PD CEN ISO/TS 21177:2019

BSI Standards Publication

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

Documents
Document Sharing Hub

Full document details: PD CEN ISO/TS 21177:2019

National foreword

This Published Document is the UK implementation of CEN ISO/TS 21177:2019. It is identical to ISO/TS 21177:2019.

The UK participation in its preparation was entrusted to Technical Committee EPL/278, Intelligent transport systems.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2020
Published by BSI Standards Limited 2020

ISBN 978 0 580 93448 3

ICS 03.220.01; 35.030; 35.240.60

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 April 2020.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: PD CEN ISO/TS 21177:2019

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN ISO/TS 21177

October 2019

ICS 03.220.01; 35.030; 35.240.60

English Version

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

Systèmes intelligents de transport - Interface véhicule sécurisée - Services de sécurité de la station ITS pour l'établissement et l'authentification des sessions sécurisées (ISO/TS 21177:2019)

Intelligente Verkehrssysteme - Sicherheitsdienste für eine ITS-Station zum sicheren Aufbau und Authentizierung einer Sitzung zwischen zuverlässigen Geräten (ISO/TS 21177:2019)

This Technical Specification (CEN/TS) was approved by CEN on 13 August 2019 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

© 2019 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. CEN ISO/TS 21177:2019 E

Documents
Document Sharing Hub

Full document details: PD CEN ISO/TS 21177:2019

European foreword

This document (CEN ISO/TS 21177:2019) has been prepared by Technical Committee ISO/TC 204 "Intelligent transport systems" in collaboration with Technical Committee CEN/TC 278 “Intelligent transport systems” the secretariat of which is held by NEN.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO/TS 21177:2019 has been approved by CEN as CEN ISO/TS 21177:2019 without any modification.

Documents
Document Sharing Hub

Full document details: PD 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

© ISO 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 21177:2019

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 Apdu ... 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

Documents
Document Sharing Hub

© ISO 2019 – All rights reserved

Full document details: PD CEN ISO/TS 21177:2019

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**

© ISO 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 21177:2019

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*.

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.

© ISO 2019 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 21177:2019

Introduction

This document is about ITS station security services required to ensure the authenticity of the source and confidentiality and integrity of application activities taking place between ***trusted devices***.

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.

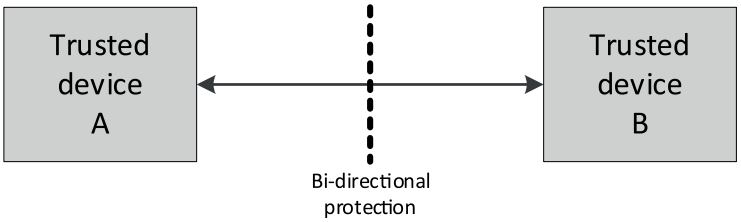

Figure 1 — Interconnection of trusted devices

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-SCU) 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[15], 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[5] and ISO 17419. Station-internal management communications between ITS-SCUs of the same ITS-SU is specified in ISO 24102-4[7]. 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 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, e.g. sustainability, road safety and transportation efficiency.

Over the last decade, ITS services have arisen that require secure access to data from Sensor and Control Networks (SCN), e.g. from In-Vehicle Networks (IVN) and from Infrastructure/Roadside Networks (IRN), some of which require secure local access to time-critical information; see Figures 2 and 3.

© ISO 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 21177:2019

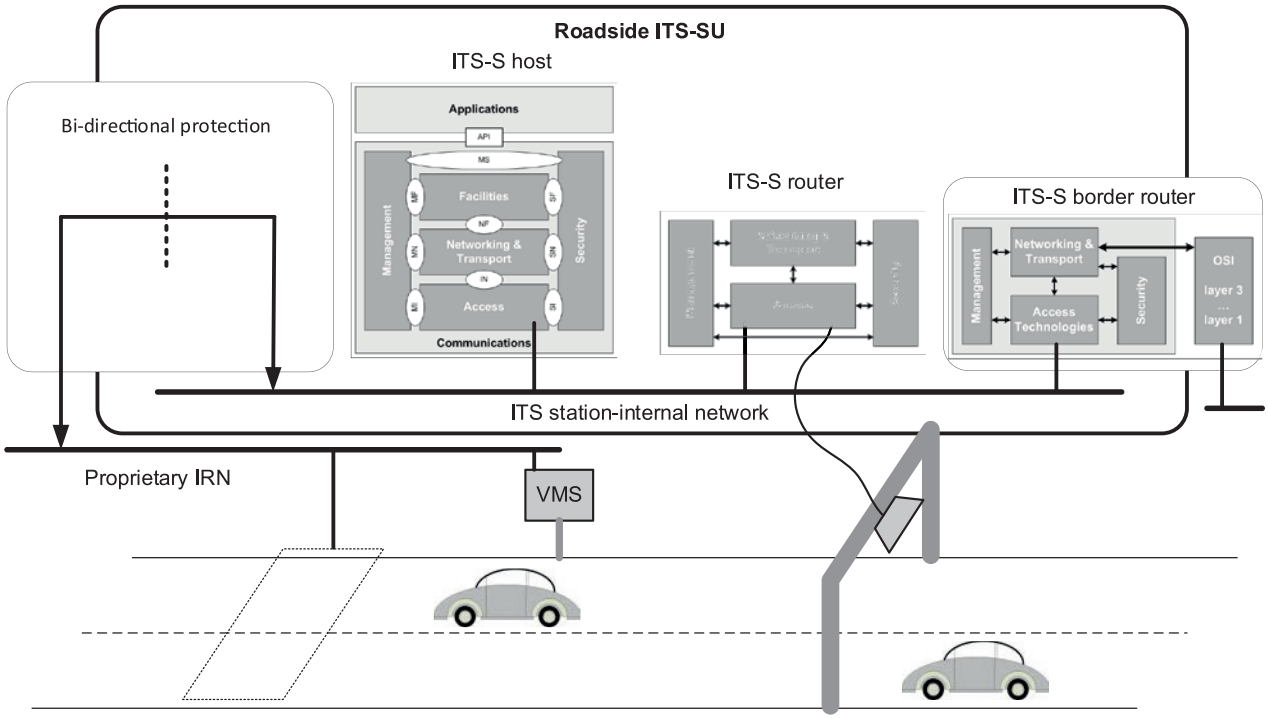

Figure 2 — Example of a roadside ITS-SU connected with proprietary IRN

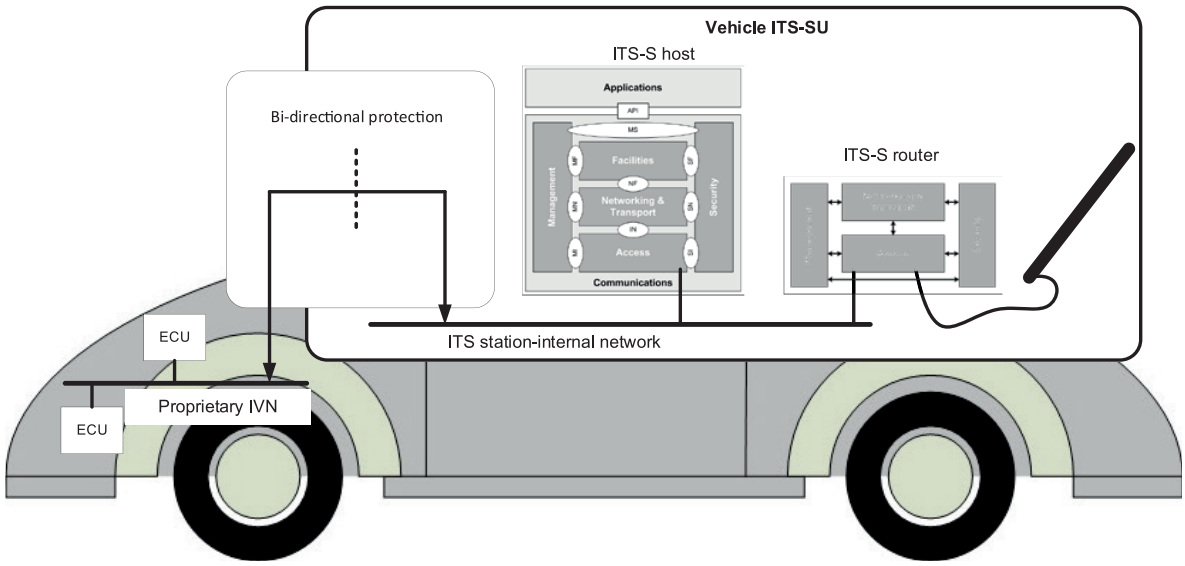

Figure 3 — Example of a vehicle ITS-SU connected with proprietary IRN

Trust in the ITS domain primarily is between ITS Station Communication Units (ITS-SCUs) introduced in ISO 21217; see Figure 4.

© ISO 2019 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 21177:2019

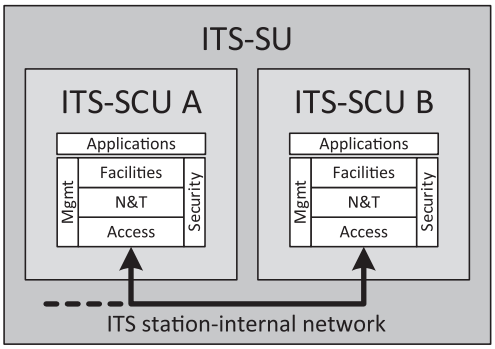

Figure 4 — Interconnection of ITS-SCUs in an ITS-SU

ITS-SCUs are interconnected via an ITS station-internal network. Applying basic security means specified in this document, the ITS-SCUs trust each other. Additionally, protocol data units exchanged between ITS-SCUs may be further protected by additional means, e.g. applying encryption. Major application domains of secure communications between ITS-SCUs of the same ITS-SU are local station management specified in ISO 24102-1[4] using station-internal management communications specified in ISO 24102-4[7].

Trust in the ITS domain further is between ITS-SUs introduced in ISO 21217; see Figure 5.

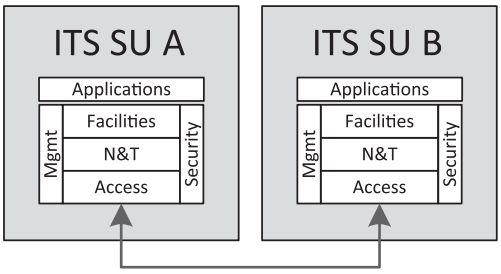

Figure 5 — Interconnection of ITS-SUs

Applying basic security means specified in this document, the ITS-SUs can establish secure application sessions. Establishment of sessions either needs a-priori knowledge about a session partner or can be achieved by means of service announcement specified in ISO 22418[3]. Further on, broadcast of messages is secured by means of authenticating the sender of such a message, applicable for the service advertisement message (SAM) specified in ISO/TS 16460[1] and used in ISO 22418[3]. Additionally, other security means may be applied, e.g. encryption of messages.

A further trust relation in the ITS domain is between an ITS-SU consisting of one or several ITS-SCUs and a sensor and control network (SCN). Trust is achieved by applying security means in an interface as illustrated in Figure 6 with details specified in this document.

© ISO 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 21177:2019

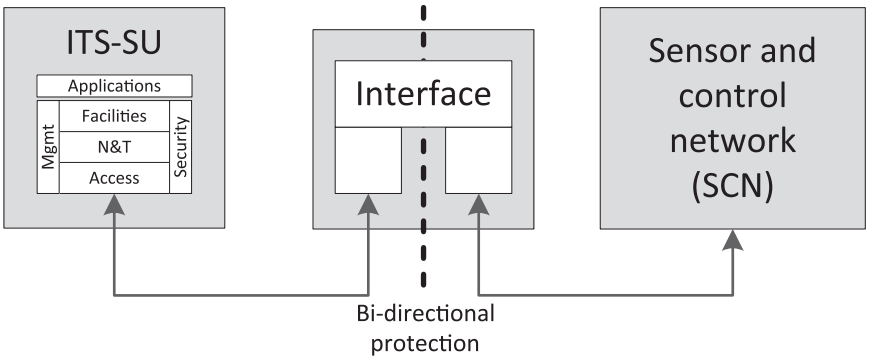

Figure 6 — Interface between ITS-SU and sensor and control network

The interface presented in Figure 6 may be a stand-alone device, or may be integrated in the ITS-SU, or may be part of the SCN. Examples of SCNs are "In-Vehicle Networks" (IVN) and "Infrastructure/ Roadside Networks" (IRN).

Related use cases of these ITS services have largely been derived from regulatory requirements and ITS operational needs, and they include:

— secure real-time access to time-critical vehicle-related data for safety of life and property applications, e.g. collision avoidance, emergency electronic brake light and event determination;

— secure local access to detailed real-time data for efficiency applications (traffic management), e.g. intersection interaction, congestion avoidance, dynamic priorities;

— protection of private data, e.g. in compliance with the European "General Data Protection Regulation" (GDPR)[16];

— local access to certified real-time data for sustainability applications, e.g. dynamic emission zones (controlled zones as currently standardized in CEN TC 278 within the Project Team PT 1705 funded by the European Commission), intersection priorities based on emissions, interactive optimum vehicle settings to minimize fuel consumption.

There are many use cases of ITS services currently identified where real-time exchange of time-critical information between ITS-SUs in close proximity is essential, and the number will grow, see e.g. the US National ITS Reference Architecture[17]. It is critical that ultimately all ITS-SUs in a given area are able to be engaged in these distributed services. This, in turn, requires vehicle ITS-SUs to have real-time access to vehicle data, and roadside ITS-SUs to have real-time access to infrastructure data. All ITS-SUs need being capable of secure software updates.

According to ISO 21217, an ITS-SCU of an ITS-SU can communicate with devices that, in a strict sense, are not compliant with the architecture specified in ISO 21217. However, in order to have trusted communications, a certain minimum level of security measures must be shared between an ITS-SCU and such an external device. Examples of such external devices are a node in the Internet, or a node in a sensor and control network. In this document, the assumption is made that ITS-S application processes operating on ITS-SUs are issued with *certificates* by a Certificate Authority (CA), and that the CA is a trusted third party in the sense that before issuing the certificate to the ITS-S application process, it ensures that the ITS-SU on which the ITS-S application process is resident meets the minimum security requirements for that application. This allows peer ITS-S application processes which observe that an ITS-S application process possesses a valid certificate to have a level of assurance that the ITS-S application process is in fact secure and trustworthy.

© ISO 2019 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 21177:2019

The subject of this document thus is three-fold:

1) Specify ITS station security services for enabling trust between ITS-S application processes running on different ITS-SCUs of the same ITS-SU, i.e. establishing a trusted processing platform, considering also trust inside an ITS-SCU:

   — protection of applications from the actions of other applications;

   — protection of shared information;

   — protection of shared processing resources such as communications software and hardware, which includes methods of prioritisation and restricted access.

2) Specify ITS station security services for enabling trust between ITS-S application processes running on the same ITS-SU.

3) Extend these ITS security services for enabling trust between an ITS-SCU and devices being part of a sensor and control network.

NOTE 3 It is intended to extend the subject of this document in future editions.

Such security services include e.g. the basic security features of:

a) authentication and authorisation;

b) confidentiality and privacy;

c) data integrity;

d) non-repudiation.

Tasks related to communications are:

a) establishing secure sessions for bi-directional communications, e.g. based on service advertisement specified in ISO 22418[3];

b) authenticating a sender of broadcast messages, e.g. CAM, DENM, BSM, SPaT, MAP, FSAM, WSA;

c) encrypting messages.

NOTE 4 Tasks b) and c) above related to communications are already specified in other standards, see e.g. IEEE Std. 1609.2™ and several related standards from ETSI TC ITS.

© ISO 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 21177:2019

Documents
Document Sharing Hub

Full document details: PD CEN ISO/TS 21177:2019

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

1 Scope

This document contains specifications for a set of ITS station security services required to ensure the authenticity of the source and integrity of information exchanged between trusted entities:

— devices operated as bounded secured managed entities, i.e. "ITS Station Communication Units" (ITS-SCU) and "ITS station units" (ITS-SU) specified in ISO 21217, and

— between ITS-SUs (composed of one or several ITS-SCUs) and external trusted entities such as sensor and control networks.

These services include authentication and secure session establishment which are required to exchange information in a trusted and secure manner.

These services are essential for many ITS applications and services including time-critical safety applications, automated driving, remote management of ITS stations (ISO 24102-2[5]), and roadside/infrastructure related services.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 17419, *Intelligent transport systems — Cooperative systems — Globally unique identification*

IEEE Std 1609.2™, *IEEE Standard for Wireless Access in Vehicular Environments — Security Services for Applications and Management Messages*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
Access Control PDU
PDU generated by the Security Subsystem for purposes of establishing the authorisation status of a peer ITS-S application process

3.2
Access Control Policy
data source governing what access to resources is permissible by peer Applications

© ISO 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 21177:2019

3.3
application
functional entity, i.e. an ITS-S application process

3.4
security subsystem
functional entity providing security functionality for use by an ITS-S application process

3.5
Security Adaptor Layer
functional entity providing multiplexing and demultiplexing functionality for data and session control commands

3.6
Secure Session
functional entity providing confidentiality, integrity, authentication, guaranteed in-order delivery, and replay protection on the datagrams that are passed over it

3.7
resources
functional entity constituting endpoints of ITS-S application process activity

3.8
Cryptomaterial Handle
reference to Cryptomaterial allowing that Cryptomaterial to be used in cryptographic operations, i.e. sign, verify, encrypt, decrypt

3.9
Cryptomaterial
cryptographic keys and associated material, either a secret key for a symmetric algorithm, or a private key for an asymmetric algorithm, and the associated public key or certificate

3.10
Secure Session Service
functional entity responsible for establishing secure communications sessions with its peer instances

4 Symbols and abbreviated terms

ACK	acknowledge
ALPDU	adaptor layer PDU
APDU	application protocol data unit
DTLS	datagram TLS
ID	identifier
IRN	infrastructure/roadside network
ITS	intelligent transport systems
ITS-S	ITS station [SOURCE: ISO 21217:2014]
ITS-SCP	ITS station communication profile Note to entry: From ISO 21217

© ISO 2019 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 21177:2019

ITS-SU	ITS station unit [SOURCE: ISO 21217:2014]
IVN	in-vehicle network
OSI	open system interconnection
OTP	one time password
PDU	protocol data unit
PDU	protocol data unit
PSID	provider service identifier
SAM	service advertisement message [SOURCE: ISO/TS 16460]
SCN	sensor and control network
SDEE	secure data exchange entity
SPAKE2	secure password authenticated key exchange 2
SRM	service response message [SOURCE: ISO/TS 16460]
SSP	service specific permission
SSTD	secure session between trusted devices
TLS	transport layer security

5 Overview

5.1 Goals

Clause 5 presents the logical architecture followed in this document. The logical architecture is designed to accomplish the following goals:

— Two peer ITS-S application processes can communicate securely, i.e. in an authorized, integrity protected and confidential manner.

— The ITS-S application processes can authenticate to each other using role- or attribute-based access control.

— Each individual incoming application protocol data unit (APDU) can be subject to individual access control processes.

— The security state of the connection (i.e. the authentication status of one ITS-S application process with respect to access to the other connection) can be updated within the secure session as follows.

— An ITS-S application process can prove to the other that it knows a shared secret (Enhanced Authentication, see 7.3) — the intended use of this is to allow the owner or other legitimate operator of one ITS-S application process to permit access by a specific peer ITS-S application process, see Clause 6 for further discussion.

© ISO 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 21177:2019

— An ITS-S application process can provide additional authentication within the secure session (Extended Authentication, see 7.4) — for example to provide an identity as well as application permissions, or to provide additional application permissions.

— Secure session communication uses the same credentials as ITS-S application processes use.

— An ITS-S application process can configure a secure session so that it terminates under specific conditions (e.g. timeouts of different kinds) and can also terminate the secure session directly.

— To allow secure and private service discovery, the initialization stage (the “handshake”) of one secure session between two peer ITS-S application processes can be proxied over an existing secure session between two different peers.

5.2 Architecture and functional entities

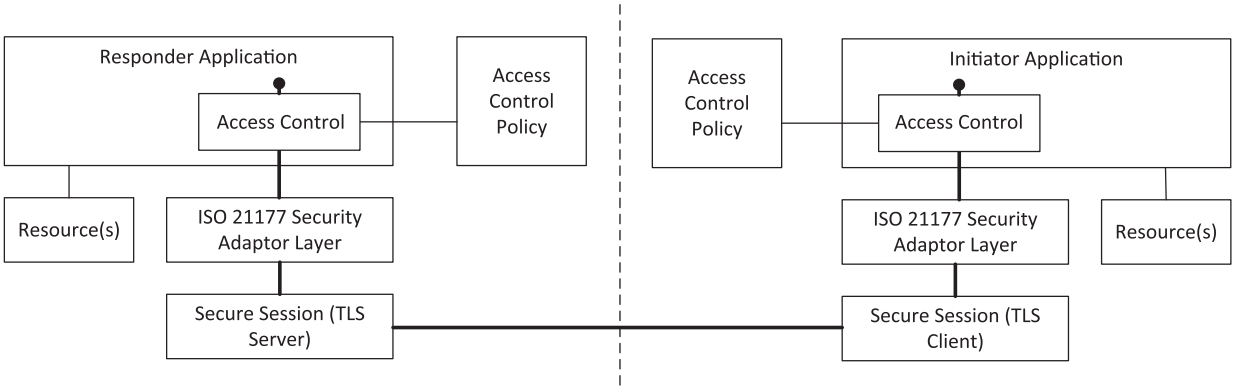

Figure 7 — Logical Architecture

Figure 7 shows the functional entities and data sources involved in secure communications between pairs of ITS-S application processes using mechanisms specified in this document. A pair of ITS-S application processes can reside

— either on the same ITS-SCU,

— or in different ITS-SCUs of the same ITS-SU,

— or in different ITS-SUs,

— or in an ITS-SU and another trusted entity not being a dedicated ITS device.

This description refers in general to activities on the “home trusted entity" and the “peer trusted entity".

NOTE 1 If an entity is described as “fully specified in this document”, that includes the case where some of the specification is in external documents that are incorporated in this document by reference.

Functional entities are:

— **Resources:** These are endpoints of ITS-S application process activity and may be inside or outside the ITS-SU on which the ITS-S application process resides.

— **Application:** This is an ITS-S application process that uses input from resources, from a peer ITS-S application process (peer Application), and from its own state to carry out application activities.

NOTE 2 To simplify reading of this document, the term "Application" is used as a replacement for "ITS-S application process", where appropriate. The term "application" is used in its generic meaning.

— **Security Subsystem:** The security subsystem applies security mechanisms to determine what actions the peer Application is permitted to take and implements support functionality in support

© ISO 2019 – All rights reserved
AVA Documents Document Sharing Hub
Full document details: PD CEN ISO/TS 21177:2019

of making those decisions. The Security Subsystem contains some non-application-specific functionality, specified in this document, and also application-specific functionality (it has to understand the semantics of application PDUs in order to make access control decisions); as such, it is shown within the Application in Figure 7.

The Security Subsystem is configured using input from the Access Control Policy data source. For outgoing communications, it takes as input commands and data from the Application and applies appropriate security processing. For incoming communications, it takes as input commands and data from the Security Adaptor Layer and applies the appropriate access control policy; as a result of applying the access control policy it either passes the input to the application or generates an access control response. See Clause 7.

The Security Subsystem in its own turn contains two distinct functional elements: the Authentication State Subsystem and the Access Control Subsystem. The Authentication State Subsystem stores the authentication state of the secure session, and can also generate Access Control request PDUs to enable this state to be updated. The Access Control Subsystem makes decisions on the permissibility of actions requested by the peer entity in the secure session, using the authentication state as an input. This document defines the Authentication State Subsystem in full, as this system is not application-specific. The Access Control Subsystem is part of the application specification for an individual application and is defined as part of that specification..

— **Security Adaptor Layer:** This is a multiplexer/demultiplexer that allows both data, i.e. communications between the Applications themselves, and session control commands, i.e. communications between peer instances of Security Subsystem or the Security Adaptor Layer, to be sent over the same secure session. See Clause 8.

— **Secure session:** This provides confidentiality, integrity, authentication, guaranteed in-order delivery, and replay protection on the datagrams that are passed over it. In this version of this document there are two types of secure session:

  — **Cryptographic secure session:** this uses cryptography to achieve the listed security properties. Any secure session which passes outside the secure boundary of the ITS-SU shall be a cryptographic secure session. In this version of this document the only supported cryptographic secure session mechanism is TLS 1.3 with certificates specified in IEEE Std. 1609.2™. See Clause 9.

  — **Physical secure session**: this is a session between two Applications running in the same ITS-SU, i.e. the information flow does not pass outside the ITS-SU secure boundary. In this case, because the ITS-SU is a trusted domain, all the security properties listed above are assumed to hold. This document does not provide a specification of a physical secure session but permits the use of a physical secure session.

The "Access Control Policy" data source governs whether a secure session is cryptographic, physical, or both.

Data sources are:

— **Access Control Policy**: Governs what access to resources is permissible by peer applications communicating via the mechanisms in this document. Used as input by the Security Subsystem functional entity. Data from the Access Control Policy is provided to the Secure Session functional entity to configure secure sessions. This document does not provide a specification of the Access Control Policy language.

The relationships between instances of these functional elements and data sources on a single trusted entity are shown in Figure 8. In Figure 8, heavy arrows between functional elements indicate flows containing information that is exchanged with processes on the peer trusted entity, and light arrows with dots between functional elements indicate control flows within the home ITS-SU. Grey dashed arrows within functional elements indicate relationships between different data flows handled by those functional elements.

© ISO 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 21177:2019

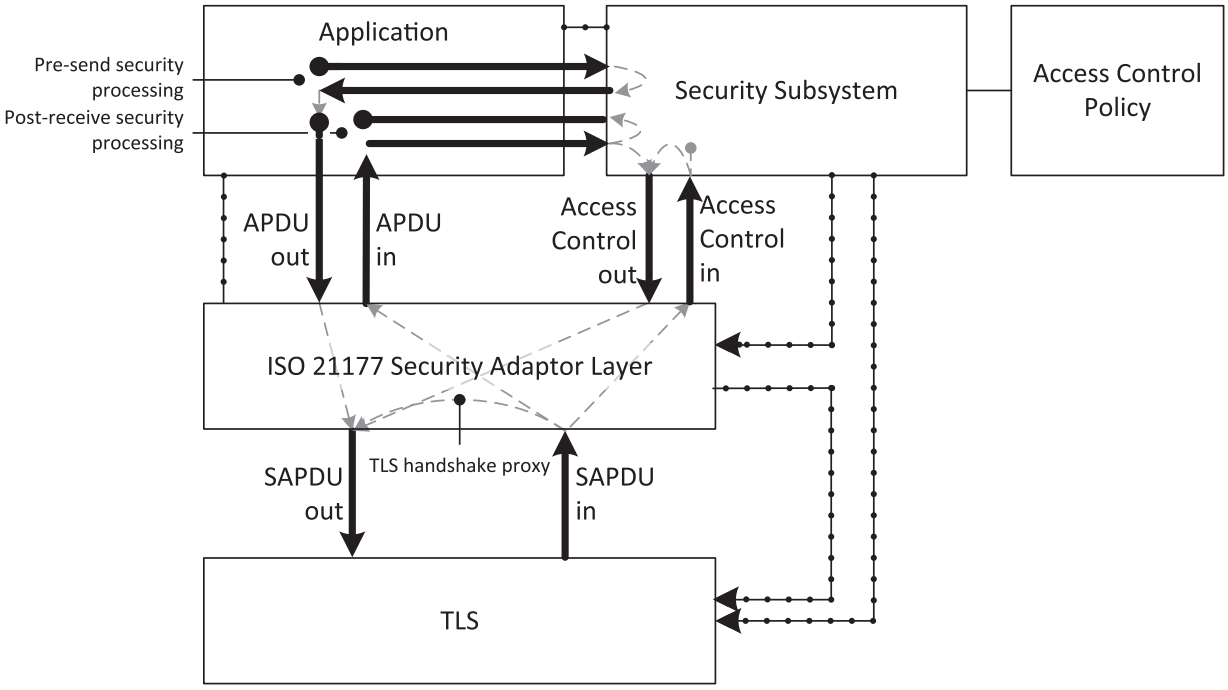

Figure 8 — Interactions between local functional elements

— The **Application** acts as a source and a sink for APDUs.

— The **Application-Security Subsystem** interface is specified in 7.5. It is used:

  — Optionally, by the Application, to request IEEE 1609.2 application-level processing for outgoing APDUs specified in IEEE Std. 1609.2™as described in 6.6.

  — By the Application, to request that access control services are applied to activities that might be carried out as a result of incoming APDUs. Specifically, in this document, the interface provided is an internal interface between the Authorization State Subsystem and the Access Control Subsystem that allows the Access Control Subsystem to request the authorization state. A full application specification also contains a specification of the interface between the Application and the Access Control Subsystem that allows the Application to request access control decisions and provide full context. This second interface is application-specific and is not provided in this document.

  — By the Application, to configure, end, and deactivate secure session services.

  — By the Security Subsystem, to notify the Application of a decision to end or deactivate secure session services.

— The **Security Subsystem** is specified in Clause 7. It acts as:

  — A source for outgoing Access Control commands, which may be generated without a trigger or in response to incoming Access Control commands or APDUs.

  — A sink for incoming Access Control commands, which may result in the Security Subsystem updating its state or in the Security Subsystem generating an outgoing Access Control commands (or both).

  — A source and a sink for security configuration commands.

— The **Security Subsystem-Adaptor Layer** interface is specified in 8.4. It is used to exchange APDUs and Access Control PDUs between the Adaptor Layer and the other functional entities, and for the Application or Security Subsystem to control and configure the Adaptor Layer.

© ISO 2019 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 21177:2019

- The **Adaptor Layer** is specified in Clause 8. It:
  - Wraps outgoing APDUs and outgoing Access Control PDUs as security Adaptor Layer Protocol Data Units (ALPDUs) and passes them to the Secure Session service.
  - Acts as a proxy for TLS handshake PDUs as specified in 6.9.
  - Inspects incoming ALPDUs and
    - Unwraps incoming APDUs and incoming Access Control PDUs and passes them to the Security Subsystem.
    - Proxies incoming TLS handshake proxy PDUs as specified in 6.9.4.
- The **Security Subsystem-Secure Session service** interface is specified in 9.2. It is used to control and configure persistent properties of the Secure Session service.
- The **Adaptor Layer-Secure Session service** interface is specified in 9.5. It is used to control and configure session-specific properties of the Secure Session service.
- The **Secure Session service** is specified in Clause 9. In this version of this document it is required to be based on TLS, DTLS, or physical secure sessions. It:
  - Receives ALPDUs from the Security Adaptor Layer and treats them as application input to record layer operations, performing outgoing TLS processing on them.
  - Receives secure session datagrams from the network stack and performs incoming TLS processing on them, resulting in ALPDUs which the TLS service passes to the Security Adaptor Layer.

5.3 Cryptomaterial handles

This document uses the concept of Cryptomaterial Handles specified in IEEE Std 1609.2™ to represent logical access to cryptographic keys and, if appropriate, their associated certificates. The reader is referred to IEEE Std 1609.2™ for more details.

5.4 Session IDs and state

The Security Subsystem service, Adaptor Layer service, and Secure Sessions service maintain state information of each (application, session)-tuple.

NOTE The interfaces presented in this document are passing (application ID, session ID)-tuples to the relevant primitives.

Unique identification of an instance of an ITS-S application process of an ITS application is by means of the identifier ITS-SAPIID of ASN.1 type `ITSapiid` specified in ISO 17419.

An implementation shall ensure that state information corresponding to a specific (application, session)-tuple is not made available for use by activities corresponding to a different (application, session)-tuple except through the interfaces defined in this document.

In the case where an Application has the role of the client in a secure session, the session ID is generated by this Application. The Application ensures that the session ID is unique among active sessions for that Application. The Application supplies the session ID to the client via the `App-Sec-Configure.request` and `Sec-Sess-Configure.request` primitives.

In the case where an Application has the role of the server in a secure session, the session ID is generated by the server in response to an incoming connection. The server ensures that the session ID is unique among active sessions for that application. The session ID is provided to the application using the `Sec-Sess-StartSession.indication` and `App-Sec-StartSession.indication` primitives.

© ISO 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 21177:2019

5.5 Access control and authorisation state

The Security Subsystem maintains the authorisation state of the session. The authorisation state is the collection of all “authorisation statements” made by the peer party which were valid at the time made and which have not timed out (where the timeout conditions are set by the access control policy). An "authorisation statement" is any PDU sent by the peer party that contains cryptographically protected information about the authorisation of that peer party. Specifically, in this document, the authorisation statements presented in Table 1 are defined.

Table 1 — Authorisation statements

Type	Description	Related subclauses	Service primitives for provision to Security Subsystem
Initial authorisation	The credentials presented during the handshake of the secure session, if one occurs	6.5	`Sec-Sess-StartSession.indication`
Enhanced authorisation	A demonstration that the peer party shares a secret value with the home party, presented during the secure session via an Access Control PDU of type `EnhancedAuthPdu` as specified in 7.5.11	6.7, 6.8, 7.3	`Sec-AL-AccessControl.indication`
Extended authorisation	Additional credentials presented during the secure session via an Access Control PDU of type ExtendedAuthPdu as specified in 7.5.5.	6.7, 6.8, 7.4	`Sec-AL-AccessControl.indication`

This document defines Access Control Request PDUs and Access Control Response PDUs in 7.5.

An Access Control PDU containing an extended authorisation statement may be generated in response to an Access Control Request PDU or may be generated without a request. An Access Control PDU containing an enhanced authorisation statement is always made in response to an Access Control PDU containing an enhanced authorisation request. Sending Access Control PDUs is specified in 6.7. Receiving Access Control PDUs is specified in 6.8.

Exactly how the authorisation statements are used by the Security Subsystem and governed by the Access Control Policy is to be specified in the specification of an application that uses the mechanisms provided by this document.

5.6 Application level non-repudiation

An Application may apply non-repudiation to individual application PDUs by signing them with the mechanisms of IEEE 1609.2. An Application that applies non-repudiation to individual APDUs shall format any non-signed APDUs as Ieee1609Dot2Data structures of type unsecured, to ensure consistent interpretation of the incoming APDUs. A detailed specification of this process is provided in 6.6 for outgoing APDUs and 6.8 for incoming APDUs.

5.7 Service primitive conventions

This document uses service primitives to specify information flows between functional entities, i.e. information flows through "Service Access Points" (SAPs). This document is organized such that each functional entity is specified in a separate clause:

— Security Subsystem in Clause 7,

— Adaptor Layer in Clause 8,

— Secure Session services in Clause 9.

© ISO 2019 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 21177:2019

NOTE ISO 24102-3[6] specifies service primitives and service primitive functions for various SAPs introduced in ISO 21217 at the level of ASN.1 type definitions. The service primitive functions identified in this document can be used to complement the specifications in ISO 24102-3[6].

Service primitives are not testable but indicate the information that one functional entity must make available to another in order for the second functional entity to carry out the indicated activities.

Following the conventions of the layered OSI model specified in ISO/IEC 7498-1[10], in this document, a message from a higher layer entity to a lower layer entity is specified with an

— `XXX.request` service primitive of the service *XXX*,

and the response is specified with an

— `XXX.confirm` service primitive.

Similarly a message from a lower layer entity to a higher layer entity is specified with an

— `XXX.indication` service primitive,

and the response from the higher layer entity to the lower layer entity is specified with an

— `XXX.response` service primitive.

The information contained in a service primitive is referred to as "service primitive function"; see ISO 24102-3[6].

This document uses the convention that a `.confirm` service primitive can be correctly associated with its corresponding `.request` service primitive, and a `.response` service primitive can be correctly associated with its corresponding .indication service primitive. In other words, for example, a `.confirm` primitive's parameters do not include an identifier for the corresponding `.request` primitive; the recipient of the `.confirm` primitive is assumed to "just know" which `.request` primitive it is associated with.

6 Process flows and sequence diagrams

6.1 General

Clause 6 specifies process flows supported by the security services specified in this document and the sequence of data flows associated with each of these process flows.

6.2 provides an overview on process flows. 6.3 presents state diagram conventions.

6.2 Overview of process flows

This document supports the following process flows; see Annex A for use cases that make use of these process flows:

— Configure, see 6.4: Prepare the functional elements to participate in secure communications.

— Start Session, see 6.5: Perform processing once a secure session has been established but before data is exchanged.

— Send data, see 6.6: Send data from the home Application to the peer Application.

— Send Access Control PDU, see 6.7: Exchange messages between the home Security Subsystem and the peer Security Subsystem with a goal of updating the state of one or both.

— Receive PDU, see 6.8: Receive an APDU, an Access Control PDU, or a proxied TLS handshake packet.

© ISO 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 21177:2019

— Secure connection brokering, see 6.9: Proxy a TLS handshake between two other applications, one of which already has a secure connection to the home Application and one of which already has a secure connection to the peer Application.

— Force end session, see 6.10: Terminate a secure session between the home Application and one peer Application, with the termination initiated by the Application or the Security Subsystem.

— Session terminated at session layer, see 6.11.

— Deactivate, see 6.12: Prevent the functional elements from starting any more sessions with the current set of parameters.

An example of how these process flows are combined to create a full secure session, start to end, is given in 6.13.

6.3 Sequence diagram conventions

The sequence diagrams follow the following graphical conventions. In this description the word "message" is used in the UML sequence diagram sense of a communication between two participants and is not meant to imply any over the air communications.

— In each sequence diagram, each message between participants is associated with a descriptive name and with the identifier of the service primitive that is used to implement that message. For example, in the clipping of Figure 9, the message contains an APDU and is sent using the primitive `App-Sec-Data.request`, see 7.6.4.

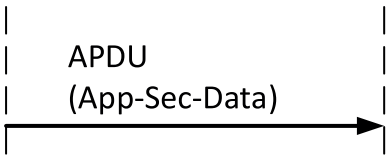

Figure 9 — Convention for sequence diagram — 1

— If the descriptive name is in italics, it is associated with a local message, i.e. a message that does not directly contain data that has passed or is intended to pass to the peer trusted entity. For example, in the clipping of Figure 10, the message *configure* contains only local information and is sent using the `App-Sec-Configure.request` service primitive.

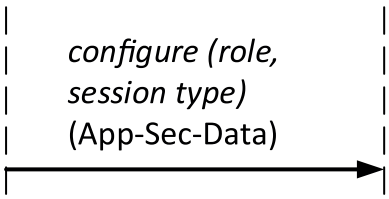

Figure 10 — Convention for sequence diagram — 2

— **Mapping to primitives**: See 5.7 on service primitive conventions. In the sequence diagrams presented in Clause 6, the suffixes `.request`, `.confirm`, `.indication` and `.response` are omitted for compactness. In addition, also for compactness, the `.confirm` and `.response` service primitives are not shown in the diagrams of Clause 6 unless they are significant information flows (in other words, amount to anything other than an ACK). In all cases, the description of the diagrams includes the service primitive suffixes and describes whether the `.confirm` and `.response` service primitives are used as anything other than an ACK.

© ISO 2019 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 21177:2019

6.4 Configure

In this process flow the Application configures the Security Subsystem with configuration information necessary to run the secure communications.

The process steps for this process flow are:

a) The Application uses the `App-Sec-Configure.request` primitive, see 7.6.1, to inform the Security Subsystem of:

   1) The role it has in the secure session (client or server).

   2) The socket to be used for communications with the peer trusted entity (this is pass-through information for the Secure Session service). This includes an indication of whether the other endpoint is inside or outside the secure boundary. This socket is not used by the Security Subsystem but is passed on to the Secure Session services via `Sec-Sess-Configure.request`.

   3) If the other endpoint is outside the secure boundary, i.e. if cryptographic security mechanisms are to be used to protect the session:

      i) whether the socket shall be used for reliable or unreliable communications (i.e. TLS or DTLS);

      ii) which cryptomaterial handle should be used for authentication of the secure session.

b) The Security Subsystem:

   1) Uses the Access Policy to determine what secure session types are permitted. In this version of this document, three secure session types are permitted:

      — TLS for reliable transport mechanisms;

      — DTLS for unreliable transport mechanisms;

      — No specific security mechanism for communications sessions within a secure boundary of an ITS-SCU (which are secure by assumption).

   2) Acknowledges the request from the Application using `App-Sec-Configure.confirm`, see 7.6.2, (not shown in the diagram). This may include an indication that the secure session type requested (physical versus cryptographic) is not permitted for this Application by the access control policy. If the secure session type is not permitted, the sequence terminates here. Otherwise, go to the next step.

   3) If a cryptographic secure session is requested, uses the `Sec-Sess-Configure.request`, see 9.3.1, to pass the following to the secure session service:

      i) From the application:

         I) role,

         II) cryptomaterial handle,

         III) socket type.

      ii) From the access control policy:

         I) The permissions constraints to apply to incoming 1609.2 certificates.

         II) The SDEE Identifier used to identify the Application to the 1609.2 Secure Data Service.

         III) The timeout parameters for the session:

            — How long the session may be inactive before a fresh handshake is required.

            — How long the session may be active before a fresh handshake is required.

© ISO 2019 – All rights reserved

AVA Documents Document Sharing Hub
Full document details: PD CEN ISO/TS 21177:2019

— If the Secure Session services are playing a server role, how long the service shall be open to incoming requests.

c) The Secure Session service uses `Sec-Sess-Configure.confirm`, see 9.3.2, to ACK the exchange.

A sequence diagram for this process flow is given in Figure 11.

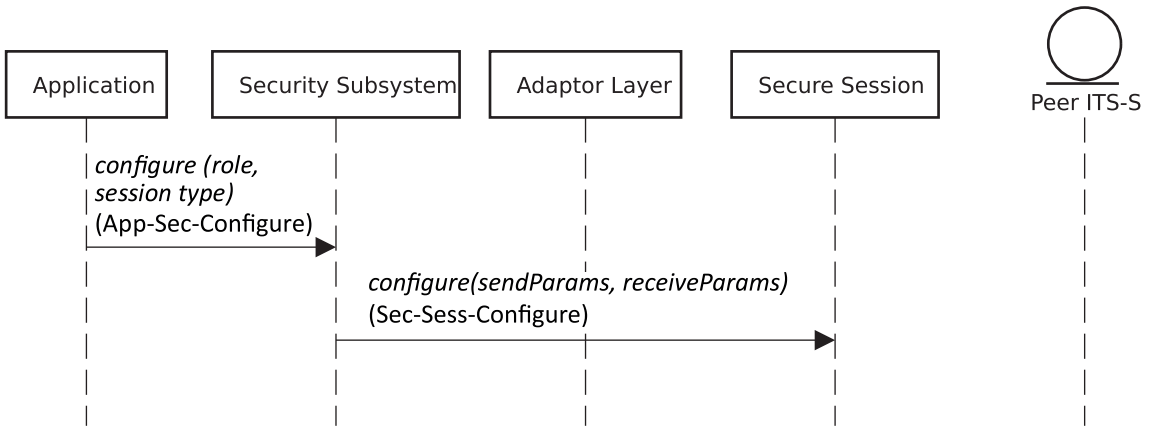

Figure 11 — Sequence diagram for Configure process flow

NOTE To change the key (the cryptomaterial handle) to be used for sessions, the application or security subsystem can Deactivate the current Secure Session instance as specified in 6.11 and Configure a new Secure Session instance using the mechanisms of this sub-clause.

6.5 Start Session

In this process flow, following a handshake between the Secure Session service on the home ITS-SU and the Secure Session Service on the peer trusted entity, the Secure Session service provides the Security Subsystem with the credentials received from the peer trusted entity and the Security Subsystem initiates any additional Access Control activities that the Access Policy specifies must complete before data can be exchanged.

In the case of a physical secure session, the session may start without credentials being exchanged. In this case the extended authentication mechanisms of this document may be used to send credentials during the session.

Prequisite:

— The Secure Session is a secure session as defined in 5.2.

— The Secure Session service has been configured using the methods of 6.4.

— The certificate received in the handshake of the secure session (if applicable) matches the constraints provided to the Secure Session service during the Configure process flow.

The process steps for this process flow are:

a) The local Secure Session Service uses the `Sec-Sess-StartSession.indication` service primitive to communicate with the Security Subsystem, see 9.3.3, providing:

1) An indication that the secure session has started and passed the validity conditions that were specified to be checked by the Secure Session Service.

2) The certificate from the Secure Session Service on the peer trusted entity.

© ISO 2019 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 21177:2019

3) If the secure session services are acting in the server role, the Session ID to be used to identify the session; otherwise, the Session ID provided in `Sec-Sess-Configure.request`, see 9.3.1.

b) The Security Subsystem uses the Access Control Policy to determine the status of the incoming connection. The status may be:

1) Success;

2) Unauthorised, communication rejected. In this case the Security Subsystem ends the secure session as specified in 6.10;

3) Additional Access Control actions are necessary. The additional access control actions specified in this document are:

i) Request Extended Authentication, as specified in 7.4.

ii) Request Enhanced Authentication, as specified in 7.3.

c) If additional access control actions are to be carried out or if the policy indicates that success or failure are to be communicated to the peer:

1) The Security Subsystem generates an Access Control PDU and passes it to the Adaptor Layer via the `Sec-AL-AccessControl.request` service primitive, see 8.4.1.

i) In the case where success is being communicated to the peer, this is an Access Control PDU of type `AccessControlResult.success`, as specified in 7.5.4.

ii) In the case where failure is being communicated to the peer, this is an Access Control PDU of type `AccessControlResult.failure`, as specified in 7.5.4.

iii) In the case of Enhanced or Extended Authentication, the contents are as specified in 7.3 and 7.4 respectively.

2) The Adaptor Layer acknowledges the Access Control PDU via the `Sec-AL-AccessControl.confirm` primitive, see 8.4.2.

3) The Adaptor Layer wraps the Access Control PDU in an Adaptor Layer PDU of the appropriate subtype as specified in 8.2.

4) The Adaptor Layer passes the ALPDU to the Secure Session service via the `AL-Sess-Data.request` primitive, see 9.4.1.

5) The Secure Session service acknowledges the ALPDU via the `AL-Sess-Data.confirm` service primitive, see 9.4.2, secures the ALPDU, and passes it to the network stack for transmission.

d) If the status is success and the secure session services are acting in the server role, the Security Subsystem uses the `App-Sec-StartSession.indication` service primitive, see 7.6.3, to provide the session ID to the Application.

Additional access control requests may be sent within the secure session, see 6.7 (sending) and 6.8 (receiving).

A sequence diagram for this process flow is given in Figure 12.

© ISO 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 21177:2019

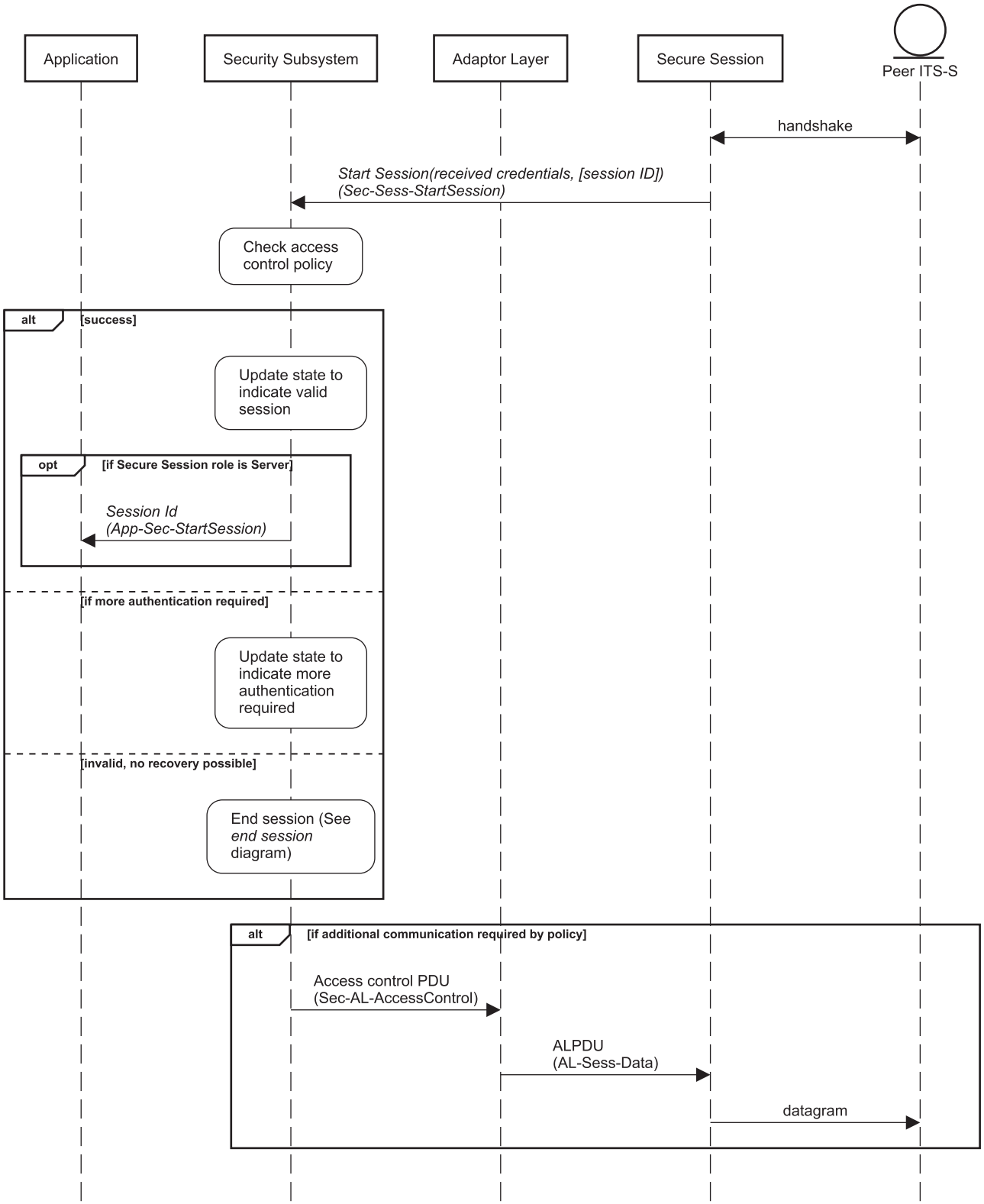

Figure 12 — Sequence diagram for Start Session

6.6 Send data

In this process flow the app on the home ITS-SU sends a datagram over an established ISO/TS 21177 secure session. This sub-clause describes sending activities. The receive-side sequence is specified in 6.8.

© ISO 2019 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 21177:2019

Prerequisites:

— The Secure Session service has been configured using the methods of 6.4.

— If the secure session is a cryptographic secure session as defined in 5.2, there has been an initialize step using the methods of 6.5.

There are two alternate paths for this process flow. In one path, the Application has the option to apply Application-level non-repudiation to individual APDUs. In the other, the Application never applies Application-level non-repudiation to individual APDUs. This document does not provide a mechanism to negotiate which of these paths is followed; this choice is assumed to be a part of the Application specification.

The process steps for this process flow are:

a) If the Application has the option to apply Application-level non-repudiation to individual APDUs:

   1) If the current APDU shall apply non-repudiation, the Application uses `App-Sec-Data.request`, see 7.6.4, to send the APDU to the Security Subsystem for signing. The Security Subsystem returns the signed APDU (or, if appropriate, an error message) via `App-Sec-Data.confirm`, see 7.6.5.

   2) Otherwise, the Application creates an Ieee1609Dot2Data as defined in IEEE 1609.2, of type unsecured, containing the APDU.

b) The Application uses the `App-AL-Data.request` primitive, see 8.3.1, to provide the original APDU or the APDU output from step a), as appropriate, to the Adaptor Layer.

c) The Adaptor Layer:

   1) ACKs the data using `App-Sec-Data.confirm`, see 7.6.5.

   2) Adds the session non-repudiation service if so configured. This service is not specified in this version of this Document but is planned for future versions.

   3) adds the Data header as specified in 8.2, to indicate that the ALPDU is an Application datagram.

   4) The Adaptor Layer provides the data to the Secure Session service via the `AL-Sess-Data.request` primitive, see 9.4.1.

d) The Secure Session service:

   1) ACKs the data using `AL-Sess-Data.confirm`, see 9.4.2;

   2) fragments (if necessary) and cryptographically protects the data and passes it to the network stack for transmission to the peer trusted entity.

A sequence diagram for this process flow is given in Figure 13.

© ISO 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TS 21177:2019

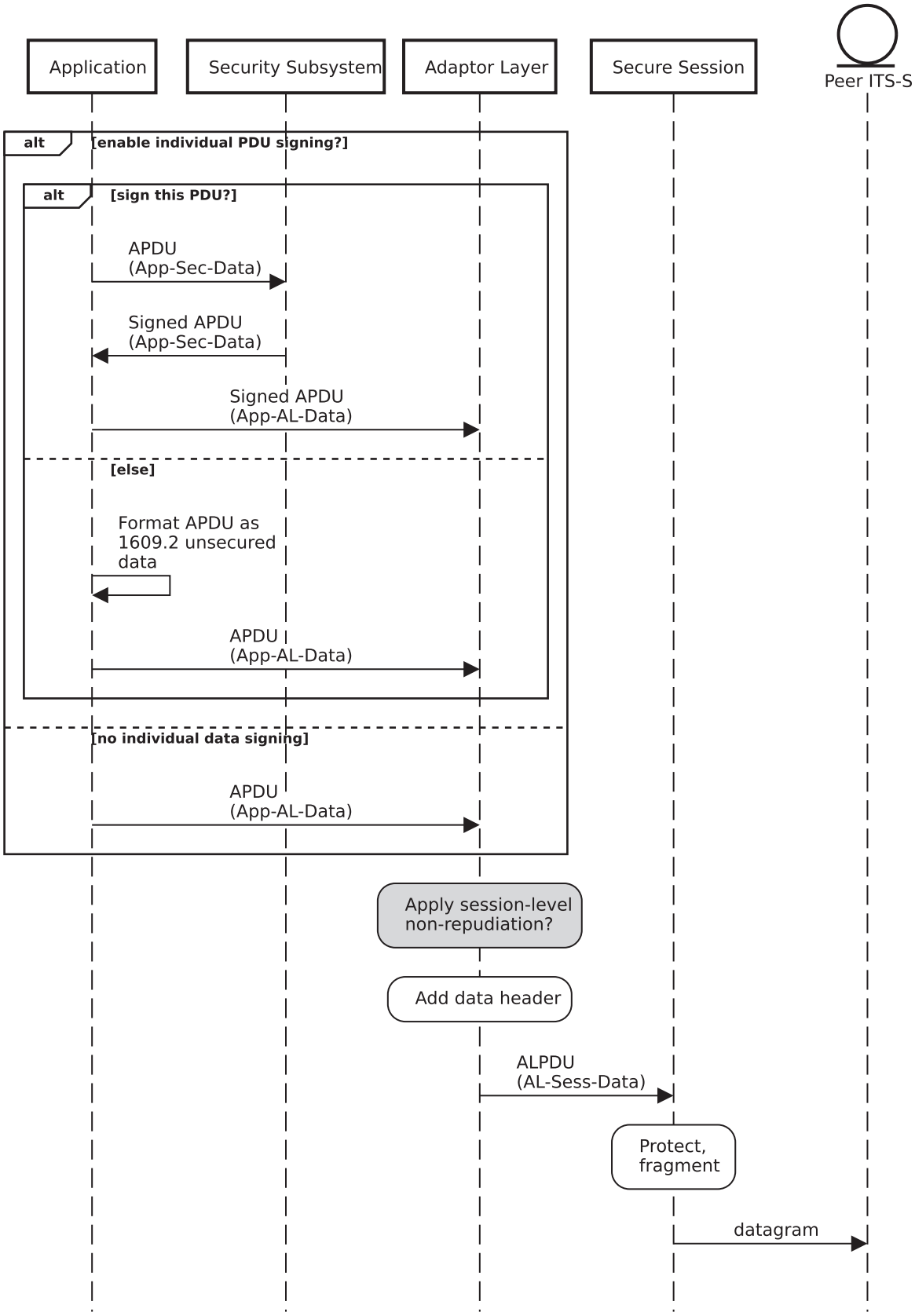

Figure 13 — Sequence diagram for sending data

© ISO 2019 – All rights reserved

Documents
Document Sharing Hub

Full document details: PD CEN ISO/TS 21177:2019