

DIN CEN ISO/TS 21177:2020-01 (E)

Intelligent transport systems - ITS station security services for secure session establishment and authentication between trusted devices (ISO/TS 21177:2019); English version CEN ISO/TS 21177:2019

Contents		Page
Foreword		vi
Introduction		vii
1 Scope		1
2 Normative references		1
3 Terms and definitions		1
4 Symbols and abbreviated terms		2
5 Overview		3
5.1 Goals.....		3
5.2 Architecture and functional entities.....		4
5.3 Cryptomaterial handles.....		7
5.4 Session IDs and state.....		7
5.5 Access control and authorisation state.....		8
5.6 Application level non-repudiation.....		8
5.7 Service primitive conventions.....		8
6 Process flows and sequence diagrams		9
6.1 General.....		9
6.2 Overview of process flows.....		9
6.3 Sequence diagram conventions.....		10
6.4 Configure.....		11
6.5 Start Session.....		12
6.6 Send data.....		14
6.7 Send access control PDU.....		17
6.8 Receive PDU.....		18
6.9 Secure connection brokering.....		23
6.9.1 Goals.....		23
6.9.2 Prerequisites.....		24
6.9.3 Overview.....		24
6.9.4 Detailed specification.....		25
6.10 Force end session.....		33
6.11 Session terminated at session layer.....		35
6.12 Deactivate.....		35
6.13 Secure session example.....		36
7 Security Subsystem: interfaces and data types		38
7.1 General.....		38
7.2 Access control policy and state.....		39
7.3 Enhanced authentication.....		40
7.3.1 Definition and possible states.....		40
7.3.2 States for owner role enhanced authentication.....		40
7.3.3 State for accessor role enhanced authentication.....		41
7.3.4 Use by Access Control.....		42
7.3.5 Methods for providing enhanced authentication.....		42
7.3.6 Enhanced authentication using SPAKE2.....		42
7.4 Extended authentication.....		43

7.5	Data types.....	44
7.5.1	General.....	44
7.5.2	Imports.....	44
7.5.3	Iso21177AccessControlPdu.....	44
7.5.4	AccessControlResult.....	44
7.5.5	ExtendedAuthPdu.....	44
7.5.6	ExtendedAuthRequest.....	45
7.5.7	InnerExtendedAuthRequest.....	45
7.5.8	AtomicExtendedAuthRequest.....	46
7.5.9	ExtendedAuthResponse.....	46
7.5.10	ExtendedAuthResponsePayload.....	46
7.5.11	EnhancedAuthPdu.....	47
7.5.12	SpakeRequest.....	47
7.5.13	SpakeResponse.....	47
7.5.14	SpakeRequesterResponse.....	48
7.6	App-Sec Interface.....	48
7.6.1	App-Sec-Configure.request.....	48
7.6.2	App-Sec-Configure.confirm.....	49
7.6.3	App-Sec-StartSession.indication.....	49
7.6.4	App-Sec-Data.request.....	50
7.6.5	App-Sec-Data.confirm.....	50
7.6.6	App-Sec-Incoming.request.....	51
7.6.7	App-Sec-Incoming.confirm.....	51
7.6.8	App-Sec-EndSession.request.....	52
7.6.9	App-Sec-EndSession.confirm.....	52
7.6.10	App-Sec-EndSession.indication.....	52
7.6.11	App-Sec-Deactivate.request.....	53
7.6.12	App-Sec-Deactivate.confirm.....	53
7.6.13	App-Sec-Deactivate.indication.....	53
7.7	Security Subsystem internal interface.....	54
7.7.1	General.....	54
7.7.2	Sec-AuthState.request.....	54
7.7.3	Sec-AuthState.confirm.....	55
8	Adaptor Layer: Interfaces and data types.....	55
8.1	General.....	55
8.2	Data types.....	56
8.2.1	General.....	56
8.2.2	Iso21177AdaptorLayerPDU.....	56
8.2.3	A pdu.....	57
8.2.4	Access Control.....	57
8.2.5	TlsClientMsg1.....	57
8.2.6	TlsServerMsg1.....	57
8.3	App-AL Interface.....	57
8.3.1	App-AL-Data.request.....	57
8.3.2	App-AL-Data.confirm.....	58
8.3.3	App-AL-Data.indication.....	58
8.3.4	App-AL-EnableProxy.request.....	59
8.4	Sec-AL Interface.....	61
8.4.1	Sec-AL-AccessControl.request.....	61
8.4.2	Sec-AL-AccessControl.confirm.....	61
8.4.3	Sec-AL-AccessControl.indication.....	61
8.4.4	Sec-AL-EndSession.request.....	62
8.4.5	Sec-AL-EndSession.confirm.....	62
9	Secure Session services.....	62
9.1	General.....	62
9.2	App-Sess interfaces.....	62
9.2.1	App-Sess-EnableProxy.request.....	62

9.3	Sec-Sess interface.....	63
9.3.1	Sec-Sess-Configure.request.....	63
9.3.2	Sec-Sess-Configure.confirm.....	65
9.3.3	Sec-Sess-Start.indication.....	65
9.3.4	Sec-Sess-EndSession.indication.....	66
9.3.5	Sec-Sess-Deactivate.request.....	66
9.3.6	Sec-Sess-Deactivate.confirm.....	67
9.4	AL-Sess interface.....	67
9.4.1	AL-Sess-Data.request.....	67
9.4.2	AL-Sess-Data.confirm.....	67
9.4.3	AL-Sess-Data.indication.....	68
9.4.4	AL-Sess-EndSession.request.....	68
9.4.5	AL-Sess-EndSession.confirm.....	68
9.4.6	AL-Sess-ClientHelloProxy.request.....	69
9.4.7	AL-Sess-ClientHelloProxy.indication.....	69
9.4.8	AL-Sess-ServerHelloProxy.request.....	70
9.4.9	AL-Sess-ServerHelloProxy.indication.....	70
9.4.10	AL-Sess-EndSession.request.....	71
9.4.11	AL-Sess-EndSession.confirm.....	72
9.5	Permitted mechanisms.....	72
9.5.1	TLS 1.3.....	72
9.5.2	DTLS 1.3.....	73
Annex A (informative) Usage scenarios.....		74
Annex B (normative) ASN.1 module.....		81
Bibliography.....		82

