

English Version

Electronic fee collection - Security framework (ISO/TS 19299:2015)

Perception de télépéage - Cadre de sécurité (ISO/TS
19299:2015)

Elektronische Gebührenerhebung -
Sicherheitsgrundstruktur (ISO/TS 19299:2015)

This Technical Specification (CEN/TS) was approved by CEN on 26 June 2015 for provisional application.

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

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

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, 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: Avenue Marnix 17, B-1000 Brussels

Contents	Page
European foreword.....	3

European foreword

This document (CEN ISO/TS 19299:2015) 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 [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

This document supersedes CEN/TS 16439:2013.

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

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

Endorsement notice

The text of ISO/TS 19299:2015 has been approved by CEN as CEN ISO/TS 19299:2015 without any modification.

TECHNICAL SPECIFICATION

ISO/TS 19299

First edition
2015-10-01

Electronic fee collection — Security framework

Perception de télépéage — Cadre de sécurité



Reference number
ISO/TS 19299:2015(E)

© ISO 2015



COPYRIGHT PROTECTED DOCUMENT

© ISO 2015, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

	Page
Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	2
3 Terms and definitions	4
4 Symbols and abbreviated terms	9
5 Trust model	10
5.1 Overview.....	10
5.2 Stakeholders trust relations.....	10
5.3 Technical trust model.....	11
5.3.1 General.....	11
5.3.2 Trust model for TC and TSP relations.....	11
5.3.3 Trust model for TSP and service user relations.....	13
5.3.4 Trust model for Interoperability Management relations.....	13
5.4 Implementation.....	13
5.4.1 Setup of trust relations.....	13
5.4.2 Trust relation renewal and revocation.....	14
5.4.3 Issuing and revocation of sub CA and end-entity certificates.....	14
5.4.4 Certificate and certificate revocation list profile and format.....	15
5.4.5 Certificate extensions.....	15
6 Security requirements	17
6.1 General.....	17
6.2 Information security management system.....	18
6.3 Communication interfaces.....	18
6.4 Data storage.....	19
6.5 Toll charger.....	19
6.6 Toll service provider.....	21
6.7 Interoperability Management.....	23
6.8 Limitation of requirements.....	23
7 Security measures — countermeasures	24
7.1 Overview.....	24
7.2 General security measures.....	24
7.3 Communication interfaces security measures.....	25
7.3.1 General.....	25
7.3.2 DSRC-EFC interface.....	26
7.3.3 CCC interface.....	27
7.3.4 LAC interface.....	28
7.3.5 Front End to TSP back end interface.....	28
7.3.6 TC to TSP interface.....	29
7.3.7 ICC interface.....	30
7.4 End-to-end security measures.....	30
7.5 Toll service provider security measures.....	32
7.5.1 Front end security measures.....	32
7.5.2 Back end security measures.....	33
7.6 Toll charger security measures.....	34
7.6.1 RSE security measures.....	34
7.6.2 Back end security measures.....	34
7.6.3 Other TC security measures.....	35
8 Security specifications for interoperable interface implementation	35
8.1 General.....	35
8.1.1 Subject.....	35

8.1.2	Signature and hash algorithms.....	35
8.2	Security specifications for DSRC-EFC.....	36
8.2.1	Subject.....	36
8.2.2	OBE.....	36
8.2.3	RSE.....	36
9	Key management.....	36
9.1	Overview.....	36
9.2	Asymmetric keys.....	36
9.2.1	Key exchange between stakeholders.....	36
9.2.2	Key generation and certification.....	37
9.2.3	Protection of keys.....	37
9.2.4	Application.....	37
9.3	Symmetric keys.....	38
9.3.1	General.....	38
9.3.2	Key exchange between stakeholders.....	38
9.3.3	Key lifecycle.....	39
9.3.4	Key storage and protection.....	40
9.3.5	Session keys.....	41
	Annex A (normative) Security profiles.....	42
	Annex B (normative) Implementation conformance statement (ICS) proforma.....	46
	Annex C (informative) Stakeholder objectives and generic requirements.....	64
	Annex D (informative) Threat analysis.....	68
	Annex E (informative) Security policies.....	124
	Annex F (informative) Example for an EETS security policy.....	131
	Annex G (informative) Recommendations for privacy-focused implementation.....	133
	Annex H (informative) Proposal for end-entity certificates.....	135
	Bibliography.....	136