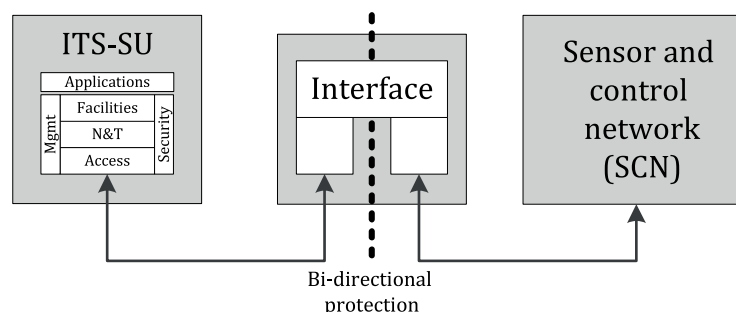
**Figure 4 — Interconnection of ITS-SCUs in an ITS-SU****Key**

N&amp;T Networking &amp; 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&amp;T Networking &amp; Transport

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