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

bsi.

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.

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

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

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

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.

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 67

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

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 authoring 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).

TECHNICAL REPORT **ISO/TR 21186-3:2021(E)**

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