

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 Verkehrssysteme (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

Contents	Page
European foreword.....	3

CEN ISO/TR 21186-3:2021 - Preview only Copy via ILNAS e-Shop

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.

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





COPYRIGHT PROTECTED DOCUMENT

© ISO 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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	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