

ISO/TS 21177:2019 (E)

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

Contents

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

7.5.2	Imports
7.5.3	Iso21177AccessControlPdu
7.5.4	AccessControlResult
7.5.5	ExtendedAuthPdu
7.5.6	ExtendedAuthRequest
7.5.7	InnerExtendedAuthRequest
7.5.8	AtomicExtendedAuthRequest
7.5.9	ExtendedAuthResponse
7.5.10	ExtendedAuthResponsePayload
7.5.11	EnhancedAuthPdu
7.5.12	SpakeRequest
7.5.13	SpakeResponse
7.5.14	SpakeRequesterResponse
7.6	App-Sec Interface
7.6.1	App-Sec-Configure.request
7.6.2	App-Sec-Configure.confirm
7.6.3	App-Sec-StartSession.indication
7.6.4	App-Sec-Data.request
7.6.5	App-Sec-Data.confirm
7.6.6	App-Sec-Incoming.request
7.6.7	App-Sec-Incoming.confirm
7.6.8	App-Sec-EndSession.request
7.6.9	App-Sec-EndSession.confirm
7.6.10	App-Sec-EndSession.indication
7.6.11	App-Sec-Deactivate.request
7.6.12	App-Sec-Deactivate.confirm
7.6.13	App-Sec-Deactivate.indication
7.7	Security Subsystem internal interface
7.7.1	General
7.7.2	Sec-AuthState.request
7.7.3	Sec-AuthState.confirm
8	Adaptor Layer: Interfaces and data types
8.1	General
8.2	Data types
8.2.1	General
8.2.2	Iso21177AdaptorLayerPDU
8.2.3	Apdu
8.2.4	Access Control
8.2.5	TlsClientMsg1
8.2.6	TlsServerMsg1
8.3	App-AL Interface
8.3.1	App-AL-Data.request
8.3.2	App-AL-Data.confirm
8.3.3	App-AL-Data.indication
8.3.4	App-AL-EnableProxy.request
8.4	Sec-AL Interface
8.4.1	Sec-AL-AccessControl.request
8.4.2	Sec-AL-AccessControl.confirm
8.4.3	Sec-AL-AccessControl.indication
8.4.4	Sec-AL-EndSession.request
8.4.5	Sec-AL-EndSession.confirm
9	Secure Session services
9.1	General
9.2	App-Sess interfaces
9.2.1	App-Sess-EnableProxy.request
9.3	Sec-Sess interface
9.3.1	Sec-Sess-Configure.request
9.3.1.1	Function
9.3.1.2	Semantics
9.3.1.3	Effect of receipt
9.3.2	Sec-Sess-Configure.confirm
9.3.3	Sec-Sess-Start.indication

- 9.3.4 Sec-Sess-EndSession.indication
- 9.3.5 Sec-Sess-Deactivate.request
- 9.3.6 Sec-Sess-Deactivate.confirm
- 9.4 AL-Sess interface
- 9.4.1 AL-Sess-Data.request
- 9.4.2 AL-Sess-Data.confirm
- 9.4.3 AL-Sess-Data.indication
- 9.4.4 AL-Sess-EndSession.request
- 9.4.5 AL-Sess-EndSession.confirm
- 9.4.6 AL-Sess-ClientHelloProxy.request
- 9.4.7 AL-Sess-ClientHelloProxy.indication
- 9.4.8 AL-Sess-ServerHelloProxy.request
- 9.4.9 AL-Sess-ServerHelloProxy.indication
- 9.4.10 AL-Sess-EndSession.request
- 9.4.11 AL-Sess-EndSession.confirm
- 9.5 Permitted mechanisms
- 9.5.1 TLS 1.3
- 9.5.2 DTLS 1.3

Annex A (informative) Usage scenarios

- A.1 General
- A.2 File upload via proxy
- A.3 Connect RSU and signal controller to enable SPaT operations
- A.4 Connect TMC and RSU so that RSU can sign TIMs on behalf of TMC
- A.5 Diagnostic device connection to gateway
- A.5.1 General
- A.5.2 Enhanced Authentication scenario
- A.5.2.1 General
- A.5.2.2 Shared weak secret
- A.5.2.3 Physical proximity
- A.5.2.4 Time-limited access
- A.5.2.5 Shared strong secret
- A.6 Secure connections to advertised services and secure service discovery

Annex B (normative) ASN.1 module

Page count: 83