SLOVENSKI STANDARD
SIST-TS CEN/TS 16702-1:2020

01-marec-2020

Nadomešča:
SIST-TS CEN/TS 16702-1:2015

Elektronsko pobiranje pristojbin - Varnostno spremljanje avtonomnih cestninskih sistemov - 1. del: Preverjanje skladnosti

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

Elektronische Gebührenerhebung - Sichere Überwachung von autonomen Mautsystemen - Teil 1: Einhaltsprüfung

Ta slovenski standard je istoveten z: **CEN/TS 16702-1:2020**

ICS:

35.240.60	Uporabniške rešitve IT v prometu	IT applications in transport

SIST-TS CEN/TS 16702-1:2020 **en,fr,de**

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 Mautsystemen - Teil 1: Einhaltsprüfung

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

Ref. No. CEN/TS 16702-1:2020 E

Contents

Page

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 17575 (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 TC 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 undetected/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*

ISO/IEC 8824-1, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation – Part 1*

ISO/IEC 8825-1, *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) – Part 1*

ISO/IEC 8825-2, *Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER) – Part 2*

ISO/IEC 8825-4, *Information technology – ASN.1 encoding rules: XML Encoding Rules (XER) – Part 4*

ISO/IEC 9594-8, *Information technology – Open Systems Interconnection – The Directory – Part 8: Public-key and attribute certificate frameworks*

ISO/IEC 9797-1:2011, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher*

ISO/IEC 11770-3:2015, *Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques*

ISO/IEC 18033-3:2010, *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers*

IETF RFC 4648, *October 2006, The Base16, Base32, and Base64 Data Encodings*

IETF RFC 5280, *January 2013, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

FIPS PUB 180-4, *Secure Hash Standard (SHS)*

FIPS PUB 186-3, *June 2009, Digital Signature Standard (DSS)*

NIMA TR8350.2, Third Edition – Amendment 1, January 2000, Department of Defense – World Geodetic System 1984, Its Definition and Relationships With Local Geodetic Systems, issued by National Imagery and Mapping Agency (NIMA), US Department of Defense

3 Terms and definitions

For the purposes of this document, the following terms and definitions 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
attribute
addressable package of data consisting of a single data element or structured sequences of data elements

3.2
authenticator
data, possibly encrypted, that is used for authentication

3.3
back end
part of a back office system interfacing to one or more front ends

3.4
charge report
information containing road usage and related information originated at the front end

3.5
context data
toll context data
information defined by the responsible Toll Charger necessary to establish the toll due for using a vehicle on a particular toll context and to conclude the toll transaction

3.6
context dependent itinerary
itinerary of which the syntax and semantics depend on the toll domain's context data

3.7
context independent itinerary
itinerary of which the syntax and semantics are independent of the toll domain's context data

3.8
electronic fee collection
fee collection by electronic means

3.9
freezing per declaration
process that freezes the itinerary related to the toll declaration by sending a cryptographic commit or the whole itinerary to the Toll Charger

3.10
front end
part of a tolling system consisting of on-board equipment (OBE) and possibly a proxy where road tolling information and usage data are collected and processed for delivery to the back end

3.11
itinerary
travel diary organized in one or more itinerary records enabling assessment of the correctness of the toll declaration

3.12
itinerary leaf
sequence of sequential itinerary records of the same type all pertaining to a defined set of toll domains

3.13
itinerary freezing
registering an itinerary and undeniably committing oneself to it

3.14
itinerary trunk
sequence of aggregated data committing to a number of underlying itinerary leaves

3.15
itinerary record
atomic data element describing use of the road network or use of the vehicle

3.16
MAC
message authentication code

fixed-length string of bits used to verify the authenticity of a message, generated by the sender of the message, transmitted together with the message, and verified by the receiver of the message

3.17
on-board equipment
all required equipment on-board a vehicle for performing required electronic fee collection (EFC) functions and communication services

3.18
real-time freezing
freezing of each itinerary record as soon as its acquisition has terminated using a trusted recorder

3.19
secure monitoring compliance checking
concept that allows a Toll Charger to rely on the trustworthiness of toll declarations produced by Toll Service Providers

3.20
time lock
mechanism ensuring that a new operation can only be commissioned after a configurable period of time or processor clock cycles since the previous operation

3.21
toll declaration
statement to declare the usage of a given toll service to a Toll Charger

3.22
toll domain
area or a part of a road network where a certain toll regime is applied

3.23
trusted recorder
logical entity capable of cryptographic functions, used to provide the OBE with security services, including data confidentiality, data integrity, authentication and non-repudiation

3.24
undetected observation
observation of road usage, performed by the Toll Charger, which is neither known to the driver or OBE before nor after the observation

3.25
unexpected observation
observation of road usage, performed by the Toll Charger, which is unknown to the driver or OBE before but might be known after the observation

4 Abbreviations

For the purpose of this document, the following abbreviations apply throughout the document unless otherwise specified.

AES	Advanced Encryption Standard
CA	Certification Authority
CDIR	Context Dependent Itinerary Record
CIF	Checking of Itinerary Freezing
CIIR	Context Independent Itinerary Record
CRL	Certificate Revocation List
CTD	Checking of Toll Declaration
DSRC	Dedicated Short-Range Communication
EETS	European Electronic Toll Service
EFC	Electronic Fee Collection
FIFO	First In - First Out
FpD	Freezing per Declaration
GNSS	Global Navigation Satellite System
IR	Itinerary Record
MAC	Message Authentication Code
OBE	On-Board Equipment
OBU	On-Board Unit
PICS	Protocol Implementation Conformance Statement
PIF	Proof of Itinerary Freezing
RSE	Roadside Equipment
RTF	Real-Time Freezing
SAM	Secure Application Module
SM_CC	Secure Monitoring Compliance Checking
SM_TR	Secure Monitoring Trusted Recorder
SU	Service User
TC	Toll Charger
TC_SAM	Toll Charger SAM
TR	Trusted Recorder
TSP	Toll Service Provider
TSP_SAM	Toll Service Provider SAM
TTP	Trusted Third Party
UML	Unified Modelling Language

5 Processes

5.1 Overview

This clause introduces the conceptual framework of Secure Monitoring Compliance Checking in terms of requirements to a system or devices implementing it. It also describes the relations between different processes and information classes. An overview of the main stakeholders and processes of Secure Monitoring can be found in Figure 1.

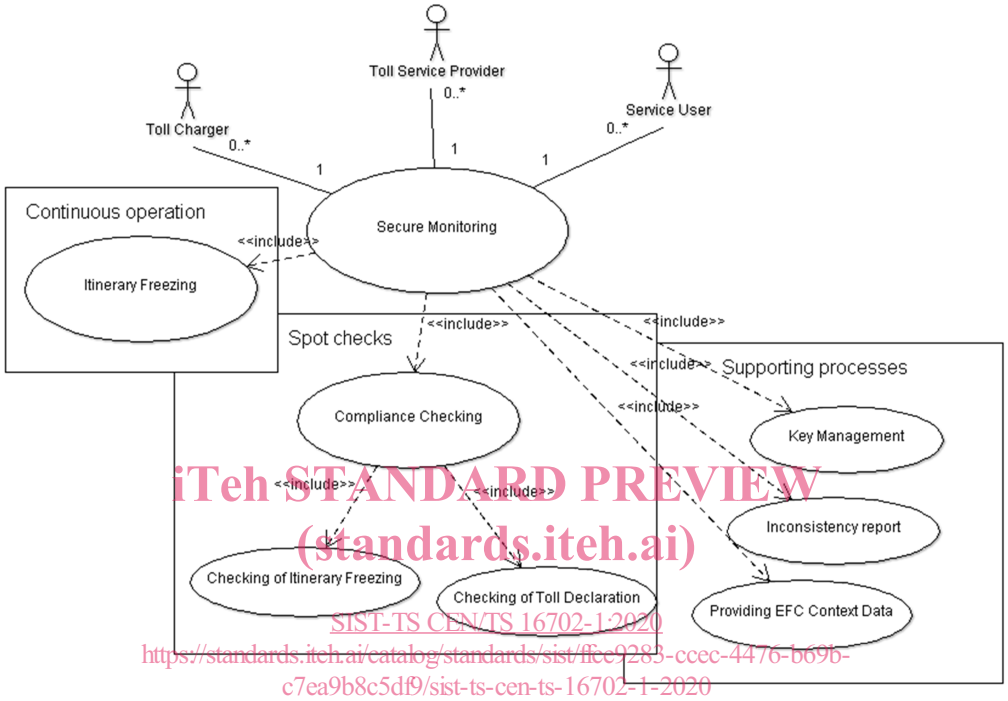

Figure 1 — The main stakeholders and processes of Secure Monitoring (UML use case diagram)

The Secure Monitoring Compliance Checking processes regulates the interactions between the three stakeholders Toll Charger (TC), Toll Service Provider (TSP) and Service User (SU) in the following main processes:

a) Itinerary Freezing: generate and freeze the itinerary;

b) Checking of Itinerary Freezing: check the frozen itinerary for correctness against the observation;

c) Checking of Toll Declaration: check the correctness of the Toll Declaration against the itinerary;

and the following supporting processes:

d) Inconsistency Report: information from TC to TSP about a negative outcome of Checking of Itinerary Freezing and/or Checking of Toll Declaration;

e) Providing EFC Context Data: TCs specification of itinerary characteristics such as format and periodicity;