ISO 21177:2024-03 (E)

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

Contents

Page

Foreword ..... **vi**

Introduction ..... **vii**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Abbreviated terms **2**

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 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

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 38

6.12 Session terminated at session layer 39

6.13 Deactivate 40

6.14 Secure session example 41

7 Security subsystem: interfaces and data types **43**

7.1 General 43

7.2 Access control policy and state 43

7.3 Enhanced authentication 44

7.3.1 Definition and possible states 44

7.3.2 States for owner role enhanced authentication 45

7.3.3 State for accessor role enhanced authentication 46

7.3.4 Use by access control 46

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 48
7.5.1 Rationale 48
7.5.2 General 49
7.6 Data types 50
7.6.1 General 50
7.6.2 Imports 50
7.6.3 “Helper” data types 50
7.6.4 Iso21177AccessControlPdu 51
7.6.5 AccessControlResult 51
7.6.6 ExtendedAuthPdu 51
7.6.7 ExtendedAuthRequest 52
7.6.8 InnerExtendedAuthRequest 52
7.6.9 AtomicExtendedAuthRequest 53
7.6.10 ExtendedAuthResponse 53
7.6.11 ExtendedAuthResponsePayload 53
7.6.12 EnhancedAuthPdu 53
7.6.13 SpakeRequest 54
7.6.14 SpakeResponse 54
7.6.15 SpakeRequesterResponse 54
7.6.16 SecurityMgmtInfoPdu 54
7.6.17 SecurityMgmtInfoRequest 55
7.6.18 EtsiCrlRequest 55
7.6.19 CertChainRequest 55
7.6.20 SecurityMgmtInfoResponse 56
7.6.21 SecurityMgmtInfoErrorResponse 56
7.6.22 EtsiCrlResponse 56
7.6.23 EtsiCtlResponse 56
7.6.24 IeeeCrlResponse 57
7.6.25 CertChainResponse 57
7.6.26 SessionExtensionPdu 57
7.7 App-Sec Interface 59
7.7.1 App-Sec-Configure.request 59
7.7.2 App-Sec-Configure.confirm 60
7.7.3 App-Sec-StartSession.indication 60
7.7.4 App-Sec-Data.request 60
7.7.5 App-Sec-Data.confirm 61
7.7.6 App-Sec-Incoming.request 61
7.7.7 App-Sec-Incoming.confirm 62
7.7.8 App-Sec-EndSession.request 63
7.7.9 App-Sec-EndSession.indication 63
7.7.10 App-Sec-Deactivate.request 63
7.7.11 App-Sec-Deactivate.confirm 64
7.7.12 App-Sec-Deactivate.indication 64
7.8 Security subsystem internal interface 64
7.8.1 General 64
7.8.2 Sec-AuthState.request 65
7.8.3 Sec-AuthState.confirm 65

8 Adaptor layer: interfaces and data types 66
8.1 General 66
8.2 Data types 67
8.2.1 General 67
8.2.2 Iso21177AdaptorLayerPDU 67
8.2.3 Apdu 68
8.2.4 AccessControl 68
8.2.5 TlsClientMsg1 68
8.2.6 TlsServerMsg1 68
8.3 App-AL Interface 68
8.3.1 App-AL-Data.request 68
8.3.2 App-AL-Data.confirm 69
8.3.3 App-AL-Data.indication 69
8.3.4 App-AL-EnableProxy.request 70
8.4 Sec-AL Interface 71

8.4.1 Sec-AL-AccessControl.request ... 71
8.4.2 Sec-AL-AccessControl.confirm ... 72
8.4.3 Sec-AL-AccessControl.indication ... 72
8.4.4 Sec-AL-EndSession.request ... 73
8.4.5 Sec-AL-EndSession.confirm ... 73

9 Secure session Services ... 73
9.1 General ... 73
9.2 App-Sess interfaces ... 73
9.2.1 App-Sess-EnableProxy.request ... 73
9.3 Sec-Sess interface ... 74
9.3.1 Sec-Sess-Configure.request ... 74
9.3.2 Sec-Sess-Configure.confirm ... 76
9.3.3 Sec-Sess-Start.indication ... 76
9.3.4 Sec-Sess-EndSession.indication ... 77
9.3.5 Sec-Sess-Deactivate.request ... 77
9.3.6 Sec-Sess-Deactivate.confirm ... 78
9.4 AL-Sess interface ... 78
9.4.1 AL-Sess-Data.request ... 78
9.4.2 AL-Sess-Data.confirm ... 78
9.4.3 AL-Sess-Data.indication ... 78
9.4.4 AL-Sess-EndSession.request ... 79
9.4.5 AL-Sess-EndSession.confirm ... 79
9.4.6 AL-Sess-ClientHelloProxy.request ... 79
9.4.7 AL-Sess-ClientHelloProxy.indication ... 80
9.4.8 AL-Sess-ServerHelloProxy.request ... 81
9.4.9 AL-Sess-ServerHelloProxy.indication ... 81
9.5 Permitted mechanisms ... 82
9.5.1 TLS 1.3 ... 82
9.5.2 DTLS 1.3 ... 83

Annex A (informative) **Usage scenarios ... 84**

Annex B (normative) **ASN.1 module ... 92**

Annex C (normative) **Session extension PDU functional type ... 93**

Annex D (normative) **Owner authorization ... 94**

Bibliography ... 98