

STN	Elektronický výber poplatkov. Bezpečné monitorovanie autonómnych mýtnych systémov. Časť 2: Bezpečnostný záznamník.	STN P CEN TS 16702-2 01 8512
------------	---	--

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 06/15

Táto predbežná STN je určená na overenie. Pripomienky zasielajte ÚNMS SR najneskôr do 31. 3. 2017.

Obsahuje: CEN/TS 16702-2:2015

120868

Úrad pre normalizáciu, metrológiu a skúšobníctvo SR, odbor SÚTN, 2015
Podľa zákona č. 264/1999 Z. z. v znení neskorších predpisov sa môžu slovenské technické normy rozmnožovať a rozširovať iba so súhlasom Úradu pre normalizáciu, metrológiu a skúšobníctvo SR.

TECHNICAL SPECIFICATION
SPÉCIFICATION TECHNIQUE
TECHNISCHE SPEZIFIKATION

CEN/TS 16702-2

March 2015

ICS 03.220.20; 35.240.60

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 19 January 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
Foreword.....	4
Introduction	5
1 Scope	7
2 Normative references	7
3 Terms and definitions	8
4 Symbols and abbreviations	11
5 SAM concept and scenarios.....	12
5.1 General.....	12
5.2 The concepts of TR and Verification SAM	13
5.3 Scenarios for a Trusted Recorder	14
5.3.1 General.....	14
5.3.2 Real-Time Freezing without using a Trusted Time Source	14
5.3.3 Real-Time Freezing using a Trusted Time Source	15
5.4 Scenarios for a Verification SAM	15
5.4.1 General.....	15
5.4.2 MAC verification.....	16
5.5 General Scenarios	16
5.5.1 General.....	16
5.5.2 Assigning a Toll Domain Counter	17
5.5.3 Obtaining SAM Information	17
6 Functional requirements	18
6.1 General.....	18
6.1.1 SAM options	18
6.1.2 Presentation of requirements	19
6.2 Basic requirements.....	19
6.3 Key management	20
6.4 Cryptographic functions	20
6.5 Real-time freezing	21
6.6 Verification SAM	21
6.7 Toll Domain Counter	22
6.8 Trusted time source	23
6.9 Security protection level	24
7 Interface requirements	24
7.1 General.....	24
7.2 Calculate MAC for real-time freezing	24
7.2.1 General.....	24
7.2.2 Calculation of MAC	25
7.2.3 Coding of request	25
7.2.4 Coding of response	26
7.3 Calculate digital signature for real-time freezing	26
7.3.1 General.....	26
7.3.2 Calculation of digital signature	26
7.3.3 Coding of request	27
7.3.4 Coding of response	27

7.4	Get device information.....	28
7.4.1	General	28
7.4.2	Coding of request.....	28
7.4.3	Coding of response	28
7.5	Get toll domain counter information	28
7.5.1	General	28
7.5.2	Coding of request.....	29
7.5.3	Coding of response	29
7.6	Get key information	29
7.6.1	General	29
7.6.2	Coding of request.....	30
7.6.3	Coding of response	30
7.7	Error handling.....	31
Annex A	(normative) Data type specification	32
A.1	General	32
A.2	Data specifications	32
Annex B	(normative) Implementation Conformance Statement (ICS) proforma	33
B.1	Guidance for completing the ICS proforma	33
B.1.1	Purposes and structure	33
B.1.2	Abbreviations and conventions	33
B.1.3	Instructions for completing the ICS proforma.....	34
B.2	ICS proforma for Trusted Recorder	35
B.2.1	Identification implementation	35
B.2.2	Identification of the standard	35
B.2.3	Global statement of conformance	35
B.2.4	ICS proforma tables for TR.....	36
B.3	ICS proforma for Verification SAM	39
B.3.1	Identification implementation	39
B.3.2	Identification of the standard	39
B.3.3	Global statement of conformance	39
B.3.4	ICS proforma tables for Verification SAM.....	40
Annex C	(informative) Trusted time source implementation issues	43
C.1	General	43
C.2	Possible implementations of a TTS	43
C.2.1	TTS based on a real time clock.....	43
C.2.2	TTS with the need for external calibration.....	43
C.3	TTS power supply.....	44
Annex D	(informative) Use of this Technical Specification for the EETS	45
D.1	General	45
D.2	Overall relationship between European standardization and the EETS.....	45
D.3	European standardization work supporting the EETS	45
D.4	Correspondence between this Technical Specification and the EETS	46
	Bibliography.....	47

CEN/TS 16702-2:2015 (E)**Foreword**

This document (CEN/TS 16702-2:2015) has been prepared by Technical Committee CEN/TC 278 “Intelligent transport systems”, the secretariat of which is held by NEN.

This part 2, the trusted recorder is the second part of the standard suite of the secure monitoring for autonomous toll systems. The overall concept of secure monitoring is defined in part one, CEN/TS 16702-1:2014.

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 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.

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 onboard 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 enabling interoperability. In Europe, for example, this need has been officially recognized and legislation on interoperability has been adopted (see directive 2004/52/EC) and the associated commission decision.

The Technical Specification “Electronic fee collection – Security framework” (CEN/TS 16439) provides an overview of general security requirements of the stakeholders and provides a comprehensive threat analysis for the assets in an interoperable EFC scheme. A number of identified threats may result into less revenue of the Toll Charger, undercharging and/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 specified in CEN/TS 16439. However, most of the security measures necessary to combat the identified threats are to be addressed and specified in other standards.

One example of threats that cannot be mitigated by security measures specified in CEN/TS 16439 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 is 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, while respecting the privacy of the user. This concept is defined in two Technical Specifications. CEN/TS 16702-1:2014 “Secure monitoring for autonomous toll systems – Part 1: Compliance checking” gives the full description of the secure monitoring compliance checking concept. The current Technical Specification, CEN/TS 16702-2 “Secure Monitoring for autonomous toll systems – Part 2: Trusted recorder” defines the Trusted Recorder, a secure element required for some of the different types of secure monitoring compliance checking defined in CEN/TS 16702-1:2014.

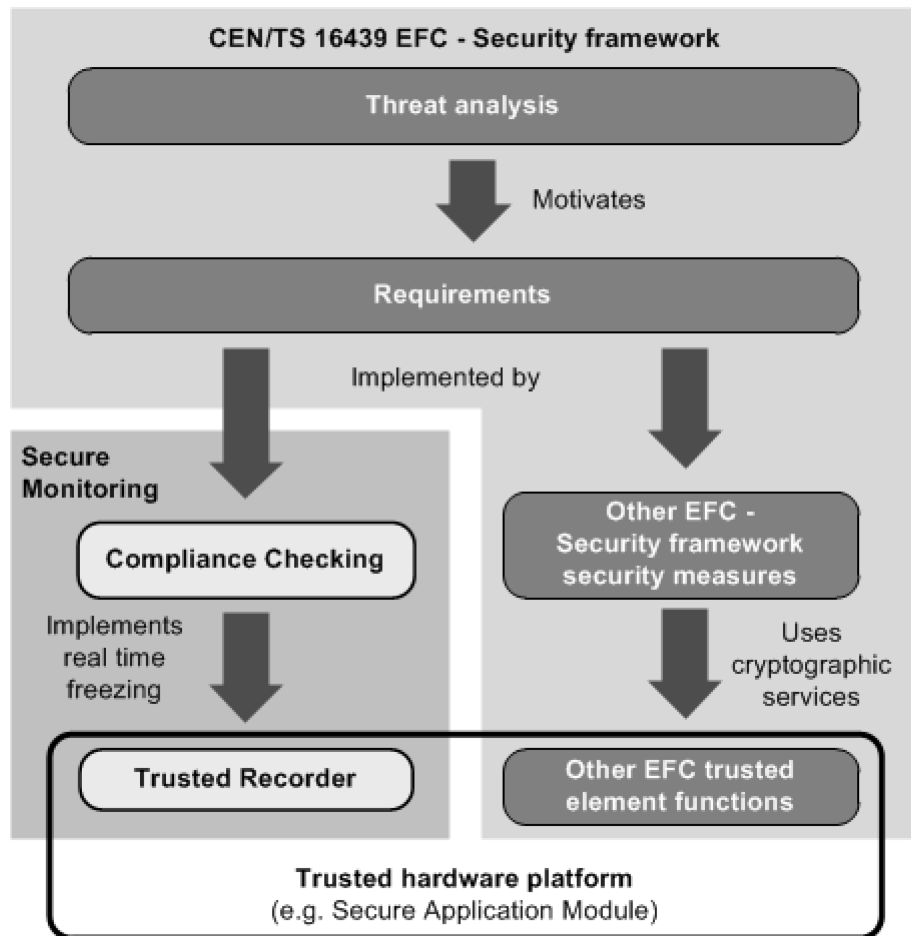


Figure 1 — Relation between EFC - Security framework and the overall secure monitoring concept

Figure 1 shows the relations between the CEN/TS 16439 EFC Security Framework and EFC Secure monitoring for autonomous toll systems, i.e. the two parts Compliance Checking and Trusted Recorder. 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 “Secure Monitoring for autonomous toll systems – Part 1: Compliance checking”. The “Secure Monitoring for autonomous toll systems – Part 2: Trusted Recorder” specifies 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 Technical Specification 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 an OBE;
- Verification SAM, for use in other EFC system entities.

The Technical Specification describes

- terms and definitions used to describe the two Secure Application Module configurations;
- operation of the two Secure Application Modules in the secure monitoring compliance checking concept;
- functional requirements for the two Secure Application Modules configurations, 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 Technical Specification is consistent with the EFC architecture as defined in ISO 17573 and the derived suite of standards and Technical Specifications, especially CEN/TS 16702-1:2014 and CEN/TS 16439.

The following is outside the scope of this Technical Specification:

- The life cycle of a Secure Application Module and the way in which this is managed.
- The interface commands needed to get a Secure Application Module in an operational state.
- The interface definition of the Verification SAM.
- Definition of a hardware platform for the implementation of a Secure Application Module.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

CEN/TS 16439:2013¹, *Electronic fee collection - Security framework*

CEN/TS 16702-1:2014, *Electronic fee collection - Secure monitoring for autonomous toll systems - Part 1: Compliance checking*

EN ISO 14906:2011, *Electronic fee collection - Application interface definition for dedicated short-range communication (ISO 14906:2011)*

¹) CEN/TS 16439:2013 is currently under revision and accepted as a CEN/ISO work item. The next edition will be assigned the reference CEN ISO/TS 19299.

CEN/TS 16702-2:2015 (E)

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

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

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

ISO/IEC 14888-3:2006, *Information technology — Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms*

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

ISO/IEC 18033-3:2010, *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*

koniec náhľadu – text ďalej pokračuje v platenej verzii STN