This is a free 11 page sample. Access the full version online.

NSAI Standards

Irish Standard Recommendation
S.R. CEN/TS 16702-2:2020

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

© CEN 2020 No copying without NSAI permission except as permitted by copyright law.

S.R. CEN/TS 16702-2:2020

Incorporating amendments/corrigenda/National Annexes issued since publication:

The National Standards Authority of Ireland (NSAI) produces the following categories of formal documents:

I.S. xxx: Irish Standard — national specification based on the consensus of an expert panel and subject to public consultation.

S.R. xxx: Standard Recommendation — recommendation based on the consensus of an expert panel and subject to public consultation.

SWiFT xxx: A rapidly developed recommendatory document based on the consensus of the participants of an NSAI workshop.

This document replaces/revises/consolidates the NSAI adoption of the document(s) indicated on the CEN/CENELEC cover/Foreword and the following National document(s):

NOTE: The date of any NSAI previous adoption may not match the date of its original CEN/CENELEC document.

This document is based on:	*Published:*
CEN/TS 16702-2:2020	2020-01-22

This document was published under the authority of the NSAI and comes into effect on:	ICS number:
2020-02-09	03.220.20 35.240.60 NOTE: If blank see CEN/CENELEC cover page

NSAI	T +353 1 807 3800	Sales:
1 Swift Square,	F +353 1 807 3838	T +353 1 857 6730
Northwood, Santry	E standards@nsai.ie	F +353 1 857 6729
Dublin 9	W NSAI.ie	W standards.ie

Údarás um Chaighdeáin Náisiúnta na hÉireann

This is a free 11 page sample. Access the full version online.

National Foreword

S.R. CEN/TS 16702-2:2020 is the adopted Irish version of the European Document CEN/TS 16702-2:2020, Electronic fee collection - Secure monitoring for autonomous toll systems - Part 2: Trusted recorder

This document does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

For relationships with other publications refer to the NSAI web store.

Compliance with this document does not of itself confer immunity from legal obligations.

In line with international standards practice the decimal point is shown as a comma (,) throughout this document.

This is a free 11 page sample. Access the full version online.

This is a free 11 page sample. Access the full version online.

This page is intentionally left blank

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.

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.

This is a free 11 page sample. Access the full version online.

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

Contents

Page

European foreword 4
Introduction 5
1 Scope 7
2 Normative references 7
3 Terms and definitions 8
4 Symbols and abbreviations 12
5 SAM concept and scenarios 13
5.1 General 13
5.2 The concepts of TR and verification SAM 13
5.3 Scenarios for a trusted recorder 15
5.3.1 General 15
5.3.2 Real-Time Freezing without using a Trusted Time Source 15
5.3.3 Real-Time Freezing using a Trusted Time Source 16
5.4 Scenarios for a verification SAM 16
5.4.1 General 16
5.4.2 MAC verification 16
5.5 General Scenarios 17
5.5.1 General 17
5.5.2 Assigning a Toll Domain Counter 17
5.5.3 Obtaining SAM Information 18
6 Functional requirements 19
6.1 General 19
6.1.1 SAM options 19
6.1.2 Presentation of requirements 20
6.2 Basic requirements 20
6.3 Key management 21
6.4 Cryptographic functions 21
6.5 Real-time freezing 22
6.6 Verification SAM 23
6.7 Toll Domain Counter 23
6.8 Trusted time source 24
6.9 Security protection level 25
7 Interface requirements 26
7.1 General 26
7.2 Calculate MAC for real-time freezing 26
7.2.1 General 26
7.2.2 Calculation of MAC 27
7.2.3 Coding of request 27
7.2.4 Coding of response 28
7.3 Calculate digital signature for real-time freezing 28
7.3.1 General 28

This is a free 11 page sample. Access the full version online.

7.3.2 Calculation of digital signature 29
7.3.3 Coding of request 29
7.3.4 Coding of response 29
7.4 Get device information 30
7.4.1 General 30
7.4.2 Coding of request 30
7.4.3 Coding of response 31
7.5 Get toll domain counter information 31
7.5.1 General 31
7.5.2 Coding of request 31
7.5.3 Coding of response 32
7.6 Get key information 32
7.6.1 General 32
7.6.2 Coding of request 33
7.6.3 Coding of response 33
7.7 Error handling 34
Annex A (normative) Data type specification 35
Annex B (normative) Implementation Conformance Statement (ICS) proforma 36
Annex C (informative) Trusted Time Source implementation issues 49
Annex D (informative) Use of this document for the EETS 51
Bibliography 53

This is a free 11 page sample. Access the full version online.

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:

— references to underlaying standards updated to latest version;

— updated terminology;

— 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.

This is a free 11 page sample. Access the full version online.

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.

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:

- 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.

This is a free 11 page sample. Access the full version online.

This is a free 11 page sample. Access the full version online.

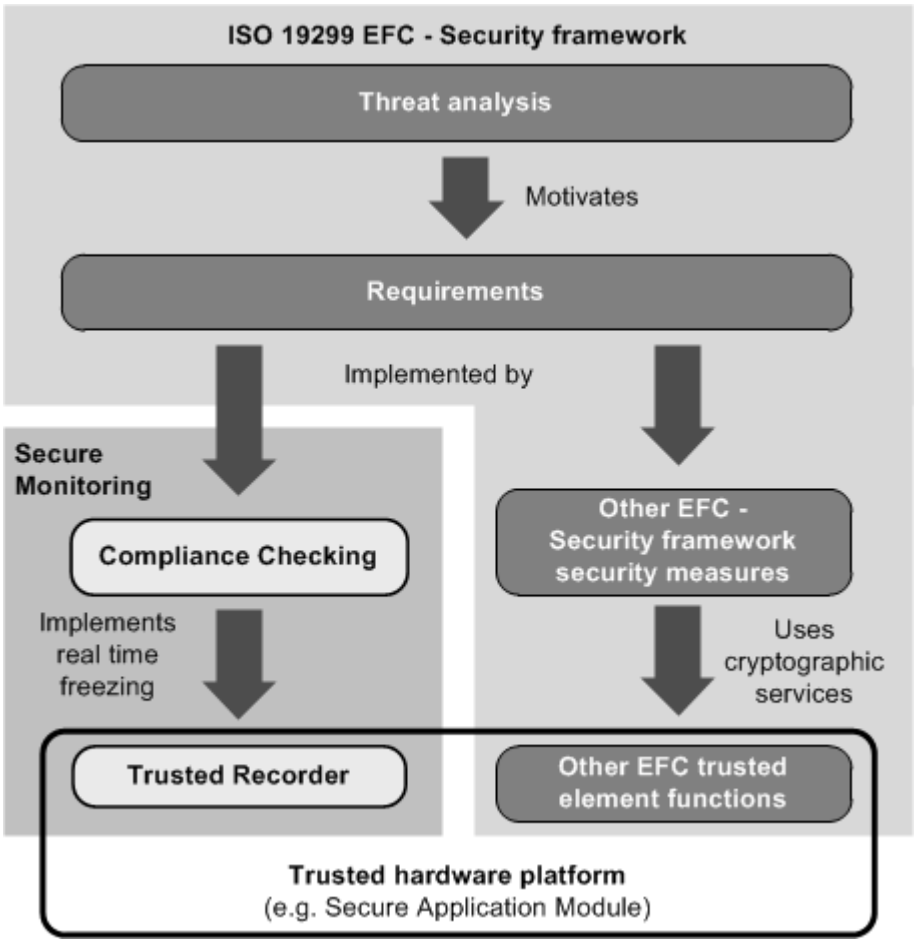

Figure 1 — Relation between EFC – Security framework and the overall secure monitoring concept

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.

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.

The following is outside the scope of this document:

— 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:*

This is a free 11 page sample. Access the full version online.

This is a free 11 page sample. Access the full version online.

SAI GLOBAL

This is a free preview. Purchase the entire publication at the link below:

SR CEN/TS 16702-2 : 2020 : EN : COMBINED PDF

Looking for additional Standards? Visit SAI Global Infostore

Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation

Need to speak with a Customer Service Representative - Contact Us