PD CEN/TS 16702-1:2014

BSI Standards Publication

Electronic fee collection — Secure monitoring for autonomous toll systems

Part 1: Compliance checking

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of CEN/TS 16702-1:2014.

The UK participation in its preparation was entrusted to Technical Committee EPL/278, Intelligent transport systems.

A list of organizations represented on this committee can be obtained on request to its secretary.

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

ISBN 978 0 580 84810 0

ICS 35.240.60

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 November 2014.

Amendments issued since publication

Date	Text affected

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 16702-1

November 2014

ICS 35.240.60

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: Einhaltungsprüfung

This Technical Specification (CEN/TS) was approved by CEN on 14 June 2014 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

Ref. No. CEN/TS 16702-1:2014 E

Contents

Page

Foreword

This document (CEN/TS 16702-1:2014) 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 [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.

0 Introduction

0.1 Overview

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 CEN ISO/TS 12813:2009 provides useful indications to a TC of whether the 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 Technical Specification 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. Trustworthiness equals the confidence in the reliable operation of the Toll Service Provider's EFC System and / or in case of errors gives technical indications about possible failures or manipulations which may be attributed to the SU and/or the TSP or an external party. An operational EFC System can use a combination of the CCC and SM_CC tools to keep misuse under control effectively.

This Technical Specification is the first part in a set of two that together specify Secure Monitoring for Autonomous Toll Systems: This technical specification, "**Secure Monitoring – Compliance Checking**", specifies the transactions between RSE of the TC over 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. It also specifies the interface between OBE and TR. Most – but not all – available options for secure monitoring require the use of a TR to provide for integrity, authenticity and non-repudiation services.

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 CEN ISO/TS 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).

0.2 Processes

SM_CC provides a TC operating an autonomous toll system with the tools to check whether or not the usage of a transport service by a vehicle in his toll domain is correctly recorded in what is called the itinerary.

In the OBE the registration of a vehicle's road usage is represented by a so-called itinerary which is committed to in real-time or with a defined delay by a process called itinerary freezing. Itinerary freezing ensures that the integrity of the itinerary is undeniably committed to. After an itinerary is frozen, deletion or manipulation/replacement of itinerary data will invalidate the proof of integrity and can thus be detected. The freezing process comes in two variants:

— **real-time freezing**: In this case the presence of a tamper proof trust anchor in the OBE is assumed. This trust anchor is called the Trusted Recorder (TR) and takes care of digitally signing itinerary records thereby committing to them in real-time.

— **freezing per declaration**: In this case, the itineraries are signed by the TSP back end and committed to by sending the signature to the TC using the standard EN ISO 12855:2012 message Toll Declaration.

The road usage itself can be detected via (automatic or manual) observations. In order to be fully effective, the concept requires either ***unexpected*** or ***undetected*** observations, depending on the type of secure monitoring applied.

SM_CC provides the TSP with tools to check the consistency of the Charge Reports obtained from his Front-end and/or the related Toll Declarations with the itinerary. SM_CC is based on a double principle and related processes which are loosely coupled but need to be executed both: **Checking of Itinerary Freezing (CIF)** and **Checking of Toll Declaration (CTD).**

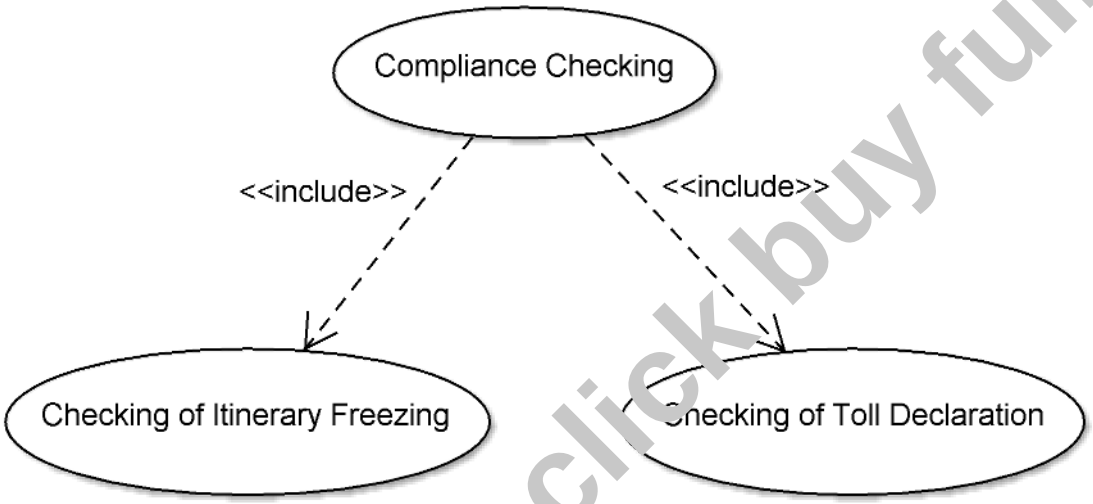

Figure 1 — The sub-processes of Compliance Checking (UML use case diagram)

For CIF the aim is to check the registered itinerary data against an observation of road usage. The concept ensures that such data cannot be corrected in case of an unexpected spot check observation or deleted/changed in case of an absence of checks.

CIF can be done in real-time at the roadside using an SM_CC transaction via DSRC and / or with delay in the back end using the CTD transaction. CIF gives the TC confidence in that all road usage is registered as an itinerary in the freezing process. The frozen itineraries in turn are used as a reference for checking the plausibility of the Toll Declarations.

It is mandatory that the TSP checks that the itinerary is plausible and that the Toll Declaration is consistent with the Itinerary. The Toll Chargers confidence that this process is carried out continuously can be established through the CTD Process, but it is also possible to achieve this through audits or other processes not described in this standard.

CTD is a spot check operation in which the Toll Declaration is checked against the underlying detailed itinerary data (which is not necessarily part of the Toll Declaration) in order to verify that the aggregated fields that are reported (e.g. distance travelled in charging zone, aggregated fee etc.) have been computed correctly. CTD also aims to verify the integrity, the completeness and plausibility of the itinerary data. Since CTD requires the TC to analyse the detailed itineraries corresponding to the Toll Declaration of the SU it is desirable from a privacy perspective to limit the number of CTD transactions.

CIF and CTD can be executed independently, however to achieve the complete coverage of Secure Monitoring CIF needs to be complemented with CTD and vice-versa.

0.3 Options

For a derivation of the different types of Secure Monitoring from the available options, see Table 1. Annex E provides further background information on the use of and the rationale for these options. Annex F how this TS can be used for the EETS.

Type of Secure Monitoring	Description	Capabilities needed				Conditions for effective compliance checks		Privacy impact
		Trusted Recorder	Trusted Time Source	High communication availability	CIF via DSRC	*UNEXPECTED* observations	*UNDETECTED* observations	
SM_CC-1	1. Real-time Freezing using a Trusted Recorder without trusted time source 2. Unexpected observation 3. Real-time Checking of itinerary freezing over DSRC Option: Occasional delayed (back end) Checking of Itinerary Freezing	X			X	X		An itinerary record (IR) is evaluated on the spot by the TC and deleted together with the images in case of correctness. In case of delayed (back end) Checking of Itinerary Freezing: Observation data for those checks (images) are stored until itinerary records can be checked.
SM_CC-2	1. Real-time Freezing using a Trusted Recorder with trusted time source 2. Unexpected observation 3. Delayed (back end) Checking of Itinerary Freezing	X	X			X		Observation (images) data are stored until itinerary records can be checked.
SM_CC-3a	1. Freezing per Declaration 2. Undetected observation 3. Delayed (back end) Checking of Itinerary Freezing						X	Observation (images) data are stored until itinerary records can be checked.
SM_CC-3b	1. Freezing per Declaration with High Frequency 2. Unexpected observation 3. Delayed (back end) Checking of Itinerary Freezing			X		X		Observation (images) data are stored until itinerary records can be checked.

Table 1 — Different types of Secure Monitoring

A TC or TSP that wants to operate under one (or many) types of Secure Monitoring needs to implement the required capabilities.

Trusted Recorder capability: To equip the OBE with a TR (SM_CC-1) or even a TR with Trusted Time Source (SM_CC-2) is a TSP decision. Amongst other things, the TR needs to:

1. have a high level protection against unauthorised disclosure and/or modification of stored data;

2. be capable of secure cryptographic computations;

3. include a secure monotonous transaction counter;

4. be capable of enforcing a minimum time lock between records to be signed (frozen) or explicitly checking the correctness of their timestamp (in case of presence of a trusted time source).

High communication availability: High communication availability (for SM_CC-3b) is in practice determined by the telecommunication coverage of the toll domain. This is primarily something the TSP can influence by contracting the appropriate service level with the mobile communications provider.

CIF via DSRC: The possibility to perform CIF in real-time (SM_CC-1) depends on the capability to have this SM_CC transaction implemented over DSRC and for both TSP and TC to be equipped with DSRC transponders and transceivers respectively.

Unexpected or undetected observations: An ***unexpected*** observation is not known to the driver or OBE beforehand but might well be after. The reason could for example be because the user observed a road side compliance checking equipment, or because a DSRC transaction took place which informs the OBE that it has been observed. An ***undetected*** observation, by contrast, is known neither before nor after to the driver and OBE.

SM_CC-1: The OBE is equipped with a TR which freezes all itineraries in real-time. By performing a CIF transaction via DSRC, the RSE is able to check that the observed road usage of the vehicle is correctly accounted for in the last frozen itinerary record. Because itinerary records are consecutively numbered and can only be signed by the specific TR in the OBE, the TC can be confident that this itinerary record will be included in the itinerary data underlying the declaration. (Missing or altered records can be detected through CTD.) Consequently the observation data can be deleted immediately after the check, unless irregularities were detected.

SM_CC-2: Here the OBE is equipped with a TR with trusted time source. This type is quite similar to SM_CC-1 but does not require that CIF is performed in real-time over DSRC. The full effectiveness can be accomplished with unexpected observations in combination with delayed CIF in the back end using the CTD transaction. This is due to a trusted timestamp associated with a frozen record, as opposed to the previous implementation scenario SM_CC-1 where only the order of records can be guaranteed through the toll domain counter. With a trusted timestamp, attacks where (fake) itineraries are frozen afterwards are rendered ineffective as they will be recorded with the actual time of creation.

SM_CC-3a: In this scenario no TR is needed, because the TSP performs freezing per declaration. An observation of the vehicle is checked for consistency with the itinerary in the back end using the CTD transaction. Observation data have to be stored until the toll declaration and requested underlying itinerary data are received from the TSP. It is noted that this approach will be effective against manipulation of charge and itinerary data by the SU (or TSP) only if observations are, at least occasionally, undetected by the SU (or TSP). Otherwise, the SU (or TSP) could always take care that his manipulation goes undetected by including correct data for the points of observation.

SM_CC-3b: In case there is no confidence that observations can be performed undetected, freezing per declaration can still be effective if the reporting frequency for the declaration is high. It will be difficult to manipulate itinerary data while including detected observation points under the condition that the resulting

itinerary data still constitute a realistic pattern. However, it depends on the scheme details what reporting frequency would be sufficient. A high reporting frequency also imposes requirements and costs on mobile communications and TSP back end.

0.4 Privacy aspects

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 and/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 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

1.1 General scope

This Technical Specification specifies transactions and data for Compliance Checking - Secure Monitoring. The scope of this technical specification consists of:

— The concept and involved processes for Secure Monitoring.

— The definition of new transactions and data.

— The use of the OBE compliance checking transaction as specified in CEN ISO/TS 12813:2009, for the purpose of Compliance Checking - Secure Monitoring.

— The use of back end transactions as specified in EN ISO 12855:2012, 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 organisational 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.

Outside the scope of this Technical Specification are:

— 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 and/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.

— Choices concerning the storage location of itinerary records, and data retention policy.

— Recommendations for a single specific implementation due to different applicable privacy laws. Instead, a set of options is provided.

1.2 Relation to CEN/TS 16439

Secure Monitoring can be regarded as a set of specific measures addressing a number of serious threats identified in the EFC Security Framework, namely:

Threats assigned to the User agent:

— Manipulating the system to not register road usage.

— Manipulating the system to register the wrong (lower) road usage.

— Manipulating the system to lose road usage data.

Threats assigned to Toll Service Provider agent:

— Modifying usage data reported from the OBE.