

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)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/PRF 21177

<https://standards.iteh.ai/catalog/standards/sist/af800e2e-f10d-44bd-9ee0-a14f995e0453/iso-prf-21177>

Edited DIS - MUST BE USED FOR FINAL DRAFT

© ISO 20222023

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

Website: www.iso.org

Published in Switzerland

Formatted

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/PRF 21177

<https://standards.iteh.ai/catalog/standards/sist/af800e2e-f10d-44bd-9ee0-a14f995e0453/iso-prf-21177>

Contents

Foreword.....	vii
Introduction.....	viii
1 — Scope.....	1
2 — Normative references.....	1
3 — Terms and definitions.....	2
4 — Symbols and abbreviated terms.....	3
5 — Overview.....	5
5.1 — General description, relationship to Transport Layer Security (TLS), and relationship to application specifications.....	5
5.2 — Goals.....	5
5.3 — Architecture and functional entities.....	6
5.4 — Cryptomaterial handles.....	10
5.5 — Session IDs and state.....	10
5.6 — Access control and authorisation state.....	11
5.7 — Application level non-repudiation.....	11
5.8 — Service primitive conventions.....	12
6 — Process flows and sequence diagrams.....	12
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.....	30
6.12 — Session terminated at session layer.....	41

6.13	Deactivate	41
6.14	Secure session example	42
7	Security subsystem: interfaces and data types	44
7.1	General	44
7.2	Access control policy and state	45
7.3	Enhanced authentication	46
7.3.1	Definition and possible states	46
7.3.2	States for owner role enhanced authentication	46
7.3.3	State for accessor role enhanced authentication	47
7.3.4	Use by access control	48
7.3.5	Methods for providing enhanced authentication	48
7.3.6	Enhanced authentication using SPAKE2	48
7.4	Extended authentication	49
7.5	Security Management Information Request	50
7.5.1	Rationale	50
7.5.2	General	51
7.6	Data types	51
7.6.1	General	51
7.6.2	Imports	51
7.6.3	“Helper” data types	52
7.6.4	Iso21177AccessControlPdu	52
7.6.5	AccessControlResult	53
7.6.6	ExtendedAuthPdu	53
7.6.7	ExtendedAuthRequest	54
7.6.8	InnerExtendedAuthRequest	54
7.6.9	AtomicExtendedAuthRequest	54
7.6.10	ExtendedAuthResponse	55
7.6.11	ExtendedAuthResponsePayload	55
7.6.12	EnhancedAuthPdu	55
7.6.13	SpakeRequest	56
7.6.14	SpakeResponse	56
7.6.15	SpakeRequesterResponse	56
7.6.16	SecurityMgmtInfoPdu	56
7.6.17	SecurityMgmtInfoRequest	56
7.6.18	EtsiCrlRequest	57
7.6.19	CertChainRequest	57
7.6.20	SecurityMgmtInfoResponse	58
7.6.21	SecurityMgmtInfoErrorResponse	58
7.6.22	EtsiCrlResponse	58
7.6.23	EtsiCtlResponse	58
7.6.24	IeeeCrlResponse	59
7.6.25	CertChainResponse	59
7.6.26	SessionExtensionPdu	59
7.7	App-Sec Interface	61
7.7.1	App-Sec-Configure.request	61
7.7.2	App-Sec-Configure.confirm	63
7.7.3	App-Sec-StartSession.indication	63
7.7.4	App-Sec-Data.request	63
7.7.5	App-Sec-Data.confirm	64
7.7.6	App-Sec-Incoming.request	65
7.7.7	App-Sec-Incoming.confirm	66
7.7.8	App-Sec-EndSession.request	66

7.7.9	App-Sec-EndSession.indication	67
7.7.10	App-Sec-Deactivate.request	67
7.7.11	App-Sec-Deactivate.confirm	68
7.7.12	App-Sec-Deactivate.indication	68
7.8	Security subsystem internal interface	69
7.8.1	Sec-AuthState.request	69
8	Adaptor layer: interfaces and data types	71
8.1	General	71
8.2	Data types	72
8.2.1	General	72
8.2.2	Iso21177AdaptorLayerPDU	72
8.2.3	Apdu	73
8.2.4	AccessControl	73
8.2.5	TlsClientMsg1	73
8.2.6	TlsServerMsg1	73
8.3	App-AL Interface	73
8.3.1	App-AL-Data.request	73
8.3.2	App-AL-Data.confirm	74
8.3.3	App-AL-Data.indication	74
8.3.4	App-AL-EnableProxy.request	75
8.4	Sec-AL Interface	77
8.4.1	Sec-AL-AccessControl.request	77
8.4.2	Sec-AL-AccessControl.confirm	78
8.4.3	Sec-AL-AccessControl.indication	78
8.4.4	Sec-AL-EndSession.request	79
8.4.5	Sec-AL-EndSession.confirm	79
9	Secure session Services	79
9.1	General	79
9.2	App-Sess interfaces	79
9.2.1	App-Sess-EnableProxy.request	79
9.3	Sec-Sess interface	80
9.3.1	Sec-Sess-Configure.request	80
9.3.2	Sec-Sess-Configure.confirm	80
9.3.3	Sec-Sess-Start.indication	80
9.3.4	Sec-Sess-EndSession.indication	81
9.3.5	Sec-Sess-Deactivate.request	81
9.3.6	Sec-Sess-Deactivate.confirm	85
9.4	AL-Sess interface	85
9.4.1	AL-Sess-Data.request	85
9.4.2	AL-Sess-Data.confirm	86
9.4.3	AL-Sess-Data.indication	86
9.4.4	AL-Sess-EndSession.request	86
9.4.5	AL-Sess-EndSession.confirm	87
9.4.6	AL-Sess-ClientHelloProxy.request	87
9.4.7	AL-Sess-ClientHelloProxy.indication	88
9.4.8	AL-Sess-ServerHelloProxy.request	88
9.4.9	AL-Sess-ServerHelloProxy.indication	89
9.5	Permitted mechanisms	90
9.5.1	TLS 1.3	90
9.5.2	DTLS 1.3	92
Annex A (informative)	Usage scenarios	93

A.1	General	93
A.2	File upload via proxy	93
A.3	Connect RSU and signal controller to enable SPaT operations	93
A.4	Connect TMC and RSU so that RSU can sign TIMs on behalf of TMC	94
A.5	Diagnostic device connection to gateway	95
A.5.1	General	95
A.5.2	Enhanced authentication scenario	95
A.5.2.1	General	95
A.5.2.2	Shared weak secret	96
A.5.2.3	Physical proximity	96
A.5.2.4	Time limited access	97
A.5.2.5	Shared strong secret	97
A.6	Secure connections to advertised services and secure service discovery	98
Annex B (normative)	ASN.1 module	99
Annex C (normative)	Session extension PDU functional type	100
Annex D (normative)	Owner authorization	101
D.1	General	101
D.2	Ownership use case	101
D.2.1	Authorization use case	101
D.2.2	Ownership management use case	101
D.2.3	D.3 Owner authorized flowchart	102
Bibliography		104
Foreword		x
Introduction		xii
1	Scope	1
2	Normative references	1
3	Terms and definitions	2
4	Abbreviated terms	3
5	Overview	4
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	6
5.4	Cryptomaterial handles	13
5.5	Session IDs and state	13
5.6	Access control and authorization state	13
5.7	Application level non-repudiation	14
5.8	Service primitive conventions	14
6	Process flows and sequence diagrams	15
6.1	General	15
6.2	Overview of process flows	15
6.3	Sequence diagram conventions	16
6.4	Configure	17
6.5	Start session	19
6.6	Send data	23

6.7	Send access control PDU	27
6.8	Receive PDU.....	28
6.9	Extend session	36
6.9.1	Goals	36
6.9.2	Processing	37
6.10	Secure connection brokering	37
6.10.1	Goals	37
6.10.2	Prerequisites	38
6.10.3	Overview	38
6.10.4	Detailed specification.....	40
6.11	Force end session.....	53
6.12	Session terminated at session layer	55
6.13	Deactivate.....	56
6.14	Secure session example.....	58
7	Security subsystem: interfaces and data types	60
7.1	General	60
7.2	Access control policy and state.....	61
7.3	Enhanced authentication	62
7.3.1	Definition and possible states.....	62
7.3.2	States for owner role enhanced authentication	63
7.3.3	State for accessor role enhanced authentication	64
7.3.4	Use by access control.....	65
7.3.5	Methods for providing enhanced authentication	65
7.3.6	Enhanced authentication using SPAKE2	65
7.4	Extended authentication	66
7.5	Security Management Information Request	67
7.5.1	Rationale.....	67
7.5.2	General	68
7.6	Data types	69
7.6.1	General	69
7.6.2	Imports.....	69
7.6.3	"Helper" data types	69
7.6.4	Iso21177AccessControlPdu	70
7.6.5	AccessControlResult.....	70
7.6.6	ExtendedAuthPdu.....	71
7.6.7	ExtendedAuthRequest	71
7.6.8	InnerExtendedAuthRequest	71
7.6.9	AtomicExtendedAuthRequest	72
7.6.10	ExtendedAuthResponse	72
7.6.11	ExtendedAuthResponsePayload	73
7.6.12	EnhancedAuthPdu	73
7.6.13	SpakeRequest.....	74
7.6.14	SpakeResponse.....	74
7.6.15	SpakeRequesterResponse	74
7.6.16	SecurityMgmtInfoPdu	74
7.6.17	SecurityMgmtInfoRequest.....	74
7.6.18	EtsiCrlRequest	75
7.6.19	CertChainRequest	75
7.6.20	SecurityMgmtInfoResponse	76
7.6.21	SecurityMgmtInfoErrorResponse.....	76
7.6.22	EtsiCrlResponse	77
7.6.23	EtsiCtlResponse.....	77

7.6.24	IeeeCriResponse	77
7.6.25	CertChainResponse	77
7.6.26	SessionExtensionPdu	77
7.7	App-Sec Interface	80
7.7.1	App-Sec-Configure.request	80
7.7.2	App-Sec-Configure.confirm	81
7.7.3	App-Sec-StartSession.indication	81
7.7.4	App-Sec-Data.request	82
7.7.5	App-Sec-Data.confirm	82
7.7.6	App-Sec-Incoming.request	83
7.7.7	App-Sec-Incoming.confirm	84
7.7.8	App-Sec-EndSession.request	84
7.7.9	App-Sec-EndSession.indication	85
7.7.10	App-Sec-Deactivate.request	85
7.7.11	App-Sec-Deactivate.confirm	86
7.7.12	App-Sec-Deactivate.indication	86
7.8	Security subsystem internal interface	86
7.8.1	General	86
7.8.2	Sec-AuthState.request	87
7.8.3	Sec-AuthState.confirm	87
8	Adaptor layer: interfaces and data types	88
8.1	General	88
8.2	Data types	89
8.2.1	General	89
8.2.2	Iso21177AdaptorLayerPDU	89
8.2.3	Apdu	90
8.2.4	AccessControl	90
8.2.5	TlsClientMsg1	90
8.2.6	TlsServerMsg1	90
8.3	App-AL Interface	91
8.3.1	App-AL-Data.request	91
8.3.2	App-AL-Data.confirm	91
8.3.3	App-AL-Data.indication	91
8.3.4	App-AL-EnableProxy.request	92
8.4	Sec-AL Interface	94
8.4.1	Sec-AL-AccessControl.request	94
8.4.2	Sec-AL-AccessControl.confirm	95
8.4.3	Sec-AL-AccessControl.indication	95
8.4.4	Sec-AL-EndSession.request	96
8.4.5	Sec-AL-EndSession.confirm	96
9	Secure session Services	96
9.1	General	96
9.2	App-Sess interfaces	96
9.2.1	App-Sess-EnableProxy.request	96
9.3	Sec-Sess interface	97
9.3.1	Sec-Sess-Configure.request	97
9.3.2	Sec-Sess-Configure.confirm	99
9.3.3	Sec-Sess-Start.indication	100
9.3.4	Sec-Sess-EndSession.indication	100
9.3.5	Sec-Sess-Deactivate.request	101
9.3.6	Sec-Sess-Deactivate.confirm	101
9.4	AL-Sess interface	101

9.4.1 AL-Sess-Data.request	101
9.4.2 AL-Sess-Data.confirm	102
9.4.3 AL-Sess-Data.indication	102
9.4.4 AL-Sess-EndSession.request	102
9.4.5 AL-Sess-EndSession.confirm	103
9.4.6 AL-Sess-ClientHelloProxy.request	103
9.4.7 AL-Sess-ClientHelloProxy.indication	104
9.4.8 AL-Sess-ServerHelloProxy.request	104
9.4.9 AL-Sess-ServerHelloProxy.indication	105
9.5 Permitted mechanisms	106
9.5.1 TLS 1.3	106
9.5.2 DTLS 1.3	107
Annex A (informative) Usage scenarios	108
Annex B (normative) ASN.1 module	118
Annex C (normative) Session extension PDU functional type	119
Annex D (normative) Owner authorization	120
Bibliography	125

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/PRF 21177](#)

<https://standards.iteh.ai/catalog/standards/sist/af800e2e-f10d-44bd-9ee0-a14f995e0453/iso-prf-21177>

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: 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

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

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)

iTeh STANDARD PREVIEW (standards.iteh.ai)

ISO/PRF 21177

<https://standards.iteh.ai/catalog/standards/sist/af800e2e-f10d-44bd-9ee0-a14f995e0453/iso-prf-21177>

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_A) 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 ~~must~~needs to include an access control policy, indicating ~~what~~which properties ~~must~~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.

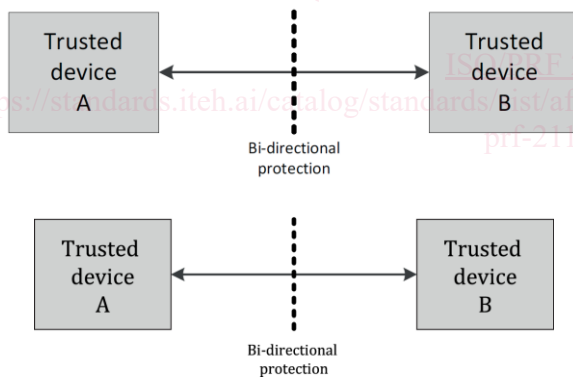


Figure 1 — Interconnection of trusted devices

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.

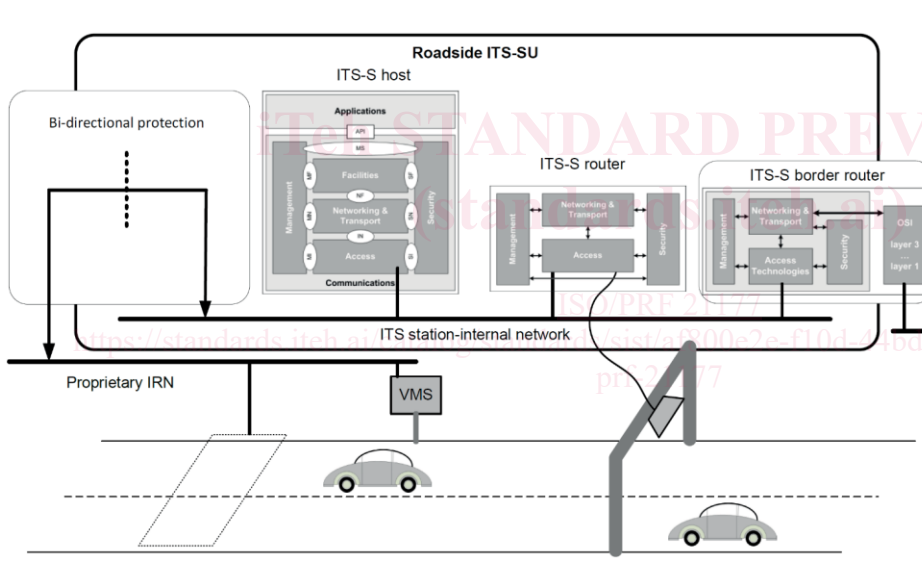
NOTE 2 An ITS-SU can be composed of ITS-SCUs from different vendors where each ITS-SCU is linked to a different ITS-SCU configuration and management centre specified in ISO 24102-2 and ISO 17419. Station-internal

Formatted: std_docPartNumber

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 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, 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.



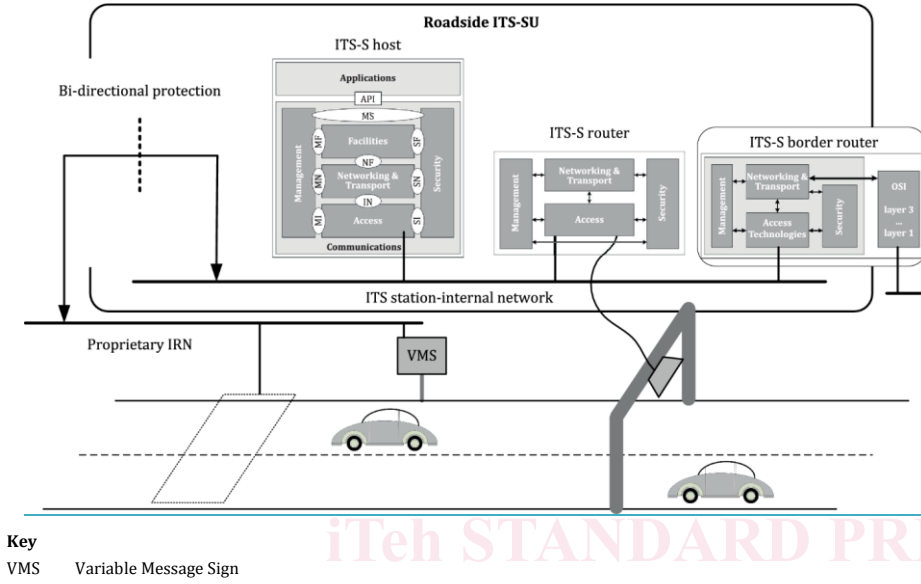


Figure 2 — Example of a roadside ITS-SU connected with proprietary IRN

ISO/PRF 21177

<https://standards.iteh.ai/catalog/standards/sist/af800e2e-f10d-44bd-9ee0-a14f995e0453/iso-prf-21177>

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

