PD CEN ISO/TR 21186-3:2021

BSI Standards Publication

Cooperative intelligent transport systems (C-ITS) – Guidelines on the usage of standards

Part 3: Security

Documents
Document Sharing Hub

Full document details: PD CEN ISO/TR 21186-3:2021

National foreword

This Published Document is the UK implementation of CEN ISO/TR 21186-3:2021. It is identical to ISO/TR 21186-3:2021.

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 committee manager.

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 2021
Published by BSI Standards Limited 2021

ISBN 978 0 539 12426 2

ICS 01.120; 03.220.01; 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 28 February 2021.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: PD CEN ISO/TR 21186-3:2021

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN ISO/TR 21186-3

February 2021

ICS 01.120; 03.220.01; 35.240.60

English Version

Cooperative intelligent transport systems (C-ITS) - Guidelines on the usage of standards - Part 3: Security (ISO/TR 21186-3:2021)

Systèmes de transport intelligents coopératifs (C-ITS) - Lignes directrices pour l'utilisation des normes - Partie 3: Sécurité (ISO/TR 21186-3:2021)

Kooperative intelligente Verkehrssyteme (C-ITS) - Leitfäden zur Nutzung von Normen - Teil 3: Security (ISO/TR 21186-3:2021)

This Technical Report was approved by CEN on 1 February 2021. It has been drawn up by the Technical Committee CEN/TC 278.

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

© 2021 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. CEN ISO/TR 21186-3:2021 E

Documents
Document Sharing Hub

Full document details: PD CEN ISO/TR 21186-3:2021

European foreword

This document (CEN ISO/TR 21186-3:2021) 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.

Endorsement notice

The text of ISO/TR 21186-3:2021 has been approved by CEN as CEN ISO/TR 21186-3:2021 without any modification.

Documents
Document Sharing Hub

Full document details: PD CEN ISO/TR 21186-3:2021

Contents

Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Symbols and abbreviated terms **2**
5 Security in C-ITS **4**
5.1 General 4
5.2 Security design process for C-ITS applications 4
5.3 Communications security mechanisms in C-ITS 5
5.4 Source authentication and access control mechanisms 7
5.5 Certificate authorities and certification processes 10
5.6 Introduction to the rest of this document 11
6 Security analysis and controls for an IDX device **12**
6.1 Background 12
6.2 IDX device concept 12
6.2.1 General 12
6.2.2 System architecture and device 14
6.2.3 Threat modelling data scenarios and examples 16
6.2.4 Assumed device functions and activities 19
6.3 Device assets 22
6.4 Threats 24
6.4.1 General 24
6.4.2 Threat modelling process 25
6.4.3 Threat categories and actor motivations 25
6.4.4 Scenario comparison of threats 27
6.5 Security objectives 29
6.5.1 Summary and comparison by scenario 29
6.5.2 Analysis 31
6.6 SFR and rationales 32
6.7 Comparison to other common criteria PPs 39
6.7.1 General 39
6.7.2 Summary and analysis of gaps 39
6.7.3 Gap analysis with Car2Car HSM PP 39
6.7.4 Gap analysis against V-ITS base PP 41
6.7.5 Gap analysis against V-ITS Comms Module PP 45
7 ISO/TS 21177 access control implementation guidance **45**
7.1 General 45
7.2 High level architecture and access scenario 46
7.3 Application protocol architecture and ISO/TS 21177 integration 47
7.3.1 General 47
7.3.2 Example protocol architecture 47
7.3.3 Protocol integration strategy 49
7.4 Access control policy structure 50
7.5 Access control approach 51
7.6 Access control use cases and sequence diagrams 54
7.6.1 General 54
7.6.2 Define an access policy 54
7.6.3 Load an access control policy 58
7.6.4 Configure TLS 62
7.6.5 Start a secure TLS session 64
7.6.6 Secure access-controlled resource discovery 65

AVA Documents
Document Sharing Hub

© ISO 2021 – All rights reserved

Full document details: PD CEN ISO/TR 21186-3:2021

7.6.7 Server controls access to UGP service based on role ... 73

8 C-ITS CP security requirements gaps and needs ... 77
8.1 General ... 77
8.2 Overview of European C-ITS CP ... 78
8.3 PKI threat categories and mitigations ... 79
8.4 European C-ITS CP changes to support news C-ITS applications ... 90
8.4.1 General ... 90
8.4.2 CP Section 1.6.1 ... 90
8.4.3 CP Section 1.6.2 ... 91
8.4.4 CP Section 6.1.5.2 ... 91
8.4.5 CP Section 4.1.2.4 ... 92

Annex A (informative) **Scenario threats ... 93**

Annex B (informative) **Scenario security objectives to security functional requirements mapping ... 107**

Annex C (informative) **Informative proposal for improvements of TS 21177:2019: CRL request 109**

Annex D (informative) **Informative proposal for complements to TS 21177:2019: Ownership and access policy ... 116**

Annex E (informative) **Informative proposal for improvements of TS 21177:2019: Errata, additional rationale material, and session persistence across certificate expiry ... 120**

Bibliography ... 124

© ISO 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

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*, 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).

A list of all parts in the ISO 21186 series can be found on the ISO website.

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 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

Introduction

This document provides informative material of interest to implementers deploying secure systems to carry out ITS applications. ITS stations are rapidly maturing with regards to specification, use and security conformance standards. In support of the ITS station ecosystem new standards have been developed, such as ISO/TS 21177, which provide a framework for device-to-device secure sessions and resource access authorization. Common criteria protection profiles have been developed and adopted for use in distinctive European ITS service domains, such as automotive V2X safety services, as well as a narrow set of infrastructure messaging based services.

NOTE ITS services are provided by means of ITS applications.

Given the diversity of anticipated ITS services and potential data sensitivities, this document was constructed to provide ITS stakeholders with a holistic analysis and indication of possible extensions to the ITS station security ecosystem.

This document includes the following sections:

1) An overview of security considerations for application specification and deployment in ITS. This overview also provides a detailed rationale for the following sections.

2) A use-case driven threat model based roughly on common criteria processes in establishment of threats, security objectives and SFR relative to three genericized ITS station data sensitivity and access control scenarios. Each scenario can be used by security practitioners as a starting point to baseline ITS station platform protection profiles of varying application types and data sensitivities. The genericized protection profile security requirements are then compared to several existing (or under development) protection profiles established for automotive use cases to determine possible gaps in security controls that should be addressed when tailoring subsequent security targets or related protection profiles.

3) An implementation example of the development of an access control policy implementation for an ISO/TS 21177 conformant ITS station unit. The example access control policy is application-specific and depends on many factors, including the type of ITS station unit on which the access control policy is used. Consequently, this access control policy implementation example is not suitable for being copy-pasted to the context of other ITS applications. Rather, the process described in this example can be considered as a suitable template for a process aimed at creating an access control policy for any ITS application running in an ISO/TS 21177 conformant unit.

4) Inputs for the development of a CP governing the issuance of certificates for ITS station units. A CP is necessary for the deployment of a system to ensure consistent behaviour of different CAs (or, more generally, credential issuance actors) within the system. This consistent behaviour enables receiving devices to trust all received messages to the appropriate level, knowing that those devices have been through the same certificate-issuing process no matter where the certificates were obtained. In early 2019, the European Commission published a CP for use for "Day 1" ITS applications, to be enforced by a top-level root of trust implemented in an entity called the TLM. This document concludes with a set of high-level gaps and potential mitigations for ITS PKI participants and implementers.

5) A description of additional functionality that extends the functionality of ISO/TS 21177. This material is written in a manner which will enable it to be inserted into a future revision of ISO/TS 21177.

These five areas of content significantly ease the process of deploying new ITS applications securely.

© ISO 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

This document is forms part of the ISO 21186 series on "Guidelines on the usage of standards," which is comprised of the following Parts:

1) Standardization landscape and releases;

2) Hybrid communications;

3) Security (this document).

© ISO 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

Documents
Document Sharing Hub

Full document details: PD CEN ISO/TR 21186-3:2021

Cooperative intelligent transport systems (C-ITS) — Guidelines on the usage of standards —

Part 3: Security

1 Scope

This document provides guidelines on security applicable in Intelligent Transport Systems (ITS) related to communications and data access.

In particular, this document provides analyses and best practice content for secure ITS connectivity using ISO/TS 21177.

This document analyses and identifies issues related to application security, access control, device security and PKI for a secure ITS ecosystem.

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/IEC 27000, *Information technology — Security techniques — Information security management — Overview and vocabulary*

ISO/IEC 27032, *Information technology — Security techniques — Guidelines for cybersecurity*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and ISO/IEC 27032 and the following 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
attack vector
extensible program-code-template for creating objects, providing initial values for state (member variables) and implementations of behaviour (member functions or methods) in object-oriented programming

© ISO 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

4 Symbols and abbreviated terms

AA	authorization authority
ACL	access control list
APDU	application protocol data unit
API	application programming interface
CA	certificate authority
CAM	cooperative awareness message
CP	certificate policy
CPS	certification practice statement
C-ITS	cooperative intelligent transportation systems
COER	canonical octet encoding rules
CPOC	certification point of contact
CRL	certificate revocation list
CTL	certificate trust list
DEK	data encryption key
DoS	denial-of-service
EA	enrolment authority
ECDSA	elliptic curve digital signature algorithm
ECIES	elliptic curve integrated encryption scheme
ECTL	European certificate trust list
ECU	electronic control unit
HSM	hardware security module
IDX	ITS data exchange
IVN	in-vehicle network
ITS	intelligent transport systems
ITS-AID	ITS application object identifier
ITS-S	ITS station
ITS-SU	ITS station unit
IVIM	infrastructure to vehicle information message
KEK	key encryption key
MAPEM	MAP extended massage

© ISO 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

ND	nomadic device
NIST	National Institute for Standards and Technology
OCSP	online certificate status protocol
OEM	original equipment manufacturer
PAKE	password authenticated key exchanges
PDU	protocol data unit
PII	personally identifiable information
PKI	public key infrastructure
PP	protection profile
RSU	roadside unit
SCMS	security credentials management system
SCN	sensor and control network
SDEE	secure data exchange entity
SFR	security functional requirements
SPaT	signal phase and timing
SPaTEM	SPaT extended message
SPDU	secured protocol data unit
SPII	sensitive or personally identifiable information
SREM	signal request extended message
SSEM	signal request status extended message
SSP	service specific permission
TLM	trust list manager
TOE	target of evaluation
TSF	TOE security functions
TVRA	threat, vulnerability and risk analysis
UGP	unified gateway protocol
V-ITS	vehicle intelligent transport systems
VMS	variable message sign

© ISO 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

5 Security in C-ITS

5.1 General

This subclause provides an overview of security in C-ITS and a rationale for the material in the rest of the document.

Systems have functional goals, and also have security goals which support these functional goals. The details of security goals depend on context, but high-level security goals are always the same:

— Provide assurance that parties within the system receive the right information necessary for acheiving their functional goals.

— Provide assurance that parties who are not authorized to receive information do not receive that information.

Systems use security controls to achieve their security goals. A security control is a specific mechanism implemented as part of a strategy to achieve the security goal. (For ease of discussion, this document also uses the concept of a security service. A security service is an identifier of the kind of action which needs to be performed in order to achieve a security goal, while a control is concrete and implementable). There are many different kinds of security controls, including the following:

— Communications security controls, which provide assurance that communications between two trusted parties meet the security goals of the system, i.e. that if two parties are legitimate, then there can be a data exchange between them in which each party is assured that the data came from the other party, is of known quality, and is not revealed in the course of the communications to unapproved parties.

— Platform security controls, which provide assurance that a device that is trustworthy at one point can remain trustworthy.

— Data processing security controls, which provide assurance that data is appropriately handled before or after it is communicated.

— Access control security controls, which provide assurance that activities within the system are carried out only by parties that have authorization to carry them out.

— Organizational and process security controls, which provide assurance that the other security controls in the system are implemented properly.

5.2 Security design process for C-ITS applications

A number of security design process approaches have been proposed for ITS applications. ETSI has specified a TVRA process[23] and applied it to the ETSI Day 1 ITS services[24]. The output of this TVRA process is a recommendation for specific security mechanisms. An alternative approach is outlined in ISO/IEC 15408-1, ISO/IEC 15408-2 and ISO/IEC 27001, which form the basis for the common criteria approach to security certification. A third approach is given in Federal Information Processing Standards (FIPS) 199[31], published by the NIST in the USA. Finally, SAE J2945/5[26] specifies an approach to deriving SSPs, a mechanism used to enable fine-grained access control statements to be made with IEEE 1609.2 certificates. As part of this process, it outlines an overall approach to deriving security requirements for a connected vehicle application.

All of these approaches use a systems engineering approach with three stages of the design: use case and concept of operations, requirements, and detailed design. Each stage can be considered more detailed than the previous one.

All of these approaches have a similar overall structure:

— Firstly, the ITS application is detailed to a level where information flows are specified allowing the ITS application to achieve its functional goals.

© ISO 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

— Then, a security analysis is performed to identify the security requirements on the information flows and on the parties and to derive from the requirements on the flows the corresponding requirements on the parties that interact with each other in the ITS application.

— The security analysis can reveal that the application design needs to be changed, either to directly address identified security issues, or because the security analysis has uncovered additional use cases or features of the application which need to be incorporated into the main design.

— The analysis/design update process iterates until the design is stable at the current level of detail. At that point, the design can be moved forwards to the next, more detailed, level of detail and the security analysis is performed and iterated on that next level of detail until the third and final level of detail is reached.

— The output is a full specification of the application, including the security controls.

Security controls to be specified include communications security controls, implementation security controls, organizational security controls, policy security controls, and others. Details of how controls are to be derived are given in the referenced methodologies ([23],[10],[31],[26]).

Clause 5 focuses on the communications security controls and supporting security controls necessary for enabling communications security:

— An overview of communications security mechanisms in the C-ITS context is provided in 5.3.

— An overview of the role of CAs and certification processes is provided in 5.5.

— A rationale for the additional detailed technical material included in this document is provided in C.1.

Although interface standards typically focus on communications security controls, all types of controls are important and a full specification on how to securely deploy a system includes a full specification of all of the relevant security controls.

5.3 Communications security mechanisms in C-ITS

The communications security services and controls that are appropriate for a distributed ITS application depend on the communications topology. At a high level, there are two types of communication strategies: broadcast and non-broadcast. From a security perspective, "non-broadcast" includes both unicast and groupcast: the important thing from a security perspective is that in both the unicast and groupcast cases, some potential receivers are being excluded from receiving information (and so confidentiality mechanisms, and key management to enable those confidentiality mechanisms, are necessary).

Figure 1 illustrates typical communications security mechanisms in a non-broadcast setting. In this setting, one actor (the host or responder) has certain resources which the other actor (the accessor or initiator) wishes to access in order to carry out an operation. Typical operations include reading the resource value (potentially with associated metadata), writing to the resource location, or causing the execution of some operation on the resource. In this setting:

— The host uses an access control policy to determine which operations can be carried on each resource by different types of accessor.

— The accessor uses the security service authorization to access to demonstrate that it has rights to the particular access that it is requesting. See 5.4 for a discussion of access control types.

— The following security services are applied to each individual APDU sent as part of the exchange:

  — source authentication, to provide assurance that the message is sent by a valid participant in the exchange;

  — confidentiality to ensure that the contents cannot be read by an unauthorized actor;

© ISO 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

— protection against modification to ensure that the contents are not modified in transit (or, more specifically, to ensure that if the contents are modified in transit, that this can be detected).

Protection against modification can include the application of multiple services, such as anti-replay (protecting a receiver against acting on the same APDU twice, as if it was two different APDUs) and freshness checking (protecting a receiver against acting on an APDU which is too old to be relevant). In the security service categorization developed by the NIST (USA), all of the services designed to ensure that the receiver of the APDU has the correct understanding of the PDU's properties (time of generation, generating party, data integrity, etc.) are considered part of one high-level service called integrity. This is the convention followed in this document.

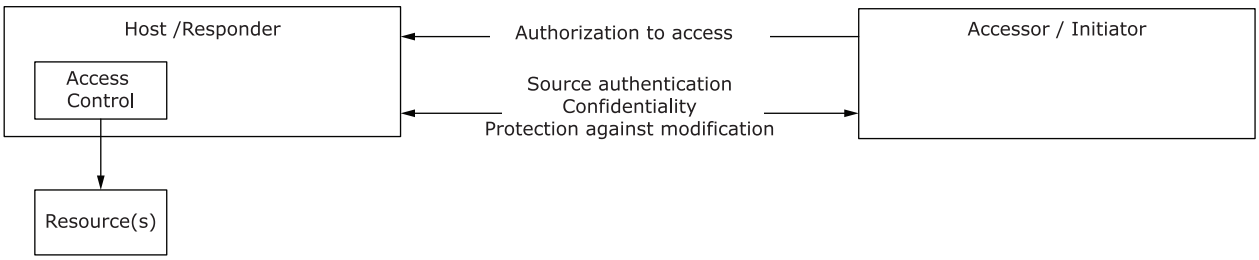

Figure 1 — Security services for non-broadcast communications topologies

Figure 2 illustrates typical communications security mechanisms in a broadcast setting. In this setting, the actor (the broadcaster) has locally available resources on the basis of which it broadcasts a PDU which receivers can opportunistically make use of. In this setting, the following security services are applied to each individual APDU sent as part of the exchange:

— source authentication to provide assurance that the message is sent by a valid participant in the exchange; and

— protection against modification to ensure that the contents are not modified in transit (or, more specifically, to ensure that if the contents are modified in transit, this can be detected).

  Protection against modification can also include services such as anti-replay and freshness checking, as in the non-broadcast case.

— The sent PDU can also make use of pseudonymity, which is a security service that enables receivers of the message to understand the instantaneous state of the broadcaster, but provides protection against the receivers being able to track the state of the broadcaster over time. (For example, if the broadcaster is a vehicle sending CAMs, pseudonymity inhibits receivers from being able to use the CAMs to determine the entire route that the vehicle took). Pseudonymity is not achieved by a single mechanism, but is an outcome of multiple mechanisms acting in concert.

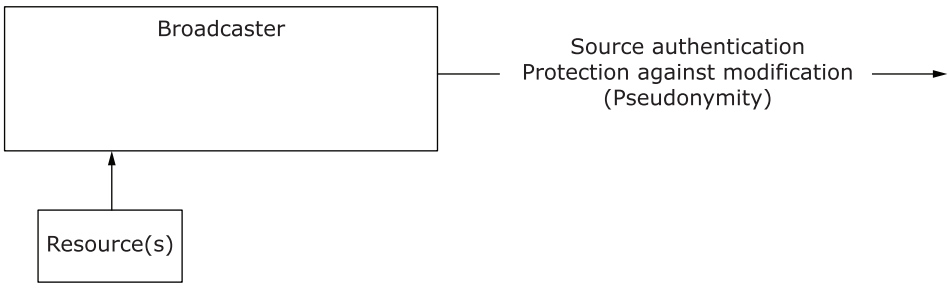

Figure 2 — Security services for broadcast communications topologies

© ISO 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

5.4 Source authentication and access control mechanisms

This section discusses appropriate mechanisms for source authentication within ITS applications, starting from a discussion of access control types.

In this document, communications security is primarily discussed in terms of access control. Access control mechanisms are mechanisms that manage access to resources. Access control policies are a configuration of access control mechanisms that allow the integrity and confidentiality goals of the system to be achieved.

A key mechanism for enabling access control is source authentication. This mechanism provides assurance to the receiver of an incoming message (which can be data, a command, or both) that the sender has a particular property. There are two main types of source authentication.

— **Identity authentication**: In identity authentication, the property transmitted is a unique identifier of the sender. Identity authentication enables identity-based access control. In this case, the receiver maintains an ACL which maps from the sender's identity to the actions that the sender is permitted to take. Identity-based access control is common for managing access to centralized systems, as these systems can manage individual permissions for each accessing party. Identity-based access control allows the certification of accessing parties to be tied to a single, long-lived, property of the device, i.e. the identity. Permissions can then be mapped to the identity and managed by a single centralized process using this identity as a look-up key. This enables permissions to be changed dynamically (e.g. if an employee changes job role, they can be granted access to different corporate information without needing to change how they authenticate to the system). However, identity-based authentication creates a requirement for parties granting access to maintain some information file (a username/password file, an ACL, or some equivalent) with one entry for each accessing party and to update this if new parties are granted access.

— **Role-based authentication**: In role-based authentication, the property transmitted contains explicit semantics and is not just an identifier. For example: the sender is entitled to act as a police vehicle; the sender is entitled to send CAMs; the sender is entitled to request tolling information; the sender is entitled to create a software image that is appropriate for installation on a particular device. In role-based authentication, the property transmitted can be about a physical property of the sender, or about a role in which the device is entitled to act, or about any other property that will enable the receiver to make an access control decision. In some contexts, a distinction is made between role-based and attribute-based access control, where attribute-based access control uses more fine-grained properties of the sender than role-based access control. This document does not make use of that distinction. Additionally, attribute-based access control can include properties of the environment or the resource itself in making access control decisions. In role-based access control, the receiver maintains an access control policy mapping properties or combinations of properties to the activities that a party with those properties is entitled to carry out, similarly to the use of the ACL in identity-based access control. The distinction is that in role-based access control, a receiver does not need to maintain separate access control permissions for each individual sender, just for each individual role. This means that the receiver does not need to manage information for each party in the system, allowing for more robust access control when edge devices interact without going through a centralized system. The trade-off is that if a device's role changes, the device needs to be issued with new credentials indicating that new role. Role-based authentication has an advantage over identity-based authentication in those cases where the cost of updating each sender is less than the cost of updating each of the likely receivers.

In either case, the receiving device will apply an access control policy to determine whether the sending device is entitled to take the particular action requested. Examples of access control policy include the following.

NOTE 1 The following examples are linked to use cases (i.e. applications) for illustrative purposes, not to suggest that the use case uses the exact access control policy specified below.

© ISO 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

NOTE 2 The access control policy examples below are for action taken on the receiving side. The assumption is that the sender is aware of the access control policy likely to be implemented on the receiving side and will create outgoing messages and metadata that provide the information needed for the message to be accepted under the receiver's access control policy.

— **Cooperative awareness**: For a broadcast message, if the message is validly signed by an IEEE 1609.2 certificate with the Cooperative Awareness Basic Service ITS-AID and meets other conditions for freshness and relevance, accept. Otherwise, reject. See [19].

— **Attaching an RSU to a signal controller for SPaT message generation**: If the RSU is a valid RSU for generating SPaT messages, and is owned by the road authority that owns the signal controller, and is being installed by a licensed installer, accept. Otherwise, reject.

Regarding the choice between identity-based and role-based authentication based on communications topology, note that for many application data exchanges between two edge devices there are two natural topologies to consider: a centralized topology, where communications are routed through one or more cloud services, and a local topology, where the edge devices communicate directly. (See Figure 3).

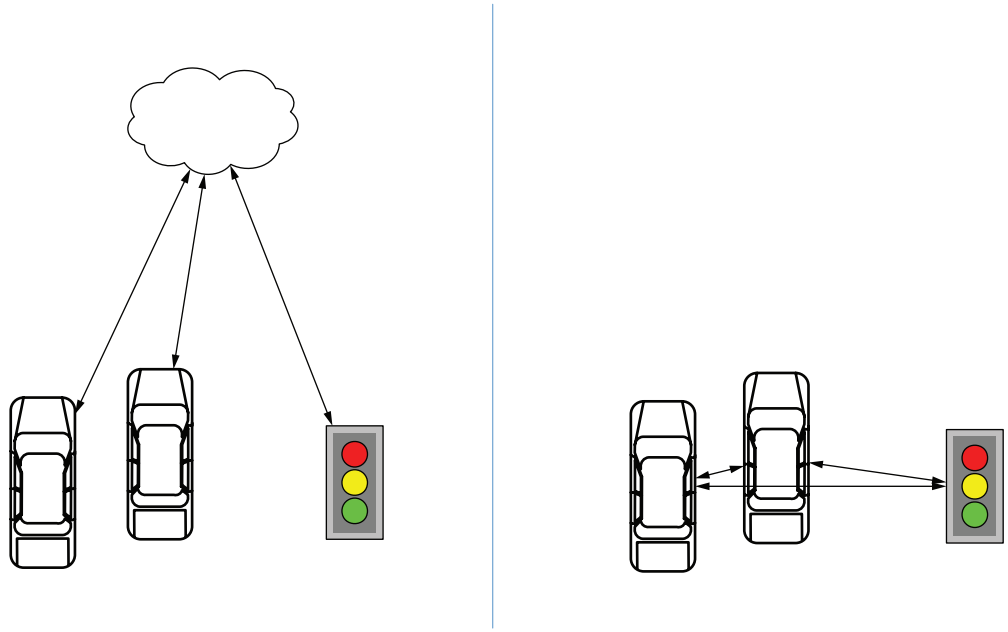

Figure 3 — Centralized topology (left); decentralized topology (right)

For the centralized topology it will often make sense to use identity-based access control on each of the communications links. A natural example of this topology is in Figure 4, where each device has its own "home server" and the two home servers communicate to carry out the technical goals of the ITS application. In this setting, identity-based access control is used as follows:

— The initiating device has a persistent connection i.1 to its home server. The connection is associated with the device's identity. The home server manages the initiating device's attributes and authorizations, including for example its balance in any financial accounts.

— The responding device also has a persistent connection i.3 with its own home server.

— The two home servers have a persistent connection with each other. Each home server manages a list of the actions that the other home server is entitled to authorize. When one device attempts to carry out an action through the cloud connection, its home server determines whether it is authorized and communicates the authorization to the other home server.

© ISO 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

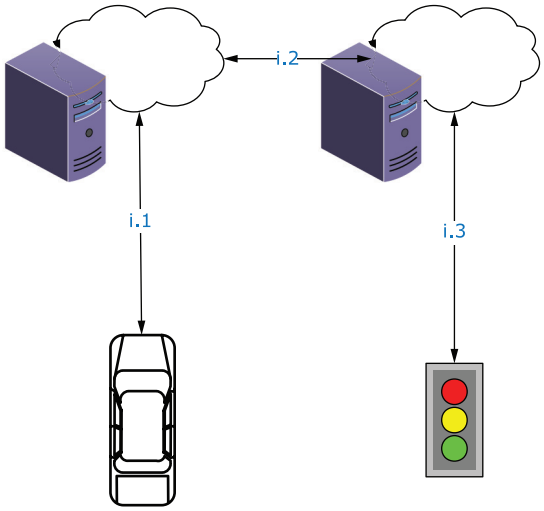

Figure 4 — Devices communicating via their home servers

Typically these connections will be authorized by standard web technologies such as cookie based authentication, token based authentication, OAuth over TLS[12], and others. The initial authentication of the field device to its home server can be via username and password, or X.509 certificates, or a PIN transmitted out of band, or some other means. The authentication mechanism also manages continuity of authentication through the lifetime of the connection.

For the direct or decentralized topology, a natural approach is to use IEEE 1609.2 certificates for authorization, either to sign the messages directly in the case of broadcast or to authorize a persistent secure session using ISO/TS 21177 in the case of multicast/unicast. The ISO/TS 21177 approach supports the case where one device needs to provide evidence of multiple properties to the other device, by allowing the device to provide multiple certificates within a given flow. This allows properties with different lifecycles to be managed separately: for example, the sensors that are built in to a device are a long-lived property, but the fact that it is operated by a registered operator might be short-lived. In the ISO/TS 21177 model, these two properties can be attested separately but associated with the same counterparty, allowing the application of sophisticated access control policies. This is illustrated in Figure 5, which shows an example of the access control policy that can be in place for a police car requesting signal pre-emption.

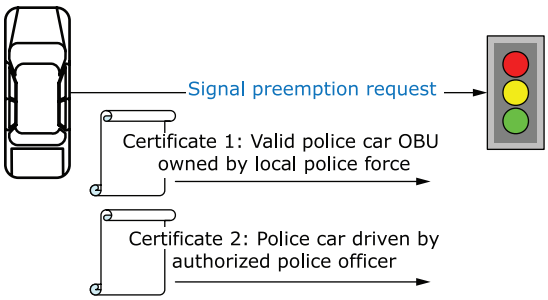

Figure 5 — Example of a police car requesting signal preemption under an access control policy that requires multiple certificates

A natural way to architect applications is so that they can be executed in two ways: via a cloud service and via a local service. The cloud service approach allows for processing associated with the application activities to be carried out in the cloud, where scalability and new functionality is easier to implement. The local approach allows activities to be carried out with less latency and also to be robust against loss of connectivity to the cloud service for any reason. If an application is architected in this way, it can be appropriate for the application to be provided with two different sets of security credentials:

© ISO 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

one set of identity-based credentials for use with the cloud service approach, and one set of role-based credentials for use with the local service approach.

For some applications a natural architecture is to have no direct communications between distinct edge devices. An example of this would be an application where a central service directly carries out the service of interest to the edge device with no direct involvement of other edge devices. Another example would be an application where the central service aggregates and analyses data from edge devices before providing post-processed, statistical data to its client edge devices. In these cases, an authorization approach based solely on identity-based authorization can be appropriate.

For other applications a natural architecture can be to only have direct communications between edge devices. An example of this would be applications with extremely time-critical communications latency requirements, or applications where the volume of data is so large that it would cause a significant network burden to send it "up" to a server and then back "down" to a neighbouring edge device, or applications where it is critical that the application can operate in the absence of connectivity and so it does not make sense to deploy a version that depends on network connectivity. In this case, an authorization approach based solely on role-based authorization (using IEEE 1609.2 certificates and, if appropriate, ISO/TS 21177 secure sessions) can be appropriate.

5.5 Certificate authorities and certification processes

Almost all secured digital communications are secured using cryptography. The general model is as follows:

— A device obtains a credential, which is a binding between a secret value and a property of the device (or of an actor using the device, or of an application processes running on the device). More specifically, it is a binding between a means of demonstrating that the device knows the secret value and the property of the device.

  The means of demonstrating that the device knows the secret value can take different forms:

  — If the secret value is a shared secret, used in a centralized system, the means of demonstrating that the device knows the secret can simply be the secret itself or some value derived from it.

  — If the secret value is a private key for an asymmetric cryptosystem, the means of demonstrating that that the device knows the secret is to perform an operation involving the private key and a related operation with the public key – either using the private key to sign a message and the public key to verify it, or using the public key to encrypt random data and using the private key to decrypt it.

  The binding between the knowledge of the secret value and the property can also take different forms:

  — The data used to prove knowledge can be stored in a database with the property. This is common in centralized/identity-based systems as discussed above.

  — The property can be distributed with the data used to prove knowledge, for example in an X.509 or IEEE 1609.2 certificate containing the public key (the data used to prove knowledge) a name or a set of permissions. In this case, a third party is trusted to ascertain that the actor using the device does in fact have the property being claimed.

— When an actor using the device engages in secure communications, the device demonstrates that it knows the secret value. The receiver trusts the binding between the data used to prove knowledge of the secret and the property. In other words, it trusts that if the device knows the secret, then it has the claimed property. Cryptographically secure operations can then be carried out, leveraged by the secret value, as is done in (for example) Transport Layer Security (TLS)[13], ISO/TS 21177, or IEEE 1609.2.

© ISO 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

The purpose of this discussion is to illustrate that the communications security in any system relies fundamentally on two things:

1) The secret known to the device is protected from being extracted from the device, as any actor who knows that secret can claim to be the device or have the device's permissions.

2) The binding process establishes without dispute that the device or the actor using the device does in fact have the properties claimed.

Examples of "the properties claimed" in point 2) are: that the device's name is what it says it is, or that the device is operated by licensed operators (for example, the police), or that the device has the sensors and data quality checks necessary to enable it to usefully send CAMs.

To provide assurance that 1) is true, an ITS application specification includes (inline or by reference) a specification of the physical, operating system, and software security requirements on the device. This specification can take many forms, but a standard type of this specification is a PP as defined in ISO/IEC 15408-1 and ISO/IEC 15408-2. A PP allows certification laboratories to determine that a particular type of device meets the security properties necessary for it to operate. An application deployment plan is not complete unless there is a PP or similar document. PPs exist for different types of devices in the context of C-ITS[10],[11],[12]. Clause 6 of this document contains input material for a PP for IDX devices, i.e. devices that use ISO/TS 21177 to access and make use of data on other ITS devices.

To provide assurance that 2) is true, in the specific case of certificates, a certificate issuer (certificate authority, or CA) can be required to follow a CP and CPS. A CP and CPS already exist for the ETSI Day ITS applications. Clause 8 of this document provides input material for a CP for CAs that issue certificates to IDX devices.

5.6 Introduction to the rest of this document

As discussed in 5.5, a full specification of an aplpication includes a CP and a PP (either directly in the specification or by reference to external documents). As of December 2019, there is only a limited number of CPs and PPs suitable for use with ITS-SUs. Specifically, there is a European Certificate and Security Policy[27],[28] which addresses the "ETSI Day 1 applications", but there is no policy for other types of application, and there is no published policy for any type of application in other regions.

The goal of this document is to facilitate deployment of an additional class of applications in addition to the ETSI Day 1 applications. This class is IDX applications. An IDX application is any ITS application that uses unicast connectivity to exchange data (including commands/requests) directly with a peer. IDX applications are defined in more detail in Clause 6.

To facilitate deployment of these IDX applications, this document provides the following:

— Security analysis and controls for three types of IDX device in Clause 6. Additional analysis of the security functional requirements for each type of device is provided in Annex B.

— Worked example of the development of an access control implementation for an IDX device in Clause 7.

— Identification of threats to the PKI from a stakeholder perspective, along with proposed mitigations. Additionally, an analysis of changes necessary to the EU CP to enable the deployment and certification of IDX devices is provided in Clause 8.

This document also provides the following new material related to ISO/TS 21177. This material is motivated by feedback from industry stakeholders on additional functionalities that would enhance the abilities of the ISO/TS 21177 approach:

— Ability to provide up-to-date information about the revocation status of CAs, specified in Annex C.

— Support for the concept of an "owner" of an IDX device. The owner has the ability to explicitly permit, prohibit, or end rights to access that devices. This is specified in Annex D.

— Additional proposed modifications and enhancements to ISO/TS 21177, specified in Annex E.

© ISO 2021 – All rights reserved

AVA Documents Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

6 Security analysis and controls for an IDX device

6.1 Background

An IDX application is any application that uses unicast connectivity to exchange data (including commands/requests) directly with a peer. Examples include:

— RSU to signal controller connections to enable SPaT messages to be generated;

— vehicle to road weather control station connections to enable weather condition reporting per SAE J2735/3[25];

— vehicle diagnostic interactions when carried out over a local interface rather than through a cloud service. Implicit in the definition of the IDX application is the concept that ISO/TS 21177 is an appropriate communications security mechanism.

NOTE Individual application specifications can use a different communications security mechanism if this is appropriate for that application.

As discussed in 5.2, a full deployment-oriented application specification includes platform security requirements for devices running instances of that application in specific roles. A standard approach for specifying these requirements is to develop a common criteria PP for that application. Common criteria PPs have been developed and adopted for use in individual European ITS service domains, including automotive V2X safety and a narrow set of infrastructure messaging applications. They are widely accepted as an appropriate way to specify testable security requirements for different types of devices or modules.

Clause 6 provides material that can be used as input to the specification of PPs for the three types of IDX device. The material includes SFRs as well as the analysis leading to the derivation of those SFRs.

Clause 6 also presents a gap analysis, comparing the derived security requirements for the three device types are compared to several, existing (or under development) PPs for automotive use cases. This assists device suppliers who wish to supply devices that can run both IDX and other C-ITS applications, by indicating a set of security features to support IDX applications and enabling a gap analysis of these features against the features of C-ITS devices.

6.2 IDX device concept

6.2.1 General

This subclause defines the basic concept of operations for three types of IDX device analysed using an abbreviated common criteria-like requirements analysis process.

The aim of this section is to provide clear architectural definitions and functional activities for an IDX device that interfaces with an ITS-SU fronting a SCN in order to access or upload data resources of varying sensitivity. The functional activities provide the context for defining assets and more complex use cases making use of those assets. The three generic IDX device/application types are listed below. The assumption of this description is that every IDX application is fundamentally one of these types. Each application can have unique features of its own that cause it to have unique security requirements and, as such, each application's security features should be independently analysed and derived. However, by providing this analysis of the three fundamental types of application, this document aims to kickstart the process of providing a security analysis, security requirements, PP and CP for each and every new application. The three types are as follows:

— IDX devices running public data retrieval applications, where the accessing device is requesting data that would not be subsequently linked to the device providing the data (for example, a road weather management system requesting road weather data from a vehicle on the road, as per SAE J2945/3).

© ISO 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

— IDX devices running private data exchange applications, where the accessing device is requesting data that might be subsequently linked to the device providing the data, for example malfunction reports from a traffic signal controller, or path information from a pedestrian ITS-SU.

— IDX devices running active access applications, where the accessing device is requesting to write to the host device or execute operations on the home device. An example of this is a management device wirelessly accessing a VMS to change the message.

Additional analysis of the security functional requirements for each type of device is provided in Annex B.

For each device type, this document provides a security analysis in the form of a) threats, b) security objectives and c) SFR. These form the basis of IDX device PP which can be useful for:

1) analysing existing European ITS-S-related PPs to determine if they are suitable for applying to IDX devices; and

2) establishing new PPs and security targets intended for varying ITS data sensitivity levels. The goal is that this material can be used to develop a consistent set of PPs for a wide range of device and data sensitivities in the ITS domain.

Security analysis uses the concept of a TOE, which is the system that is to undergo security analysis and which is contained within a security boundary, such that all interactions across the boundary are known and observable. A high-level flow of the PP development process is shown in Figure 6.

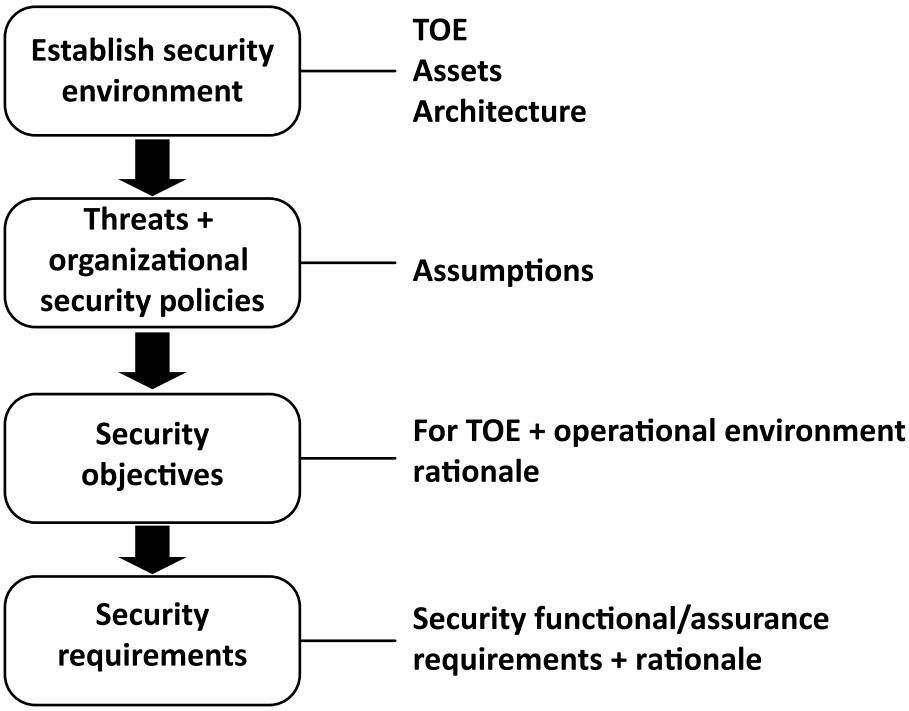

Figure 6 — High-level depiction of ISO 15408 series PP development process

The TOE in this case is the IDX device that is assumed to interact with another ITS-S in order to obtain access to that ITS-S's resources. The terms TOE and IDX device are used interchangeably throughout this material.

Readers of this clause are assumed to be proficient in the language and processes of the common criteria.

Contrast with full common criteria approach: The security requirements in this clause are not identified as being derived from a full common criteria evaluation, as a full common criteria evaluation is dependent on the specifics of the application definition. A full common criteria evaluation requires

© ISO 2021 – All rights reserved

AVA Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

detailed knowledge of the application interfaces, physical connections and intended usage environment in order to arrive at a detailed threat model, set of inherited organizational policy requirements, SFR and customized operations for those requirements. This document does not provide specific customizations of SFR for specific applications. Developers of specific applications are expected to carry out their own analysis of security assumptions and requirements, using this section as an example.

Additionally, the focus of common criteria is on developing security requirements for the whole system, including organizational security requirements. The goal of this document is to enable development of a certification programme for devices, and so very few organizational security requirements are assumed or provided.

6.2.2 System architecture and device

6.2.2.1 Target of evaluation

The TOE can be any type of IDX device, for example a unit that is used in automotive maintenance facilities to connect to and electronically interact with a SCN for diagnostics, maintenance, emissions testing or other purposes.

The IDX device high-level view is indicated in Figure 7. The IDX device is assumed to conform to the architectures for an ITS-S standardized in ISO 21217. A certificate management functional block is explicitly shown in the block diagram due to the high significance and dependence that other management blocks and applications have on it.

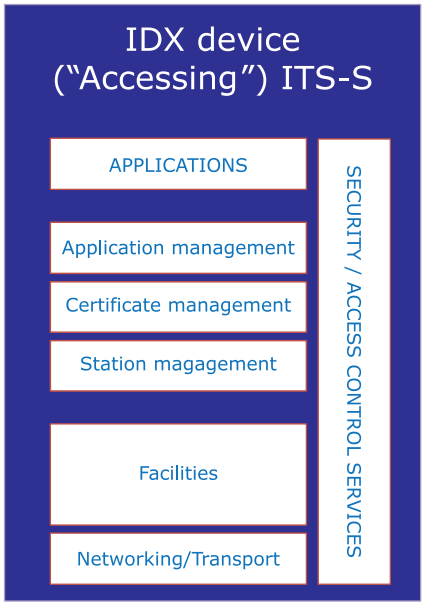

Figure 7 — Target of Evaluation (IDX device that accesses an SCN ITS-S application)

6.2.2.2 General system view

The IDX device is assumed to be used within an untrusted security environment. It can be manually or remotely commanded by a user and will connect to an ITS application (e.g. in a vehicle) using either a wired or wireless protocol stack.

NOTE ISO/TS 21185 specifies a methodology to identify globally uniquely communication protocol stacks and communication profiles and provides a list of respective globally unique identifiers.

© ISO 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

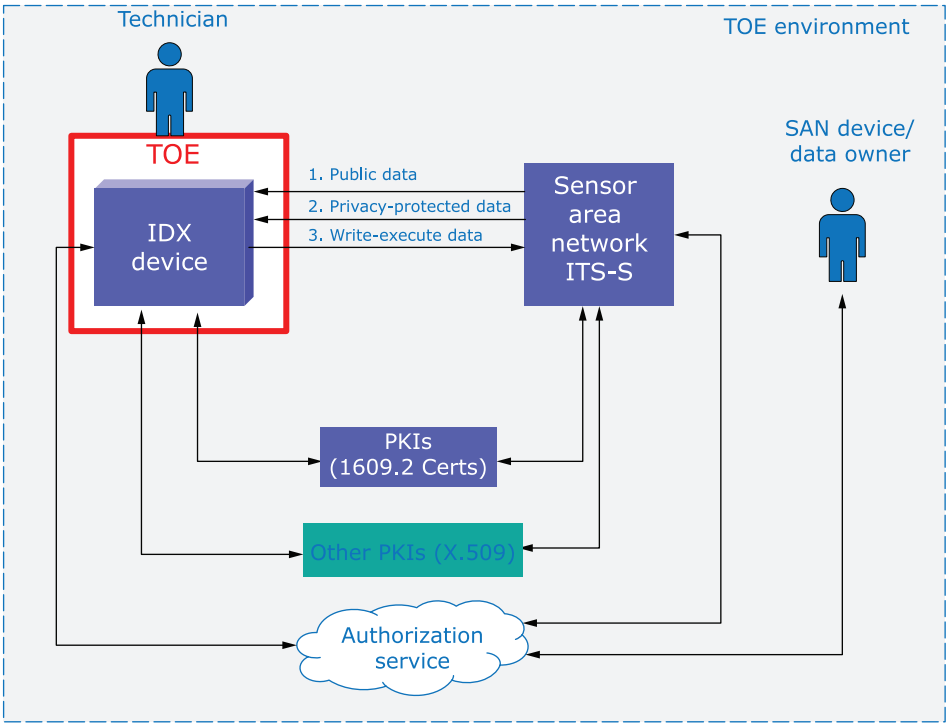

Figure 8 — System View: TOE and TOE Environment

Three resource sensitivity types:

1) public,

2) privacy-relevant, and

3) write-execute data,

each corresponding to the IDX device classes described in 6.2.2, are shown to be accessed in Figure 7.

These resource types vary in security/privacy sensitivity and are used to differentiate the three access scenarios defined later in this clause. These scenario-driven accesses are used to differentiate the level of threats to an IDX device ITS-S based on the resource sensitivity of the data it accesses via the SCN ITS-SU.

6.2.2.3 Connections and trusted relationships

This subclause defines connectivity between the TOE and other system actors. Connections to and from the TOE are characterized as the following:

— **User to IDX device:** This connection can be manual (local) or remote. In most cases, the user is assumed to be local to the IDX device (used to access the resources of the SCN) and able to leverage its User Interface to request and perform various resource accesses via the SCN ITS-S to which it is connected. If the user is remote to the IDX device, this CONOP assumes that a secure connection, for example TLS, exists between the user and the IDX device.

— **IDX Device to SCN**: This connection uses a communications protocol stack (see ISO/TS 21185) conformant with ISO/TS 21177. ISO/TS 21177 will provide secure connectivity using TLS 1.3 over the underlying stack. ISO/TS 21177 is a secure connection and authorization framework; its capabilities can be leveraged for secure access between the IDX device and SCN ITS-SU. This document makes no assumptions related to the duration of the connection between an IDX device and a SCN. The connection can be persistent or ad-hoc.

— **IDX device to PKI:** An IDX device is assumed to possess IEEE 1609.2 certificates for securely accessing SCN resources. Therefore, IDX devices require certificate provisioning services of a 1609.2

© ISO 2021 – All rights reserved

AVA Documents Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

PKI. At minimum, this requires bootstrapping an IDX device with PKI trust anchors and providing it with an enrolment certificate it can use to request application-specific certificates.

— **IDX device to evice Vevndor:** The device is expected to communicate directly (i.e. secure sessions) or indirectly (i.e. end-to-end file security) with its vendor in order to receive updated software, firmware or configurations.

— **IDX device to other PKIs**: All other secure connections are assumed to leverage conventional, internet-based PKIs based on X.509. The provisioning steps of these certificates can vary between manufacturers and PKI providers.

— **Connections to third-party authorization service**: Facilitating secure access between an IDX device and a SCN ITS-SU are connections each has with an external authorization service. In cases when sensitive accesses require consent of the data owner (e.g. entity owning the sensor network data), the SCN ITS-SU can either directly/locally request owner consent, or the SCN ITS-SU and IDX device can interact via a 3rd party authorization service to obtain owner consent (e.g. via a concurrence message or PIN to enter via mobile app).

6.2.3 Threat modelling data scenarios and examples

6.2.3.1 Scenario 1— non-sensitive public data

Scenario 1 consists of an IDX device that is only used to access non-confidential 'public' data such as diagnostics data not intended for any regulatory use. The information is assumed to be publicly viewable and does not require integrity or source authentication protections. While this scenario is unlikely, except for the most consumer-oriented devices, it is useful for differentiating the level of protections needed with rising, scenario-based sensitivity levels.

It is assumed that a Scenario 1 IDX device enrols with a PKI in order to obtain certificates for interface connectivity to a peer device (e.g. SCN ITS-S).

The Scenario 1 data access and flow area indicated in Figure 9.

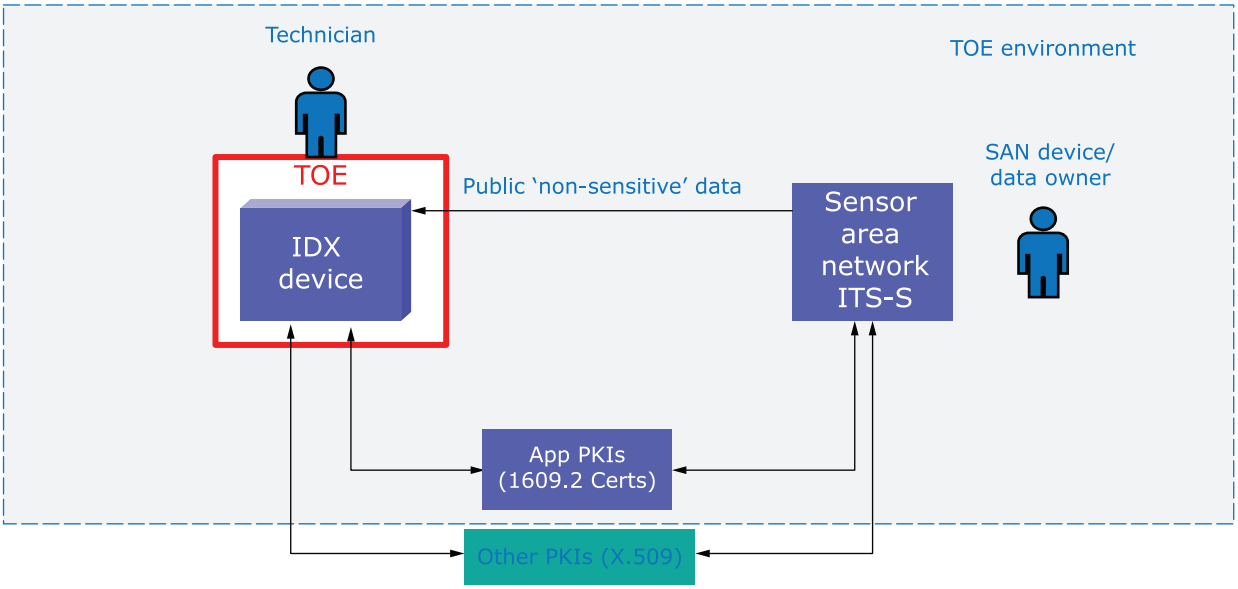

Figure 9 — Scenario 1: Access of public, diagnostics data

© ISO 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

6.2.3.2 Scenario 2 — privacy-protected data assets

Scenario 2 is distinguished from Scenario 1 in that the IDX device accesses:

— privacy-sensitive data, i.e. data that reveals identifying or trackable data (e.g., location history) associated with the SCN or its owner, or

— public data that requires integrity protection, as can be the case with data used for regulatory adherence.

The principle data threats in this scenario include unauthorized information disclosure and a violation of data source or integrity. For privacy-sensitive data, it is assumed that the data is not only access-controlled, but that the data owner has a right to authorize the disclosure through a local or external authorization service. Scenario 2 is depicted in Figure 10.

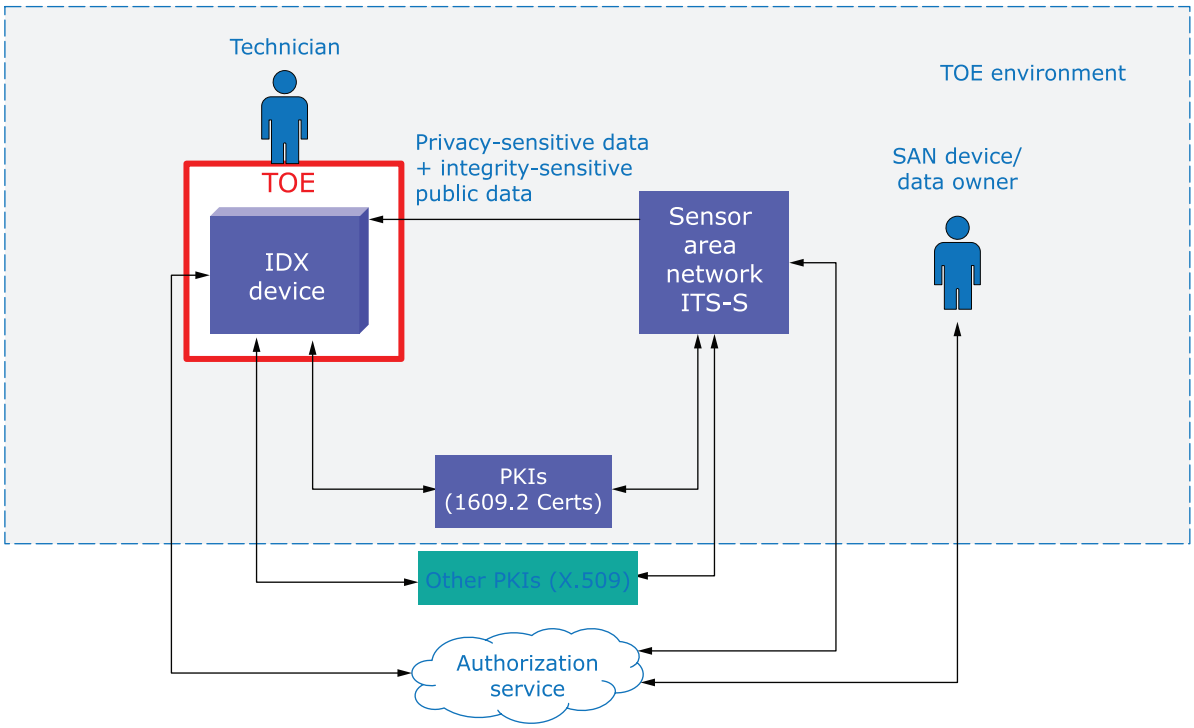

Figure 10 — Scenario 2: Access of privacy-sensitive data

6.2.3.3 Scenario 3 — executable or writeable data assets

Scenario 3 introduces the ability of an IDX device to perform actions that modify the state of the SCN, i.e. perform write actions such as execution of sensitive commands/files or loading of new firmware or configurations to the SCN or its fronting ITS-SU. This scenario is illustrated by two primary examples of IDX device functionality:

1) The IDX device supports the trusted load of new software images for the SCN.

2) The IDX device supports the trusted modification of existing SCN access control policies.

Scenario 3 is depicted in Figure 11.

© ISO 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

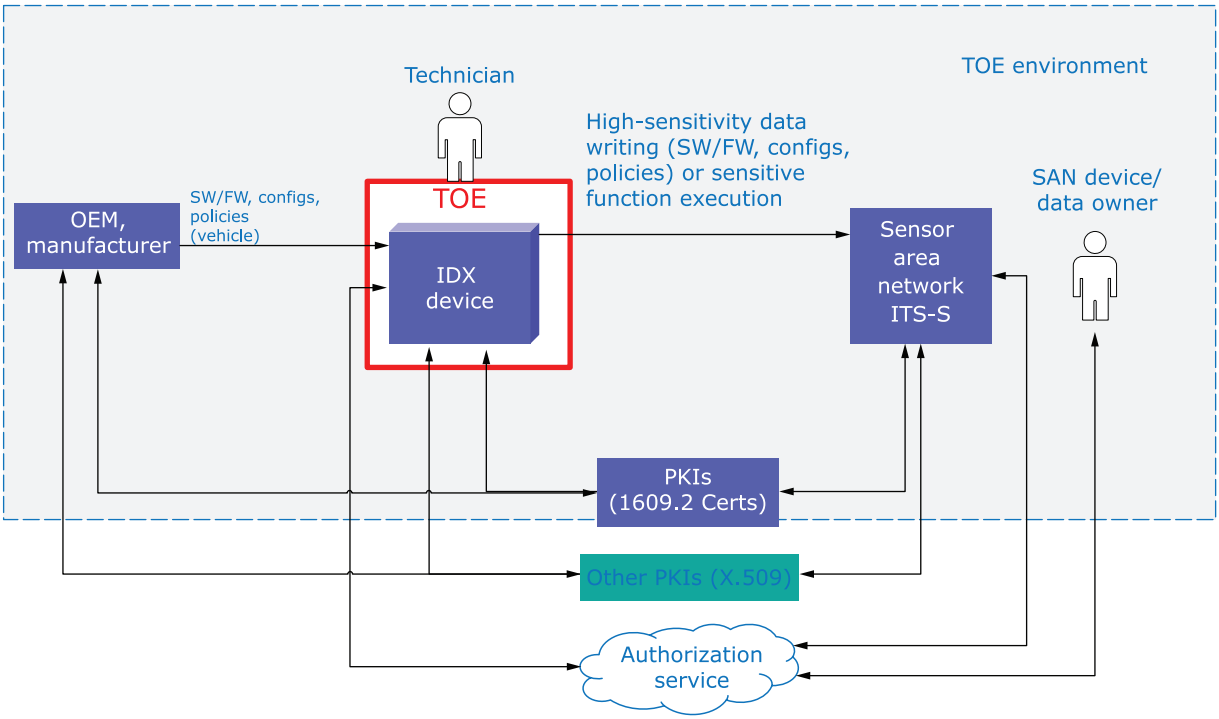

Figure 11 — Scenario 3: Access of sensitive write, execute or load functions

Examples of Scenario 3 include:

Example 1: Load software image: The desired result of this action is the successful update of one or more software images to a device within the SCN. The IDX device is loaded with a software image received from an OEM, Tier 1 supplier or other organization. Delegation of authority to sign software image updates can also occur. Metadata associated with the software image is assumed to be included in the load package. This metadata can include cryptographic signatures, timestamps, and other data. Supporting industry trends in firmware update frameworks, it is assumed that metadata can be signed by different actors than those who sign the software image.

Access control functions of the device are configured to evaluate the permissions of the signers to distribute or package both software image files and metadata files. This can be accomplished using the ITS-AID/SSP parameters provided in SCMS certificates.

Example 2: Modify (write) access control policy: The desired result of this action is a change to the SCN ITS-S ISO/TS 21177 access control policy. This example focuses on an access control modification that allows any software updates signed by a SCN device supplier to be installed without requiring future user-explicit authorization grants. In this example, ISO/TS 21177 enhanced authorization is used to receive authorization from the user to make the permanent change to the SCN access control policy.

Threat modelling assumptions pertinent to Scenario 3 include:

1) The trust relationship between the logged-in user and the IDX device is based on organizational policy and not in scope for any PP requirements derived from this example. It is assumed that the organization responsible for provisioning user accounts to the IDX device has procedures in place to properly vet users and map users to roles.

2) There is a secure access cloud service available to support extended authorization requests that solicit the SCN data owner for approval.

3) The software image is digitally signed by an authorized organization.

4) Metadata associated with the SCN software image is digitally signed by an authorized organization.

© ISO 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

NOTE Software and firmware signing by manufacturers need not use the IEEE 1609.2 certificate on which ISO/TS 21177 resource access control decisions are made. Manufacturers can use X.509 certificates emanating from private or public PKIs.

6.2.4 Assumed device functions and activities

The activities pertinent to the three IDX device scenarios are provided in Table 1. Each activity represents an assumed capability of a generic IDX device. The table is broken into the following sections:

— General activities pertain to all Scenarios and can be used to construct more elaborate use cases. These activities are identified with an ID starting with "G" and are common to all IDX devices.

— Scenario-specific activities pertain to use cases involving access of each Scenario's SCN data and their unique sensitivities. IDs starting with S1, S2 or S3, respectively, indicate that the capability only applies to an IDX device in the indicated scenario.

For the purposes of scenario-centric threat modelling and traceability, it is assumed that each Scenario-capable device is exclusive to a given scenario. For example, a Scenario 3 access device is not able to perform Scenario 2 privacy data accesses. In practice, if a Scenario 3 device also performs Scenario 2 data accesses, security practitioners can baseline a PP by merging and reconciling the Scenario 2 and 3 threats and associated security controls.

The activities depicted in this section are intended provide an understanding of the capabilities, assumed limitations and other miscellaneous assumptions concerning the IDX device, such that security practitioners can understand and adjust the scenario threats and baseline security controls when building their own PPs.

Table 1 — General and scenario-specific operational activities

ID	Activity	Description
General activities (all Scenarios)		
G01	Bootstrap/enrol device into application PKI	The IDX device is bootstrapped and enroled into the PKI that generates such 1609.2 certificates. This activity includes type certification, provisioning with initial key material or random number generation seeds, and (if applicable) registration of the device platform with an appropriate registry.
G02	Download and install IDX device firmware	An IDX device manager downloads/retrieves and installs new IDX device platform firmware.
G03	Download and install IDX device applications	A device manager downloads/retrieves and installs new IDX device applications. These applications are installed on the IDX device for accessing SCN resources; they are not installed on the SCN.
G04	Obtain initial authorization certificates	The IDX device is provisioned with authorization certificate(s) in order to connect with SCN application(s). Scenario 1 authorization certificates do not require sensitive access. It is assumed that they only indicate that a valid IDX device is attached since they are only intended to read public data. Scenarios 2 and 3 authorization certificates are assumed to indicate authorized roles associated with special accesses.
G05	Refresh authorization certificates	The service updates its authorization certificate(s) in order to continue to be able to connect to peer ITS-SUs fronting an SCN.
G06	IDX device is configured with new user and mapped to role	The IDX device ITS-S should not allow all device functions to be available to all users. This can be restricted using roles mapped to permitted activities. Roles are indicated by certificate ITS-AIDs and SSPs associated with those ITS-AIDs. This activity results in an application access policy whereby some user identities are permitted to access certain applications and others are not.

© ISO 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

Table 1 *(continued)*

ID	Activity	Description
G07	Securely connect to a peer ITS-SU	The user, using the IDX device, connects to SCN application via ISO/TS 21177 ITS-Station secure session. The protocol stack is conformant with ISO 21185.
G08	Enrol into external authorization service	The IDX device can optionally participate in an external authorization service to enable cloud-supported authorization transactions between the accessing entity and the SCN owner/operator.
Scenario 1 activities		
S1-01	Request/retrieve public diagnostics data from SCN	Pre-requisites: G01-G07 The IDX device connection to the SCN is complete after the SCN has determined that a valid IDX device has connected. The IDX device application performs read requests on public data elements (e.g. Diagnostic Test Codes) via the peer SCN-fronting ITS-SU.
S1-02	SCN ITS-S performs policy check to determine if non-repudiation is required based on request	Pre-requisites: S1-01 The peer SCN-fronting ITS-SU checks policy based on the resource requested by the IDX ITS-SU and makes a non-repudiation decision. If non-repudiation is needed, the SCN peer ITS-SU digitally signs the requested data using the correct 1609.2 certificate. If non-repudiation is not needed, the peer ITS-SU returns the response over the ISO/TS 21177 secure session without application layer non-repudiation.
S1-03	SCN device provides report for IDX device (user) consumption only	Pre-requisites: S1-01, S1-02 The application provides the requested resources in a report, e.g. an emissions/diagnostics test report. In this activity, the read service invoked via the SCN-fronting ITS-SU assumes the requested data is for local user consumption only, i.e. does not contain data needed in a mandated or formalized regulatory report. The data is read and displayed to the user using the IDX device. Data is not further disseminated.
S1-04	SCN reports data for remote consumption by regulatory authority	Pre-requisites: S1-01, S1-02 The IDX device in this activity requests data via the SCN-fronting ITS-SU. The peer ITS-SU generates report data for an external regulator. In this activity, the IDX device is an intermediary facilitating the transaction between the SCN and the regulator, for example, passing a road weather data report from the SCN to to a weather management centre. It is assumed the regulator requires reasonable assurance the data came from a valid SCN or SCN-fronting ITS-SU.
S1-05	IDX device reports public data for remote consumption by regulatory authority	Pre-requisites: S1-01, S1-02 The IDX device in this activity requests and receives diagnostics data from the SCN-fronting ITS-SU. The IDX device performs additional analysis over the data/report and generates its own report for external regulator consumption. It is assumed the regulator requires non-repudiation and high assurance the data came from the indicated user, shop or IDX device (not the SCN).

© ISO 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

Table 1 *(continued)*

ID	Activity	Description
Scenario 2 activities		
S2-01	IDX device ITS-SU requests from SCN ITS-SU a resource listing	Pre-requisites: G01-G07 The IDX device ITS-S should be capable of asserting its privileges to request details related to what privacy-protected data it is allowed to access. This activity consists of the IDX device requesting a resource listing after completing its TLS handshake with the peer ITS-SU. The resource listing should list only the privacy-protected resources that the IDX device, based on its presented 1609.2 certificate, should be allowed to know about. Note that an available resource listing can include resources that the user's certificate role is allowed to discover but not access. Some SCN resources, after discovered, can require additional authentication/authorization checks prior to accessing. The existence of other resources can be highly sensitive and not disclosed in the resource listing unless the user initiated the secure session with the appropriate role.
S2-02	Request privacy-sensitive data from SCN	Pre-requisites: G01-G07 and optionally G08 and S2-01 The IDX device connection to the SCN-fronting peer ITS-SU is complete after the peer has determined that a valid IDX device has connected. The user initiates via the IDX device a read-request on privacy-sensitive data elements or files. The IDX device checks if the user is authorized to perform this request. If yes, the IDX device sends the request to the SCN peer ITS-SU. If not, the IDX device indicates to the user that authorization is denied.
S2-03	SCN processes service-device request for privacy-sensitive data	Pre-requisites: G01-G08, S2-02 The peer SCN ITS-SU receives the request for privacy-sensitive data and using ISO/TS 21177 checks the application's security policy to determine if the secure session's client certificate is authorized to access the data. The response is either 1) yes, 2) no, 3) enhanced authentication required, or 4) extended authorization required via third-party authorization service. If yes: Provide data directly as a response to the request. If no: Return authorization error. If enhanced authentication is required: Utilize ISO/TS 21177 primitive to indicate to the IDX device that enhanced authentication is required. If extended authorization required: Utilize ISO/TS 21177 primitive to indicate to the IDX device extended authorization is required. The two ITS-SUs make use of the third-party authorization service as indicated by the peer ITS-SU to the IDX device displaying to maintenance worker the message "waiting for owner approval...").

© ISO 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

Table 1 *(continued)*

ID	Activity	Description
S2-04	SCN uses third-party authorization service to obtain data owner consent for local data release	Pre-requisites: S2-03 If third-party authorization is required, the SCN initiates the third-party authorization service provider with a request for owner consent. It summarizes or references the type of data being requested by the IDX device. By policy, it can also request from the SCN owner a) a one-time access, b) a time block over which the access can be performed or c) some other conditions on the access. The third-party authorization service sends a secure request to the SCN owner (e.g. smart phone). The owner responds with a grant or denial of the request. The owner response is indicated back to the SCN (or IDX device, depending on implementation) with the result of the requested access. If granted, the SCN application via the peer ITS-SU provides the privacy protected data to the IDX device.
S2-05	SCN uses third-party authorization service to obtain SCN owner/operator consent for remote data release	Pre-requisites: S2-02 This activity is identical to S2-03 with the exception that the disclosure, i.e. read access, of the privacy-protected data will only be to a known, remote entity, not the IDX device. It is expected in this case that the SCN-fronting ITS-SU provides the protected data to the IDX device in encrypted form so that the IDX device cannot read it. The IDX device is then expected to relay this data to a remote consumer that is able to decrypt and read the data.
Scenario 3 activities		
S3-01	IDX device ITS-SU stages a SCN software image load via SCN ITS-SU	The IDX device downloads critical software/firmware or configurations for the SCN. (Note: The IDX device ITS-S will perform a pre-validation including ISO21177 access control check on certificate ITS-AID prior to allowing a software image to be loaded to a SCN).
S3-02	IDX device performs write-execute functions in the SCN	The IDX device performs the load of a software image file to a SCN and receives a confirmation status in return.
S3-03	IDX device manages SCN access policy (application-specific)	The IDX device initiates a request to manage/update the SCN ITS-SU access control policy. This results in the download of the existing policy and request to make an update to that policy.

6.3 Device assets

This subclause details the assumed assets related the IDX device, the device environment, including assets of the connected SCN application, and the scenarios to which the assets pertain. Threats can impact any one or more of the listed assets.

The scenario-specific asset listing is intended to provide the security practitioner the assumed assets of the IDX device that can be threatened in the operational environment.

Asset	Description	S1	S2	S3
IDX device firmware (platform)	Firmware for the IDX device.	x	x	x
IDX device application software	Software applications on the IDX device. IDX device applications access resources from SCN applications via the SCN ITS-SU.	x	x	x
IDX device user account data	Names, identifiers, logins, role assignments, account terms and other account data that controls which users can access the IDX device and what local applications they can accessing via the SCN ITS-SU.	x	x	x

© ISO 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

Asset	Description	S1	S2	S3
IDX device access control policies	Policies that control access to IDX device applications and services based on the accessor's identity. These policies can also map certificates to specific users. The existence of some policies and related services can be sensitive, therefore there can be a confidentiality sensitivity of this asset.	x	x	x
User passwords and other authenticators	Authenticators that authorized users use to prove their identities.	x	x	x
IDX device platform configuration data	Configurable parameters that can change the behaviour of the IDX device. This can be in the form of flat files, MIBs, etc. The existence of some policies and related services can be sensitive, therefore there can be a confidentiality sensitivity for this asset.	x	x	x
IDX device firewall settings	A type of configuration data that controls external access to the device.	x	x	x
SCN ITS-SU access control policy(s)	Access control policy resident on the SCN ITS-SU that controls access to SCN application and data resources. This policy can be used by the SCN ITS-SU to make grant/deny requests to requested resources over ISO/TS 21177.	x	x	x
IDX device application and data access control policy(s)	Access control policy resident on the IDX device that controls access to IDX device's client applications and data resources. This policy can be used by the IDX device to make grant/deny requests when the user using the IDX device requests certain operations or data accesses.		x	x
Certificate provisioning reachability settings	Network/application location information used by the IDX device certificate provisioning logic to obtain/refresh certificates and trust credentials.	x	x	x
IDX device platform logs	Logs that are accessible by a device administrator or possibly vendor.			
SCN ITS-SU access control policies	These access control policies are resident on the SCN ITS-SU. They can control the following: 1) which certificates/SSPs can invoke which services or access certain data; and 2) which certificates/SSPs can access which vehicular applications.	x	x	x
SCN firmware, software and applications	SCN executables that originate from the SCN or aftermarket vendor and can be invoked or loaded by an IDX device.			x
SCN public diagnostics data	Low-sensitivity application data originating from the SCN. Typically, these are diagnostics test codes, emissions or other diagnostics-related data that are not privacy-sensitive. Integrity and source authentication potentially needed in some applications.	x		
SCN public diagnostics ata Rerports	Assume that public diagnostics data are components of a report, in addition to other metadata. These assets can be meant for consumption by the diagnostics user or by some type of regulator or other organization. Reports can be directly generated by the SCN or can be generated by the IDX device. Integrity and source authentication potentially needed in some applications. It is assumed that any metadata in the report is also not privacy-sensitive.	x		

© ISO 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

Asset	Description	S1	S2	S3
SCN PII / tracking data / proprietary data	Data originating from the SCN that is privacy-sensitive or required to be privacy-protected. This can include metadata about the SCN owner, data that links the SCN to the owner, tracking-related data, PII/SPII or OEM/vendor-proprietary data. This information has an expectation of confidentiality and should require either a policy or technical control to restrict who has access to it. Regulatory test reports originating from the SCN can fall into this category if they contain data or metadata that is privacy-sensitive. Potentially sensitive to confidentiality, integrity and authenticity lapses.		x	
Writable or executable data	This data asset can include: — Commands or API calls from the IDX device to the SCN that enable writing of sensitive data. — SCN ECU firmware or applications. — Sensitive configuration files/data originating from the IDX device or vendor. This data can include confidentiality sensitivity if it contains vendor-proprietary information.			x
Cloud services trust anchors	Roots of trust for device, application or cloud service vendors that enable the IDX device to trust service endpoints.	x	x	x
Cloud services TLS public keys (incl. certificates)	These are public keys/certificates associated with the IDX device and also associated with the cloud service (e.g. third-party authorization service).	x	x	x
Cloud services TLS private keys	Private keys belonging to the IDX device that can be used to authenticate itself to cloud/vendor services.	x	x	x
IDX device application certificates	1609.2 certificates used by the IDX device to authenticate via ISO/TS 21177 TLS to the SCN ITS-SU.	x	x	x
IDX device application private keys	Private keys (pairwise to the IDX device application certificate public keys) belonging to the IDX device that can be used to authenticate itself to the SCN ITS-SU using ISO/TS 21177.	x	x	x
Application encryption public keys	An entity's application-specific 1609.2 encryption public key, typically embedded in a 1609.2 certificate.			x
Application encryption private keys	The pairwise private key for the encryption public key. This key is not shared/disclosed by the owner. It is used to perform an ECIES encryption over data.			x
SCN ITS-SU application certificates	Certificate(s) presented by the SCN ITS-SU when establishing secure TLS sessions with the IDX device. These certificates and the SCN ITS-SU's private keys can also be used for non-repudiation on transactions/data coming from the SCN ITS-SU.	x	x	x
Revocation information	Information sourced from applicable PKIs that indicates the revocation status of CA and end entity certificates. Can be in the form of CRLs or OCSP-type services/structures.	x	x	x

6.4 Threats

6.4.1 General

This subclause provides a listing and description of threats against the IDX device, its assets and environment according to the different data types that the IDX device is intended to access in the SCN.

© ISO 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

Threats are considered from the following perspectives:

— **Threat sources/actors**: Some threats are device-oriented and can be local or remote to the device and its intended operational environment, i.e. threats are not necessarily local to the device or its immediate physical proximity.

— **Device threats are data threats**: The purpose of this threat model is to ascertain required protections for a generic ITS-S that can or cannot be vehicular in nature. Accordingly, the three data access scenarios are threat modeled both from a device and data perspective, i.e. the impact of certain device compromises necessarily assumes that the data it was protecting is also compromised.

— **System threats**: System-level threats are considered for overall impact to either the owner or other stakeholders of the SCN (e.g. surrounding drivers) and the larger ecosystem. For example, the document also addresses device-oriented PKI threats.

— **PKI ecosystem threats**: Associated with the TOE environment is the larger PKI ecosystem serving that environment. To that end, this document highlights threats to the PKI, which, if not mitigated, can flow down substantial impacts to the TOE and its operating environment.

The threats identified in this section are neither exhaustive nor tailored for any particular ITS domain. Given that the scenarios are genericized in terms of data sensitivities, the threats identified for each are based on assumptions and rationale listed for each. Developers of specific applications are expected to carry out their own analysis of security assumptions and requirements, using this section as a template.

6.4.2 Threat modelling process

The threat modelling in this technical report loosely follows the formalized process of the common criteria (ISO 15408-1 and ISO 15408-2). However, it is abbreviated due to the genericized nature of the data types and devices. The threats are principally attack-oriented.

Prior to starting the threat modelling, the following pre-requisite actions are performed:

a) Characterize the data sensitivities for each Scenario, based on generic examples of those data types; see 6.2.3.

b) Model and depict the IDX device as a generic ITS-S; see 6.2.2.

c) Model and depict the operational environment; see 6.2.2:

   1) peer devices,

   2) assumed communication modes, i.e. the ability to communicate both X.509 TLS and ISO/TS 21177 secure communications, and

   3) assumed capabilities and/or services, such as an external authorization service.

The threat modelling process relevant to the development or validation of PP material includes the following steps:

a) Identify threat categories and attack vector types.

b) Characterize different attack motivations.

c) Identify the threats.

d) For each threat, provide a qualitative risk rating based on impact and probability.

6.4.3 Threat categories and actor motivations

Threat categories factored into modelling are presented in Table 2:

© ISO 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

Table 2 — Threat categories and vectors

Threat category or attack vector	Attack vector type
Supply chain	Cyber
Maintenance environment	Cyber
External network connection	Cyber
External shared or infrastructure services	Cyber
Trusted or partner network connection	Cyber
Internal network	Cyber
Internal shared or infrastructure services	Cyber
Mobile or transiently connected devices	Cyber
Authorized actions of non-privileged user	Cyber
Authorized actions of privileged user	Cyber
Device port (e.g. removable media)	Cyber
Data	Cyber
Immediate physical proximity	Physical
Indirect attack (e.g. tampering with HVAC, etc.)	Physical
Privileged user	Human (intended effects: coercion, subversion, deception, incapacitation)
Normal user	Human (intended effects: coercion, subversion, deception, incapacitation)
External actor	Human (intended effects: coercion, subversion, deception, incapacitation)
Maintainer	Human (intended effects: coercion, subversion, deception, incapacitation)
Developer/integrator	Human (intended effects: coercion, subversion, deception, incapacitation)
Denial of service	Human or Cyber
System error	Other
Misconfiguration (intentional or accidental)	Human

Threat/Attacker motivations factored into the modelling are provided in Table 3.

Table 3 — Possible attacker motivations

Motivation	Description
Ideology	The attacker is motivated by a fundamental belief that the attack is needed and justifiable.
Coercion	The attacker seeks for compel some action or behaviour of the victim or a stakeholder to the attack.
Notoriety	The attacker seeks publicity and fame, whether or not the attacker is individually credited.
Personal satisfaction	The attacker's motivation is to satisfy a basic urge or inclination to perform the attack.
Organizational gain	Competitive advantage.
Financial gain	Financial gain (fraud against or theft from the organization, acquisition of sellable/usable PII, acquisition of sellable/usable competitive information), extortion, fraud against or theft from the organization's customers, suppliers, or partners).
Disgruntlement	Personal motives (attention, malice/resentment, acquisition of PII about targeted individuals).
Accidental	The realization of the threat is accidental, i.e. not purposeful.

© ISO 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

Table 3 *(continued)*

Motivation	Description
Dominance	The attacker seeks to overcome and/or overwhelm the victim or another stakeholder.
Unpredictable	The attacker is unstable or otherwise unpredictable in his/her motivations.
Positional/stepping-stone	Acquisition of a launching point for targeted attacks, acquisition of resources that can be used in targeted attacks, acquisition of intelligence about other entities.
Tracking/stalking	Exploitation of the trackability of the device or its data in order to stalk.

6.4.4 Scenario comparison of threats

Table 4 identifies threats relevant to the three data sensitivity scenarios. For each, a description is provided in addition to a mapping to one or more of the three data sensitivity scenarios.

Table 4 — Scenario-based applicability and comparison of threats

Threat	Description	S1	S2	S3
T.THEFT	An attacker could try to gain illicit knowledge of the IDX design and thereby more easily mount an attack to compromise the integrity or authenticity the data processed by the device.	x	x	x
T.PHYSICAL_TAMPER	An attacker could attempt to access the internal components of the TOE to bypass software security controls and extract data including firmware which could lead to exposure of default passwords and other information.	x	x	x
T.INTERFACE_EXPLOITATION	Attacker is able to gain access to an IDX device through misconfigured or insecure physical or logical interfaces. Note that this threat is not indicated for Scenario 1 data sensitivities. However, it is possible for exploitation of the interface to target resource exhaustion of the ITS-S. If resource exhaustion is a threat to a design and implementation, then it should be included for Scenario 1.		x	x
T.UNAUTHORIZED_LOCAL_TRUST_CHAIN_MODIFICATION	An attacker is able to gain write access to the IDX device trust store, resulting in the ability to delete existing root or other CA certificates that would cause message validation failure or to add new root/CA certificates that would introduce unexpected and unauthorized trust relationships.	x	x	x
T.ENVIRONMENT_CA_COMPROMISE	An attacker is able to compromise one of the SCMS CAs resulting in illegitimate issuance of trusted certificates that allow SCN ITS-SU and IDX devices to spoof legitimate system components.	x	x	x
T.ENVIRONMENT_UNREPORTED_MISBEHAVIOUR_MALFUNCTION	Misbehaving components are not reported in a timely manner for revocation action, resulting in the ability for a compromised IDX device or SCN ITS-SU to establish trusted relationships with other components until the revocation process is completed.	x	x	x
T. PRIVATE_KEY_DISCLOSURE	An attacker is able to obtain the private keys for authentication of the IDX device, allowing the attacker to masquerade as the device and perform trusted functions with the SCN ITS-SU. Note that this threat is not indicated for Scenario 1 data sensitivities. However, it is possible for disclosure of private key material to be a prerequisite to targeting resource exhaustion of the ITS-S. If resource exhaustion is a threat to a design and implementation, then disclosure of private key material should be included for Scenario 1.		x	x
T.EPHEMERAL_OR_SESSION_KEY_DISCLOSURE	An attacker is able to intercept the session keys generated using ECIES resulting in a loss of confidentiality for data exchanges between the IDX device and SCN ITS-SU.		x	x

© ISO 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

Table 4 *(continued)*

Threat	Description	S1	S2	S3
T.UNAUTHORIZED_PRIVATE_KEY_USE	An unauthorized user is able to gain access to an unprotected private key and use the key for messaging and transactions between the IDX device and SCN ITS-SU, allowing an unauthorized user to perform potentially privileged transactions or masquerade as authorized system components. Note that this threat is not indicated for Scenario 1 data sensitivities. However, it is possible for unauthorized private key use to be a prerequisite to targeting resource exhaustion of the ITS-S. If resource exhaustion is a threat to a design and implementation, then disclosure of private key material should be included for Scenario 1.		x	x
T.SOFTWARE_FIRMWARE_TAMPER_IN_TRANSIT	An attacker could alter the firmware of the IDX device during or prior to the update process to introduce malicious functionality or backdoors or identify ways to take root permissions on the IDX device. In this way, an attacker achieves potentially privileged operation of the IDX device.		x	x
T.SOFTWARE_FIRMWARE_TAMPER_AT_REST	An attacker could gain access to IDX device firmware by extracting from the device and then alter the firmware to a malicious one or identify ways to take root permissions on the device. In this way an attacker achieves potentially privileged operation of the IDX device.		x	x
T.SOFTWARE_FIRMWARE_INTEGRITY_ERROR	IDX firmware validation results in an integrity error, disrupting the operations and availability of the IDX device.	x	x	x
T.UNAUTHORIZED_ACCESS_POLICY_MODIFICATION	An attacker is able to obtain write access to the IDX device access policy configurations, resulting in the ability for the attacker to grant him/herself permissions for performing sensitive functions.		x	x
T.LACK_OF_REVOCATION_INFORMATION_AVAILABILITY	The IDX device is unable to retrieve the latest revocation information, resulting in the device potentially trusting compromised/revoked certificates until revocation information is available.	x	x	x
T.PRIVILEGE_ESCALATION	A logged in user to the IDX device is able to escalate privileges on the device to perform functions that were not authorized for his/her role.		x	x
T.UNAUTHORIZED_ACCOUNT_ASSUMPTION	Users could try to access functions not allowed to them when previous user has not properly logged out, to modify or delete user data, download sensitive SCN information or modify downloaded SCN data.		x	x
T.EAVESDROPPING	An attacker exposed to the communications medium between the IDX device and SCN ITS-SU is able to tap into the communications and decode messaging resulting in a loss of confidentiality.		x	x
T.ENIVIRONMENT_NETWORK_ATTACKER_IN_THE_MIDDLE	A successful modification of data exchanged between the IDX device and SCN ITS-SU would allow an attacker to view or change configurations, upload new software, or download sensitive data.		x	x
T.ENVIRONMENT_SCN_SPOOFING	SCN is masquerading as a genuine SCN ITS-SU sending false information in messages that are otherwise valid.		x	x
T.DEVICE_SPOOFING	Equipment masquerading as a genuine IDX device is able to upload new software or change configurations in the SCN.		x	x
T.ENVIRONMENT_UNKNOWN_COMPROMISED_PEER	The IDX device is threatened due existence of a compromised SCN ITS-SU peer; data loss, privacy losses, integrity losses.		x	x
T.ENVIRONMENT_EXECUTION_SENSITIVE_COMMANDS_ON_COMPROMISED_PEER	The IDX device connects to a compromised SCN ITS-SU system and executes sensitive commands on it. In this case, a loss of integrity of the peer device could mean that the sensitive command invoked by the IDX device is modified, doesn't work correctly, or is otherwise obstructed or hijacked. Commands executed on integrity violated/compromised SCN ITS-SU peers are modified prior to execution resulting in a loss of its functionality.			x
T.ENVIRONMENT_ACCESS_PRIVACY_PROTECTED_DATA_WITHOUT_CONSENT	Privacy protected data is transmitted from the SCN ITS-SU to the IDX device and accessed without data owner's explicit permission.		x	

© ISO 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

Table 4 *(continued)*

Threat	Description	S1	S2	S3
T.ENVIRONMENT_SCN_SOFTWARE_IMAGE_TAMPER	A tampered software image is received by the IDX device from the OEM or supplier. This threat can leverage local or remote access to firmware files prior to the IDX device's download from the manufacturer and staging to the SCN via the SCN ITS-SU. Includes access to OEM/supplier web services repositories. If the device cannot identify that the software image has been altered, then it will stage a potentially malicious image for loading into the SCN.		x	x
T.ENVIRONMENT_SCN_SOFTWARE_IMAGE_REVERSE_ENGINEER	IDX device is physically accessed allowing extraction of staged software image from storage. Once extracted from storage, the binary can be reverse engineered to support security analysis by an attacker leading to identification of vulnerabilities, default passwords, software library versions (e.g. vulnerable versions) and other security intelligence.		x	x
T.MALICIOUS_SOFTWARE_LOAD_TO_SCN	An IDX device loads a malicious software image into the SCN because it did not either 1) validate the software signature itself prior to staging, or 2) maintain a trusted storage environment on itself for all software image staging.		x	x
T.LOAD_KNOWN_VULNERABLE_SOFTWARE_VERSION	IDX device loads a previous version of software to vehicle. Previous software version contains known vulnerabilities, thus constituting a downgrade attack.		x	x
T.SOFTWARE_METADATA_MODIFICATION	IDX device allows an attacker to access and modify the metadata associated with a software image file. Metadata can be used by vehicle components to support loading and validation of cryptographic signatures.		x	x
T.ENVIRONMENT_SCN_ACCESS_POLICY_UPDATE	An attacker is able to modify the access control policy of the SCN ITS-SU, allowing anyone to load firmware or read/write sensitive data and/or functions.		x	x
T.DATA_LEAKAGE	Attackers could try to leak data from the IDX device to third parties who should not receive this data. Data includes user account information, sensitive vehicle/owner data, keys and certificates.		x	x
T.MALICIOUS_CODE_INJECTION	A compromised IDX device could introduce malicious code into the SCN firmware or software executable.		x	x
T.SCN_DATA_TAMPERING	An authorized attacker can access data and reports and change details (e.g. emissions logs, maintenance history) prior to providing them to a vendor, regulatory authority, etc.		x	x
T.USER_ACCOUNT_MASQUERADE	An unauthorized user is able to access the IDX device due to no password protections or weak password protections.		x	x
T.DATA_TO_DEVICE_OWNER_LINKAGE	Asset: PII/tracking data. It is assumed the SCN or its fronting SCN ITS-SU has data, which if accessed could link an individual to the data. If this data is intended to be accessed for external use, some applications or policies can require that it either 1) be accessed by an authorized party, or 2) undergo some type of sanitization prior to the access (i.e. to make the data public).		x	x
T.ENVIRONMENT_PKI_SPOOFING	IDX device stores reachability information and trust anchors for connecting to a PKI. An attacker can modify the stored PKI location (e.g. URL) and/or the trust anchors needed to connect to the PKI, thus allowing the attacker to perform MITM attacks against the PKI.		x	x

6.5 Security objectives

6.5.1 Summary and comparison by scenario

This subclause provides a set of derived security objectives that security practitioners can use in building or comparing PPs. Table 5 provides the security objectives, based on threats identified in 6.4, required to counter the threats specific to each data sensitivity scenario.

NOTE The security objectives are high level definitions of security capabilities of a TOE, and one or more common criteria SFR are designed to map to each; see 6.6 for SFR mappings. A PP includes the full traceability of a) threats to security objectives, and b) security objectives to SFR (and in some cases organizational policy).

© ISO 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

In addition to security objectives, Table 6 provides a listing and brief description of organizational policies needed to counter threats. This document does not map organizational policies to SFRs, as this level of granularity is much more specific to the applications and environments at hand. Annex A provides the full mapping of both security objectives and organizational policies to the defined threats.

If an IDX device is expected to host applications of more than one of the identified types, the device will be expected to be conformant with the PP requirements for each application.

Table 5 — Scenario-specific security objectives

Security objective (SO)	Description	S1	S2	S3
General platform objectives				
OT_PLATFORM_USER_MGMT	Securely manage users including the creation, update and deletion of user accounts and allocation to roles/groups.		x	x
OT_PLATFORM_PRIVILEGED_USER_AUTHORIZATION	Ensure that only registered legitimate users are able to gain access to system's file system and services with privileged rights.		x	x
OT_PLATFORM_SECURE_KEY_MGMT	Provide secure key management and provisioning of platform cryptographic key material.	x	x	x
OT_EXT_FW_PROTECT	Device validates signatures on all software/firmware loads. It is assumed that this is applied only to external firmware intended to be loaded to the SCN.			x
OT_PLATFORM_AUTHENTICATION	The TOE requires authenticated access for all services.		x	x
OT_PLATFORM_SECURE_BOOT	Device performs secure boot.		x	x
OT_PLATFORM_DATA_AT_REST_PROTECT	Device uses trusted storage to secure data at rest.		x	x
OT_PLATFORM_MALWARE_PROTECT	Device guards against the installation and execution of malware.			x
OT_PLATFORM_LOG	Device logs security-sensitive events.		x	x
OT_PLATFORM_TAMPER_PROTECT	Device guards against tamper.		x	x
OT_PLATFORM_COMM_INTERFACE_PROTECT	The TOE does not expose insecure network services, has firewall functionality and enforces against a policy.	x	x	x
OT_PLATFORM_PHYSICAL_INTERFACE_PROTECT	Access to all physical ports is authenticated.	x	x	x
OT_PLATFORM_REMOTE_CONNECTION_PROTECT	All remote connections are secured.		x	x
OT_PLATFORM_TRUST_CHAIN_PROTECT	The TOE ensures the integrity of the local trust chain.	x	x	x
OT_PLATFORM_CERT_REVOCATION	Device monitors for updates to certificate revocation information (CRLs, OCSP, etc.)	x	x	x
OT_EXT_FW_PROTECT	Device firmware is signed by the developer.			x
OT_EXT_FW_PROTECT	Device firmware is encrypted.			x
OT_PLATFORM_ALERT_INFORM	The device issues alerts/notices for significant security events including lack of available revocation information.		x	x
OT_PLATFORM_SESSION_PROTECT	Service device applications enforce screen timeouts/locks and require re-authentication after a configurable period of timeout.		x	x
OT_PLATFORM_AC_POLICY_PROTECT	Access policy is integrity protected and requires authentication for access.		x	x
OT_PLATFORM_RELIABLE_TIME	Reliable timestamping required for secure authorization checks for applications.		x	x
Device application security objectives				
OT_APP_AUTHENTICATION	Users authenticate before the application provides any services.		x	x
OT_APP_SECURE_KEY_MGMT	Provide secure key management and provisioning of application-specific cryptographic key material.	x	x	x
OT_APP_VALIDATE_PEER_STATE	Device can validate the current peer's security state through attestation transaction prior to loading or retrieving sensitive data.			x
OT_APP_ANONYMIZATION	Data is anonymized to ensure that privacy protected data cannot be later tied to a specific SCN operator or data owner.		x	x
OT_APP_THIRD_PARTY_AUTHORIZATION	Owner consent is required for access to all sensitive information.		x	x
OT_APP_ALERT_INFORM	Owners are notified of all attempts to access sensitive information.		x	x
OT_APP_USER_MANAGEMENT	Ensure that only registered legitimate users are able to gain access to system's file system.		x	x
OT_APP_DATA_AT_REST_PROTECT	Data received from a SCN ITS-SU as well as device-internal data (e.g., Configuration files, firmware) is encrypted and access controls applied.		x	x
OT_APP_EXT_FW_PROTECT	Service device validates signatures on firmware to be loaded.			x

© ISO 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021

Table 5 *(continued)*

Security objective (SO)	Description	S1	S2	S3
OT_APP_CERT_REVOCATION	Application monitors for updates to CRL.	x	x	x
OT_APP_TRUSTED_STORAGE	IDX implements integrity protection on user data stored within the device.		x	x
OT_APP_SECURE_BOOT	IDX implements secure boot process to guard against malicious code and identify integrity failures.			x
OT_APP_AC_POLICY_PROTECT	System provides integrity protection for access policy and requires authentication for access or update.		x	x
OT_APP_ROLLBACK_RECOVERY	Rollback sensitive configuration changes or operations, especially during configuration of a SCN.			x
PKI provider security objectives				
OT_PROV_KEY_MGMT_AUTHORITY_REVOCATION	CA infrastructure processes and communicates authority revocation list information and revokes all certificates issued under a revoked CA.	x	x	x
OT_PROV_KEY_MGMT_AUTHORITY_MISBEHAVIOUR_DETECTION	Key management infrastructures that manage keys for device implement misbehaviour detection systems.	x	x	x

Table 6 provides a listing of organizational policies that should be incorporated to counter threats to IDX devices and their environments.

Table 6 — Organizational Policies

Organizational Policy	Description
P. LOG_ASSET_INVENTORY	The environment that a TOE is used or stored within should implement procedures to log any removal of the device from the environment.
P.PHYSICAL_ACCESS	The environment that a TOE is used or stored within provides proper monitoring/escort for unauthorized users.
P.PHYSICAL_MONITORING	The environment that a TOE is used or stored within is be monitored for unauthorized entry after hours.
P.SECURE_MANAGEMENT	The TOE provides management means for the authorized administrator to manage the IDX device in a secure manner.
P.DATA_UNLINKABILITY	The IDX device protects data that is linkable to individuals.
P.UNLINKABILITY_OF_TRANSMITTED_DATA	The IDX device and SCN ITS-S secure session and transport protocol disassociate session information and artifacts from data owners.
P.MISBEHAVIOUR_REVOCATION_REPORTING	The organization implements policies and procudures to 1) detect misbehaviour, 2) obtain misbehaviour metadata, 3) report misbehaviour and, as needed, 4) request misbehaviour-based revocation of devices.

6.5.2 Analysis

The security objectives defined in Table 5 provide a defence-in-depth approach towards securing an IDX device that operates under the constraints of one of the three defined scenarios.

Scenario 1 is focused on processing only non-sensitive data, and it was assumed that any connectivity to the SCN ITS-SU requires a secure connection as per ISO/TS 21177 and also to satisfy a basic need in the environment to promote honest actors and devices that have undergone basic provisioning. This drives the allocation of security objectives that support secure key management and secure interface/connectivity. Additionally, security objectives have been allocated to Scenario 1 that focus on good cyber hygiene in order to limit the likelihood that a legitimate but infected requestor device attempts to connect to sensitive SCN systems. Security objectives include malware protection and session protection. Also identified are application-layer security objectives that would be allocated to the various software applications expected to be installed on an IDX device. These security objectives align with the objectives allocated to the IDX device itself, with the understanding that some objectives can be demonstrated by the host (IDX device) instead of the application.

Scenario 2 security objectives build upon the objectives allocated to Scenario 1. Scenario 2 is based on the receipt, storage and/or processing of sensitive data, privacy-protected data, and data that can support regulatory decision making (e.g. emissions test results). Thus, Scenario 2 security objectives are focused heavily on the design/implementation of a secure platform and secure management of users and roles. Data at rest protections, tamper protections, and remote connectivity protections are

© ISO 2021 – All rights reserved

AVA Documents Document Sharing Hub
Full document details: PD CEN ISO/TR 21186-3:2021