SLOVENSKI STANDARD
kSIST-TS FprCEN/TS 16702-2:2014

01-november-2014

Elektronsko pobiranje pristojbin - Varnostno spremljanje avtonomnih sistemov cestninjenja - 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

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

ICS:

03.220.20	Cestni transport	Road transport
35.240.60	Uporabniške rešitve IT v transportu in trgovini	IT applications in transport and trade

kSIST-TS FprCEN/TS 16702-2:2014 **en,fr,de**

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

FINAL DRAFT FprCEN/TS 16702-2

September 2014

ICS

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 draft Technical Specification is submitted to CEN members for Technical Committee Approval. It has been drawn up by the Technical Committee CEN/TC 278.

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.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a Technical Specification. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a Technical Specification.

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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. FprCEN/TS 16702-2:2014 E

Contents

Page

Foreword

This document (FprCEN/TS 16702-2:2014) has been prepared by Technical Committee CEN/TC 278 “Intelligent transport systems”, the secretariat of which is held by NEN.

This document is currently submitted to the Formal Vote.

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.

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-enabled OBE in every vehicle. 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. FprCEN/TS 16702-1 “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, FprCEN/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 FprCEN/TS 16702-1.

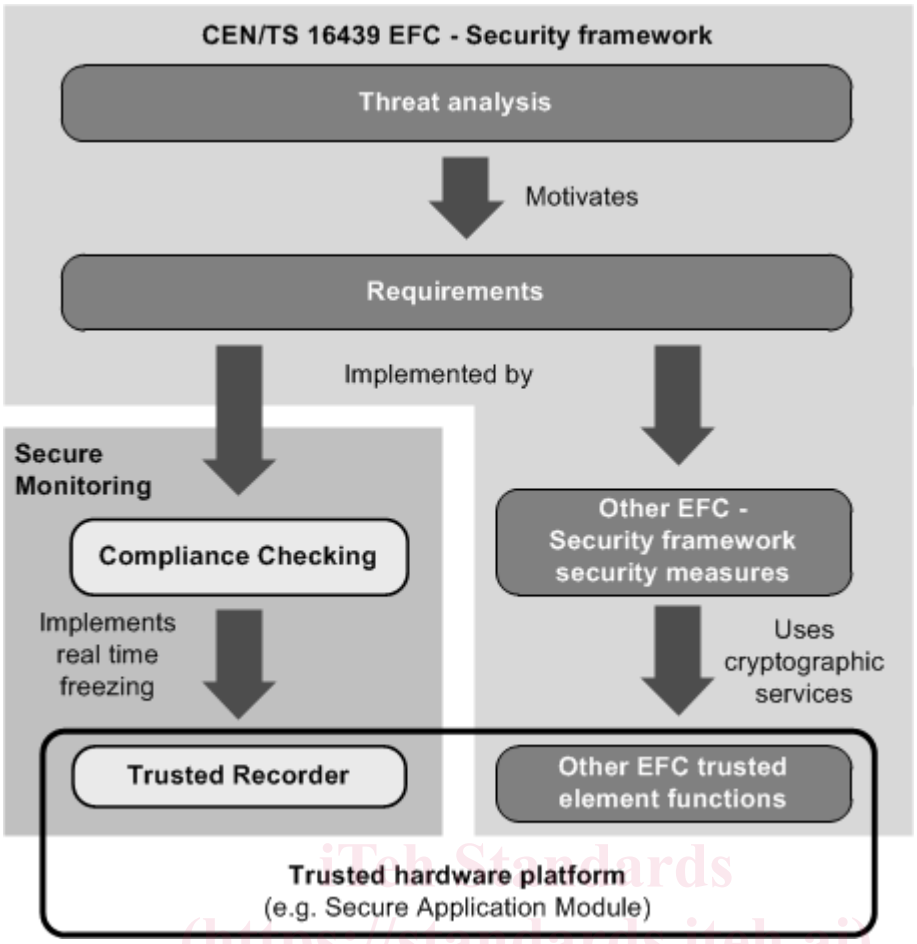

Figure 1 — Relation between EFC - Security framework and the overall secure monitoring concept

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, “Secure Monitoring for autonomous toll systems – Part 2: Trusted recorder” specifies the requirements for the Secure Application Module used in the secure monitoring compliance checking concept. The Technical Specification describes two different configurations of a Secure Application Module (SAM) required for the secure monitoring compliance checking concept:

— 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 FprCEN/TS 16702-1 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 referenced documents are indispensable for the application 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.

ISO/IEC 7816-4:2005, *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*

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

CEN/TS 16439:2013[1)], *Electronic fee collection - Security framework*

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

CEN ISO/TS 17575-1:2010, *Electronic fee collection - Application interface definition for autonomous systems - Part 1: Charging (ISO/TS 17575-1:2010)*

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.

3.1
authentication
provision of assurance that a claimed characteristic of an entity is correct

[SOURCE: ISO/IEC 27000:2009, 2.5]

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

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: ISO/IEC 27000:2009, 2.6]

3.4
Back End
computing and communication facilities of an actor (e.g. a Toll Charger or a Toll Service Provider) exchanging data with a Front or Back End

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.

[SOURCE: CEN ISO/TS 17575-1:2010, 3.4]

3.5
Big Endian
Big Endian systems are systems in which the *most significant byte* of the word is stored in the *smallest address* given and the least significant byte is stored in the largest

3.6
confidentiality
property that information is not made available or disclosed to unauthorised individuals, entities, or processes

[SOURCE: ISO/IEC 27000:2009, 2.9]

3.7
Front End
parts of the toll system where usage data for an individual user are collected, processed and delivered to the Back End

Note 1 to entry: The Front End comprises the on-board equipment and an optional proxy.

[SOURCE: CEN ISO/TS 17575-1:2010, 3.13]

3.8
integrity
the property that data has not been altered or destroyed in an unauthorized manner

3.9
itinerary
travel diary organized in one or more itinerary records enabling assessment of the correctness of the toll declaration

3.10
issuer
institution (or its agent) that issues the Trusted Recorder

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

3.11
Key Verification Code
calculated by encrypting one block of zeroes with the actual symmetric key, then truncated to leftmost three bytes

[SOURCE: CEN/TS 16439:2013]

3.12
message authentication code
MAC
string of bits which is the output of a MAC algorithm

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

[SOURCE: ISO/IEC 9797-1:2011, 3.9]

3.13
non-repudiation
ability to prove the occurrence of a claimed event or action and its originating entities, in order to resolve disputes about the occurrence or non-occurrence of the event or action and about the involvement of entities in the event

[SOURCE: ISO/IEC 27000:2009, 2.27]

3.14
on-board equipment
OBE
equipment fitted within or on the outside of a vehicle and used for toll purposes

[SOURCE: ISO 17573:2010, 3.9]

3.15
real-time freezing
freezing of each itinerary record as soon as its acquisition has terminated, using a Trusted Recorder

3.16
road side equipment
equipment located along the road, ether fixed or mobile

3.17
signature
one or more data elements resulting from the signature process

[SOURCE: ISO/IEC 14888-1:2008, 3.12]

3.18
Signing Time Lock
pre-configured time interval that shall have elapsed since the last successful request to calculate an authenticator before a Trusted Recorder calculates another authenticator

3.19
Secure Application Module
SAM
physically, electrically and logically protected module intended to contain algorithm(s), related keys, security procedures and information to protect an application in such a way that unauthorized access is avoided by tamper protection features

3.20
secure monitoring compliance checking
concept that allows a Toll Charger to rely on the trustworthiness of toll declarations produced by Toll Service Providers

3.21
Toll Charger
TC
entity which levies toll for the use of vehicles in a toll domain

[SOURCE: ISO 17573:2010, 3.16]

3.22
toll declaration
statement to declare the usage of a given EFC service to a Toll Charger

3.23
toll domain
an area or part of a road network where a toll regime is applied

[SOURCE: ISO 17573:2010, 3.18]

3.24
toll domain ID
unique identifier of a toll domain

3.25
toll service
a service enabling users having only one contract and one set of OBE to use a vehicle in one or more toll domains

[SOURCE: ISO 17573:2010, 3.22]

3.26
Toll Service Provider
TSP
entity providing toll services in one or more toll domains

[SOURCE: ISO 17573:2010, 3.23]

3.27
toll system
off board equipment and possible other provisions used by a Toll Charger for the collection of toll for vehicles

[SOURCE: ISO 17573:2010, 3.24]

3.28
Trusted Recorder
TR
logical entity capable of providing cryptographic services, including confidentiality, integrity, authenticity and non-repudiation to be used inside an OBE

3.29
Trusted Third Party
TTP
security authority, or its agent, trusted by other entities with respect to security related activities

3.30
user
customer of a toll service provider, one liable for toll, the owner of the vehicle, a fleet operator, a driver, etc

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

[SOURCE: ISO 17573:2010, 3.29]

3.31
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

4 Symbols and abbreviations

ADU	Application Data Unit
AES	Advanced Encryption Standard (ISO/IEC 18033-3:2010)
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
ID	Identifier
INS	Instruction byte
KVC	Key Verification Code
MAC	Message Authentication Code
NTP	Network Time Protocol
OBE	On-Board Equipment
P1, P2	Parameter bytes
PKI	Public Key Infrastructure
PP	Protection Profile
RQ	Requirement
RSA	Algorithm for public-key cryptography (Rivest, Shamir and Adleman)
RSE	Road Side 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

5 SAM concept and scenarios

5.1 General

FprCEN/TS 16702-1 defines requirements for a Trusted Recorder used in an OBE supporting 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. 5.2 of thisTechnical Specification is describing the two different configurations of the Secure Application Module in the EFC context.

5.3, 5.4 and 5.5 describe the scenarios for the use of the TR and Verification SAM, motivated by FprCEN/TS 16702-1. 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 5 are symbolic and do not always give all details. For details, refer to Clause 7.