

INTERNATIONAL STANDARD

ISO-~~/~~**FDIS 21177:2023(E)**

ISO-~~/~~TC-204/~~/~~WG-18

Secretariat: ANSI

Date: 2023-~~04~~**10-30**

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

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

iTeh Standards
(<https://standards.itih.ai>)
Document Preview

FDIS stage

<https://standards.itih.ai/catalog/standards-tripoint-sf-3c3f6959b06f/iso-fdis-21177>

© 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~~E-mail: copyright@iso.org
Website: ~~www.iso.org~~www.iso.org

Published in Switzerland

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO/FDIS 21177

<https://standards.iteh.ai/catalog/standards/sist/30b9a06f-851a-456f-beaf-3c3f6959b06f/iso-fdis-21177>

Contents

Foreword	xi
Introduction.....	xiii
1 Scope	1
2 Normative references.....	1
3 Terms and definitions	1
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.....	37
6.10.3 Overview.....	38
6.10.4 Detailed specification	40
6.11 Force end session.....	53
6.12 Session terminated at session layer	56
6.13 Deactivate.....	57
6.14 Secure session example.....	58

7	Security subsystem: interfaces and data types.....	61
7.1	General.....	61
7.2	Access control policy and state.....	62
7.3	Enhanced authentication.....	63
7.3.1	Definition and possible states.....	63
7.3.2	States for owner role enhanced authentication.....	64
7.3.3	State for accessor role enhanced authentication.....	65
7.3.4	Use by access control.....	66
7.3.5	Methods for providing enhanced authentication.....	66
7.3.6	Enhanced authentication using SPAKE2.....	66
7.4	Extended authentication.....	67
7.5	Security Management Information Request.....	68
7.5.1	Rationale.....	68
7.5.2	General.....	69
7.6	Data types.....	70
7.6.1	General.....	70
7.6.2	Imports.....	70
7.6.3	“Helper” data types.....	70
7.6.4	Iso21177AccessControlPdu.....	71
7.6.5	AccessControlResult.....	72
7.6.6	ExtendedAuthPdu.....	73
7.6.7	ExtendedAuthRequest.....	74
7.6.8	InnerExtendedAuthRequest.....	74
7.6.9	AtomicExtendedAuthRequest.....	75
7.6.10	ExtendedAuthResponse.....	75
7.6.11	ExtendedAuthResponsePayload.....	75
7.6.12	EnhancedAuthPdu.....	76
7.6.13	SpakeRequest.....	77
7.6.14	SpakeResponse.....	77
7.6.15	SpakeRequesterResponse.....	77
7.6.16	SecurityMgmtInfoPdu.....	78
7.6.17	SecurityMgmtInfoRequest.....	78
7.6.18	EtsiCrlRequest.....	79
7.6.19	CertChainRequest.....	79
7.6.20	SecurityMgmtInfoResponse.....	80
7.6.21	SecurityMgmtInfoErrorResponse.....	81
7.6.22	EtsiCrlResponse.....	81
7.6.23	EtsiCtlResponse.....	82

7.6.24	IeeeCrIResponse	82
7.6.25	CertChainResponse	82
7.6.26	SessionExtensionPdu	82
7.7	App-Sec Interface	85
7.7.1	App-Sec-Configure.request	85
7.7.2	App-Sec-Configure.confirm	87
7.7.3	App-Sec-StartSession.indication	87
7.7.4	App-Sec-Data.request	88
7.7.5	App-Sec-Data.confirm	89
7.7.6	App-Sec-Incoming.request	89
7.7.7	App-Sec-Incoming.confirm	90
7.7.8	App-Sec-EndSession.request	91
7.7.9	App-Sec-EndSession.indication	91
7.7.10	App-Sec-Deactivate.request	92
7.7.11	App-Sec-Deactivate.confirm	92
7.7.12	App-Sec-Deactivate.indication	92
7.8	Security subsystem internal interface	93
7.8.1	General	93
7.8.2	Sec-AuthState.request	93
7.8.3	Sec-AuthState.confirm	94
8	Adaptor layer: interfaces and data types	95
8.1	General	95
8.2	Data types	96
8.2.1	General	96
8.2.2	Iso21177AdaptorLayerPDU	97
8.2.3	Apdu	98
8.2.4	AccessControl	98
8.2.5	TlsClientMsg1	98
8.2.6	TlsServerMsg1	98
8.3	App-AL Interface	98
8.3.1	App-AL-Data.request	98
8.3.2	App-AL-Data.confirm	99
8.3.3	App-AL-Data.indication	99
8.3.4	App-AL-EnableProxy.request	100
8.4	Sec-AL Interface	102
8.4.1	Sec-AL-AccessControl.request	102
8.4.2	Sec-AL-AccessControl.confirm	103
8.4.3	Sec-AL-AccessControl.indication	103

8.4.4	Sec-AL-EndSession.request.....	104
8.4.5	Sec-AL-EndSession.confirm.....	104
9	Secure session Services.....	104
9.1	General.....	104
9.2	App-Sess interfaces.....	104
9.2.1	App-Sess-EnableProxy.request.....	104
9.3	Sec-Sess interface.....	105
9.3.1	Sec-Sess-Configure.request.....	105
9.3.2	Sec-Sess-Configure.confirm.....	108
9.3.3	Sec-Sess-Start.indication.....	108
9.3.4	Sec-Sess-EndSession.indication.....	109
9.3.5	Sec-Sess-Deactivate.request.....	109
9.3.6	Sec-Sess-Deactivate.confirm.....	110
9.4	AL-Sess interface.....	110
9.4.1	AL-Sess-Data.request.....	110
9.4.2	AL-Sess-Data.confirm.....	110
9.4.3	AL-Sess-Data.indication.....	111
9.4.4	AL-Sess-EndSession.request.....	111
9.4.5	AL-Sess-EndSession.confirm.....	112
9.4.6	AL-Sess-ClientHelloProxy.request.....	112
9.4.7	AL-Sess-ClientHelloProxy.indication.....	113
9.4.8	AL-Sess-ServerHelloProxy.request.....	113
9.4.9	AL-Sess-ServerHelloProxy.indication.....	114
9.5	Permitted mechanisms.....	115
9.5.1	TLS 1.3.....	115
9.5.2	DTLS 1.3.....	116
	Annex A (informative) Usage scenarios.....	117
A.1	General.....	117
A.2	File upload via proxy.....	117
A.3	Connect RSU and signal controller to enable SPaT operations.....	117
A.4	Connect TMC and RSU so that RSU can sign TIMs on behalf of TMC.....	118
A.5	Diagnostic device connection to gateway.....	119
A.5.1	General.....	119
A.5.2	Enhanced authentication scenario.....	119
A.6	Secure connections to advertised services and secure service discovery.....	125
	Annex B (normative) ASN.1 module.....	127
	Annex C (normative) Session extension PDU functional type.....	128
	Annex D (normative) Owner authorization.....	129

D.1	General	129
D.2	Ownership use case	129
D.2.1	Authorization use case	129
D.2.2	Ownership management use case	130
D.2.3	Owner authorized flowchart	130
	Bibliography	134

Foreword — vi

Introduction — vii

1 — Scope — 1

2 — Normative references — 1

3 — Terms and definitions — 1

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 — 11

5.5 — Session IDs and state — 11

5.6 — Access control and authorization state — 11

5.7 — Application level non-repudiation — 12

5.8 — Service primitive conventions — 12

6 — Process flows and sequence diagrams — 13

6.1 — General — 13

6.2 — Overview of process flows — 13

6.3 — Sequence diagram conventions — 14

6.4 — Configure — 15

6.5 — Start session — 17

6.6 — Send data — 19

6.7 — Send access control PDU — 22

6.8 — Receive PDU — 23

6.9 — Extend session — 28

6.9.1 — Goals — 28

6.9.2 — Processing — 29

6.10 — Secure connection brokering — 29

6.10.1 — Goals — 29

6.10.2 — Prerequisites — 30

6.10.3	Overview	30
6.10.4	Detailed specification	32
6.11	Force end session	40
6.12	Session terminated at session layer	42
6.13	Deactivate	42
6.14	Secure session example	44
7	Security subsystem: interfaces and data types	45
7.1	General	45
7.2	Access control policy and state	46
7.3	Enhanced authentication	47
7.3.1	Definition and possible states	47
7.3.2	States for owner role enhanced authentication	48
7.3.3	State for accessor role enhanced authentication	49
7.3.4	Use by access control	49
7.3.5	Methods for providing enhanced authentication	50
7.3.6	Enhanced authentication using SPAKE2	50
7.4	Extended authentication	51
7.5	Security Management Information Request	52
7.5.1	Rationale	52
7.5.2	General	53
7.6	Data types	53
7.6.1	General	53
7.6.2	Imports	53
7.6.3	“Helper” data types	54
7.6.4	Iso21177AccessControlPdu	54
7.6.5	AccessControlResult	55
7.6.6	ExtendedAuthPdu	55
7.6.7	ExtendedAuthRequest	56
7.6.8	InnerExtendedAuthRequest	56
7.6.9	AtomicExtendedAuthRequest	57
7.6.10	ExtendedAuthResponse	57
7.6.11	ExtendedAuthResponsePayload	57
7.6.12	EnhancedAuthPdu	58
7.6.13	SpakeRequest	58
7.6.14	SpakeResponse	58
7.6.15	SpakeRequesterResponse	59
7.6.16	SecurityMgmtInfoPdu	59
7.6.17	SecurityMgmtInfoRequest	59

7.6.18	EtsiCrlRequest	60
7.6.19	CertChainRequest	60
7.6.20	SecurityMgmtInfoResponse	60
7.6.21	SecurityMgmtInfoErrorResponse	61
7.6.22	EtsiCrlResponse	61
7.6.23	EtsiCtlResponse	61
7.6.24	IeeeCrlResponse	62
7.6.25	CertChainResponse	62
7.6.26	SessionExtensionPdu	62
7.7	App-Sec Interface	64
7.7.1	App-Sec-Configure.request	64
7.7.2	App-Sec-Configure.confirm	65
7.7.3	App-Sec-StartSession.indication	66
7.7.4	App-Sec-Data.request	66
7.7.5	App-Sec-Data.confirm	67
7.7.6	App-Sec-Incoming.request	67
7.7.7	App-Sec-Incoming.confirm	68
7.7.8	App-Sec-EndSession.request	69
7.7.9	App-Sec-EndSession.indication	69
7.7.10	App-Sec-Deactivate.request	70
7.7.11	App-Sec-Deactivate.confirm	70
7.7.12	App-Sec-Deactivate.indication	70
7.8	Security subsystem internal interface	71
7.8.1	General	71
7.8.2	Sec-AuthState.request	71
7.8.3	Sec-AuthState.confirm	72
8	Adaptor layer: interfaces and data types	73
8.1	General	73
8.2	Data types	74
8.2.1	General	74
8.2.2	Iso21177AdaptorLayerPDU	74
8.2.3	Apdu	75
8.2.4	AccessControl	75
8.2.5	TlsClientMsg1	75
8.2.6	TlsServerMsg1	75
8.3	App-AL Interface	75
8.3.1	App-AL-Data.request	75
8.3.2	App-AL-Data.confirm	76

8.3.3	App-AL-Data.indication	76
8.3.4	App-AL-EnableProxy.request	77
8.4	Sec-AL Interface	79
8.4.1	Sec-AL-AccessControl.request	79
8.4.2	Sec-AL-AccessControl.confirm	79
8.4.3	Sec-AL-AccessControl.indication	80
8.4.4	Sec-AL-EndSession.request	80
8.4.5	Sec-AL-EndSession.confirm	80
9	Secure session Services	81
9.1	General	81
9.2	App-Sess interfaces	81
9.2.1	App-Sess-EnableProxy.request	81
9.3	Sec-Sess interface	81
9.3.1	Sec-Sess-Configure.request	81
9.3.2	Sec-Sess-Configure.confirm	84
9.3.3	Sec-Sess-Start.indication	84
9.3.4	Sec-Sess-EndSession.indication	85
9.3.5	Sec-Sess-Deactivate.request	85
9.3.6	Sec-Sess-Deactivate.confirm	86
9.4	AL-Sess interface	86
9.4.1	AL-Sess-Data.request	86
9.4.2	AL-Sess-Data.confirm	86
9.4.3	AL-Sess-Data.indication	86
9.4.4	AL-Sess-EndSession.request	87
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	89
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
Annex B (normative)	ASN.1 module	101
Annex C (normative)	Session extension PDU functional type	102
Annex D (normative)	Owner authorization	103
Bibliography		107

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~~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).

~~Attention is drawn~~ISO draws attention to the possibility that ~~some of the elements~~implementation of this document may ~~be involve~~ the ~~subject~~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. ~~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 ~~second edition cancels and replaces the~~ first edition of (ISO 21177 ~~cancels and replaces~~ ISO/TS 21177:2019, :2023), of which ~~has been technically revised~~.

~~it constitutes a minor revision.~~ 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.~~

~~— 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~~www.iso.org/members.html~~.

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO/FDIS 21177

<https://standards.iteh.ai/catalog/standards/sist/30b9a06f-851a-456f-beaf-3c3f6959b06f/iso-fdis-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~~. 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.

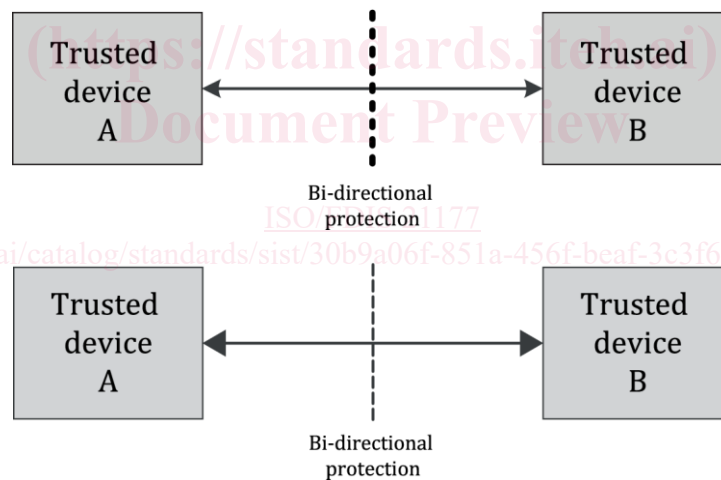


Figure 1 — Interconnection of trusted devices

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~~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.~~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 and Figure 3.

