



BSI Standards Publication

Electronic fee collection — Secure monitoring for autonomous toll systems

Part 1: Compliance checking

National foreword

This Published Document is the UK implementation of CEN/TS 16702-1:2020. It supersedes PD CEN/TS 16702-1:2014, which is withdrawn.

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 secretary.

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 2020
Published by BSI Standards Limited 2020

ISBN 978 0 580 99699 3

ICS 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 30 April 2020.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

TECHNICAL SPECIFICATION
 SPÉCIFICATION TECHNIQUE
 TECHNISCHE SPEZIFIKATION

CEN/TS 16702-1

January 2020

ICS 35.240.60

Supersedes CEN/TS 16702-1:2014

English Version

**Electronic fee collection - Secure monitoring for
 autonomous toll systems - Part 1: Compliance checking**

Perception du télépéage - Surveillance sécurisée pour
 systèmes autonomes de péage - Partie 1 : Contrôle de
 conformité

Elektronische Gebührenerhebung - Sichere
 Überwachung von autonomen Tollsystemen - Teil 1:
 Einhaltungsprüfung

This Technical Specification (CEN/TS) was approved by CEN on 25 November 2019 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, 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.....	4
Introduction	5
1 Scope.....	7
2 Normative references.....	7
3 Terms and definitions	9
4 Abbreviations	12
5 Processes.....	13
5.1 Overview	13
5.2 Profiles.....	15
5.3 Itinerary Freezing.....	20
5.3.1 Introduction	20
5.3.2 Generate Itinerary	21
5.3.3 Real-time freezing.....	22
5.3.4 Freezing per declaration	23
5.4 Checking of Itinerary Freezing.....	23
5.4.1 Introduction	23
5.4.2 Observing a vehicle	24
5.4.3 Retrieving Proof of Itinerary Freezing (PIF).....	24
5.4.4 Checking PIF against Observation.....	25
5.5 Checking of Toll Declaration.....	26
5.5.1 Introduction.....	26
5.5.2 Retrieve Itinerary Data.....	26
5.5.3 Check Itinerary Consistency.....	26
5.5.4 Checking Toll Declaration against Itinerary	27
5.6 Inconsistency report.....	27
5.7 Providing EFC Context Data.....	27
5.8 Key Management.....	28
5.8.1 Introduction.....	28
5.8.2 Requirements	28
6 Transaction.....	29
6.1 Introduction.....	29
6.2 Description of Itinerary Data.....	31
6.2.1 Introduction.....	31
6.2.2 Itinerary Leaf.....	32
6.2.3 Itinerary Record Data Elements	33
6.3 Retrieving PIF in real-time (DSRC Transaction).....	35
6.3.1 Transactional Model.....	35
6.3.2 Syntax and Semantics	36
6.3.3 Security	38
6.4 Toll Declaration	38
6.4.1 Transactional Model	38
6.4.2 Syntax and semantics.....	39

6.4.3	Itinerary Trunk	39
6.4.4	Security.....	41
6.5	Back end data checking.....	41
6.5.1	Introduction	41
6.5.2	Transactional model.....	41
6.5.3	Checks of the Itinerary.....	43
6.5.4	Syntax and semantics	44
6.5.5	Security.....	44
6.6	Inconsistency Report.....	44
6.6.1	Transactional model.....	44
6.6.2	Syntax and semantics	45
6.6.3	Security.....	46
6.7	Providing EFC Context Data	46
6.7.1	Transactional model.....	46
6.7.2	Syntax and semantics	47
6.7.3	Security.....	47
7	Security.....	47
7.1	Security functions and elements	47
7.1.1	Hash functions	47
7.1.2	MAC.....	47
7.1.3	Digital signatures.....	48
7.1.4	Public Keys, Certificates and CRL.....	48
7.2	Key Management.....	48
7.2.1	Key Exchange between Stakeholders.....	48
7.2.2	Key generation and certification	49
7.3	Trusted Recorder and SM_CC Verification SAM characteristics	49
7.3.1	Introduction	49
7.3.2	Trusted Recorder.....	50
7.3.3	SM_CC Verification SAM.....	51
	Annex A (normative) Data type specification.....	52
	Annex B (normative) Protocol Implementation Conformance Statement Proforma	53
	Annex C (informative) Example transactions.....	62
	Annex D (informative) Relationships to other standards.....	69
	Annex E (informative) Essentials of the SM_CC concept	71
	Annex F (informative) Use of this document for the EETS.....	85
	Bibliography	87

European foreword

This document (CEN/TS 16702-1:2020) has been prepared by 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.

This document supersedes CEN/TS 16702-1:2014.

This second edition of CEN/TS 16702-1 incorporates the following main modifications compared to the previous one:

- amendment of terms, in order to reflect harmonization of terms across electronic fee collection (EFC) standards;
- renaming SmccClaimADU to InconsistencyReportAdu;
- breaking up the Checking Itinerary transaction into Checking Itinerary Trunk and Checking Itinerary Leaf transactions;
- renaming itinerary sequence and itinerary batch to itinerary leaf and itinerary trunk;
- shortening the Introduction;
- presenting the ASN.1 code as a separate electronic file referenced from Annex A.

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 organisations of the following countries are bound to announce this Technical Specification: 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 the United Kingdom.

Introduction

In autonomous toll systems a Toll Service Provider (TSP) sends toll declarations to the Toll Charger (TC), i.e. statements that a vehicle was circulating within a toll domain. Compliance Check Communication (CCC) according to EN ISO 12813 provides useful indications to a TC of whether the on-board equipment (OBE) is operating correctly or not. It assumes the OBE to be secure and the TSP to be trusted. It mainly focusses on the compliance of the Service User (SU) with the toll domain's rules.

This document does not assume the OBE to be secure nor the TSP to be trusted and adds measures to deal with the associated risks. It specifies the requirements for Secure Monitoring Compliance Checking (SM_CC), a concept that allows the TC to check the trustworthiness of toll declarations produced by a TSP using an OBE operated by the SU, while respecting the privacy of the SU in accordance with the applicable regulations. An operational EFC System can use a combination of the CCC and SM_CC tools to keep misuse under control effectively.

This document is the first part in a set of two that together specify Secure Monitoring for Autonomous Toll Systems: This document, "**Secure Monitoring - Compliance Checking**", specifies the transactions between roadside equipment (RSE) of the TC over dedicated short-range communication (DSRC) as well as transactions between the Toll Charger's and the Toll Service Provider's back end systems, for the purpose of Secure Monitoring. A second part, "**Secure Monitoring - Trusted Recorder**", specifies requirements on a tamper-proof entity called a Trusted Recorder (TR) which can be part of the OBE.

The SM_CC method is suitable:

- a) for use by Toll Chargers and Toll Service Providers that do not have to trust each other and only trust parts of each other's equipment;
- b) for all types of toll regimes according to EN ISO 17577 (all parts);
- c) for providing evidence that can be used in court;
- d) for the application to local schemes as well as in interoperable sectors such as the European Electronic Toll Service (EETS).

SM_CC enables different implementations to comply with applicable privacy laws (which may depend on vehicle categories involved and the road network covered). Different options for example regarding the content of itinerary data (context dependent or independent itineraries) and different ways to access the data for real-time or delayed checks can be selected in order to apply with legal requirements. With the different options provided this concept also supports collection limitation and data minimization as main privacy principles from ISO/IEC 29100.

In some cases, generation and provision of additional data for SM_CC might be forbidden or might require modifications in legislation. It is in the responsibility of the TSP to ensure that toll domain specific privacy requirements are implemented in the OBE. As a consequence, SM_CC requires an OBE to be toll domain aware.

NOTE – For example, in the German truck tolling system collection and storage of itinerary data regarding trips outside the chargeable road network would not be allowed under the current Tolling Act (Bundesfernstraßenmautgesetz). This law also restricts storage of time stamps with tolling events to prevent derivation of concrete speed information.

In some cases it might be necessary not to collect specific data within a specific toll domain, to select an appropriate sampling rate or at least to delete the data directly on the OBE after its generation.

The TC may also be subject to toll domain specific requirements. For instance, regulations for storage of observation data can be different between countries. In some countries it might be forbidden to store observation data without a suspicion of non-compliance or to store data that are related to vehicles that are not liable to toll. In an extreme case this would allow unexpected observations using DSRC with real-time checking of itinerary freezing (CIF), but prohibit checks where roadside observations have to be stored until the corresponding toll declarations are received by the TC.

The TC should also be aware that it might be forbidden for the TSP to provide any itinerary data that are collected outside the TC's toll domain or outside the TC's country. This would limit TC's possibilities for delayed CIF. As one possible solution this concept provides the option that plausibility checks of the toll declaration against itineraries are performed by the TSP. This would require a high level of trust between the TC and the TSP.

1 Scope

This document specifies transactions and data for Compliance Checking - Secure Monitoring. The Scope of this document consists of:

- the concept and involved processes for Secure Monitoring;
- the definition of transactions and data;
- the use of the OBE compliance checking transaction as specified in EN ISO 12813, for the purpose of Compliance Checking - Secure Monitoring;
- the use of back end transactions as specified in EN ISO 12855, for the purpose of Compliance Checking - Secure Monitoring. This includes definitions for the use of optional elements and reserved attributes;
- a specification of technical and organizational security measures involved in Secure Monitoring, on top of measures provided for in the EFC Security Framework;
- the interrelations between different options in the OBE, TSP and TR domain and their high level impacts.

NOTE Outside the Scope of this document is: The information exchange between OBE and TR, choices related to compliance checking policies e.g. which options are used, whether detected/unexpected observations are applied, whether fixed, transportable or mobile compliance checking are deployed, locations and intensity of checking of itinerary freezing and checking of toll declaration, details of procedures and criteria for assessing the validity or plausibility of Itinerary Records.

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.

EN ISO 12813:2019, *Electronic fee collection – Compliance check communication for autonomous systems (ISO 12813:2019)*

EN ISO 12855:2015, *Electronic fee collection – Information exchange between service provision and toll charging (ISO 12855:2015)*

EN ISO 14906, *Electronic fee collection – Application interface definition for dedicated short-range communication (ISO 14906)*

EN ISO 17575-1:2016, *Electronic fee collection – Application interface definition for autonomous systems – Part 1: Charging (ISO 17575-1:2016)*

EN ISO 17575-3:2016, *Electronic fee collection – Application interface definition for autonomous systems – Part 3: Context data (ISO 17575-3:2016)*

CEN ISO/TS 19299:2015, *Electronic fee collection – Security framework (ISO/TS 19299:2015)*

ISO 15628:2013, *Intelligent transport systems – Dedicated short range communication (DSRC) – DSRC application layer*