TECHNICAL REPORT

ISO/TR 21186-3

First edition
2021-02

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

Part 3: Security

Systèmes de transport intelligents coopératifs (C-ITS) - Lignes directrices pour l'utilisation des normes —
Partie 3: Sécurité

Reference number
ISO/TR 21186-3:2021(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

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.

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.

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).

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

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

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

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.

— 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;

— 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.

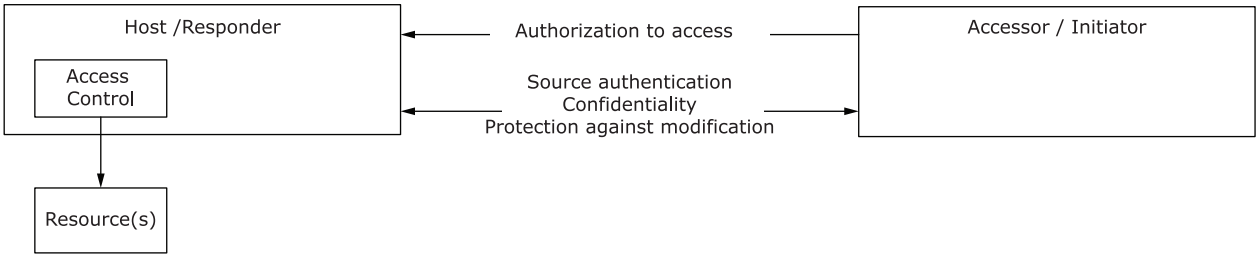

Figure 1 — Security services for non-broadcast communications topologies

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.

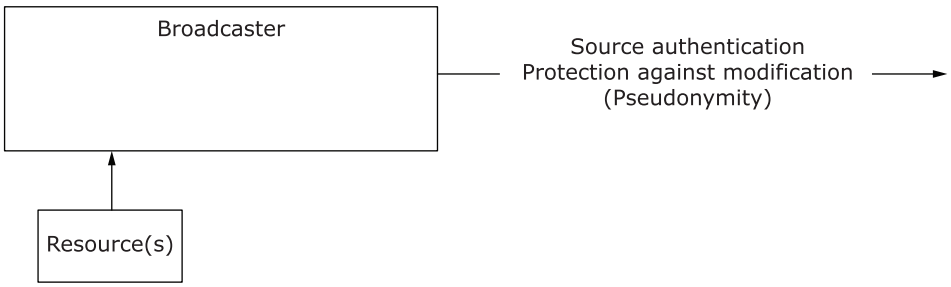

Figure 2 — Security services for broadcast communications topologies

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.