SLOVENSKI STANDARD
SIST-TS CEN/TS 16702-2:2020

01-marec-2020

Nadomešča:
SIST-TS CEN/TS 16702-2:2015

Elektronsko pobiranje pristojbin - Varnostno spremljanje avtonomnih cestninskih sistemov - 2. del: Zaupanja vreden snemalnik

Electronic fee collection - Secure monitoring for autonomous toll systems - Part 2: Trusted recorder

Elektronische Gebührenerhebung - Sichere Überwachung von autonomen Mautsystemen - Teil 2: Zuverlässige Datenaufzeichnung

Perception du télépéage - Surveillance sécurisée pour systèmes autonomes de péage - Partie 2: Enregistreur fiabilisé

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST-TS CEN/TS 16702-2:2020
https://standards.iteh.ai/catalog/standards/sist/440b80b8-8a14-409a-8729-6678a3a0cf96/sist-ts-cen-ts-16702-2-2020

Ta slovenski standard je istoveten z: **CEN/TS 16702-2:2020**

ICS:

03.220.20	Cestni transport	Road transport
35.240.60	Uporabniške rešitve IT v prometu	IT applications in transport

SIST-TS CEN/TS 16702-2:2020 **en,fr,de**

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

SIST-TS CEN/TS 16702-2:2020

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST-TS CEN/TS 16702-2:2020
https://standards.iteh.ai/catalog/standards/sist/440b80b8-8a14-409a-8729-6678a3a0cf96/sist-ts-cen-ts-16702-2-2020

SIST-TS CEN/TS 16702-2:2020

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 16702-2

January 2020

ICS 03.220.20; 35.240.60

Supersedes CEN/TS 16702-2:2015

English Version

Electronic fee collection - Secure monitoring for autonomous toll systems - Part 2: Trusted recorder

Perception du télépéage - Surveillance sécurisée pour systèmes autonomes de péage - Partie 2 : Enregistreur fiabilisé

Elektronische Gebührenerhebung - Sichere Überwachung von autonomen Mautsystemen - Teil 2: Zuverlässige Datenaufzeichnung

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

SIST-TS CEN/TS 16702-2:2020
https://standards.iteh.ai/catalog/standards/sist/440b80b8-8a14-409a-8729-6678a3a0cf96/sist-ts-cen-ts-16702-2-2020

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

© 2020 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. CEN/TS 16702-2:2020 E

SIST-TS CEN/TS 16702-2:2020

Contents

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST-TS CEN/TS 16702-2:2020
https://standards.iteh.ai/catalog/standards/sist/440b80b8-8a14-409a-8729-6678a3a0cf96/sist-ts-cen-ts-16702-2-2020

SIST-TS CEN/TS 16702-2:2020

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST-TS CEN/TS 16702-2:2020
https://standards.iteh.ai/catalog/standards/sist/440b80b8-8a14-409a-8729-6678a3a0cf96/sist-ts-cen-ts-16702-2-2020

SIST-TS CEN/TS 16702-2:2020

European foreword

This document (CEN/TS 16702-2:2020) 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 16702-2:2015.

The CEN/TS 16702 series, *Electronic fee collection – Secure monitoring for autonomous toll systems*, is composed with the following parts:

— *Part 1: Compliance checking*;

— *Part 2: Trusted recorder*.

This document about the trusted recorder is the second part of the CEN/TS 16702 series about the secure monitoring for autonomous toll systems. The overall concept of secure monitoring is defined in CEN/TS 16702-1.

This second edition will supersede the first edition (CEN/TS 16702-2:2015), which was technically revised. The main changes compared to the previous edition are as follows:

iTeh STANDARD PREVIEW
(standards.iteh.ai)

— references to underlaying standards updated to latest version;

— updated terminology;

SIST-TS CEN/TS 16702-2:2020
https://standards.iteh.ai/catalog/standards/sist/440b80b8-8a14-409a-8729-6678a3a0cf96/sist-ts-cen-ts-16702-2-2020

— slight restructuring.

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.

SIST-TS CEN/TS 16702-2:2020

Introduction

The widespread use of tolling requires provisions for users of vehicles that are roaming through many different toll domains. Users should be offered a single contract for driving a vehicle through multiple toll domains and those vehicles require on-board equipment (OBE) that is interoperable with the toll systems in these toll domains. Thus, there is a commercial and economic justification both in respect of the OBE and the toll systems for supporting interoperability. In Europe, for example, this need is recognized and legislation on interoperability has been adopted (see Directive 2004/52/EC) and the associated Commission Decision.

CEN ISO/TS 19299, *Electronic fee collection – Security framework (ISO/TS 19299)*, provides an overview of general security requirements of the stakeholders and provides a comprehensive threat analysis for the assets in an interoperable EFC scheme. Security attacks may result into less revenue of the toll charger, undercharging or not meeting required service levels between the toll service provider and the toll charger. Some of these threats can be eliminated by implementing the security measures that are specified. However, most of the security measures necessary to combat the identified threats are addressed and specified in other standards.

One example of threats that cannot be mitigated by security measures specified in CEN ISO/TS 19299 concerns the trustworthiness of Toll Declarations in autonomous toll systems. Toll declarations are statements that a vehicle has been circulating in a particular toll domain within a particular time period. In autonomous toll systems, the circulation of vehicles is measured by toll service providers, using GNSS-based OBE. Toll service providers then send Toll Declarations to the toll charger, based on which the toll charger will charge the toll service provider. The correctness and completeness of these declarations are obviously of paramount interest to toll chargers, toll service providers and users alike.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

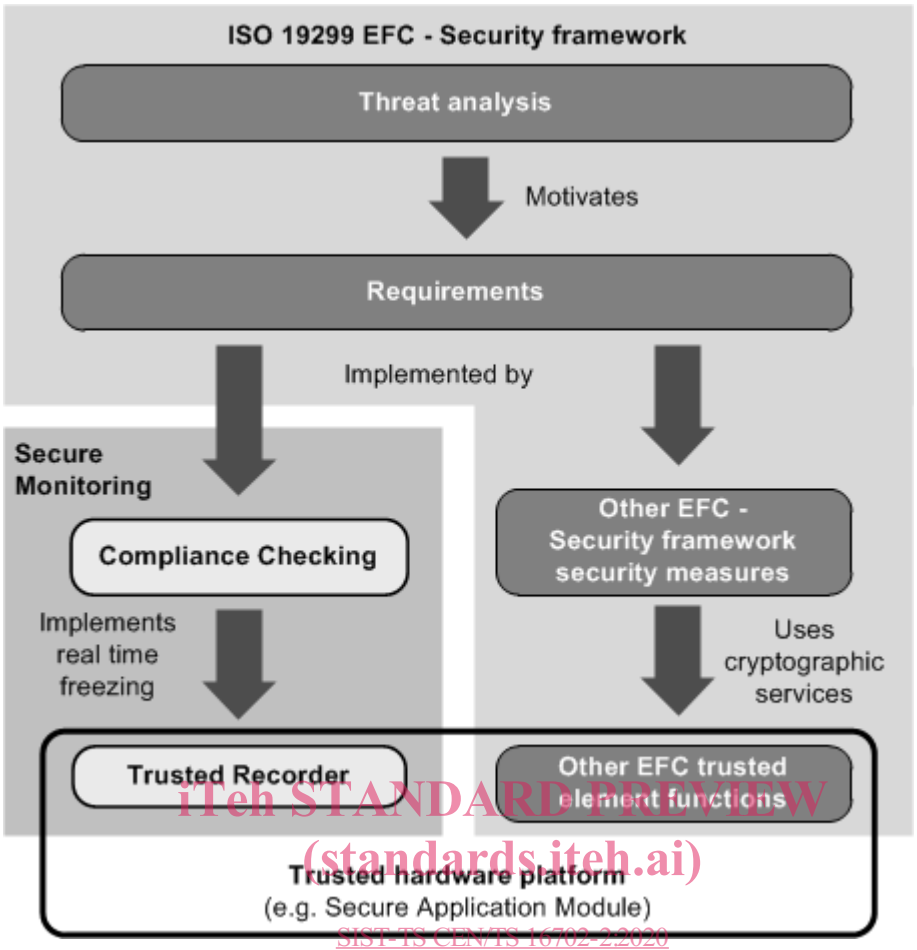
The secure monitoring compliance checking concept provides a solution that allows a toll charger to check the trustworthiness of the Toll Declarations from a toll service provider, whilst respecting the privacy of the user. This concept is defined in the CEN/TS 16702 series:

SIST-TS CEN/TS 16702-2:2020
https://standards.iteh.ai/catalog/standards/sist/440b80b8-8a14-409a-8729-

- CEN/TS 16702-1, *Electronic fee collection – Secure monitoring for autonomous toll systems – Part 1: Compliance checking*, which defines the secure monitoring compliance checking concept;

- CEN/TS 16702-2, *Electronic fee collection – Secure monitoring for autonomous toll systems – Part 2: Trusted recorder* (this document), which defines the trusted recorder, a secure element required for some of the different types of secure monitoring compliance checking concepts.

SIST-TS CEN/TS 16702-2:2020



iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST-TS CEN/TS 16702-2:2020
https://standards.iteh.ai/catalog/standards/sist/440b80b8-8a14-409a-8729-6758a30e486/sist-ts-cen-ts-16702-2-2020

Figure 1 — Relation between EFC – Security framework and the overall secure monitoring concept

Figure 1 shows the relations between CEN ISO/TS 19299, *Electronic fee collection – Security framework*, and the CEN/TS 16702 series. The threat analysis in the Security Framework motivates the security requirements of an EFC system. The requirements are implemented and fulfilled by several security measures. One of these measures is Secure Monitoring, specified in CEN/TS 16702-1, which defines the cryptographic services necessary for the secure monitoring compliance checking concept.

Figure 1 indicates also that a trusted recorder will most likely be implemented on trusted hardware, e.g. on Secure Application Module (SAM), inside the OBE or on a general trusted platform of a vehicle. Such a trusted device could support more functions, which may be required for EFC or other services.

SIST-TS CEN/TS 16702-2:2020

1 Scope

This document defines the requirements for the secure application module (SAM) used in the secure monitoring compliance checking concept. It specifies two different configurations of a SAM:

— trusted recorder, for use inside a piece of on-board equipment (OBE);

— verification SAM, for use in other EFC system entities.

This document describes

— terms and definitions used to describe the configurations of the two SAMs;

— operation of the two SAMs in the secure monitoring compliance checking concept;

— functional requirements for the configurations of the two SAMs, including a classification of different security levels;

— the interface, by means of transactions, messages and data elements, between an OBE or front end and the trusted recorder;

— requirements on basic security primitives and key management procedures to support Secure Monitoring using a trusted recorder.

This document is consistent with the EFC architecture as defined in EN ISO 17573-1 and the derived suite of standards and Technical Specifications, especially CEN/TS 16702-1 and CEN ISO/TS 19299.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

The following is outside the scope of this document:

SIST-TS CEN/TS 16702-2:2020
https://standards.iteh.ai/catalog/standards/sist/440b80b8-8a14-409a-8729-

— The life cycle of a SAM and the way in which this is managed;

— The interface commands needed to get a SAM in an operational state;

— The interface definition of the verification SAM;

— Definition of a hardware platform for the implementation of a SAM.

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.

CEN/TS 16702-1:2020, *Electronic fee collection - Secure monitoring for autonomous toll systems - Part 1: Compliance checking*

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

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

ISO/IEC 7816-4:2013, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

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

SIST-TS CEN/TS 16702-2:2020

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

ISO/IEC 10118-3, *IT Security techniques — Hash-functions — Part 3: Dedicated hash-functions*

ISO/IEC 18031, *Information technology — Security techniques — Random bit generation*

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

ISO/IEC 19790:2012, *Information technology — Security techniques — Security requirements for cryptographic modules*

FIPS PUB 140-2, December 2002, *Security requirements for cryptographic modules*

Common Criteria Protection Profile BSI-PP-0035, 2007, *Security IC Platform Protection Profile*, Version 1.0

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:

iTeh STANDARD PREVIEW
(standards.iteh.ai)

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

SIST-TS CEN/TS 16702-2:2020
https://standards.iteh.ai/catalog/standards/sist/440b80b8-8a14-409a-8729-6678a3a0cf96/sist-ts-cen-ts-16702-2-2020

3.1
authentication
security mechanism allowing the verification of the provided identity

[SOURCE: EN 301 175 V1.1.1 (1998-08), Clause 3]

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

[SOURCE: EN 15509:2014, 3.3]

Note 1 to entry: In this CEN/TS either a MAC or a signature.

3.3
authenticity
property that an entity is what it claims to be

[SOURCE: CEN ISO/TS 19299:2015, 3.5]

SIST-TS CEN/TS 16702-2:2020

3.4
back end
part of a back office system interfacing to one or more front ends

[SOURCE: CEN ISO/TS 19299:2015, 3.7, modified — "back end" and "front end" originally had upper-case characters.]

3.5
big-endian
format for transmission of binary data in which the most significant byte appears first

[SOURCE: ISO/IEC 14776-262:2017, 3.1.18, modified]

3.6
confidentiality
prevention of information leakage to non-authenticated individuals, parties or processes

[SOURCE: CEN ISO/TS 19299:2015, 3.11, modified — "and/or processes" was replaced with "or processes".]

3.7
data integrity
property that data has not been altered or destroyed in an unauthorized manner

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SOURCE: ISO 7498-2:1989, 3.3.21]

3.8
digital signature
one or more data elements resulting from the digital signature process

SIST-TS CEN/TS 16702-2:2020
https://standards.iteh.ai/catalog/standards/sist/[illegible]-8729-6678a3a0cf96/sist-ts-cen-ts-16702-2-2020

[SOURCE: CEN ISO/TS 19299:2015, 3.11, 3.38]

3.9
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

[SOURCE: CEN ISO/TS 19299:2015, 3.17, modified — "back end" and "front end" originally had upper-case characters.]

3.10
itinerary
travel diary organized in one or more itinerary records enabling assessment of the correctness of the toll declaration

SIST-TS CEN/TS 16702-2:2020

3.11
message authentication code
MAC
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

[SOURCE: ISO 16609:2012, 3.15]

Note 1 to entry: A MAC is sometimes called a cryptographic check value (see for example ISO 7498-2).

3.12
non-repudiation
ability to prove the occurrence of a claimed event or action and its originating entities

[SOURCE: CEN ISO/TS 19299:2015, 3.27]

3.13
on-board equipment
OBE
required equipment on-board a vehicle for performing required electronic fee collection (EFC) functions and communication services

3.14
real-time freezing
freezing of each itinerary record as soon as its acquisition has terminated, using a trusted recorder

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST-TS CEN/TS 16702-2:2020
https://standards.iteh.ai/catalog/standards/sist/440b80b8-8a14-409a-8729-
sist-ts-cen-ts-16702-2-2020

3.15
roadside equipment
RSE
equipment located along the road, either fixed or mobile

3.16
Secure Application Module
SAM
physical module that securely executes cryptographic functions and stores keys

[SOURCE: CEN ISO/TS 19299:2015, 3.35]

3.17
secure monitoring compliance checking
concept that allows a toll charger to rely on the trustworthiness of toll declarations produced by toll service providers

SIST-TS CEN/TS 16702-2:2020

3.18
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

3.19
TR issuer
institution (or its agent) that issues the trusted recorder

[SOURCE: ISO/IEC 7812-1:2006, 3.3, adapted]

3.20
toll charger
TC
entity which levies toll for the use of vehicles in a toll domain

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

[SOURCE: CEN ISO/TS 19299:2015, 3.44]

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.23
toll domain ID
unique identifier of a toll domain

SIST-TS CEN/TS 16702-2:2020
https://standards.iteh.ai/catalog/standards/sist/440b80b8-8a14-409a-8729-6678a3a0cf96/sist-ts-cen-ts-16702-2-2020

3.24
toll service
service enabling users to pay toll

3.25
toll service provider
TSP
entity providing toll services in one or more toll domains

SIST-TS CEN/TS 16702-2:2020

3.26
trusted recorder
TR
logical entity capable of cryptographic functions, used to provide the on-board equipment (OBE) with security services, including data confidentiality, data integrity, authentication and non-repudiation

3.27
Trusted Third Party
TTP
security authority, or its agent, trusted by other entities with respect to security related activities

[SOURCE: ISO/IEC 10181-1:1996, 3.3.30, modified]

3.28
toll service user
customer of a toll service provider, i.e. one liable for toll, owner of the vehicle, fleet operator or driver depending on the context

Note 1 to entry: This is a generic term which is context dependent.

3.29
verification SAM
Secure Application Module capable of providing cryptographic services to verify a trusted recorder MAC in such manner that the proof of non-repudiation is given

iTeh STANDARD PREVIEW
(standards.iteh.ai)

4 Symbols and abbreviations

SIST-TS CEN/TS 16702-2:2020
https://standards.iteh.ai/catalog/standards/sist/440b80b8-8a14-409a-8729-6678a3a0cf96/sist-ts-cen-ts-16702-2-2020

ADU	Application Data Unit
AES	Advanced Encryption Standard
APDU	Application Protocol Data Unit
BCD	Binary Coded Decimal
CA	Certification Authority
CLA	Class byte
CMAC	Cipher-based MAC
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EETS	European Electronic Toll Service
GNSS	Global Navigation Satellite System
ID	Identifier
INS	Instruction byte
KVC	Key Verification Code
MAC	Message Authentication Code
NTP	Network Time Protocol
OBE	On-Board Equipment

SIST-TS CEN/TS 16702-2:2020

P1, P2	Parameter bytes
PKI	Public Key Infrastructure
PP	Protection Profile
RQ	Requirement
RSA	Algorithm for public-key cryptography (Rivest, Shamir and Adleman)
RSE	Roadside Equipment
SAM	Secure Application Module
SNTP	Simple Network Time Protocol
TC	toll charger
TDC	Toll Domain Counter
TR	trusted recorder
TRID	trusted recorder Identifier
TSP	toll service provider
TTP	Trusted Third Party
TTS	Trusted Time Source
UTC	Coordinated Universal Time

iTeh STANDARD PREVIEW
(standards.iteh.ai)

5 SAM concept and scenarios

5.1 General

SIST-TS CEN/TS 16702-2:2020
https://standards.iteh.ai/catalog/standards/sist/440b80b8-8a14-409a-8729-6678a2a9cf06/sist-ts-cen-ts-16702-2-2020

CEN/TS 16702-1 defines requirements for a trusted recorder (TR) used in a piece of OBE, which supports symmetric and asymmetric algorithms. A verification SAM (for example in the RSE) is required to achieve the same cryptographic proof of non-repudiation when using the symmetric algorithm compared to the asymmetric algorithm. Subclause 6.2 of this document describes the two different configurations of the SAM in the EFC context.

Subclauses 6.3, 6.4 and 6.5 describe the scenarios for the use of the TR and verification SAM, motivated by CEN/TS 16702-1 (variations SM_CC-1 “Real-time Freezing using a TR without trusted time source” and SM_CC-2 “Real-time Freezing using a TR with trusted time source”). The scenarios in these clauses cover all possible use cases for both SAM configurations, a TR inside an OBE and a verification SAM used in the RSE or another EFC entity.

NOTE Names and data flow elements in the diagrams in Clause 6 are symbolic and do not always give all details. For details, refer to Clause 8.

5.2 The concepts of TR and verification SAM

The TR is intended for the use inside OBE. The TR is responsible for freezing itineraries by calculating an authenticator over each itinerary. This document additionally defines the requirements for a verification SAM, which shall be used in other EFC system entities, for example in the RSE, the TSP back office or the TC back office. The verification SAM is responsible for the verification of symmetric authenticators over itineraries, calculated by TRs inside OBE.

The TR used in OBE is a logical entity with certain security functions to support the secure monitoring compliance checking concept. If properly used, the TR and - if required - the verification SAM will ensure