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 - 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 5

0 Introduction 6
0.1 Overview 6
0.2 Processes 6
0.3 Options 8
0.4 Privacy aspects 11

1 Scope 12
1.1 General scope 12
1.2 Relation to CEN/TS 16439 12
1.3 Relation to other standards 14

2 Normative references 14

3 Terms and definitions 15

4 Abbreviations 17

5 Processes 18
5.1 Introduction and overview 18
5.2 Processes needed for different types of Secure Monitoring 19
5.3 Itinerary Freezing 21
5.3.1 Introduction 21
5.3.2 Generate Itinerary 21
5.3.3 Real-time freezing 23
5.3.4 Freezing per declaration 24
5.4 Checking of Itinerary Freezing 25
5.4.1 Introduction 25
5.4.2 Observing a vehicle 25
5.4.3 Retrieving Proof of Itinerary Freezing (PIF) 26
5.4.4 Checking PIF against Observation 27
5.5 Checking of Toll Declaration 27
5.5.1 Introduction 27
5.5.2 Retrieve Itinerary Data 27
5.5.3 Check Itinerary Consistency 28
5.5.4 Checking Toll Declaration against Itinerary 28
5.6 Claiming incorrectness 29
5.7 Providing EFC Context Data 29
5.8 Key Management 29
5.8.1 Introduction 29
5.8.2 Requirements 29

6 Transactions 30
6.1 Introduction 30
6.2 Description of Itinerary Data 32
6.2.1 Introduction 32
6.2.2 Itinerary Batch 34
6.2.3 Itinerary Record Data Elements 35
6.3 Retrieving PIF in real-time (DSRC Transaction) 37
6.3.1 Introduction 37
6.3.2 Transactional Model 38
6.3.3 Syntax and Semantics 38
6.3.4 Security 40
6.4 Toll Declaration 40

6.4.1 Introduction 40
6.4.2 Transactional Model 40
6.4.3 Syntax and semantics 41
6.4.4 Itinerary Sequence 42
6.4.5 Security 44
6.5 Back End Data Checking 44
6.5.1 Introduction 44
6.5.2 Transactional model 45
6.5.3 Checks of the Itinerary 46
6.5.4 Syntax and semantics 47
6.5.5 Security 50
6.6 Claiming incorrectness 50
6.6.1 Introduction 50
6.6.2 Transactional model 51
6.6.3 Syntax and semantics 52
6.6.4 Security 52
6.7 Providing EFC Context Data 53
6.7.1 Introduction 53
6.7.2 Transactional Model 53
6.7.3 Syntax and semantics 53
6.7.4 Security 55

7 Security 55
7.1 Security functions and elements 55
7.1.1 Hash functions 55
7.1.2 MAC 55
7.1.3 Digital signatures 55
7.1.4 Public Keys, Certificates and CRL 55
7.2 Key Management 56
7.2.1 Key Exchange between Stakeholders 56
7.2.2 Key generation and certification 56
7.3 Trusted Recorder and SM_CC Verification SAM characteristics 57
7.3.1 Introduction 57
7.3.2 Trusted Recorder 57
7.3.3 SM_CC Verification SAM 58

Annex A (normative) Data type specification 59

Annex B (normative) Protocol Implementation Conformance Statement 67
B.1 Guidance for completing the PICS proforma 67
B.1.1 Purposes and structure 67
B.1.2 Abbreviations and conventions 67
B.1.3 Instructions for completing the PICS proforma 69
B.2 Identification of the implementation 69
B.2.1 General 69
B.2.2 Date of the statement 69
B.2.3 Implementation Under Test (IUT) identification 69
B.2.4 System Under Test (SUT) identification 69
B.2.5 Product supplier 70
B.2.6 Applicant (if different from product supplier) 70
B.2.7 PICS contact person 70
B.3 Identification of the protocol 71
B.4 Global statement of conformance 71
B.5 Roles 71
B.6 Types of Secure Monitoring 71
B.7 Capabilities and conditions 72
B.8 Processes 73

Annex C (informative) Example transactions 74

Annex D (informative) Addressed threats (in CEN/TS 16439) **78**
D.1 Introduction **78**
D.2 Threats where Secure Monitoring can provide Security Measures **78**
D.3 Related Requirements **80**
D.4 Related Security Measures **81**

Annex E (informative) Essentials of the SM_CC concept **84**
E.1 Introduction **84**
E.2 The SM_CC concept – FAQs **84**
E.3 SM_CC options **86**
E.3.1 SM_CC_1 ..... **86**
E.3.2 SM_CC_2 ..... **90**
E.3.3 SM_CC_3a **93**
E.3.4 SM_CC_3b **95**
E.4 Managing multiple toll domains **96**
E.4.1 Overlapping toll domains **96**
E.4.2 The 'catch-all' toll domain counter **98**

Annex F (informative) Use of this Technical Specification for the EETS **99**
F.1 General **99**
F.2 Overall relationship between European standardization and the EETS **99**
F.3 European standardization work supporting the EETS **99**
F.4 Correspondence between this technical specification and the EETS **100**

Bibliography **101**

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).**

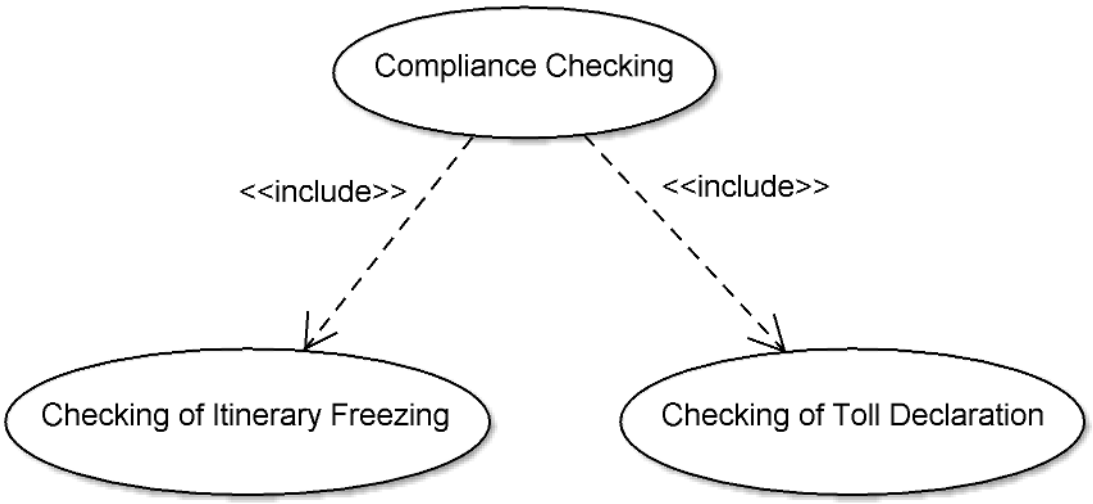

Figure 1 — The sub-processes of Compliance Checking (UML use case diagram)

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.

— Suppressing reporting of road use.

— Faulty interpretation of usage data.

— Wrongly configuring the front end.

NOTE The Technical Specification EFC Security Framework (CEN/TS 16439:2013) analyses the general requirements of the stakeholders and provides a comprehensive threat analysis for an interoperable EFC scheme. A number of identified threats may result in less revenue of the toll charger, incorrect charging and billing and not meeting required service levels between Toll Service Provider and Toll Charger. The EFC Security Framework further specifies requirements to counter the identified threats. Some of these requirements can be fulfilled by implementing basic security measures that are specified in the same document, but more specific security measures are left to other standards and specifications or to local choices.

Secure Monitoring makes use of basic cryptographic security measures and procedures provided for in the EFC Security Framework as far as possible. The relation between the EFC Security Framework and the Secure Monitoring technical specifications is illustrated in Figure 2.

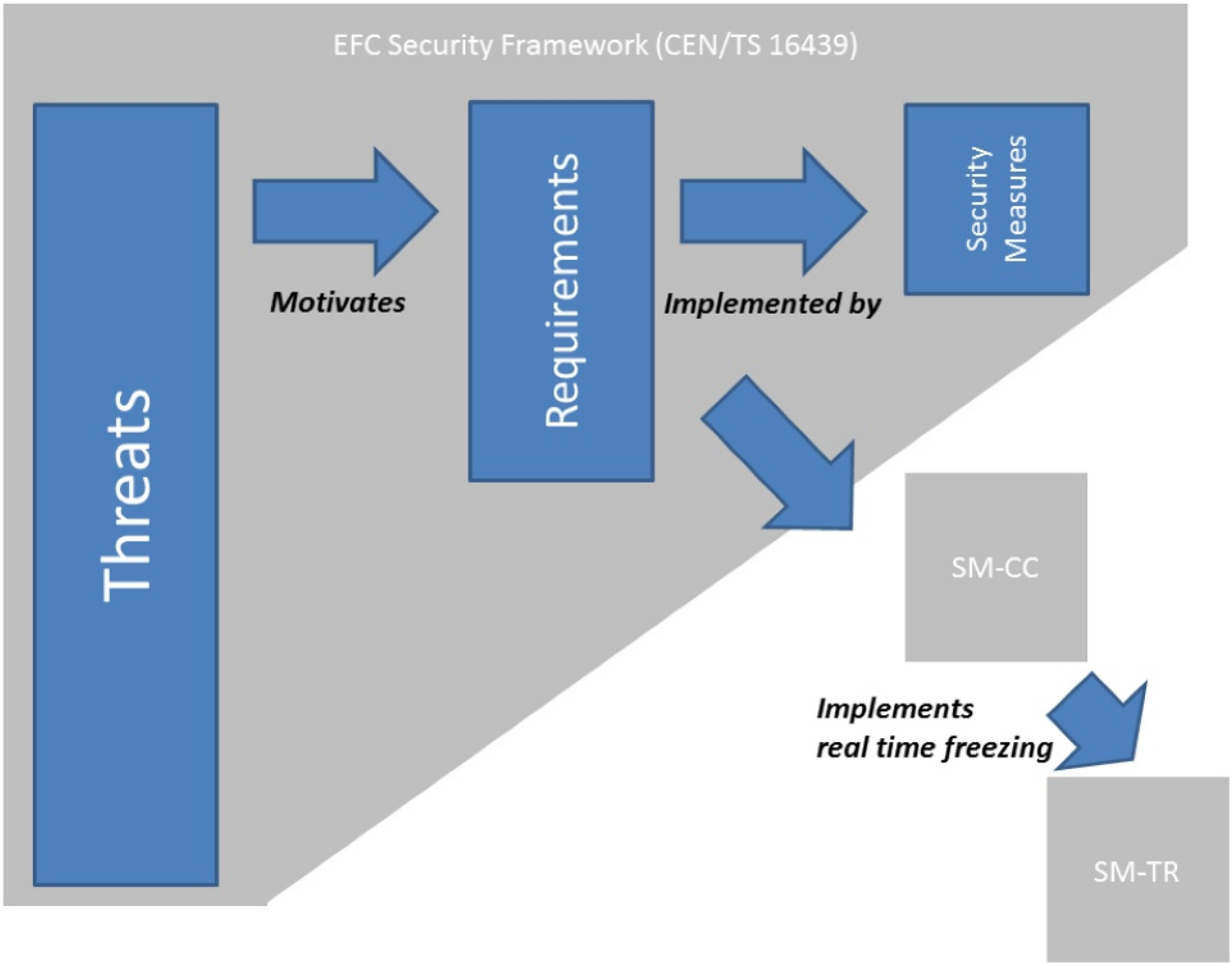

Figure 2 — Relation between the EFC Security Framework, Secure Monitoring - Compliance Checking and Secure Monitoring - Trusted Recorder

Based on the threat analysis that has been carried out in the EFC Security Framework, Figure 2 specifies which attacks Secure Monitoring addresses.

1.3 Relation to other standards

This Technical Specification complies with the allocation of roles and responsibilities as specified in ISO 17573:2010 Electronic fee collection – Systems architecture for vehicle related tolling.

This Technical Specification defines transactions in the interfaces between the TSP Front end and the Toll Charger's road side equipment (RSE) as well as between the Toll Service Providers and the Toll Chargers back end. As these interfaces are also covered by CEN ISO/TS 12813:2009 (Compliance Checking Communication) and EN ISO 12855:2012 (Information Exchange between service provision and Toll Charging), SM_CC reuses these standards by specifying which options to choose and by defining the content of data fields. Extensions and additions are only specified in cases where it is not possible to specify the SM_CC with the tools available in these standards.

The relation between this Technical Specification, the interfaces between TC and TSP and the aforementioned standards is illustrated in Figure 3 below.

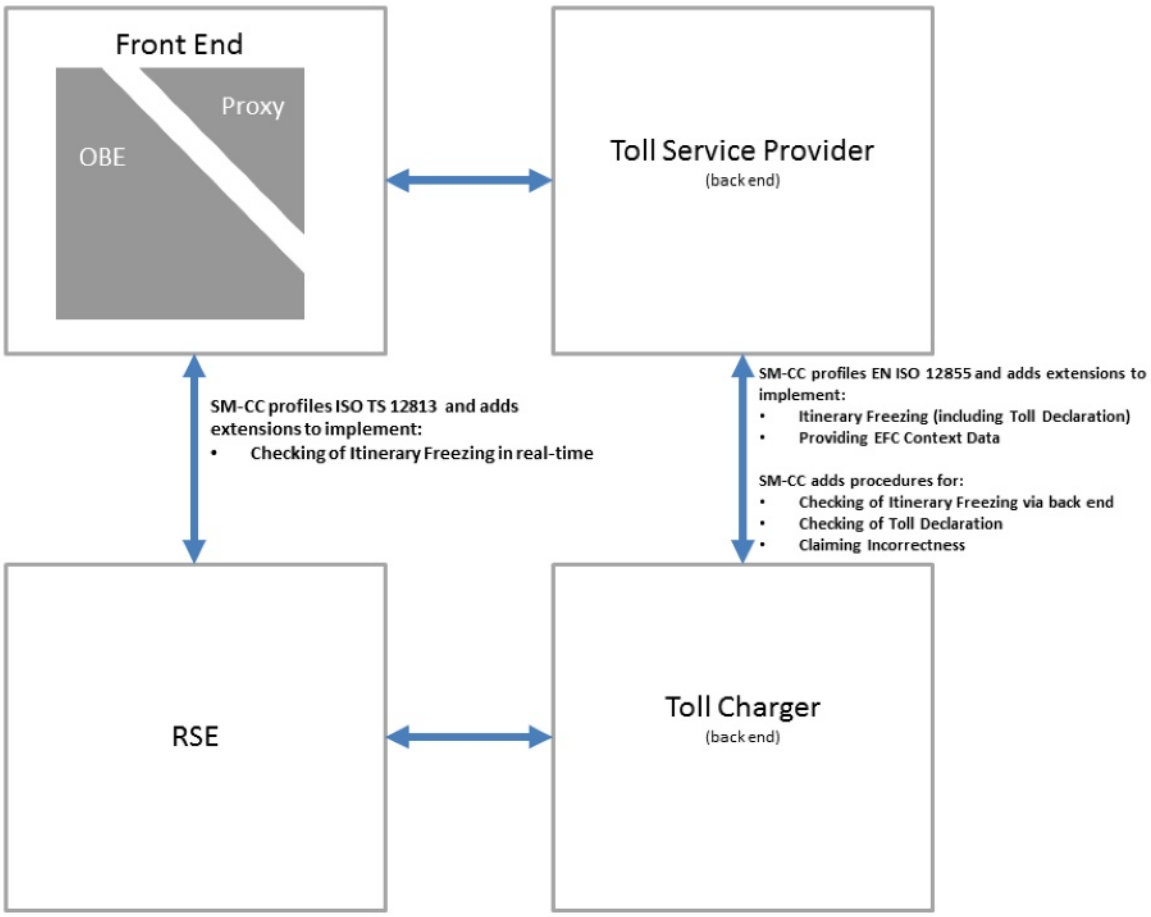

Figure 3 — Relation between Secure Monitoring – Compliance Checking, Compliance Checking Communication (CEN ISO/TS 12813:2009) and Information Exchange between service provision and Toll Chargers (EN ISO 12855:2012)

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.

ISO/IEC 8824-1:2008, *Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation*

ISO/IEC 8825-1, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

ISO/IEC 8825-2:2008, *Information technology — ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)*

ISO/IEC 8825-4:2008, *Information technology — ASN.1 encoding rules: XML Encoding Rules (XER)*

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

ISO/IEC 11770-3:2008, *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*

ISO 14813-6, *Intelligent transport systems — Reference model architecture(s) for the ITS sector — Part 6: Data presentation in ASN.1*

ISO/IEC 18033-1:2005, *Information technology — Security techniques — Encryption algorithms — Part 1: General*

ISO/IEC 18033-3:2010, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

CEN ISO/TS 12813:2009, *Electronic fee collection - Compliance check communication for autonomous systems (ISO/TS 12813:2009)*

EN ISO 12855:2012, *Electronic fee collection - Information exchange between service provision and toll charging (ISO 12855:2012)*

EN ISO 14906:2011 + A1:2014, *Electronic fee collection - Application interface definition for dedicated short-range communication (ISO 14906:2011)*

CEN/TS 16439:2013 *Electronic fee collection - Security framework*

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

CEN ISO/TS 17575-3:2011, *Electronic fee collection - Application interface definition for autonomous systems - Part 3: Context data (ISO/TS 17575-3:2011)*

NIMA TR8350.2, Third Edition – Amendment 1, January 2000, Department of Defense – World Geodetic System 1984, Its Definition and Relationships With Local Geodetic Systems, issued by National Imagery and Mapping Agency (NIMA), US Department of Defense

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
attribute
addressable package of data consisting of a single data element or structured sequences of data elements

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

3.3
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

3.4
charge report
information containing road usage and related information originated at the Front End

3.5
context data
information defined by the responsible Toll Charger necessary to establish the toll due for using a vehicle on a particular toll context and to conclude the toll transaction

3.6
context dependent itinerary
itinerary of which the syntax and semantics depend on the toll domain's context data

3.7
context independent itinerary
itinerary of which the syntax and semantics are independent of the toll domain's context data

3.8
electronic fee collection
fee collection by electronic means

3.9
freezing per declaration
process that freezes the itinerary related to the toll declaration by sending a cryptographic commit or the whole itinerary to the Toll Charger

3.10
front end
parts of the toll system where usage data for an individual user are collected, processed and delivered to the Back End

3.11
itinerary
travel diary organized in one or more itinerary records enabling assessment of the correctness of the toll declaration

3.12
itinerary batch
sequence of sequential itinerary records of the same type all pertaining to a defined set of toll domains

3.13
itinerary freezing
registering an itinerary and undeniably committing oneself to it

3.14
itinerary sequence
sequence of aggregated data committing to a number of underlying itinerary batches

3.15
itinerary record
atomic data element describing use of the road network or use of the vehicle

3.16
on-board equipment
equipment located on-board a vehicle including nomadic devices with the function of exchanging information with external systems

3.17
real-time freezing
freezing of each itinerary record as soon as its acquisition has terminated using a Trusted Recorder

3.18
secure monitoring compliance checking
concept that allows a Toll Charger to rely on the trustworthiness of toll declarations produced by Toll Service Providers

3.19
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

3.20
toll declaration
statement to declare the usage of a given EFC service to a Toll Charger

3.21
toll domain
area or a part of a road network where a certain toll regime is applied

3.22
trusted recorder
logical entity capable of cryptographic functions, used to provide the OBE with security services, including data confidentiality, data integrity, authentication and non-repudiation

3.23
undetected observation
observation of road usage, performed by the Toll Charger, which is neither known to the driver or OBE before nor after the observation

3.24
unexpected observation
observation of road usage, performed by the Toll Charger, which is unknown to the driver or OBE before but might be known after the observation

4 Abbreviations

For the purpose of this document, the following abbreviations apply throughout the document unless otherwise specified.

CDIR Context Dependent Itinerary Record

CIF Checking of Itinerary Freezing

CIIR Context Independent Itinerary Record

CRL Certificate Revocation List

CTD	Checking of Toll Declaration
DSRC	Dedicated Short Range Communication
EETS	European Electronic Toll Service
EFC	Electronic Fee Collection
FIFO	First In - First Out
FpD	Freezing per Declaration
GNSS	Global Navigation Satellite System
IR	Itinerary Record
LAC	Localisation Augmentation Communication
OBE	On Board Equipment
OBU	On Board Unit
PICS	Protocol Implementation Conformance Statement
PIF	Proof of Itinerary Freezing
RSE	Road Side Equipment
RTF	Real-Time Freezing
SAM	Secure Application Module
SM_CC	Secure Monitoring Compliance Checking
SM_TR	Secure Monitoring Trusted Recorder
SU	Service User
TC	Toll Charger
TC_SAM	Toll Charger SAM
TR	Trusted Recorder
TSP	Toll Service Provider
TSP_SAM	Toll Service Provider SAM
TTP	Trusted Third Party
UML	Unified Modeling Language

5 Processes

5.1 Introduction and overview

This clause introduces the conceptual framework of Secure Monitoring Compliance Checking in terms of requirements to a system and/or devices implementing it. It also describes the relations between different processes and information classes.

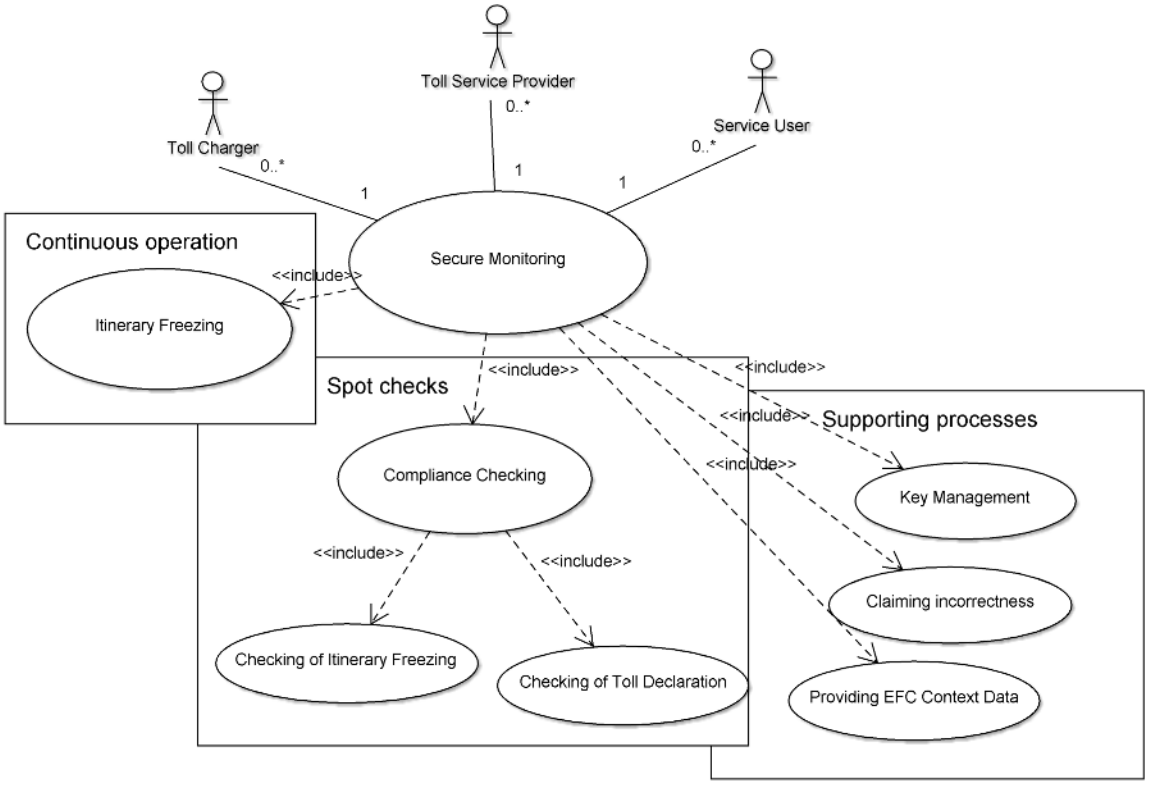

Figure 4 — The main stakeholders and processes of Secure Monitoring (UML use case diagram)

The Secure Monitoring Compliance Checking processes shall regulate the interactions between the three stakeholders Toll Charger (TC), Toll Service Provider (TSP) and Service User (SU) in the following main processes:

a) Itinerary Freezing: generate and freeze the itinerary;

b) Checking of Itinerary Freezing: check the frozen itinerary for correctness against the observation;

c) Checking of Toll Declaration: check the correctness of the Toll Declaration against the itinerary;

and the following supporting processes:

d) Claiming incorrectness: information from TC to TSP about a negative outcome of Checking of Itinerary Freezing and/or Checking of Toll Declaration;

e) Providing EFC Context Data: TCs specification of itinerary characteristics such as format and periodicity;

f) Key Management: issuing, storage and use of the cryptographic keys used for secure monitoring.

5.2 Processes needed for different types of Secure Monitoring

SM_CC provides the options described in Table 2 to the TSP.

Table 2 — Processes to be implemented by the TSP

	Processes to be supported by the TSP					
Type of Secure Monitoring	**Itinerary Freezing in Real-Time (5.3 excluding 5.3.4)**	**Itinerary Freezing in Real-Time with Trusted Time capability (5.3 excluding 5.3.4)**	**Itinerary Freezing per Declaration (5.3 excluding 5.3.3)**	**Itinerary Freezing per Declaration with High Frequency capability (5.3 excluding 5.3.3)**	**CIF via DSRC (5.4.3 and 5.4.4)**	**CIF via TSP Back End / CTD (5.4.3 and 5.4.4)**
SM_CC-1	X				X	OPTIONAL
SM_CC-2	X	X				X
SM_CC-3a			X			X
SM_CC-3b			X	X		X

NOTE The same transaction is used to perform Checking of Itinerary Freezing and Checking of Toll Declaration, the processes only differ in the required steps in the TC back end. Checking of itinerary freezing is not done via the back end in case of SM_CC-1. Therefore the transaction needs only to be implemented if Checking of Toll Declaration process is to be performed (the alternative would be to ascertain correspondence between itineraries and Toll Declarations through other processes, for example TC audits of the TSP's system).

SM_CC provides the options described in Table 3 to the TC.

Table 3 — Processes to be implemented by the TC

	Processes to be supported by the TC				
Type of Secure Monitoring	***UNEXPECTED* observations (5.4.2)**	***UNDETECTED* observations (5.4.2)**	**CIF via DSRC (5.4.3 and 5.4.4)**	**CIF via TSP Back End (5.4.3 and 5.4.4)**	**CTD (5.5)**
SM_CC-1	X		X		OPTIONAL
SM_CC-2				X	OPTIONAL
SM_CC-3a		X		X	OPTIONAL
SM_CC-3b	X			X	OPTIONAL

In case of SM_CC-3b Itinerary Freezing per Declaration is done with a high frequency, which means that the Toll Charger also shall be able to receive and process them at a high frequency (one Toll Declaration every minute is a feasible time interval).

In addition, both TSP and TC shall implement all supporting processes, Key management (see 5.8), Claiming incorrectness (see 5.6) and Providing EFC Context Data (see 5.7).

A TSP may, for example for interoperability reasons, implement procedures that cover several types of Secure Monitoring at once. By retrieving the EFCContextData (see 5.7) it can decide which procedures shall be activated for a certain toll domain. Likewise, a TC may implement several types of Secure Monitoring to allow the TSPs operating in its domain a wider range of options.

Furthermore, if a TSP implements Itinerary Freezing in Real-Time it may alternatively implement Itinerary Freezing in Real-Time with Trusted Time Source (both procedures described in 5.3.3).

If a TC implements Unexpected Observations, it may alternatively implement Undetected Observations (both procedures described in 5.4.2) if applicable regulations in the Toll Domain allows it.

5.3 Itinerary Freezing

5.3.1 Introduction

The process Itinerary Freezing has two alternative implementations; itinerary freezing in real-time (in support of SM_CC-1 and SM_CC-2) and itinerary freezing per declaration (in support of SM_CC-3a/b). The chosen alternative shall operate in parallel to the basic processes for autonomous tolling implemented by the Front-end in compliance with EN ISO 12855:2012.

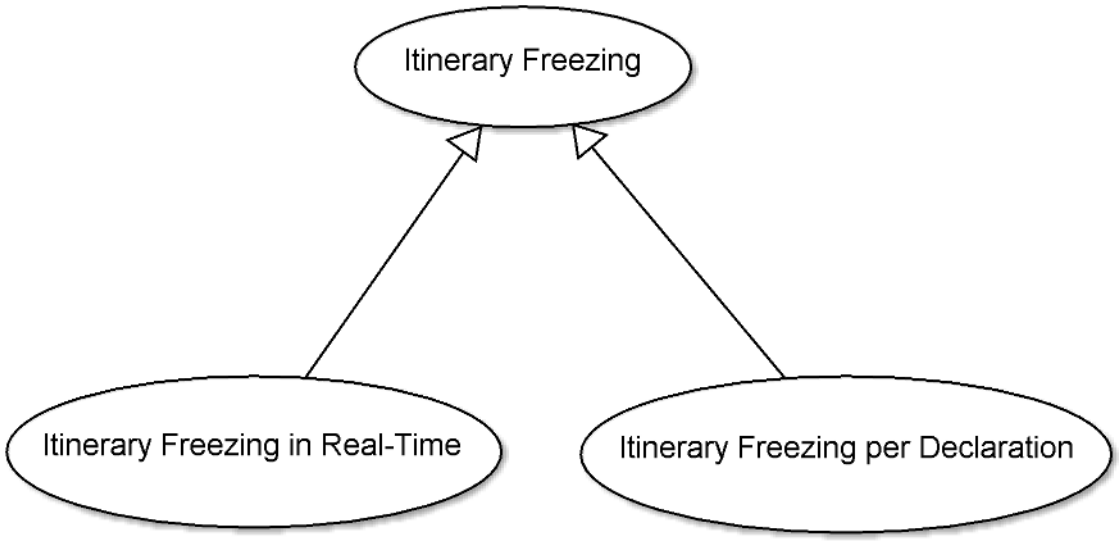

Figure 5 — The sub-processes of Itinerary Freezing (UML use case diagram)

The TSP shall implement and operate the Generate Itinerary process (first process step in both implementations). The TSP may either implement the Real-time Freezing process or the Freezing per Declaration process or both, but operate only one at a time.

5.3.2 Generate Itinerary

The OBE shall either generate a context independent or a context dependent itinerary. Not creating itineraries is only an option in non-SM_CC toll domains.

The OBE shall always generate a context independent itinerary from the same data as collected according to EN ISO 12855:2012, within the Toll Domain borders defined by the EFC Context Data, in the form of context independent itinerary records as defined in 6.2.3.4. The records shall be generated and completed periodically

according to a predefined scheme of distance and time. The OBE shall complete a record in case of a change of applicable Toll Domain or in case of shut down.

NOTE 1 Context independent itinerary records can be generated based on sensor data collected by any type of autonomous OBE without the need for processing capabilities or contextual data. Context independent itinerary records are a viable option for both thin and smart clients.

NOTE 2 SM_CC does not prevent the OBE from generating and signing intermediate usage data for production of charge data in the proxy, or from directly generating and signing charge data in form of charge reports.

The OBE may alternatively generate a context dependent itinerary within the Toll Domain borders defined by the EFC Context Data. The itinerary shall have the form of context dependent itinerary records containing information about one or more of the following Charge Report options from CEN ISO/TS 17575-1:2010, 5.2:

— One record per detected Charge Object.

— One record per fixed (configurable, see 5.7) distance or period of time, containing the driven distance within that part of a trip.

— One record per fixed (configurable, see 5.7) distance or period of time, containing the time elapsed within that part of a trip.

— One record per fixed (configurable, see 5.7) distance or period of time, containing the number of detected events within that part of the trip.

Within a record, the charge-relevant parameters shall have a fixed value.

The records shall have the format as defined in 6.2.3 and with one of the options selected in accordance to the extended EFC Context data, see 6.7. An OBE does not necessarily have to support all types of context dependent itineraries.

NOTE 3 Context dependent itinerary records are an option for smart clients only. Nevertheless also for smart clients it might be more efficient to make use of only context independent itinerary data, eliminating the need for adapting in case of switching the toll context.

The OBE shall complete a record in case of a change of applicable Toll Domain or in case of shut down.

The availability of context dependent itinerary data are under responsibility of the Toll Service Provider and subject to agreement between Toll Service Provider and Toll Charger.

In case of overlapping Toll Domains, the OBE shall generate context independent and context dependent itinerary records of the applicable types as necessary for each of the Toll Domains. Nevertheless, the OBE may generate only a single itinerary record for those overlapping Toll Domains that use the same record type and the same periodicity. In this case it shall contain the identification of each pertinent Toll Domain.

5.3.3 Real-time freezing

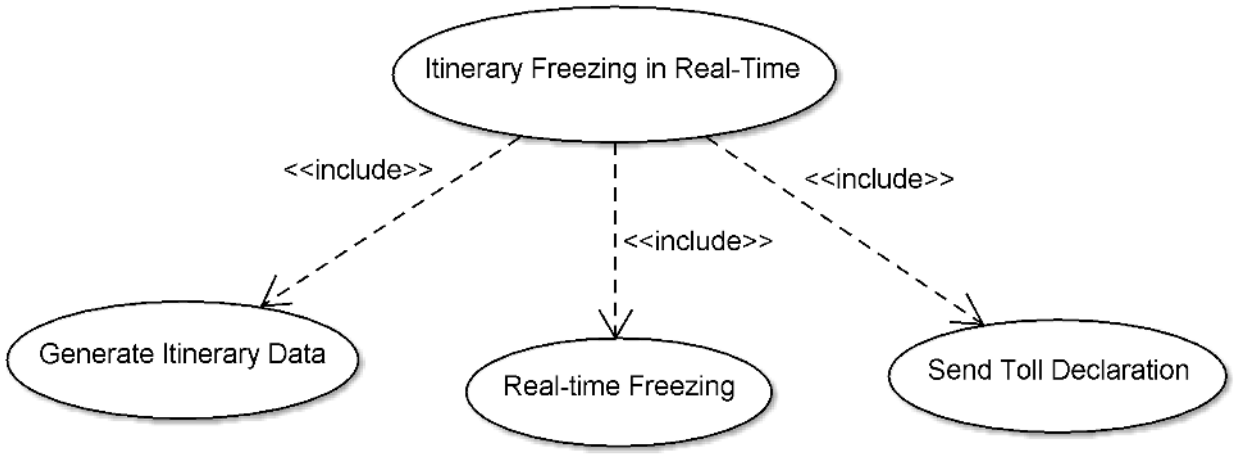

Figure 6 — The sub-processes of Itinerary Freezing in Real-Time (UML use case diagram)

In the case of real-time freezing (in support of SM_CC-1 or SM_CC-2), the OBE shall freeze each itinerary record as soon as its acquisition has terminated. To achieve this the OBE shall obtain the toll domain counter, which is the record sequence number for the given Toll Domain, and the authenticator calculated over the itinerary record data, from the Trusted Recorder. Additionally, in case of a Trusted Recorder with trusted time source, the OBE obtains the necessary time information from the Trusted Recorder.

In case of a change of date or shut down of the OBE, the last record shall be frozen accordingly.

NOTE 1 The authenticator can be generated either using symmetric cryptography and an associated secret key or asymmetric cryptography and an associated key pair. Both choices have their pros and cons and the choice which method to use is left open to the Toll Service Provider. It is to be noted that which option is used also affects the implementation of the Toll Charger.

The OBE shall store the last frozen itinerary record containing the information defined in 6.2 and in case of SM_CC-1 make it available on the DSRC interface for checking of itinerary freezing as defined in 6.3.

The OBE shall store the itinerary records in itinerary batches defined in 6.2 according to a FIFO principle.

NOTE 2 This Technical Specification does not impose requirements on the OBE's or Toll Service Provider's internal format of records and batches as long as the syntax and semantics applicable to the transactions is fulfilled.

Toll Service Provider proxy/ back end shall retrieve the itinerary records from the OBE before deletion out of the FIFO memory if Toll Charger CIF or CTD requests are still allowed. The period of time during which a Toll Charger can perform such a delayed check is to be agreed with the Toll Service Provider.

The Toll Service Provider shall check the integrity of the itinerary and generally assess its plausibility using time/distance evaluations and detecting holes in the itinerary as described in 5.5.3. The Toll Service Provider shall check the correctness of the Front-End's Charge Report using the itinerary and optionally other available usage data similarly to what is described in 5.5.4.

If all checks are OK the Toll Service Provider shall generate a Toll Declaration, sign it and send it to the Toll Charger using the TollDeclarationADU according to 8.6.5 of CEN/TS 16439:2013 (using the InformationExchangeSec mechanism). The checks and signature can be implemented as part of a trusted processing platform which can be audited/certified by the Toll Charger.

The further handling by the Toll Service Provider if any check is not OK is outside the scope of this Technical Specification.

5.3.4 Freezing per declaration

Freezing per Declaration can be done in two ways:

— Sending an Itinerary Sequence Hash. Sending the Itinerary Sequence Hash implies a commitment to the content of the underlying itinerary records, yet without including these in the message.

— Declaring detailed charge data (directly revealing the itinerary to the Toll Charger) in which case an Itinerary Sequence Hash is not needed.

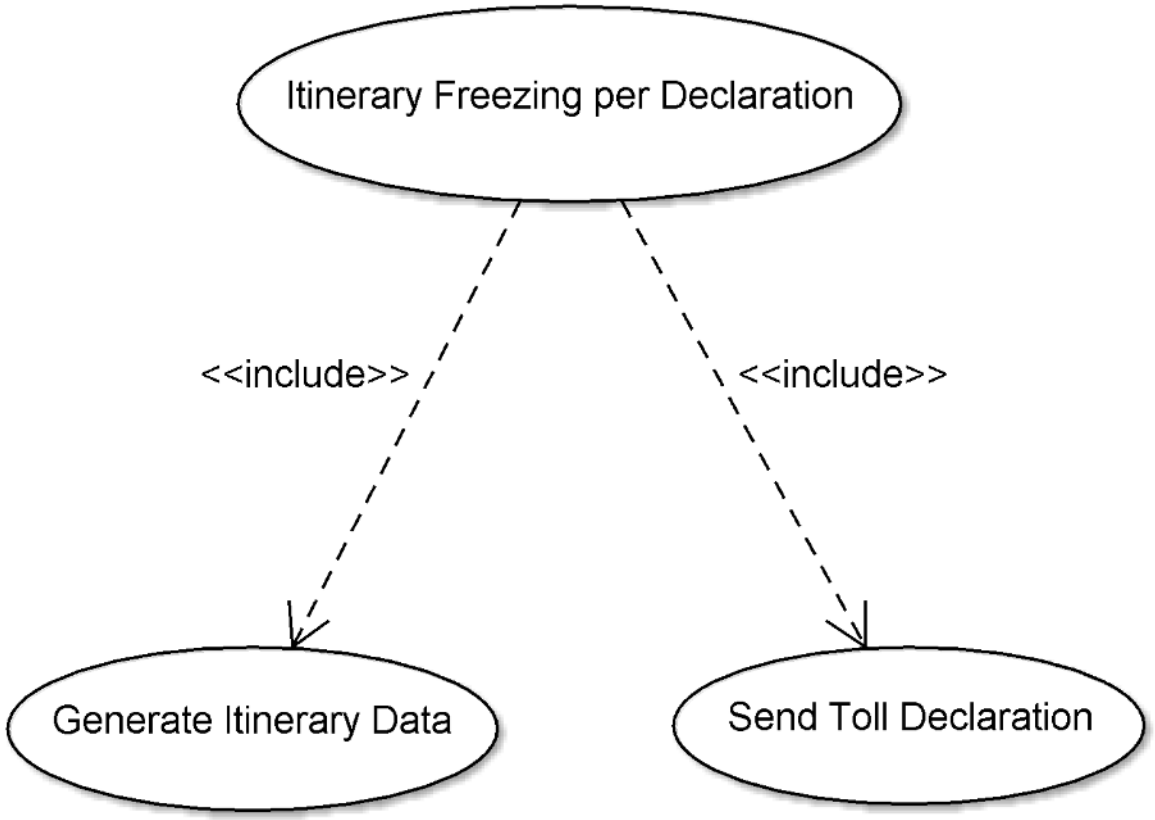

Figure 7 — The sub-processes of Itinerary Freezing per Declaration (UML use case diagram)

In the case of freezing per declaration, the Toll Service Provider shall check the integrity of the itinerary and generally assess its plausibility using time/distance evaluations and detecting holes in the itinerary as described in 5.5.3. The Toll Service Provider shall check the correctness of the Front-End's Charge Report using the itinerary and optionally other available usage data similarly to what is described in 5.5.4.

If all checks are OK the Toll Service Provider shall send a Toll Declaration to the Toll Charger as defined in 6.4.

5.4 Checking of Itinerary Freezing

5.4.1 Introduction

The checking of itinerary freezing process ascertains that the itinerary has been correctly registered and frozen. This is a tool to detect incorrect or incomplete itineraries and gives a basis to check the consistency of the Toll Declaration. Checking of Itinerary Freezing consists of three sub-processes: Observing a vehicle, Retrieving Proof of Itinerary Freezing (PIF) and Checking PIF against Observation.

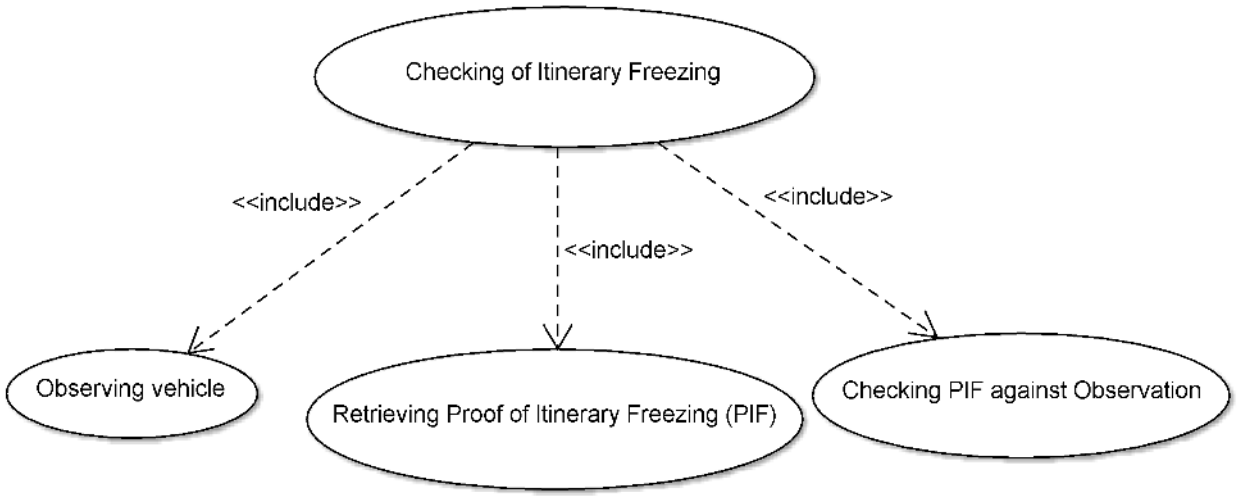

Figure 8 — The sub processes of Checking Itinerary Freezing (UML use case diagram)

5.4.2 Observing a vehicle

This process consists of a roadside observation of a vehicle in a certain location. The observation shall be recorded including Vehicle Registration Mark, time of observation, location and possibly any other dynamic parameters that affect the computation of a Toll Declaration (for example trailer on/off) and one or more images proving the observation.

There are two types of observations: Unexpected and Undetected. An Unexpected observation is not known to the driver or OBE beforehand but might well be after. If the observation is Undetected, its occurrence is neither known before nor after to the driver and OBE.

Undetected observations shall be performed in case of Freezing per declaration with low periodicity (in support of SM_CC-3a). Unexpected or Undetected observations shall be performed in case the itineraries are frozen in real-time using a Trusted Recorder (in support of SM_CC-1 and SM_CC-2) or in case of Freezing per declaration with high periodicity (in support of SM_CC-3b).

NOTE 1 At time of writing, undetected observations are difficult to perform, especially with automatic means. But as technology advances this might become a realistic option.

NOTE 2 An observation can of course also be expected. An example would be a highly visible road side installation which is operating continually and that is well known to many drivers. Since it is expected it does not have the typical properties of a spot check. Such an observation will ensure compliance of a vehicle in moment when it is passing the observing entity but neither before nor after. In practice it is likely that several observing entities will be expected to certain drivers and unexpected to others. Furthermore, even completely expected observations makes compliance checks based on trip logic possible. This however is outside of the scope of this specification.

5.4.3 Retrieving Proof of Itinerary Freezing (PIF)

The retrieving proof of itinerary freezing process has two options: retrieving the proof in real-time from the OBE (in support of SM_CC-1) or with delay from the TSP back end (in support of SM_CC-2 or SM_CC-3a/b).

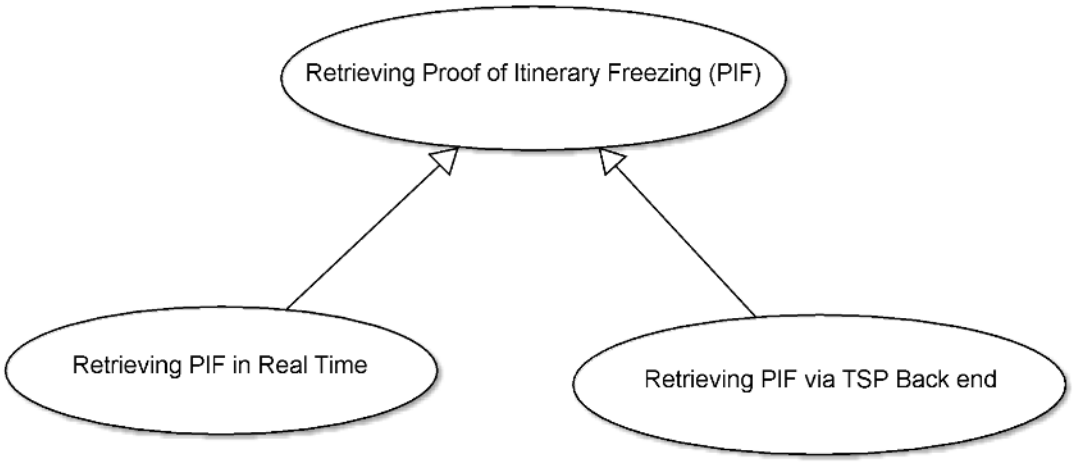

Figure 9 — The sub processes of Retrieving Proof of Itinerary Freezing (UML use case diagram)

In case of retrieving the PIF in real-time, the Toll Charger shall retrieve the last frozen itinerary record directly from the OBE using an RSE initiating a SM_CC transaction compliant to 6.3.

In case of retrieving the PIF with delay, the Toll Charger shall request, within an agreed period of time from an observation, the frozen itinerary (one or more batches) corresponding to such observation to the Toll Service Provider using a Back End Data Checking transaction with indication of the observation compliant to 6.5. In the case that many TSPs offer services in the specific toll domain, the TC has to identify the relevant TSP corresponding to the observed vehicle. If the market shares are equally distributed between the different TSPs the Toll Charger may manage white lists of registered users with a specific Toll Service Provider. Otherwise the Toll Charger may use ad hoc requests using the Retrieve User Details (RetrieveUserDetailsADU) information exchange as specified in EN ISO 12855:2012, 6.14.

NOTE In case the Toll Declaration contains charge data which inherently reveal the vehicle's itinerary, there is no need to retrieve a proof of itinerary freezing, see 5.3.4.

For privacy reasons, the Toll Service Provider shall only provide batches relevant to the observation of the Toll Charger, using a Back End Data Checking transaction compliant to 6.5.

Retrieving PIF via TSP back end implies that observations shall be saved until the back end data can be retrieved. This might be a legal problem in domains where a suspicion of non-compliance is needed in order to store observation data.

The Toll Charger shall check the integrity of the Itinerary Record(s) by checking the Itinerary Record's Authenticator as described in 7.1.2 or 7.1.3.

5.4.4 Checking PIF against Observation

In case SM_CC-1 is supported, the Toll Charger shall check if the itinerary record obtained directly from the OBE corresponds to the local observation on the road.

In order to protect privacy, the check should be done in real-time, preferably directly at the roadside.

In case SM_CC-2 or SM_CC-3a/b implemented, the Toll Charger shall check if a record within the frozen itinerary obtained from the Toll Service Provider corresponds to the registered observation on the road.

NOTE How and in which case sanctions are applied to the Service User and/or Toll Service Provider in case of non-compliance is outside the scope of this Technical Specification.

5.5 Checking of Toll Declaration

5.5.1 Introduction

The Toll Charger may use Checking of Toll Declaration to ensure that the Toll Declaration is plausible with the itinerary. This in turn gives assurance that the presence of a vehicle in a toll domain has been correctly accounted for by the Toll Service Provider in the Toll Declaration.

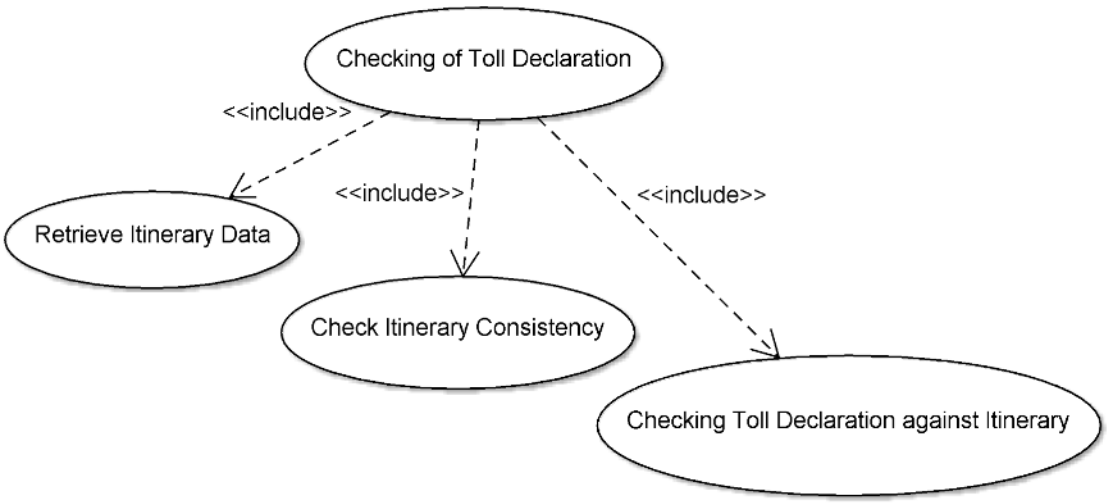

Figure 10 — The sub processes of Checking of Toll Declaration (UML use case diagram)

The Checking of Toll Declaration process consists of three sub-processes; Retrieve Itinerary Data, Check Itinerary Consistency and Checking Toll Declaration against Itinerary.

5.5.2 Retrieve Itinerary Data

The Toll Charger shall request all or a single sub-itinerary pertaining to a previously received Toll Declaration within an agreed period of time using the Back End Data Checking transaction as described in 6.5.

The Toll Service Provider shall respond as described in 6.5.

For privacy reasons, the Toll Service Provider shall check if the number of requests for a certain vehicle in a certain period exceeds a maximum level threshold and deny the request if this is the case. The maximum threshold is to be agreed in advance between the Toll Service Provider and Toll Charger.

NOTE In case of freezing per declaration in combination with the case where the Toll Declaration contains charge data which inherently reveal the vehicle's itinerary, there is no need to retrieve itinerary data, see 5.3.4.

5.5.3 Check Itinerary Consistency

The Toll Charger shall check that the itinerary is plausible by checking:

— the integrity of the single records by checking the correctness of the authenticator as described in 7.1.2 or 7.1.3

— that the records within the same batch are sequential in terms of toll domain counter value, and in terms of end and start position

— that the records in consecutive batches are sequential in terms of counter value, and in terms of end and start position

— the plausibility of the single records using time/distance evaluations

— the plausibility of the overall itinerary using time/distance evaluations.

NOTE In the case that a toll domain counter is used for more than one Toll Domain (e.g. a cluster of domains), records pertaining to the same Toll Domain may not be sequential due to records generated in the other Toll Domains (e.g. a vehicle travelling from country A to C via B and back to A via D, will generate records in A twice, but in between generate records in B, C and D).

If any check produces a negative result, the Toll Charger shall send a claim to the Toll Service Provider (see 5.6).

5.5.4 Checking Toll Declaration against Itinerary

If the complete set of itinerary batches is available, the Toll Charger can check that the aggregated data in the Toll Declaration, referred to as *S* in 6.4.3, correspond to or are plausible with these data.

If only one itinerary batch is available, the Toll Charger can check that it corresponds to or is plausible with the itinerary batch sum (in the itinerary sequence). Furthermore, the Toll Charger can also check that the itinerary batch sums correspond to the Toll Declaration.

If all checks are ok, the Toll Charger shall mark the Toll Declaration as checked incl. timestamp and signature and send it to the processes responsible for generation of Billing Details.

If any check is negative, The Toll Charger shall send a claim to the Toll Service Provider (see 5.6).

NOTE In addition, the checks generate results which also can be used for the calculation of charging metrics agreed between the Toll Service Provider and the Toll Charger in order to assess the charging performance parameter at the level of Toll Declarations. Examples are metrics that measure: a) the correctness or incorrectness of the generation of Toll Declarations as the probability that a Toll Declaration is correctly or incorrectly generated b) the overall level of late Toll Declarations as the proportion of Toll Declarations received by the TC in a defined period between the chargeable event and the receipt of the Toll Declaration against all Toll Declarations that are checked c) the ability of the TSP to correctly detect charge-relevant events to avoid undercharging as the probability that a chargeable event has been properly detected by the TSP d) the ability of the TSP to avoid overcharging as the probability that a chargeable event has been improperly detected by the TSP for vehicles not using the infrastructure. A precondition for this is that the collection of itinerary data outside the chargeable road network is allowed by local privacy laws of the specific toll domain.

5.6 Claiming incorrectness

Claiming incorrectness is one of the supporting processes by which the Toll Charger shall inform the Toll Service Provider that Checking of Itinerary Freezing and/or Checking of Toll Declaration had a negative outcome. If data were missing or incorrect the Toll Service Provider shall send new itinerary data.

Any further handling is outside the scope of this Technical Specification.

Claiming incorrectness shall be carried out in accordance with 6.6.

5.7 Providing EFC Context Data

Providing EFC Context Data are one of the supporting processes. It is based on the EN ISO 12855:2012 as redefined by CEN/TS 16439:2013 but enhanced by this Technical Specification for use by a Toll Charger to specify SM_CC EFC Context Data. SM_CC EFC Context Data are used to specify the format and periodicity of the itinerary records as well as details of the generation of the Itinerary Sequence Hash and the sub itinerary.

Providing EFC Context Data shall be done in accordance with 6.7.

5.8 Key Management

5.8.1 Introduction

In general, key management is the management of trusted objects in an information security system. This includes aspects of the generation, exchange, storage, use, and replacement of keys. In the context of Secure Monitoring, key management deals with the confidentiality and the authorized use of the secure monitoring key(s) so as to guarantee that the security measures provide the needed integrity and non-repudiation characteristics. Key management as described in CEN/TS 16439:2013, Clause 9, applies to all security measures imported from that Technical Specification. For SM_CC, the following additional security targets apply:

— Authenticators (MACs or signatures) for real-time freezing are generated by Trusted Recorders dedicated to OBEs. The Trusted Recorder is assumed to have a high resistance against read access to keys and against manipulation of the cryptographic processes it performs.

— Toll chargers and Toll Service Provider need the possibility to check the correctness of an authenticator generated by a Trusted Recorder without compromising the non-repudiation characteristics of the authenticator.

5.8.2 Requirements

As one option, SM_CC can use a TR-specific secret SM_CC key to calculate the Itinerary Record authenticator using a symmetric cipher in the sense of ISO/IEC 18033-1 and as defined in 7.1.2.

As an alternative option, SM_CC can use a pair of public and private SM_CC keys per TR to calculate the Itinerary Record authenticator using an asymmetric cipher in the sense of ISO/IEC 18033-1 and as defined in 7.1.3.

Two types of security components are relevant to SM_CC:

— The Trusted Recorder is used for Real-time freezing in the OBE (see 5.3.3)

— The SM_CC_Verification SAM is used at the Roadside (see 5.4.3) and the Back End (see 5.3.3) to verify Authenticators calculated using symmetric cryptography (MAC)

The Toll Charger and Toll Service Provider shall implement an appropriate key distribution process that provides trust that the secret and/or private keys are available in plain only inside the Trusted Recorder and in dedicated SAMs at the Toll Charger and Toll Service Provider with at least the same level of protection against disclosure as defined in CEN/TS 16439:2013, 9.2.3.

The definition of requirements to the Trusted Recorder and the SM_CC_Verification SAM are outside the scope of this Technical Specification. Assumptions on properties of each device can be found in 7.3.

NOTE 1 Requirements on the Trusted Recorder and the SM_CC Verification SAM can be found in WI 00278338, Electronic Fee Collection – Secure Monitoring – Trusted Recorder./

NOTE 2 It is conceivable to implement a scheme in which sufficient trust exists that SM_CC MACs can only be produced by an authentic TR. This requires that the TSP has no access to the SM_CC Key. Consequently, as TSP and TCs make use of SM_CC Verification SAMs in which the SM_CC Master Key is stored, it is necessary that this device can only be used for verification but not for generation of SM_CC MACs.

Table 4 below gives an overview of the various keys used in the Secure Monitoring Compliance Checking (SM_CC) context in relation to the options described above.

Table 4 — overview of keys in the SM_CC context

Key usage	In the Front-end	at TSP	at the TC
SM_CC using secret key (symmetric cryptography)	One single TR-specific Secret SM_CC key stored in TR (generation of MAC)	One single Secret SM_CC master key stored in SM_CC_Verification SAM (verification of MAC)	One single Secret SM_CC master key stored in SM_CC_Verification SAM (verification of MAC)
SM_CC using key pair (asymmetric cryptography)	Private SM_CC key stored in TR	Public SM_CC keys (certificates)	Public SM_CC keys (certificates)
Key distribution	Private TR key stored in TR	-	-

6 Transactions

6.1 Introduction

This chapter describes the semantics of the itinerary data, the SM_CC DSRC Transactions and the Toll Service Provider Back End to Toll Charger Back End transactions that support the SM_CC procedures. The full syntax descriptions are provided in Annex A.

All data that are being transmitted between actors shall be encoded according to ISO/IEC 8825-4:2008 (XER) except data sent between OBE and RSE which shall be encoded according to ISO/IEC 8825-2:2008 (PER).

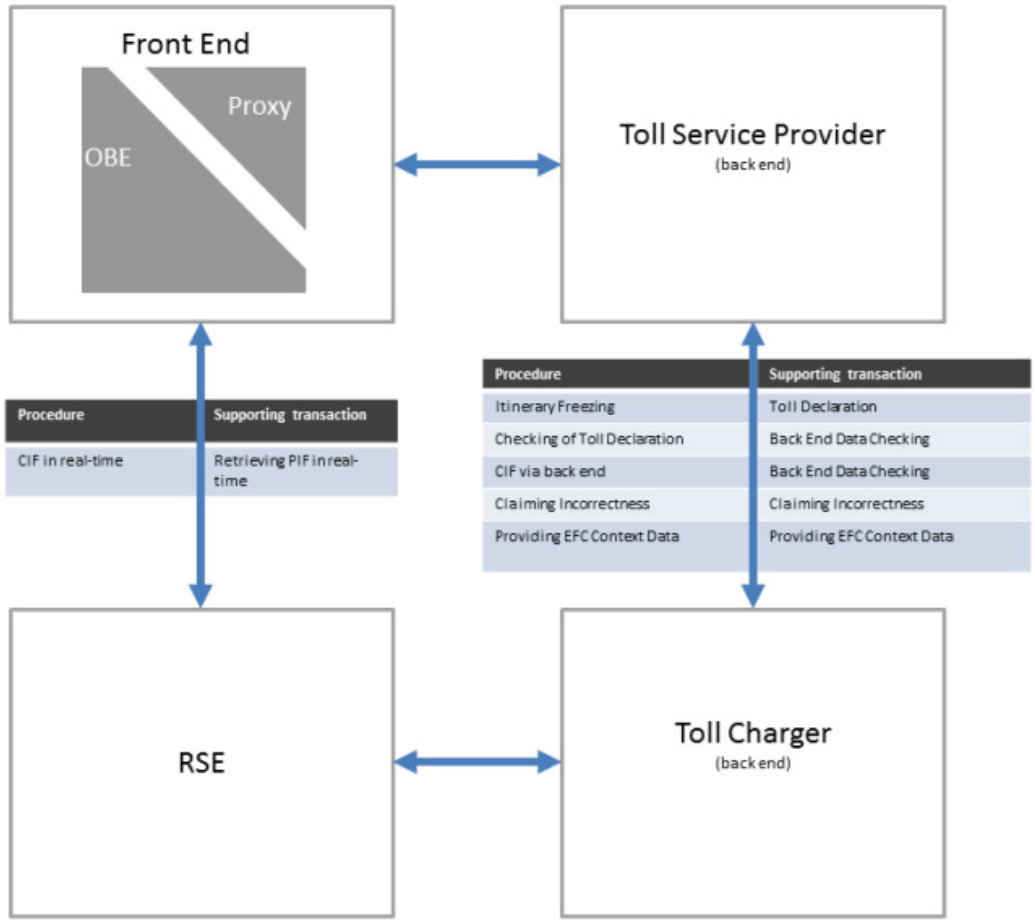

Figure 11 — Overview of relations between procedures and supporting transactions

Table 5 lists the defined transactions for Toll Service Provider and Toll Charger Back End communication (the Front-End / RSE transaction over DSRC is described in 6.3). For each object, the relevant interface messages are listed, together with the limitations, permissions and obligations for each role derived by the rules defined in previous clauses.

The rules are as follows:

— May initiate: An entity is able and allowed to initiate a message exchange

— Shall initiate: An entity is able and has to initiate a message exchange

— Shall be able to receive: An entity shall be able to receive this kind of message

— May respond: An entity is able and allowed to respond to a received Request message

— Shall respond: An entity is able and has to respond to a received Request message.

The supplier of an implementation according to this Technical Specification shall complete the proforma protocol implementation conformance statement as defined in Annex B.

Table 5 — Rules for transactions for the information exchanges between Toll Chargers' and Toll Service Providers' Back Ends

Transaction	Message	Toll Service Provider rules	Toll Charger rules
Toll Declaration (profiled for SM_CC) (see 6.4)	Retrieve specific Toll Declaration(s)	Shall be able to receive	May initiate
	Request	Shall be able to receive	May initiate
	Toll Declaration	Shall initiate, shall respond	Shall be able to receive
	Acknowledge	Shall be able to receive	Shall initiate
Back End Data Checking (specific for SM_CC) (see 6.5)	Retrieve Itinerary Check	Shall be able to receive	Shall initiate
	Itinerary Check	May respond (to retrieve itinerary check)	Shall be able to receive
	Acknowledge	May Initiate, Shall be able to receive	Shall initiate, Shall be able to receive
Claiming incorrectness (specific for SM_CC) (see 6.6)	Send claim	Shall be able to receive	Shall initiate
	Acknowledge	Shall initiate	Shall be able to receive
	Itinerary Check	May respond (to claim)	Shall be able to receive
	Toll Declaration	May respond (to claim)	Shall be able to receive
Providing EFC context data (enhanced for SM_CC) (see 6.7)	Request	May initiate	Shall be able to receive
	EFC context data	Shall be able to receive	May initiate, may respond
	Acknowledge	Shall initiate	Shall be able to receive
	Status	May initiate, shall be able to receive	May initiate, shall be able to receive

The back-office communication shall adhere to the mechanisms defined in EN ISO 12855:2012.

6.2 Description of Itinerary Data

6.2.1 Introduction

The itinerary data shall be structured in an Itinerary Batch for freezing per declaration (FpD) or for real-time freezing (RTF) according to the ASN.1 definitions provided in Annex A. The Itinerary Batch contains a list of charge relevant parameters as well as a list of records which are either in the FpD or the RTF format.

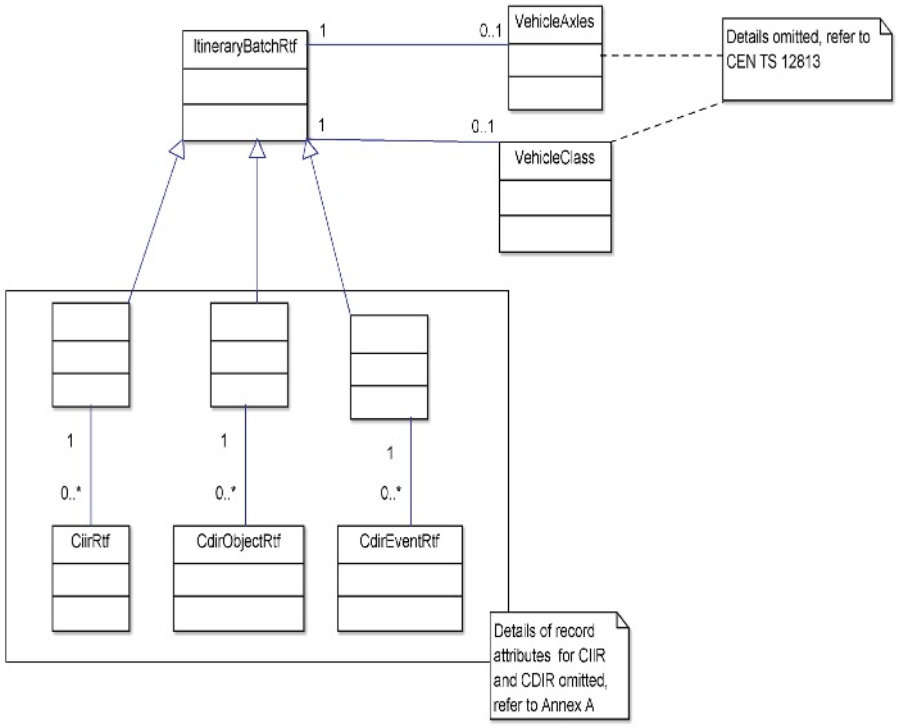

Figure 12 — The information objects of ItineraryBatchRtf (UML class diagram)

ItineraryBatchRtf is structurally identical to ItineraryBatchFpd but contains records frozen in real-time. Anonymous classes in combination with multiple generalisations, solid lines and hollow arrows in Figure 12, are here used to represent the ASN.1 construct CHOICE in combination with SEQUENCE OF.

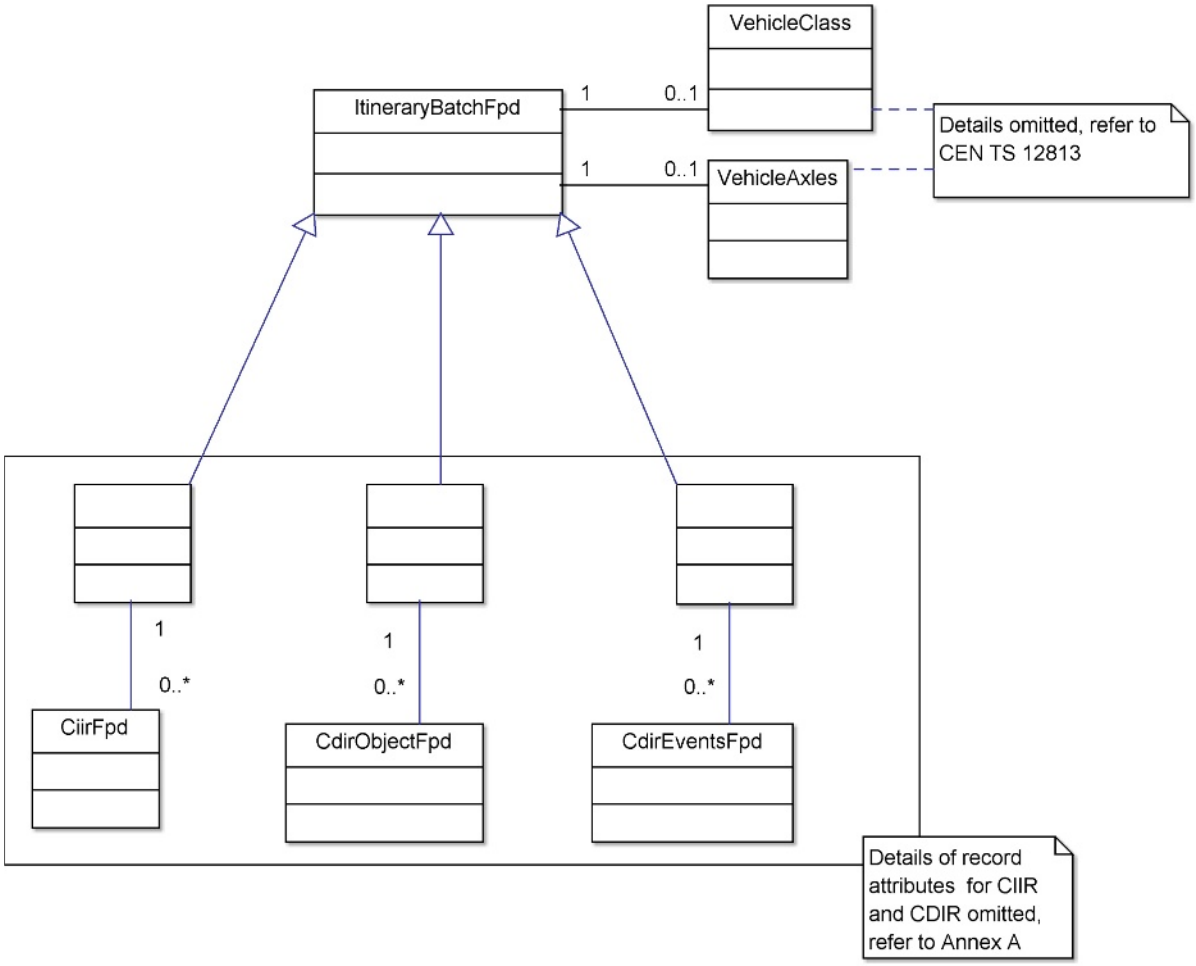

Figure 13 — The information objects of ItineraryBatchFpd (UML class diagram)

ItineraryBatchFpd is structurally identical to ItineraryBatchRtf but contains records frozen per declaration. Anonymous classes in combination with multiple generalisations, solid lines and hollow arrows in Figure 13, are here used to represent the ASN.1 construct CHOICE in combination with SEQUENCE OF.

6.2.2 Itinerary Batch

The semantic definition of the ItineraryBatchRtf and ItineraryBatchFpd is the following:

— The optional data element vehicleClass shall be present if the dynamic parameter it represents is needed for the calculation of the TollDeclarationADU. If present, the data element vehicleClass shall contain vehicle class as specified in CEN ISO/TS 12813:2009, 7.1. If the data element vehicleClass changes, the current itinerary batch shall be finished and a new itinerary batch shall be initiated with the new vehicleClass value specified.

— The optional data element vehicleAxles shall be present if the dynamic parameter it represents is needed for the calculation of the TollDeclarationADU. If present, the data element vehicleAxles shall contain vehicle axles data as specified in CEN ISO/TS 12813:2009, 7.1. If the data element vehicleAxles changes, the current itinerary batch shall be finished and a new itinerary batch shall be initiated with the new vehicleAxles value specified.

NOTE 1 Both vehicleClass and vehicleAxles contains information that is both dynamic over time and potentially charge relevant, hence the possibility to include them in the itinerary batch.

— The data element irs shall contain the list of all records in the batch, in chronological order.

An itinerary batch may contain any number of records.

NOTE 2 A maximum number of records within an itinerary batch, e.g. for privacy reasons, is to be agreed bilaterally between TSP and TC.

6.2.3 Itinerary Record Data Elements

6.2.3.1 Introduction

In case of freezing per declaration the itinerary records shall be of one of the following data types: CiirFpd, CdirObjectFpd. In case of real-time freezing the itinerary records shall be of one of the following data types: CdirEventFpd, CiirRtf, CdirObjectRtf, CdirEventRtf. The syntax shall be according to the ASN.1 definitions provided in Annex A.

6.2.3.2 Common Data Elements for all Itinerary Records

The semantics of the common data elements in the Itinerary Records shall be:

— The data element time shall contain the time and date associated to the end of the record's acquisition in case of SM_CC-3a/b and to the moment of Freezing using the Trusted Recorder in case of SM_CC-1 or SM_CC-2. If no time information shall be stored the data element time shall be filled with zeros.

NOTE As mentioned in the introduction with respect to applicable privacy laws the storage of time stamps for specific toll events might be regulated.

— The data element latitude shall contain the latitudinal coordinate of the last OBE's position, in micro degrees during record acquisition, using the reference model WGS84 as defined in NIMA TR8350.2:2000. The data type is defined and imported from CEN ISO/TS 12813:2009, Annex A.

— The data element longitude shall contain the longitudinal coordinate of the last OBE's position, in micro degrees during record acquisition, using the reference model WGS84 as defined in NIMA TR8350.2:2000. The data type is defined and imported from CEN ISO/TS 12813:2009, Annex A.

— The data element userClassId shall contain the locally defined user class information extracted from the data element tariffClass of CEN ISO/TS 17575-1:2010, 6.5.6. The TSP and TC shall come to a common agreement on a suitable one-to-one (injective) mapping between the definitions of userClassId (with types **INTEGER** in CEN ISO/TS 17575-1:2010 and **INTEGER (0..128)** in Annex A of this document).

In case input data are not available (e.g. technical failure) the data elements shall be filled with zeros.

The periodicity to generate Context Independent itinerary records shall be a fixed value for the entire toll domain, which is valid for all TSPs. In case that no specific value is fixed by the TC the periodicity shall be 30 s by default.

6.2.3.3 Common data elements for Itinerary Records frozen in real-time

The data elements common to all Itinerary Records frozen in real-time have the following semantic definitions

- The data element tollDomainCounters shall contain for each applicable Toll Domain, in the element tollDomainID the id of the Toll Domain in which the record is generated and in the element counter a unique counter which is incremented for each record in that specific Toll Domain. The pair of tollDomainID and counter give a unique identification of the record during the lifetime of the TR within the

context of a specific Toll Domain. Pairs of tollDomainID and counter that are not used shall be filled with zeros.

- The data element authenticator shall contain the Itinerary Record's authenticator which freezes the record after acquisition. The authenticator shall be calculated over the concatenation of the data elements listed in Table 6 as described in 7.1.2, in case symmetric cryptography is applied and as described in 7.1.3 in case asymmetric cryptography is applied.

Table 6 — Data elements used for input for the calculation of the authenticator data element

AttributeID	Attribute	Defined in
	Itinerary record payload (data element of type **IrRtf{CiirSpec}**, **IrRtf{CdirObjectSpec}** or **IrRtf{CdirEventSpec}**	6.2.3
0	CCC-ContextMark	CEN ISO/TS 12813:2009, 7.1
16	VehicleLicencePlateNumber	
17	VehicleClass	
18	VehicleDimensions	
19	VehicleAxles	
20	VehicleWeightLimits	
22	VehicleSpecificCharacteristics	
24	EquipmentOBUId	
32	PaymentMeans	

NOTE A toll domain counter may be also used for more than one Toll Domain (e.g. a cluster of domains) if this has been agreed between the owners of the respective domains. In this case the counter will not be consecutive for usage within one single Toll Domain. This method can be used as a fallback method in case the number of counters supported by the TR has been exhausted.

In case an OBE detects more than four overlapping toll domains the simultaneous use of more than four toll domain counters is possible but cannot be supported for SM_CC_1 due to DSRC frame size constraints. TCs and TSPs should avoid such a situation since it may create a loophole for fraud. Alternatively various countermeasures are possible like a) use the same toll domain counter for multiple toll domains and report the data via DSRC to all TCs or b) allow forwarding of itinerary data of another toll domain if there was a wrong itinerary record sent to the TC over DSRC or c) switch over to another SM_CC option.

6.2.3.4 Common data elements for Context Independent Itinerary Records

The data elements common to Context Independent Itinerary Records (CIIR) have the following semantic definitions:

— The data element of type Distance shall contain the distance driven in the Toll Domain from the record’s position to the preceding record’s position as detected by the OBE according to its technical capabilities.

NOTE Including the time and date associated to the end of the record’s acquisition or the moment of freezing in the data element time in combination of the last OBE’s position in the data elements latitude and longitude allows checking the included distance in the data element distance by comparison with the previous itinerary record.

6.2.3.5 Common data elements for Context Dependent Itinerary Records – Detected Charge Object

The data elements common to Context Dependent Itinerary Records – Detected Charge Object have the following semantic definitions:

— The data element detectedChargeObjectId shall contain the id of the detected charge object as extracted from the data element DetectedChargeObject of CEN ISO/TS 17575-1:2010, 6.5.7.

— The data element timeWhenUsed shall contain the time of detection as extracted from the data element DetectedChargeObject of CEN ISO/TS 17575-1:2010, 6.5.7.

NOTE The EFC Context Data define under which conditions a charge object is to be detected. Consequently the SM_CC process Checking PIF against Observation needs to be tuned to the definition of the EFC Context Data and vice-versa: the process checking PIF against observation needs to assume that the charge object has been detected after usage of a first part of the toll section, so that the observation and the checking of PIF can be performed on the remaining part of the toll section. In this respect, the so called Liability Rules can be used to define the conditions under which the OBE has to detect the usage of the charged object (e.g. the passage of a certain piece of a section or of location points). Alternatively, the toll section can be represented only by its first part and consequently described by the data element minTollPath of CEN ISO/TS 17575-3:2011, 8.3.4.1.2.

6.2.3.6 Common data elements for Context Dependent Itinerary Records – Number of detected Events

The data elements common to Context Dependent Itinerary Record – Number of detected Events have the following semantic definitions:

— The data element of type NumberOfDetectedEvents shall contain the number of events detected from the record's position to the preceding record's for a single tariff class.

6.3 Retrieving PIF in real-time (DSRC Transaction)

6.3.1 Introduction

Checking of itinerary data in real-time shall be performed using an RSE complying with this Technical Specification. The RSE shall retrieve Itinerary Records in the desired format from the OBE using the SM_CC application interface.

6.3.2 Transactional Model

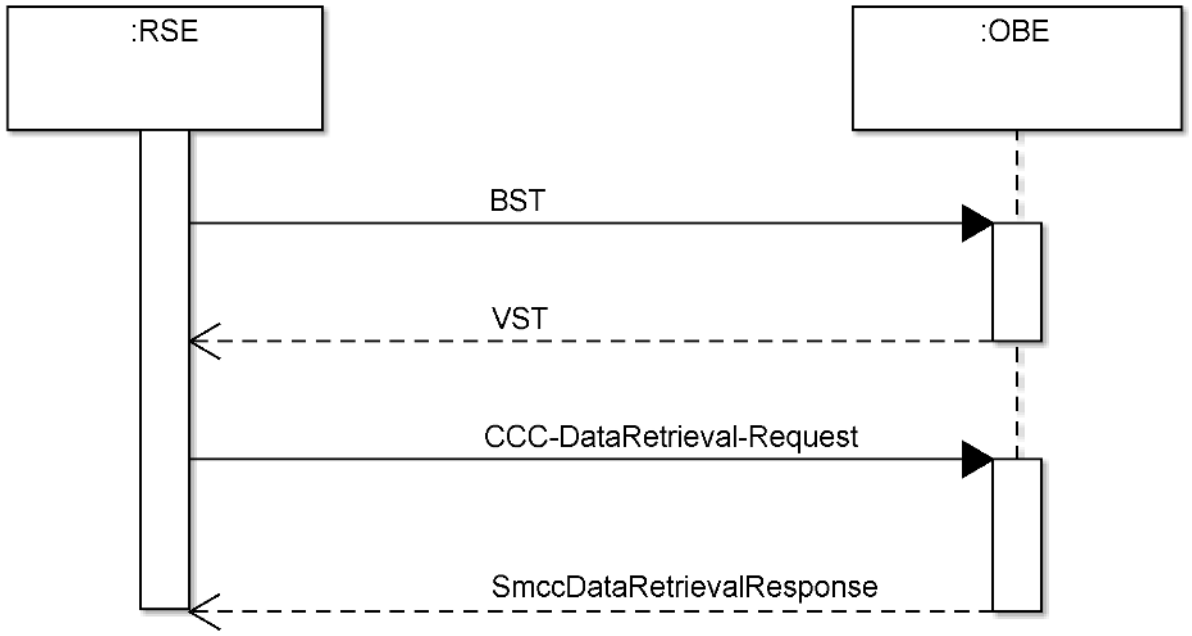

Figure 14 — The messages of Checking of Itinerary Freezing in real-time synchronous transaction (UML sequence diagram)

The SM_CC application interface shall comply with the definition of the CCC application interface defined in CEN ISO/TS 12813:2009, Clause 5, but be amended by replacing the data structure CCC-Data-Retrieval-Response by SmccDataRetrievalResponse as defined in Annex A and by adding the SM_CC attributes of table 8.

The SM_CC transaction shall comply with the transaction Model related to the CCC Application Interface for DSRC defined in CEN ISO/TS 12813:2009, Clause 8.

The SM_CC transaction may be implemented as a separate transaction for SM_CC purposes or as an extension of a CCC transaction for combined CCC and SM_CC purposes.

The messages of Checking of Itinerary Freezing in real-time synchronous transaction are depicted in Figure 14. The VST data element contains the CCC-ContextMark which is used to signal the support of SM_CC and the availability of SM_CC attributes. The function CCC-DataRetrieval-Request (as defined in CEN ISO/TS 12813:2009, 6.1.3) and SmccDataRetrievalResponse (as defined in Annex A) is used to communicate SM_CC relevant attributes.

The Service Provider shall ensure that the value of the CCC-ContextMark corresponds to one unique dated version of this standard through a reference table, which is made available to the Toll Charger, allowing it to identify to which specific version of the SM_CC application interface definition the OBU complies.

6.3.3 Syntax and Semantics

The CCC attributes defined in CEN ISO/TS 12813:2009, Clause 7 shall be available on the OBE.

The attribute TrId shall be made available on OBE side to identify the TR as part of the CCC application (AID = 20). One or more of the other SM_CC attributes defined in this Technical Specification shall be made available in the OBE as part of the CCC application (AID = 20) in accordance to 5.3.3

The CCC-ContextMark shall indicate in its data element TypeOfContract if Secure Monitoring Compliance Checking via DSRC is supported in a Toll Service Provider specific way, and shall indicate which of the SM_CC attributes are present by setting the bit related to the attribute to 1 as indicated below:

Table 7 — CCC-ContextMark structure for SM_CC

CCC-ContextMark (6 octets)					
ContractProvider	TypeOfContract				ContextVersion
3 octets	13 bits	1 bit	1 bit	1 bit	1 octet
According to CEN ISO/TS 12813:2009	Toll Service Provider specific coding	Attribute 71 Present	Attribute 72 Present	Attribute 73 Present	Toll Service Provider specific coding

The SM_CC Attributes represent the Proof of Itinerary Freezing and are defined as follows:

Table 8 — SM_CC Attributes

AttributeID	*Attribute*	*Data Element*	*Length in Octets(for information only)*
70	TrId	-	16
71	CiirRtf	time	4
		tollDomainCounters	4*7
		latitude	4
		longitude	4
		userClassId	1
		distance	2
		authenticator (symmetric /asymmetric)	18/66
72	CdirObjectRtf	time	4
		tollDomainCounters	4*7
		userClassId	1
		detectedChargeObjectId	4
		timeWhenUsed	4
		authenticator (symmetric /asymmetric)	18/66
73	CdirEventsRtf	time	4
		tollDomainCounters	4*7
		latitude	4
		longitude	4
		userClassId	1
		numberOfDetectedEvents	2
		authenticator (symmetric /asymmetric)	18/66

NOTE The number of supported toll domain counters for simultaneous recording is fixed to 4 due to DSRC frame size constraints: 128 octets minus L2 header and L7 header for GET.response = 110 octets.

The SM_CC Attributes shall contain by default the last frozen itinerary record of the applicable type according to 5.3.3. To lower the likelihood of manipulations of itinerary data by the SU close to unexpected observations, the SM_CC attributes alternatively can contain data of a preceding itinerary record. This shall be the case in when a reporting delay has been specified in the EfcContextDataSmccADU as specified in 6.7.3. In case of overlapping toll domains the involved Toll Chargers shall agree on a common reporting delay or accept that any reporting delay specified by any of the involved Toll Chargers is used by the OBE.

The specification of the corresponding data types in ASN.1 is provided in Annex A.

6.3.4 Security

The Data retrieval function shall use access credentials as defined in CEN ISO/TS 12813:2009, 6.2.3, and shall use the CCC access key.

The data element authenticator shall be calculated as described in 7.1.2, in case symmetric cryptography is applied and as described in 7.1.3 in case of asymmetric cryptography.

6.4 Toll Declaration

6.4.1 Introduction

This Technical Specification uses the available definition of the computational object Toll Declaration with specific semantics.

6.4.2 Transactional Model

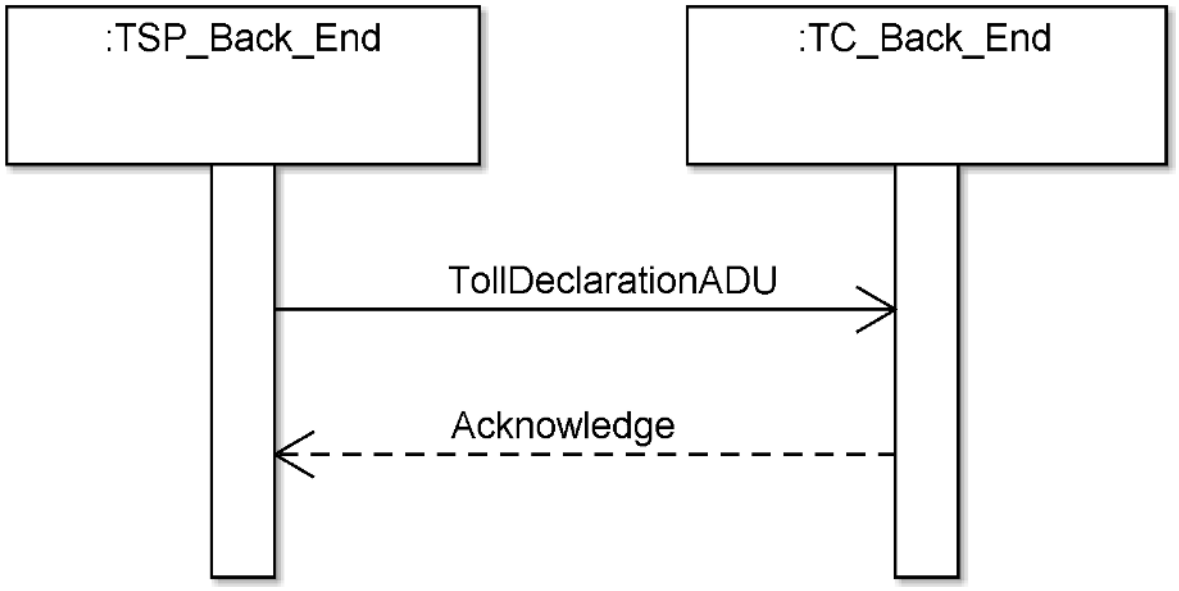

Figure 15 — Typical exchange of messages in the Toll Declaration asynchronous transaction, initiated by TSP (UML sequence diagram)

In case the EfcContextDataSmccADU requires the Toll Declaration to contain charge data which inherently reveal the vehicle's itinerary, the Toll Service Provider shall send a TollDeclarationADU to the Toll Charger according to EN ISO 12855:2012, 6.11, containing one or more Toll Declarations in accordance to the formats

and reporting rules of the EFC scheme as defined by its data element efcContextDataADU. The TollDeclarationADU shall be authenticated by the data element infoExchangeAuthenticator according to CEN/TS 16439:2013 Annex A.

In case the EfcContextDataSmccADU requires the Toll Declaration to contain only aggregated charge data, the Toll Service Provider shall send a TollDeclarationADU to the Toll Charger according to EN ISO 12855, containing one or more Toll Declarations in accordance to the formats and reporting rules of the EFC scheme as defined by its data element efcContextDataADU with further limitations as described in 6.4.3. Also in this case the TollDeclarationADU shall be authenticated by the data element infoExchangeAuthenticator according to CEN/TS 16439:2013 Annex A.

6.4.3 Syntax and semantics

The syntax of the TollDeclarationADU is defined in Annex A.

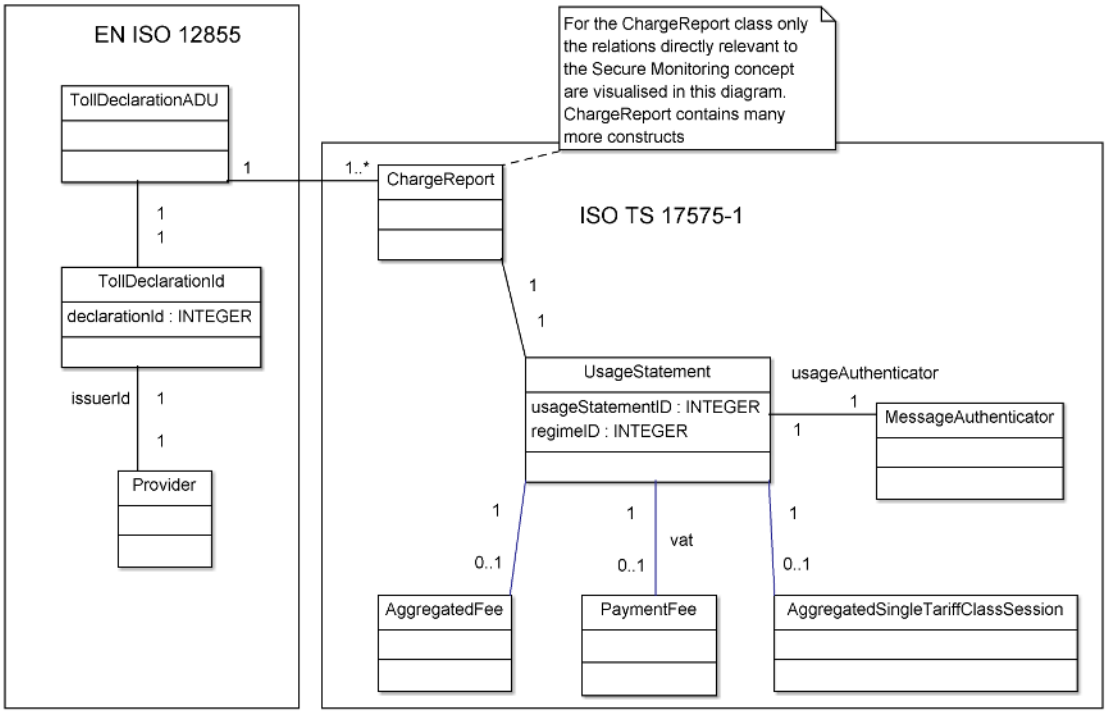

Figure 16 — The information objects of TollDeclarationADU (UML class diagram)

The TollDeclarationADU contains a gnssTolldeclaration which is made up of a sequence of data elements of type ChargeReport. According to this Technical Specification each ChargeReport data element shall only contain one data element of type UsageStatement which shall only contain aggregated data, i.e. it shall only contain the data elements: usageStatementID, regimeId, aggregatedFee, vat, aggregatedSingleTariffClassSession and usageAuthenticator.

The aggregated data aggregatedFee and aggregatedSingleTariffClassSession are in this clause indicated as the sum S: the unit shall be fee, distance, time or number of events as indicated in the extended EFC Context Data.

The usageAuthenticator field within the UsageStatement shall contain the Itinerary Sequence Hash according to what is requested by the Toll Charger in the EfcContextDataSmccADU.

6.4.4 Itinerary Sequence

The Itinerary Sequence Hash (usageAuthenticator) shall be computed as specified in 7.1.1 over an ItinerarySequenceFpd in case of freezing per declaration or over an ItinerarySequenceRtf in case of real-time freezing. Their syntax is defined in Annex A.

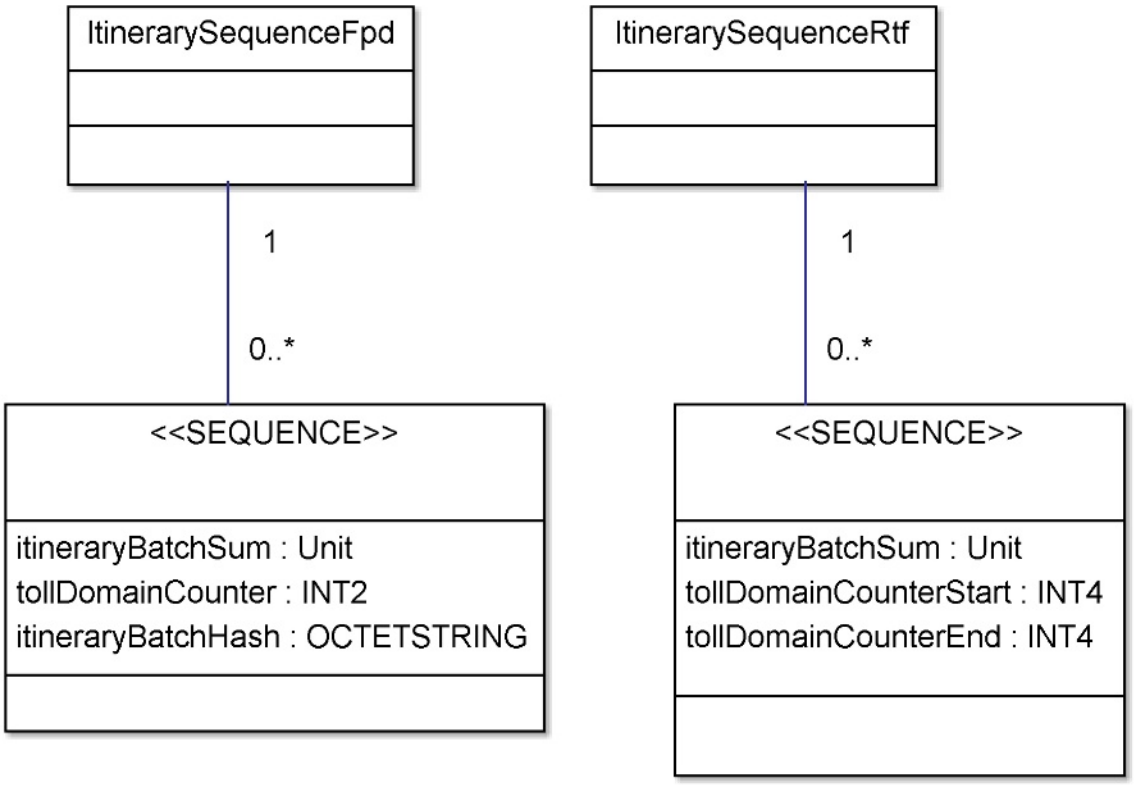

Figure 17 — The information objects of ItinerarySequenceFpD and ItinerarySequenceRtf (UML class diagram)

The itineraryBatchSum shall be the sum of the fee, distance, time or number of events as indicated in the extended EFC Context Data.

The sum for the fee shall be computed over the elements contained in the corresponding instance of ItineraryBatchFpd or ItineraryBatchRtf using the applicable tariff.

The sum for the distance, time or number of events shall be computed over the elements contained in the corresponding instance of ItineraryBatchFpd or ItineraryBatchRtf respectively.

The tollDomainCounter in an ItinerarySequenceFpd shall be an integer that is incremented by one for each recorded instance of ItineraryBatchFpd that is reported in a specific toll domain.

The itineraryBatchHash in an instance of ItinerarySequenceFpd shall be computed over the corresponding instance of ItineraryBatchFpd as specified in 7.1.1.

The underlying instance of ItineraryBatchFpd or ItineraryBatchRtf shall contain the itinerary period of the duration indicated in the extended EFC Context Data within the period covered by the Toll Declaration.

The data elements of ItineraryBatchFpd and ItineraryBatchRtf shall be ordered chronologically with respect to the underlying itinerary batches.

The Itinerary Sequence Hash (usageAuthenticator) ties the Toll Declaration to an Itinerary Sequence. Instances of ItinerarySequenceFpd are tied to the underlying instances of ItineraryBatchFpd by the itineraryBatchHash. In case of real-time freezing, records in instances of ItineraryBatchRtf are hashed one and one by the Trusted Recorder.

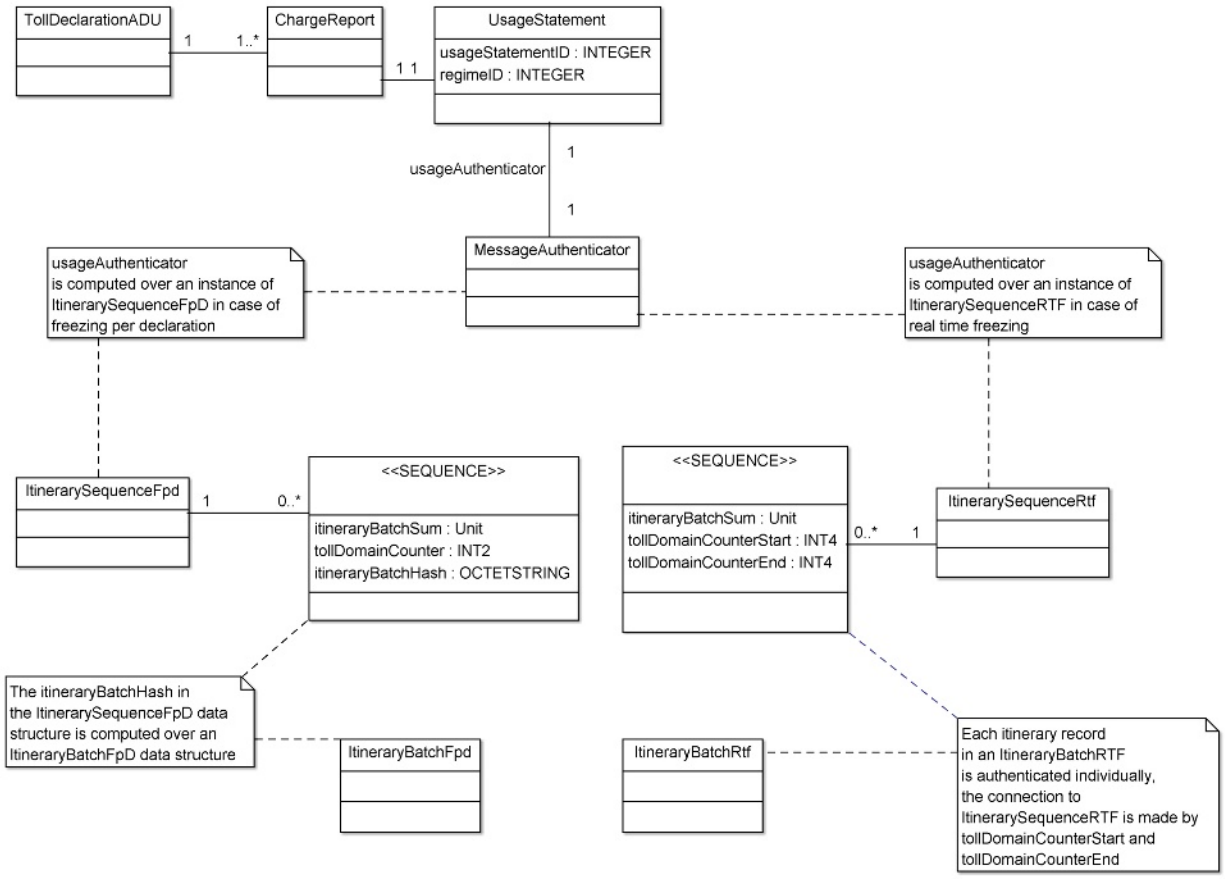

Figure 18 — Overview of how the TollDeclarationADU, the itinerary sequence structures and the itinerary batch structures are connected by hashes and authenticators (UML class diagram)

EXAMPLE 1: Freezing per Declaration, where a fee total is aggregated on an hourly basis. The Toll Declaration covers 24 h and contains an Itinerary Sequence Hash. The Itinerary Sequence Hash commits to a series of 24 hourly sums of fees, toll domain counter values and related Itinerary Batch Hashes. In this example the Itinerary Sequence would look like: ({0, 2351, h_1}; {0, 2352, h_2}; {0, 2353, h_3}; {0, 2354, h_4}; {5, 2355, h_5}; {10, 2356, h_6}; {20, 2357, h_7}; {20, 2358, h_8}; {0, 2359, h_9}; {10, 2360, h_{10}}; {20, 2361, h_{11}}; {10, 2362, h_{12}}; {5, 2363, h_{13}}; {0, 2364, h_{14}}; {0, 2365, h_{15}}; {0, 2366, h_{16}}; {0, 2367, h_{17}}; {0, 2368, h_{18}}; {0, 2369, h_{19}}; {0, 2370, h_{20}}; {0, 2371, h_{21}}; {0, 2372, h_{22}}; {0, 2373, h_{23}}; {0, 2374, h_{24}}). The first element of each triple indicates the total fee for the corresponding hour, the second element the toll domain counter value and the third element the Itinerary Batch Hash over the underlying itinerary data. The total value in the itinerary is therefore 100 Euro.

EXAMPLE 2: Freezing per Declaration. In this example, distances are aggregated on an hourly basis. The Toll Declaration (as above) covers 24 h and contains an Itinerary Sequence Hash. The Itinerary Sequence Hash commits to a series of 24

hourly sums of distances, toll domain counter values and related Itinerary Batch Hashes. In this example the Itinerary Sequence would look like: ({0, 2351, h_1}; {0, 2352, h_2}; {0, 2353, h_3}; {0, 2354, h_4}; {50, 2355, h_5}; {100, 2356, h_6}; {200, 2357, h_7}; {200, 2358, h_8}; {0, 2359, h_9}; {100, 2360, h_{10}}; {200, 2361, h_{11}}; {100, 2362, h_{12}}; {50, 2363, h_{13}}; {0, 2364, h_{14}}; {0, 2365, h_{15}}; {0, 2366, h_{16}}; {0, 2367, h_{17}}; {0, 2368, h_{18}}; {0, 2369, h_{19}}; {0, 2370, h_{20}}; {0, 2371, h_{21}}; {0, 2372, h_{22}}; {0, 2373, h_{23}}; {0, 2374, h_{24}}) The first element of each triple indicates the total distance (in km) for the corresponding hour, the second element the toll domain counter value and the third element the Itinerary Batch Hash over the underlying itinerary data. Assuming a fee of 10 eurocents per km, the total value in the itinerary is therefore again 100 Euro.

EXAMPLE 3: Real-time Freezing. As in the previous example, distances are aggregated on an hourly basis. The Toll Declaration (as above) covers 24 h and contains an Itinerary Sequence Hash. The Itinerary Sequence Hash commits to a series of 24 hourly sums of distances and related ranges of frozen Itinerary Records. In this example the set is: ({0, 0, 0}; {0, 0, 0}; {0, 0, 0}; {0, 0, 0}; {50, 0, 20}; {100, 20, 50}; {200, 50, 131}; {200, 131, 221}; {0, 221, 221}; {100, 221, 305}; {200, 305, 411}; {100, 411, 528}; {50, 528, 603}; {0, 603, 603}; {0, 603, 603}; {0, 603, 603}; {0, 603, 603}; {0, 603, 603}; {0, 603, 603}; {0, 603, 603}; {0, 603, 603}; {0, 603, 603}; {0, 603, 603}; {0, 603, 603}). The first element is the distance (in km) for the corresponding hour, the second element indicates the toll domain counter start value and the third element indicates the toll domain counter end value. As above, the total reported distance is 1000 km, leading to a fee of 100 Euro (assuming again 10 Eurocents per km).

6.4.5 Security

The TollDeclarationADU shall comply with the requirements as specified in 8.6.5 of CEN/TS 16439:2013 (using the InformationExchangeSec mechanism).

6.5 Back End Data Checking

6.5.1 Introduction

This Technical Specification defines messages and a back end data checking transaction in support of Checking of Toll Declaration, as defined in 5.5 and in support of retrieving PIF via TSP back end as defined in 5.4.3.

6.5.2 Transactional model

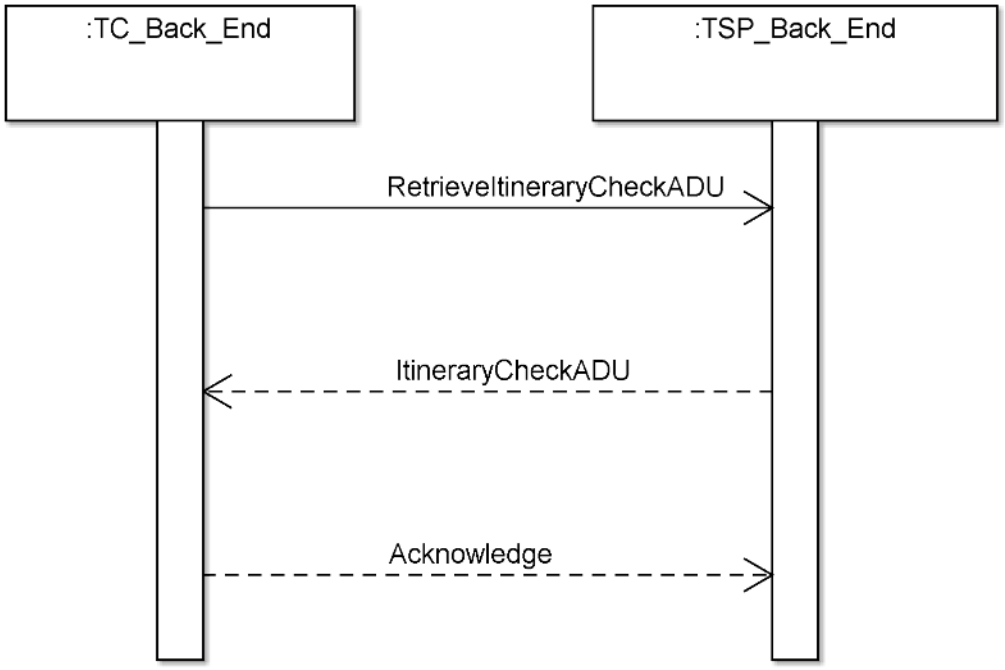

Figure 19 — Typical exchange of messages in the Checking of Toll Declaration asynchronous transaction, initiated by TC (UML sequence diagram)

This Technical Specification extends the EN ISO 12855:2012 interface as redefined by CEN/TS 16439:2013 adding the RetrieveItineraryCheckADU and the ItineraryCheckADU.

The typical exchange of messages is depicted in Figure 19. The diagram does not illustrate the case when the number of RetrieveItineraryCheckADU requests has been exceeded. The transactional model foresees that the Toll Charger shall send a RetrieveItineraryCheckADU to perform:

— the Checking of Itinerary Freezing process. In this case a relevant observation can be specified using the space-time coordinates of the observation;

— a Checking of Toll Declaration process. In this case only a relevant Toll Declaration identity needs to be specified.

The RetrieveItineraryCheckADU can be used to request:

— the upper level of the itinerary, i.e. an instance of the ItinerarySequenceFpd or ItinerarySequenceRtf to perform Checking of Toll Declaration;

— the lower level of the itinerary, i.e. instances of ItineraryBatchFpd or ItineraryBatchRtf to perform Checking of Itinerary Freezing;

— upper and lower level together to do both Checking of Itinerary Freezing and Checking of Toll Declaration.

The Toll Service Provider shall monitor the frequency of RetrieveItineraryCheckADU for a specific vehicle in a defined period and respond with an AckADU according to EN ISO 12855:2012, 6.4 with the corresponding aDUReasonCode set to 8 if a threshold, to be agreed with the Toll Charger, is exceeded.

NOTE The request threshold feature has been included with implementation of privacy regulations in mind.

In other cases the Toll Service Provider shall answer to each RetrieveItineraryCheckADU with an ItineraryCheckADU asynchronously.

The ItineraryCheckADU shall contain the information as specified in the request (upper, lower or both) for:

— the instance of an Itinerary Sequence in which a specified observation is contained (upper level);

— the Itinerary Batch with the specified toll domain counter value (in case of freezing per declaration) or range of toll domain counter values (in the case of real-time freezing) as requested (lower level);

— all Itinerary Batches in an Itinerary Sequence (upper and lower level).

If the Itinerary Sequence Hash is not supported, the ItineraryCheckADU on upper level shall be sent empty.

6.5.3 Checks of the Itinerary

On reception of an instance of the ItineraryCheckADU which includes upper level the Toll Charger can check:

— that the value of aggregatedFee or aggregatedSingleTariffClassSession respectively that is contained in the Toll Declaration is the sum of the itineraryBatchSums (fee, distance, time or number of events) in the underlying instance of ItinerarySequenceFpd or ItinerarySequenceRtf respectively;

— that the Itinerary Sequence Hash (usageAuthenticator) commits to the corresponding instance of ItinerarySequenceFpd or ItinerarySequenceRtf respectively;

— for freezing per declaration, that the tollDomainCounter values in the ItinerarySequenceFpd are consecutive;

— for real-time freezing, that the tollDomainCounterEnd value and the tollDomainCounterStart value in two consecutive instances of ItinerarySequenceRtf (if available) are consecutive.

On reception of an instance of the ItineraryCheckADU which includes lower level the Toll Charger can check:

— for real-time freezing, that the start tollDomainCounter values are consecutive;

— for real-time freezing, that the authenticator of each individual itinerary record corresponds to the payload as specified in 7.1.2 or 7.1.3 respectively;

— that a real world observation of the corresponding vehicle is correctly accounted for in the corresponding instance of ItineraryBatchFpd or ItineraryBatchRtf respectively.

On reception of an instance of the ItineraryCheckADU which includes lower and upper level the Toll Charger can perform the checks prescribed for receiving only the upper level data as well as for only the lower level data, and can in addition check:

— for freezing per declaration that the hash computed over the received ItineraryBatch produces the same value as the corresponding itineraryBatchHash value;

— check the plausibility of the itineraryBatchSum against the corresponding instance of ItineraryBatchFpd or ItineraryBatchRtf respectively.

The checks performed by the Toll Charger are also specified in 5.5.3 and 5.5.4.

If any check proves non-compliance, the Toll Charger shall send an SmccClaimADU.

6.5.4 Syntax and semantics

The syntax of the RetrieveItineraryCheckADU is defined in Annex A.

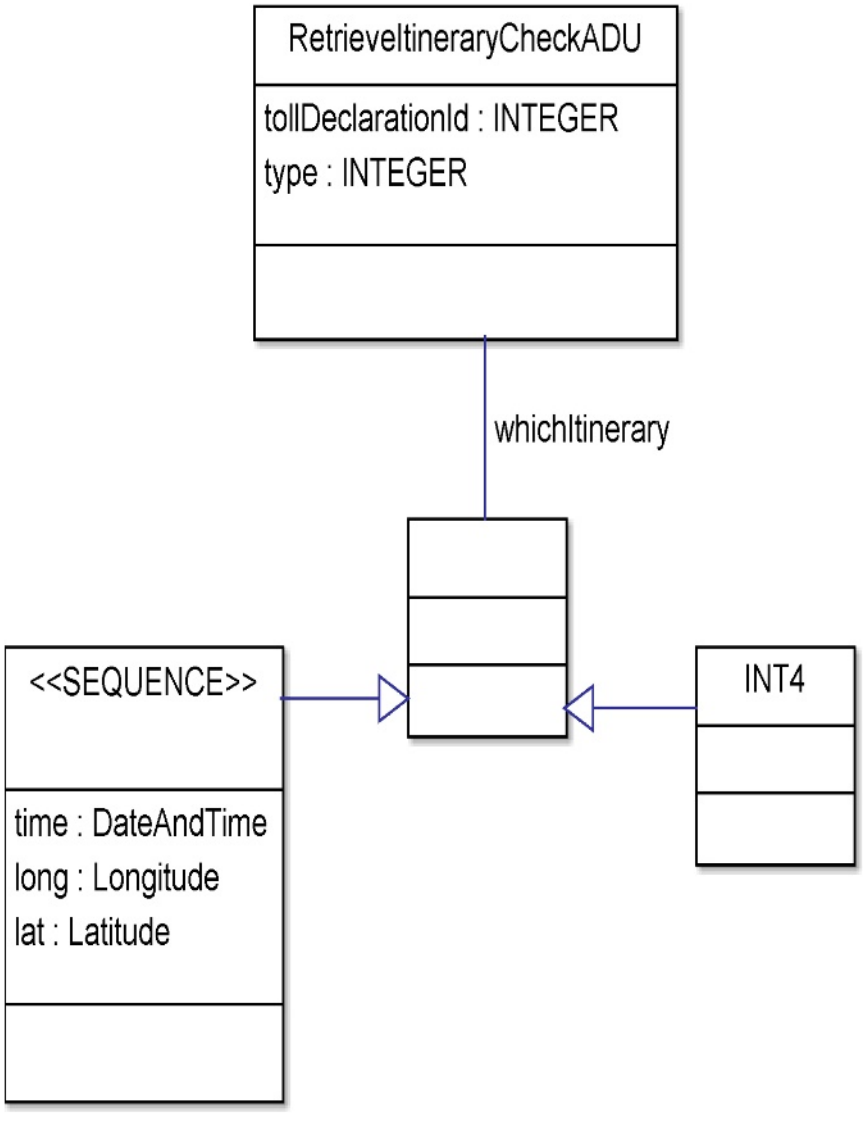

Figure 20 — The information objects of RetrieveItineraryCheckADU (UML class diagram). Generalization (hollow arrow) used to represent the ASN.1 construct CHOICE (observation or tollDomainCounter)

The tollDeclarationId field shall indicate the ID of the Toll Declaration for which the itinerary is requested.

The tollDeclarationId field shall be optional in case of lower level checking.

The tollDeclarationId field shall be mandatory in case of upper level checking and in case the tollDomainCounter in the RetrieveItineraryCheckADU is set to 0 (see below).The tollDeclarationId field shall be mandatory in case of upper level checking or checking of both levels.

The type field shall indicate the request type, indicating on which level checking is requested where 0 shall mean lower, 1 shall mean upper and 2 shall mean both levels.

The part of the itinerary that is requested is specified either by specifying an observation or by specifying an interval of toll domain counter values.

The data element observation shall indicate the time, longitude and latitude (using the reference model WGS84 as defined in NIMA TR8350.2:2000) of the observation for which the Toll Declaration is checked, i.e. the time interval of the requested itinerary batch (in case of lower level) or itinerary sequence (in case of upper level).

The tollDomainCounter field in the RetrieveItineraryCheckADU shall indicate the toll domain counter value that the time interval of the requested itinerary batch (in case of lower level) or itinerary sequence (in case of upper level) covers. In case it is set to 0 all itinerary batches (in case of lower level) or itinerary sequences (in case of upper level) of the corresponding Toll Declaration (as specified by the tollDeclarationId) is requested.

The syntax of the ItineraryCheckADU is defined in Annex A.

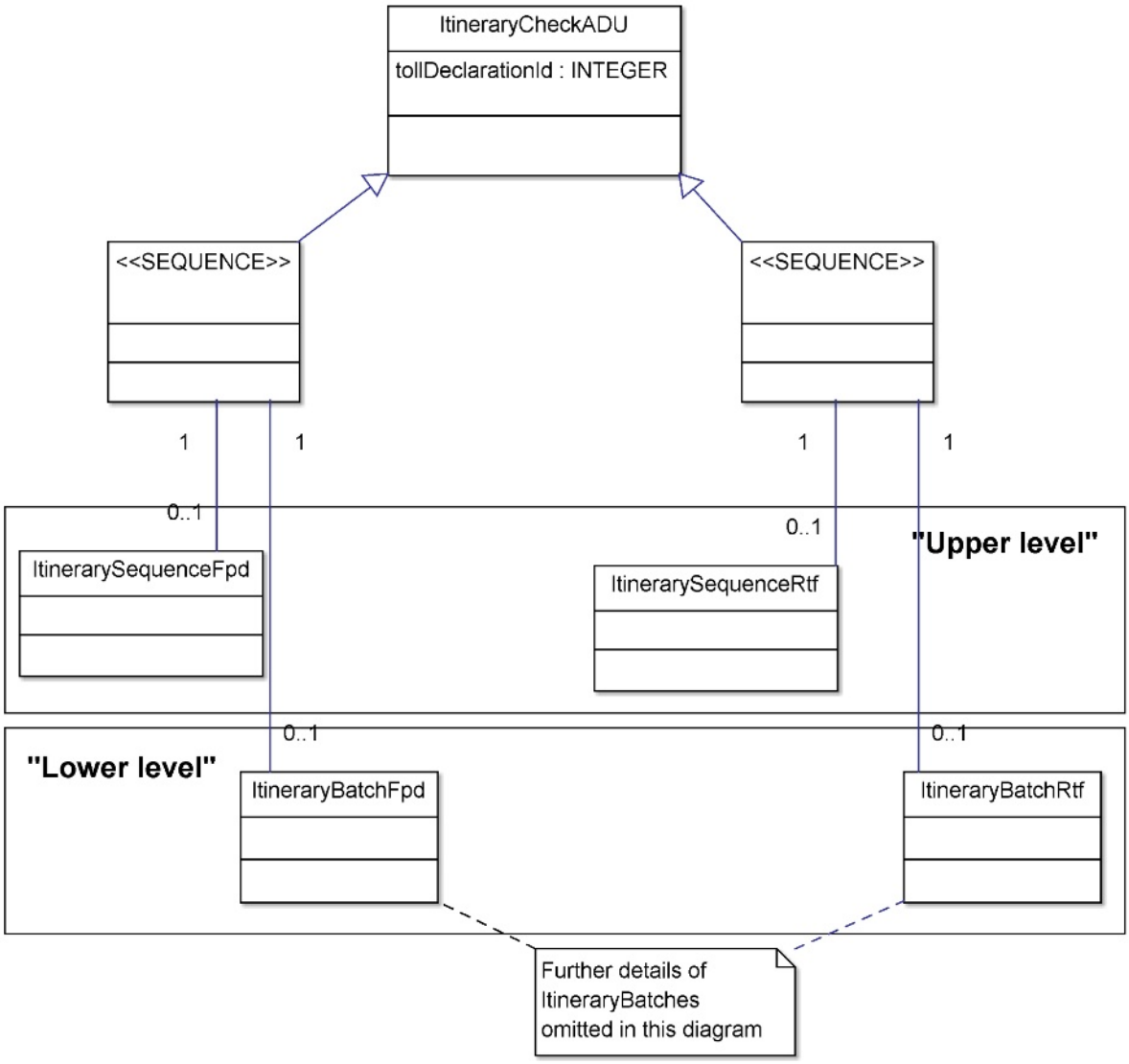

Figure 21 — The information objects of ItineraryCheckADU (UML class diagram)

The tollDeclarationId field shall indicate the ID of the Toll Declaration for which the itinerary is provided and correspond to the tollDeclarationId field in the RetrieveItineraryCheckADU.

The checkData field shall be chosen as checkDataFpd in the case of freezing per declaration and as checkDataRtf in the case of real-time freezing.

The data elements itinerarySequenceFpd, itineraryBatchFpd, itinerarySequenceRtf and itineraryBatchRtf shall be present as specified in Table 9 below.

Table 9 — Present data fields in an instance of ItineraryCheckingADU

	Freezing per declaration	Real-time freezing
Upper level	itinerarySequenceFpd	itinerarySequenceRtf
Lower level	itineraryBatchFpd	itineraryBatchRtf
Both levels	itinerarySequenceFpd and itineraryBatchFpd	itinerarySequenceRtf and itineraryBatchRtf

The values of those of the itinerarySequenceFpd, itineraryBatchFpd, itinerarySequenceRtf and itineraryBatchRtf data fields that are present shall correspond to those requested in the triggering RetrieveItineraryDataADU request as described above.

6.5.5 Security

The RetrieveItineraryCheckADU and the ItineraryCheckADU shall comply with the TC to TSP Profile A of CEN/TS 16439:2013, 6.3.4.

This means that the RetrieveItineraryCheckADU and the ItineraryCheckADU shall comply with the appropriate security specifications for TSP to TC interface of CEN/TS 16439:2013, 8.6.3: message authentication.

6.6 Claiming incorrectness

6.6.1 Introduction

This Technical Specification defines messages and a transaction to send claims to the Toll Service Provider. The Toll Charger shall use the SmccClaimADU to report any kind of inconsistency detected in relation to SM_CC.

6.6.2 Transactional model

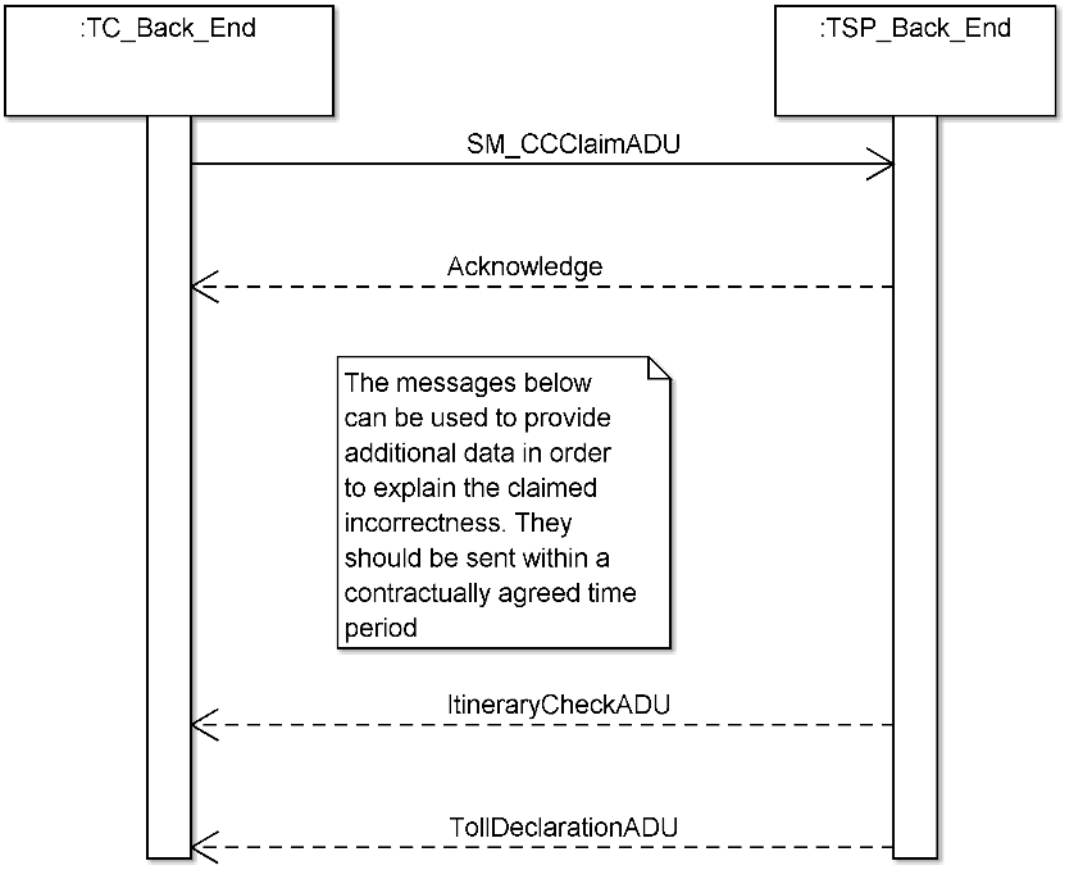

Figure 22 — Exchange of messages in the Claiming Incorrectness asynchronous transaction (UML sequence diagram)

This Technical Specification extends the EN ISO 12855:2012 interface as redefined by CEN/TS 16439:2013 by adding the SmccClaimADU.

The Toll Charger shall use the SmccClaimADU to send an SM_CC Claim if inconsistencies or errors are detected in the proof of itinerary freezing or in the Toll Declaration.

The Toll Service Provider shall use the ItineraryCheckADU to send any additional or corrected itinerary to the Toll Charger using the same TollDeclarationId as referred to in SmccClaimADU.

The Toll Service Provider shall use the TollDeclarationADU to send any additional Toll Declarations using a new TollDeclarationId or any corrected Toll Declarations using the same TollDeclarationId to the Toll Charger.

NOTE Any further handling of agreements, disagreement and penalties between Toll Charger and Toll Service Provider is outside the scope of this Technical Specification.

The Toll Charger shall send SmccClaimADU to update the status of the claim at any time (e.g. closure after agreement).

6.6.3 Syntax and semantics

The syntax of the SmccClaimADU is defined in Annex A.

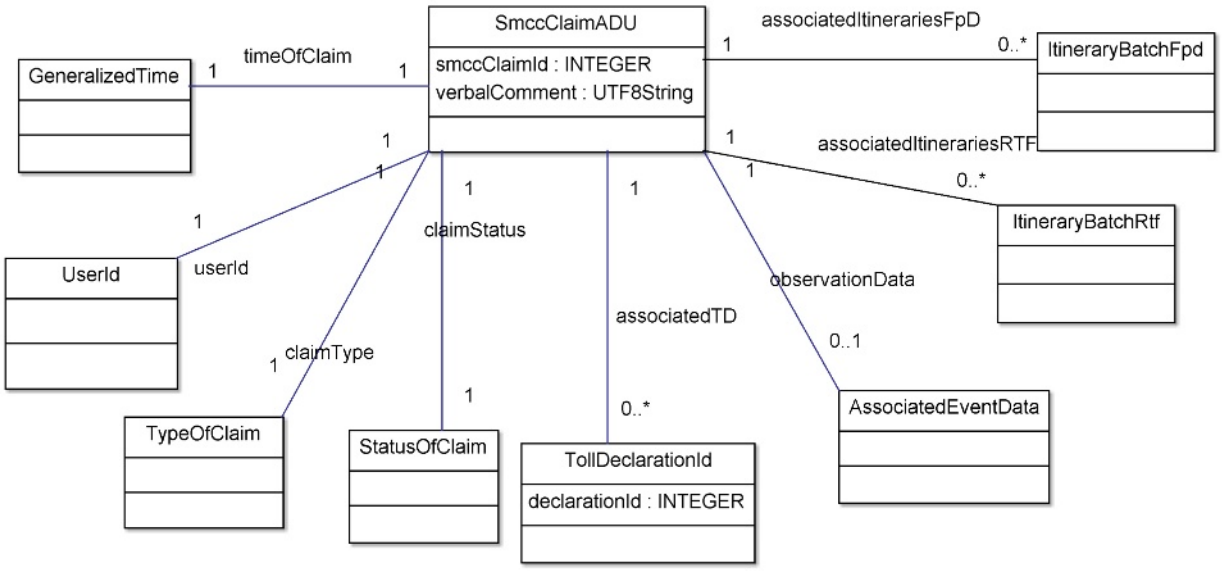

Figure 23 — The information objects of SmccClaimADU (UML class diagram)

The smccClaimId field shall contain the unique (within the originating entity) identifier for the SM_CC Claim.

The timeOfClaim field shall indicate the original generation time of the claim.

The userId shall indicate the identification of the related user/vehicle.

The typeOfClaim field shall indicate if the claim relates to an inconsistency with the Real-time CIF, the delayed CIF or Checking of Toll Declaration.

The statusOfClaim field shall indicate the status of the claim throughout its lifetime as maintained by the Toll Charger.

The associatedTd field shall be used to indicate the associated Toll Declaration in case the incorrectness relates to the Checking of Toll Declaration.

The associatedItinerariesRtf and associatedItinerariesFpd fields shall be used to send the Itinerary Batches which have been found to be incorrect in case of Checking of Itinerary Freezing.

The field observationData may be used to send the observation data which have been collected by the Toll Charger in case of CIF.

The field verbalComment may be used to indicate any relevant information which cannot be coded in the fields above.

6.6.4 Security

The SmccClaimADU shall comply with the TC to TSP Profile B of CEN/TS 16439:2013, 6.3.4 in order to avoid any repudiation attacks in case the claim leads to further procedures outside the scope of this Technical Specification such as claims to court.

This means that the SmccClaimADU shall comply with the appropriate security specifications for TSP to TC interface of CEN/TS 16439:2013, 6.3.4: message authentication incl. proof of origin and proof of delivery.

6.7 Providing EFC Context Data

6.7.1 Introduction

This Technical Specification extends the EN ISO 12855:2012 as redefined by CEN/TS 16439:2013 by adding the EfcContextDataSmccADU.

The Toll Service Provider and Toll Charger shall use the EfcContextDataSmccADU message defined in Annex A for the computational object “Originating and providing EFC context data” defined in EN ISO 12855.

6.7.2 Transactional Model

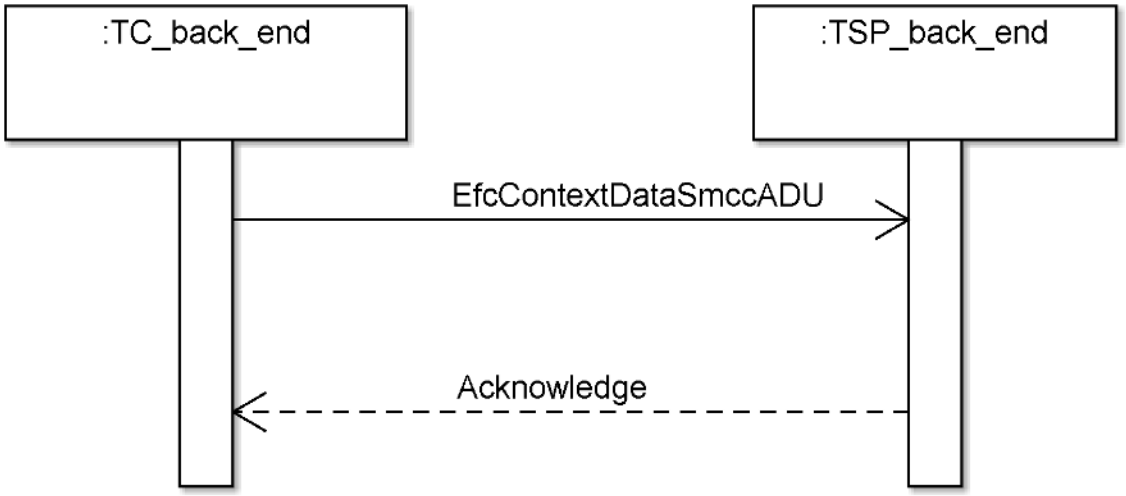

Figure 24 — Typical exchange of messages in the Originating and Providing EFC Context Data (initiated by TC) asynchronous transaction (UML sequence diagram)

The Toll Charger shall send the EfcContextDataSmccADU message defined in Annex A in order to request the desired SM_CC functionality.

The Toll Charger may send the EFCContextDataADU according to EN ISO 12855:2012, 6.7 in order to signal that SM_CC does not need to be supported.

The Toll Service Provider shall acknowledge the message.

6.7.3 Syntax and semantics

The syntax of the EfcContextDataSmccADU is defined in Annex A.

The EFCContextDataADU field shall contain the original EFC Context Data of the autonomous Toll Domain according to EN ISO 12855:2012 (which in turn refers to CEN ISO/TS 17575-3:2011).

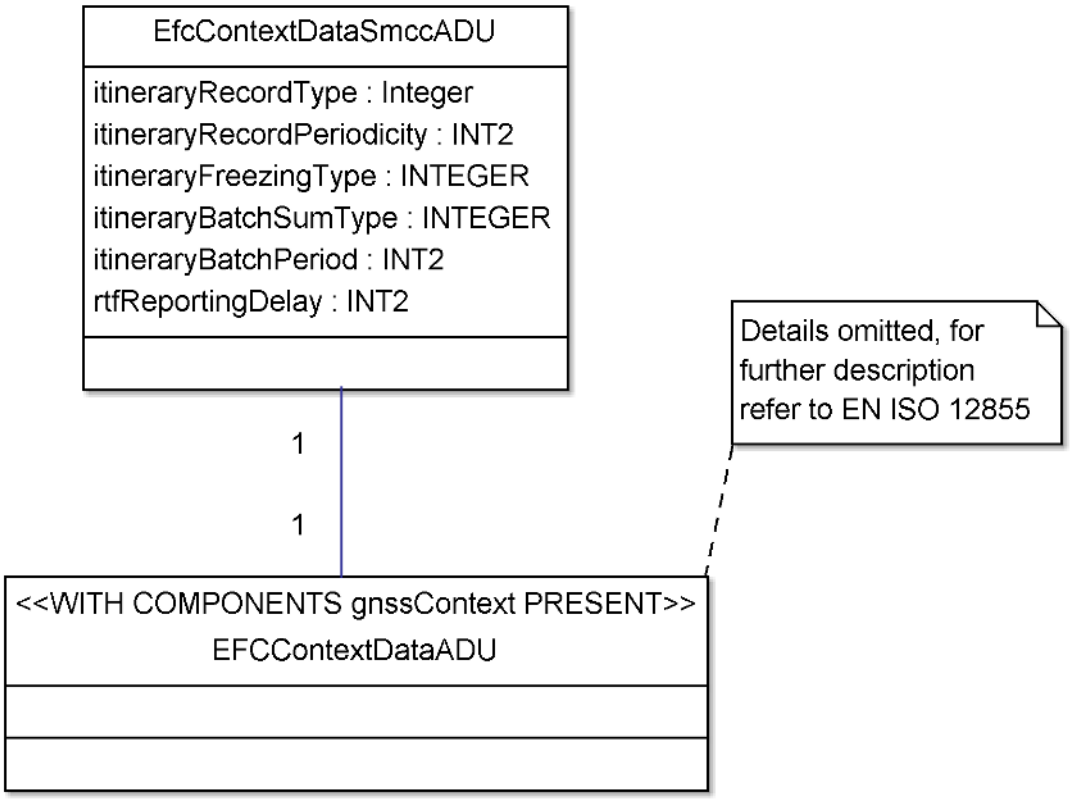

Figure 25 — The information objects of EfcContextDataSmccADU (UML class diagram)

The itineraryRecordType field shall specify the desired format of the Itinerary Record as described in 5.3.2 (if supported) in accordance with the technical possibilities offered by the Toll Service Provider.

The itineraryRecordPeriodicity field shall specify the maximum periodicity of the generation of the Itinerary Records in seconds. Toll Chargers shall accept generation periodicities that are lower than the one specified (i.e. higher frequency sampling).

The itineraryFreezingType field shall indicate if freezing shall be done:

— in real-time with a trusted recorder

— in real-time with a trusted recorder with a trusted time source

— per declaration

The itineraryBatchSumType field shall specify the desired unit of the data element itineraryBatchSum for Toll Declarations as defined in 6.4.4.

The itineraryBatchPeriod field shall specify the desired duration of the period associated to the itinerary Batches as defined in 6.4.4 in minutes

The rtfReportingDelay shall specify the desired delay in seconds between real-time freezing of a record and it being made available for read out on the DSRC interface (see 6.3 for rationale).

6.7.4 Security

The EfcContextDataSmccADU shall comply with the same requirements as specified by CEN/TS 16439:2013 for the EFCContextDataADU.

7 Security

7.1 Security functions and elements

7.1.1 Hash functions

SHA-256 as defined in FIPS PUB 180-4 shall be used as a hashing algorithm for itinerary freezing when computing the data elements usageAuthenticator (in the UsageStatement datastructure) and itineraryBatchHash (in the ItinerarySequenceFpd data structure).

7.1.2 MAC

In case symmetric authentication is used for real-time freezing, the **authenticator** data element of the itinerary record shall be calculated over data defined in 6.2.3.3 encoded according to ISO/IEC 8825-2:2008 (PER) using the CMAC according to ISO/IEC 9797-1:2011. MAC algorithm 5 shall be applied. The underlying block cipher shall be AES-128 specified in ISO/IEC 18033-3:2010. The key applied shall be the TR-specific secret SM_CC key.

NOTE The TollDeclarationADU is authenticated according to CEN/TS 16439:2013.

7.1.3 Digital signatures

In case asymmetric authentication is used for real-time freezing, the **authenticator** data element of the itinerary record shall be calculated over data defined in 6.2.3.3 encoded according to ISO/IEC 8825-2:2008 (PER) using ECDSA in accordance with FIPS PUB 186-3: 2009, Clause 6, with a key length n equal to 256 bits and using the curve P-256 as specified in appendix D.1.2.3. Input data shall be hashed in accordance with 7.1.1. The key applied shall be the TR-specific private SM_CC key.

NOTE The TollDeclarationADU is authenticated according to CEN/TS 16439:2013.

7.1.4 Public Keys, Certificates and CRL

The data element TrId in combination with the data element KeyRef shall be used to uniquely identify the public key associated with the TR-specific private SM_CC key used for the calculation of the signature generated by the Trusted Recorder.

The TR public key certificates according to ISO/IEC 9594-8, certificates version 3, and the CRL according to CRL version 2 shall comply with the profiles defined in IETF RFC 5280. A compliant implementation to this specification, to import and use the certificates and CRLs shall at least support all possible critical certificate and CRL extensions as defined in IETF RFC 5280 profile.

The public key certificates shall contain the following extensions:

— Basic Constraints;

— Key Usage;

— Certificate Owner shall contain the identification of the TrId concatenated with the Key_Ref

Other extensions may be present but marked as non-critical.

The certificate shall be encoded according to the distinguished encoding rules (DER) as defined in ISO/IEC 8825-1 and thereafter be Base64 encoded (as defined in IETF RFC 4648) and enclosed by „—– BEGIN CERTIFICATE—–“ and „—–END CERTIFICATE—–“, i.e. the PEM (privacy enhanced mail) certificate format.

The CRL shall be DER encoded as defined in ISO/IEC 8825-1 and thereafter be Base64 encoded (as defined in IETF RFC 4648) and enclosed by „—–BEGIN X.509 CRL—–“ and „—–END X.509 CRL—–“, i.e. the PEM CRL format.

The certificate and the CRL shall have a fingerprint in hexadecimal format based on the algorithms defined in CEN/TS 16439:2013, 8.1.2.

7.2 Key Management

7.2.1 Key Exchange between Stakeholders

In case asymmetric authentication is used for the itinerary records and the SM_CC attributes, the Toll Service Provider shall distribute the TR SM_CC public key certificates to the Toll Charger. The exchange of TR or SAM public key certificates and CRL (if used) shall be according to the public key transport mechanism 3 defined in ISO/IEC 11770-3:2008, 12.2.1. The receiver shall check the integrity and authenticity of the certificates and CRL (if used), and reply to the sender in case of problems. The implementation of mechanisms to verify the validity of certificates shall be in accordance with CEN/TS 16439:2013.

NOTE 1 CEN/TS 16439:2013 provides two options: a hierarchical trust model with a TTP acting as CA, as well as a peer-to-peer trust model. It is noted that a hierarchical trust model is preferred, but a peer-to-peer model is easier to realise and can be adequate in schemes with a limited number of entities.

NOTE 2 The TC may decide to only store public keys and associated TrIds and KeyRef at the RSE. Complete certificates are not required to check signatures received from the OBE.

In case symmetric authentication is used, the Toll Charger shall distribute the SM_CC Verification SAM public key certificates to the Toll Service Provider. The TSP shall only use the SM_CC Verification SAM public key after successful validation of SM_CC Verification SAM public key certificate. The following validations shall be performed:

— The signature of the certificate is correct

— The time of public key use is within the certificate time validity period

— The certificate is not on the CRL

— The certificate owner ID is unambiguously belonging to a SM_CC Verification SAM

The Toll Service Provider shall transfer the secret SM_CC Master key to the Toll Charger using the TrustObjectADU according to CEN/TS 16439:2013, 9.3.2, using KeyType = 8. Encryption shall be done using the public key of the SM_CC Verification SAM.

7.2.2 Key generation and certification

The TR-specific 16 octet secret SM_CC key shall be derived from the 32 octet Master SM_CC Key in the following way: The derived key shall be obtained encrypting the TrId with the SM_CC Master Key using AES-256 as specified in ISO/IEC 18033-3:2010, 5.2.

Public Key certificates shall clearly identify that the public key belongs to a specific TR or SM_CC Verification SAM.

7.3 Trusted Recorder and SM_CC Verification SAM characteristics

7.3.1 Introduction

Some of the options of SM_CC require the use of a Trusted Recorder and/or a SM_CC Verification SAM. The specification of the requirement to those technical elements is however outside the scope of this Technical Specification. For clarity, assumptions on properties of a Trusted Recorder and the SM_CC Verification SAM to be used for Secure Monitoring are listed under this Clause. These assumptions are a useful basis for elaboration in measurable and specific requirements for a TR in other specifications. This may lead to classes of solutions of different strength, cost, capacity and flexibility. A TSP may determine the appropriate class, based on a specific risk analysis for the toll contexts in which the solution is applied.

This clause addresses assumptions on the properties of Trusted Recorder and SM_CC Verification SAM. A TR is used in all cases where real-time freezing is applied. A SM_CC Verification SAM is used when symmetric cryptography is used for real-time freezing. In this case the SM_CC MAC Verification SAM is used by both TSP and TC.

7.3.2 Trusted Recorder

In case of using an SM_CC option requiring a TR, this TR shall have the following properties:

1. The TR features a worldwide unique ID (TrId) of 16 octets length.

2. The loading and storage of a secret SM_CC key on a TR include adequate measures to maintain confidentiality of the key (symmetric cryptography).

3. The generation or loading and storage of a private SM_CC key on the TR include adequate measures to maintain confidentiality of the key (asymmetric cryptography).

4. The SM_CC key on the TR is only used for signing operations (calculation of digital signatures or MACs).

5. The TR provides generation of a MAC according to 7.1.2 and of signatures according to 7.1.3 to the OBE.

6. The generation of a MACs or signature by the TR is provided with adequate measures to preserve the confidentiality of the key used.

7. A signing operation (the generation of a MAC or signature by the TR) for the purpose of itinerary freezing in real-time is provided with a time lock, i.e. a mechanism ensuring that a new signing operation for real-time freezing can only be commissioned after a configurable period of time or processor clock cycles since the previous signing operation for itinerary freezing in real-time. The time lock value is a fixed value for the TR, i.e. applying to all toll domains. The time lock value takes into account that the highest frequency of freezing in the supported toll domains can still be handled.

8. A toll domain counter on the TR is assigned to a tollDomainId only once, i.e. the relation is fixed for the lifetime of the TR.

9. A specific tollDomainId can only be assigned to one toll domain counter

10. A toll domain counter on the TR is incremented each time a signing operation for the purpose of itinerary freezing in real-time is executed for the associated tollDomainID.

11. The value of a toll domain counter is not affected by any TR operation or instruction other than a signing operation for the purpose of real-time freezing.

12. In case a toll domain counter has reached is maximum value, the TR does not execute any further signing operations and enters into a locked or non-operational state.

13. The TR supports a minimum number of 10 toll domain counters.

14. The durability of the implementation of toll domain counters is adequate with regard the scheduled lifetime of a TR, the maximum number of subsequent writes to a cell given the memory type used, the maximum freezing frequency and a usage profile for a heavy toll domain user.

15. In case of a TR with trusted time source, adequate measures are implemented to provide trust by TSP and TCs that the absolute time in correctly signed or stamped itinerary data are correct.

7.3.3 SM_CC Verification SAM

Secure Application Modules used for SM_CC Verification (SM_CC Verification SAMs) have the following properties:

1. The SAM features a worldwide unique ID (SAM_ID) of 16 octets length.

2. The generation or loading and storage of a secret SM_CC key on a SM_CC Verification SAM include adequate measures to maintain confidentiality of the key.

3. A SM_CC Verification SAM has no capability to generate a SM_CC MAC, only to verify an SM_CC MAC.

4. A SM_CC Verification SAM can optionally verify an SM_CC signature using the appropriate public key as an input.

5. The SM_CC Verification SAM shall store at least one key pair for key distribution purposes.

Annex A
(normative)

Data type specification

This annex presents the ASN.1 (abstract syntax notation one) definition of

— the data types related to the SM_CC functions specified in Clause 5,

— the data types related to the SM_CC attributes specified in Clause 6, and

— the ASN.1 container types for ISO Layer 7,

in accordance with the ASN.1 technique specified in ISO/IEC 8824-1.

The ASN.1 Module's Object Identifier has been assigned in accordance to the requirements of ISO 14813-6.

```
EfcSecMonCc {iso(1) identified-organization(3) cen(162) 16702 part1(1)
version1(1)}

DEFINITIONS AUTOMATIC TAGS
::= BEGIN

EXPORTS ALL;

IMPORTS

Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList,
AttributeList, Attributes, BeaconID, BST, Dsrc-EID, DSRCApplicationEntityID,
Event-Report-Request, Event-Report-Response, EventType, Get-Request, Get-
Response{}, Initialisation-Request, Initialisation-Response, SetMMIRq,
ObeConfiguration, Profile, ReturnStatus, Time, T-APDUs, VST, EFC-ContextMark,
LPN, VehicleDimensions, VehicleWeightLimits, VehicleSpecificCharacteristics,
EquipmentOBUId, PaymentMeans, GetStampedRq, GetStampedRs

FROM EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)}

TollCharger, Period, DetectedChargeObject, AggregatedSingleTariffClassSession,
CCCAttributes, DateAndTime, Duration, DisUnit, DurUnit, PaymentFee

FROM ChargingModule {iso standard 17575 modules(0) efc(0) version(1)}

CCC-DataRetrieval-Request, CCC-DataRetrieval-Response, CCC-TestComm-Request, CCC-
TestComm-Response, CCC-TerminateComm, CCC-Notification-Request, CCC-Notification-
Response, CCC-InitialiseComm-Request, CCC-InitialiseComm-Response, CCC-
AuthDataRetrieval-Request, CCC-AuthDataRetrieval-Response, Longitude, Latitude,
VehicleAxlesHistory, CommunicationStatus, GnssStatus, DistanceRecordingStatus,
ActiveContext, OBEStatusHistory, CCC-ContextMark, VehicleAxles, VehicleClass

FROM CccModule {iso standard 12813 modules(0) efc(0) version(1)}

ContextId
```

```
FROM ContextDataModule {iso standard 175753 modules(0) efc(0) version(1)}

TollDeclarationId, AssociatedEventData, RequestADU, AckADU, TrustObjectADU,
EFCContextDataADU, ExceptionListADU, ReportAbnormalOBEADU, TollDeclarationADU,
BillingDetailsADU, PaymentClaimADU, ReportQAADU, StatusADU,
RetrieveUserDetailsADU, ProvideUserDetailsADU, ReportCCCEventADU,
RetrieveTollDeclarationADU, RetrieveCCCEventADU, UserId

FROM EFCInfoExchange {iso standard 12855 modules(0) data(1) version(1)}

InfoExchangeSec, InfoExchangeContentSec, AuthenticatedChargeReportADU,
RetrieveAuthenticatedChargeReportADU

FROM EFCSecurityFramework {iso standard 99999 modules(0) data(1) version(1)};


-- ********************************************************************
-- Module part 1: SM_CC itinerary data
-- ********************************************************************


ItineraryBatchFpd::= SEQUENCE {
   vehicleClass        VehicleClass OPTIONAL,
   vehicleAxles        VehicleAxles OPTIONAL,
   irs                 CHOICE {
          ciirs            SEQUENCE OF CiirFpd,
          cdirObjects      SEQUENCE OF CdirObjectFpd,
          cdirEvents          SEQUENCE OF CdirEventFpd
   }
}


ItineraryBatchRtf::= SEQUENCE {
   vehicleClass        VehicleClass OPTIONAL,
   vehicleAxles        VehicleAxles OPTIONAL,
   irs                 CHOICE {
      ciirs               SEQUENCE OF CiirRtf,
      cdirObjects         SEQUENCE OF CdirObjectRtf,
      cdirEvents             SEQUENCE OF CdirEventRtf
   }
}


CiirFpd::=              IrFpd{CiirSpec}
CdirObjectFpd::=    IrFpd{CdirObjectSpec}
CdirEventFpd::=     IrFpd{CdirEventSpec}


CiirRtf::=              Signed{IrRtf{CiirSpec}}
CdirObjectRtf::=    Signed{IrRtf{CdirObjectSpec}}
CdirEventRtf::=     Signed{IrRtf{CdirEventSpec}}


IrRtf{IRSpec}::= SEQUENCE {
```

```
   tollDomainCounters     SEQUENCE (SIZE (4)) OF TollDomainCounter, -- A
TollDomainCounter that is not used shall have the value zero for both
tollDomainId and the counter data elements

   irCommon         IrCommon,
   iRSpec              IRSpec
}


IrFpd{IRSpec}::= SEQUENCE {
   irCommon         IrCommon,
   iRSpec           IRSpec
}

IrCommon::= SEQUENCE {
   time             DateAndTime,
   latitude         Latitude,
   longitude        Longitude,
   userClassId         INT1
}

Signed{Payload}::= SEQUENCE {
   payload      Payload,
   authenticator Authenticator
}

CiirSpec::= Distance


CdirObjectSpec::=   SEQUENCE {
   detectedChargeObjectId  INT4,
   timeWhenUsed        DateAndTime
}


CdirEventSpec::=    NumberOfDetectedEvents


NumberOfDetectedEvents::=  INT2

-- Level 2 definitions

Algorithm::= INTEGER {
   cmacAes128                        (0),
   ecdsaNistp256WithSha256       (1)
   -- 2-100 reserved for future CEN and ISO use
   -- 101-255 reserved for private use
   } (0..127, ...)

Authenticator::= SEQUENCE {
   algorithm           Algorithm,
   keyRef           INT1, -- Key Ref or Version of the key in the TR
   auth                OCTET STRING
}
```

```
Distance::= SEQUENCE {
   dist      INTEGER(0..16383),
   disUnit   DisUnit
}

INT1::= INTEGER (0..128)

INT2::= INTEGER(0..65535)

INT4::= INTEGER(0..4294967295)

ItineraryHash::= OCTET STRING -- Hash over ItinerarySequenceFpd or
 -- over ItinerarySequenceRtf

ItinerarySequenceFpd::= SEQUENCE OF SEQUENCE {
   tollDomainCounter      TollDomainCounter,
   itineraryBatchSum      Unit,
   itineraryBatchHash     OCTET STRING
}

ItinerarySequenceRtf::= SEQUENCE OF SEQUENCE {
   itineraryBatchSum      Unit,
   tollDomainCounterStart TollDomainCounter,
   tollDomainCounterEnd   TollDomainCounter
}

TollDomainCounter::= SEQUENCE {
   tollDomainId ContextId,
   counter          INT4
   }

TrId::= OCTET STRING (SIZE (16))


-- ********************************************************************
-- Module part 2: SM_CC DSRC data definitions
-- ********************************************************************

SmccDataRetrievalResponse::= Get-Response{SmccContainer} (WITH COMPONENTS {...,
eid, iid ABSENT})

SmccContainer::= CHOICE{
integer       [0]    INTEGER,
bitstring     [1]    BIT STRING,
octetstring   [2]    OCTET STRING (SIZE (0..127), ...),
universalString  [3]    UniversalString,
beaconId      [4]    BeaconID,
t-apdu        [5]    T-APDUs,
dsrcApplicationEntityId [6] DSRCApplicationEntityID,
dsrc-Ase-Id   [7]    Dsrc-EID,
attrIdList    [8]    AttributeIdList,
attrList      [9]    AttributeList,
time          [15]   Time,
gstrq         [17]   GetStampedRq,
gstrs         [18]   GetStampedRs,
efccontext    [32]   EFC-ContextMark,
```

```
vehlpn        [47]   LPN, -- vehicle licence plate number
vehclass      [49]   VehicleClass,
vehdims       [50]   VehicleDimensions,
vehaxles      [51]   VehicleAxles,
vehwtlims     [52]   VehicleWeightLimits,
vehspchars    [54]   VehicleSpecificCharacteristics,
equOBUId      [56]   EquipmentOBUId,
paymeans      [64]   PaymentMeans,
setmmirq      [69]   SetMMIRq,
contCCC1      [81]   VehicleAxlesHistory,
contCCC2      [82]   CommunicationStatus,
contCCC3      [83]   GnssStatus,
contCCC4      [84]   DistanceRecordingStatus,
contCCC5      [85]   ActiveContext,
contCCC6      [86]   OBEStatusHistory,
reserved      [87]   NULL,
trId          [103]  TrId,
ciirRtf          [104]  CiirRtf,
cdirObjectRtf    [105]  CdirObjectRtf,
cdirEventRtf     [106]  CdirEventRtf

-- Defines the SM_CC Container types as the next values in the
-- row after the CCC and LAC data types

}



-- ********************************************************************
-- Module part 3: SM_CC - BO messages in addition to the EN ISO 12855
-- adus incl. the security amendment of TS 16439
-- ********************************************************************

ADUContentSecSM::= CHOICE {
    requestADU                          [1] RequestADU,
    ackADU                              [2] AckADU,
    trustObjectADU                      [3] TrustObjectADU,
    efcContextDataADU                   [4] EFCContextDataADU,
    exceptionListADU                    [5] ExceptionListADU,
    reportAbnormalOBEADU                [6] ReportAbnormalOBEADU,
    tollDeclarationADU                  [7] TollDeclarationADU,
    billingDetailsADU                   [8] BillingDetailsADU,
    paymentClaimADU                     [9] PaymentClaimADU,
    reportQAADU                         [10] ReportQAADU,
    statusADU                           [11] StatusADU,
    retrieveUserDetailsADU              [12] RetrieveUserDetailsADU,
    provideUserDetailsADU               [13] ProvideUserDetailsADU,
    reportCCCEventADU                   [14] ReportCCCEventADU,
    retrieveTollDeclarationADU          [15] RetrieveTollDeclarationADU,
    retrieveCCCEventADU                 [16] RetrieveCCCEventADU,
    authenticatedChargeReportADU        [17] AuthenticatedChargeReportADU,
   retrieveAuthenticatedChargeReportADU [18]
RetrieveAuthenticatedChargeReportADU,
    efcContextDataSmccADU               [19] EfcContextDataSmccADU,
    retrieveItineraryCheckADU           [20] RetrieveItineraryCheckADU,
```

```
    itineraryCheckADU                    [21] ItineraryCheckADU,
    smccClaimADU                        [22] SmccClaimADU
}


ADUTypeSecSM::= ENUMERATED {
    requestADU                          (1),
    ackADU                              (2),
    trustObjectADU                      (3),
    efcContextDataADU                   (4),
    exceptionListADU                    (5),
    reportAbnormalOBEADU                (6),
    tollDeclarationADU                  (7),
    billingDetailsADU                   (8),
    paymentClaimADU                     (9),
    reportQAADU                         (10),
    statusADU                           (11),
    retrieveUserDetailsADU              (12),
    provideUserDetailsADU               (13),
    reportCCCEventADU                   (14),
    retrieveTollDeclarationADU          (15),
    retrieveCCCEvents                   (16),
    authenticatedChargeReportADU        (17),
    retrieveAuthenticatedChargeReportADU (18),
    efcContextDataSmccADU               (19),
    retrieveItineraryCheckADU           (20),
    itineraryCheckADU                   (21),
    smccClaimADU                        (22)
}


EfcContextDataSmccADU::= SEQUENCE {
   normalEFCContextData   EFCContextDataADU (WITH COMPONENTS {gnssContext
PRESENT}),
   itineraryRecordType    INTEGER {
      noItinerary  (0), -- no itinerary generation requested by TC
      ciir         (1),
      cdirObject   (2),
      cdirEvent    (3)
      -- 6-100 reserved for future CEN and ISO use
      -- 101-255 reserved for private use
   } (0..255),
   itineraryRecordPeriodicity INT2,
   itineraryRecordPeriodicityType   INTEGER{
      time   (0),
      distance  (1)
      -- 2-255 reserved for future CEN and ISO use
   } (0..255),
   itineraryFreezingType INTEGER {
      detailedData              (0), -- no freezing requested by TC
      freezingPerDeclaration    (1), -- used in case of freezing per
declaration
      realTimeFreezing    (2) -- used in case of real-time freezing with a
trusted recorder
      -- 3-100 reserved for future CEN and ISO use
      -- 101-255 reserved for private use
```

```
    } (0..255),
    itineraryBatchSumType      UnitType,
    itineraryBatchPeriod          INT2,
rtfReportingDelay              INT2
}

RetrieveItineraryCheckADU::= SEQUENCE {
    tollDeclarationId      TollDeclarationId OPTIONAL,
    type                INTEGER {
        lowerLevel              (0), -- requests lower level information
        upperLevel              (1), -- requests upper level information
        upperAndLowerLevel  (2) -- requests upper and lower level information
        -- 3-100 reserved for future CEN and ISO use
        -- 101-255 reserved for private use
        } (0..255),
    whichItinerary      CHOICE {
observation          SEQUENCE {
           time      DateAndTime,
           long      Longitude,
           lat       Latitude
        },
tollDomainCounter   INT4 -- value of the toll domain counter, 0 indicates “all”
}
}

ItineraryCheckADU::= SEQUENCE {
    tollDeclarationId      TollDeclarationId,
    checkData CHOICE {
        checkDataFpd SEQUENCE {
            itinerarySequenceFpd       ItinerarySequenceFpd OPTIONAL,
            itineraryBatchFpd          ItineraryBatchFpd OPTIONAL
        },
        checkDataRtf SEQUENCE {
            itinerarySequenceRtf       ItinerarySequenceRtf OPTIONAL,
            itineraryBatchRtf          ItineraryBatchRtf OPTIONAL
        }
    }
}
SmccClaimADU::= SEQUENCE {
    smccClaimId                INTEGER,
    timeOfClaim                GeneralizedTime,
    userId                  UserId,
    typeOfClaim                TypeOfClaim,
    statusOfClaim              StatusOfClaim,
    associatedTd            SEQUENCE OF TollDeclarationId OPTIONAL,
    associatedItinerariesRtf   SEQUENCE OF ItineraryBatchRtf OPTIONAL,
    associatedItinerariesFpd   SEQUENCE OF ItineraryBatchFpd OPTIONAL,
    observationData            AssociatedEventData OPTIONAL,
    verbalComment           UTF8String OPTIONAL
}

-- Level 2 definitions

StatusOfClaim ::= INTEGER {
    new                        (0),
    openTspResponseRequired    (1),
```

```
    stillOpen                 (2),
    closedDueToTspCorrection  (3),
    closedDueToAgreement      (4),
    closedDueToPenalty        (5)
    -- 6-100 reserved for future CEN and ISO use
    -- 101-255 reserved for private use
}


TypeOfClaim  ::= INTEGER {
    realTimeCifAuthIncorrect                   (0),
    realTimeCifInconsistentWithObservation     (1),
    realTimeCifContentNotplausible             (2),
    delayedCifAuthIncorrect                    (3),
    delayedCifRecordsNotSequential             (4),
    delayedCifTimeDistanceNotPlausible         (5),
    delayedCifInconsistentWithObservation      (6),
    tdcItinerarySequenceHashIncorrect          (7),
    tdcValueOfSIncorrect                       (8),
    tdcInconsistentWithItinerary               (9)
        -- 10-100 reserved for future CEN and ISO use
    -- 101-255 reserved for private use
} (0..255)

Unit::=   CHOICE {
    fee       PaymentFee,
    distance  Distance,
    time      Duration,
    events    INTEGER
}

UnitType::= INTEGER {
    fee       (0),
    distance  (1),
    time      (2),
    events    (3)
    -- 4-100 reserved for future CEN and ISO use
    -- 101-127 reserved for private use
} (0..127,...)

END
```

Annex B
(normative)

Protocol Implementation Conformance Statement

B.1 Guidance for completing the PICS proforma

B.1.1 Purposes and structure

The purpose of this PICS proforma is to provide a mechanism whereby a supplier of an implementation of the requirements defined in this International Standard may provide information about the implementation in a standardized manner.

The PICS proforma is subdivided into clauses for the following categories of information:

— guidance for completing the PICS proforma;

— identification of the implementation;

— identification of the protocol;

— global statement of conformance;

— PICS proforma tables.

B.1.2 Abbreviations and conventions

The PICS proforma contained in this annex comprises information in tabular form in accordance with the guidelines presented in ISO/IEC 9646-7.

— Item column

The item column contains a number which identifies the item in the table.

— Item description column

The item description column describes in free text each respective item (e.g. parameters, timers, etc.). It implicitly means “is <item description> supported by the implementation?”.

— Status column

The following notations, defined in ISO/IEC 9646-7 are used for the status column:

m	mandatory - the capability is required to be supported.
o	optional - the capability may be supported or not.
n/a	not applicable - in the given context, it is impossible to use the capability.
x	prohibited (excluded) - there is a requirement not to use this capability in the given context.
o.i	qualified optional - for mutually exclusive or selectable options from a set. “i” is an integer which identifies a unique group of related optional items and the logic of their selection which is defined immediately following the table.

ci	conditional - the requirement on the capability (“m”, “o”, “x” or “n/a”) depends on the support of other optional or conditional items. “i” is an integer identifying a unique conditional status expression which is defined immediately following the table.

— Reference column

The reference column makes reference to this International Standard, except where explicitly stated otherwise.

— Support column

The support column shall be filled in by the supplier of the implementation. The following common notations, defined in ISO/IEC 9646-7, are used for the support column:

Y or y	supported by the implementation.
N or n	not supported by the implementation.
N/A, n/a or -	no answer required (allowed only if the status is n/a, directly or after evaluation of a conditional status).

NOTE As stated in ISO/IEC 9646-7, support for a received PDU requires the ability to parse all valid parameters of that PDU. Supporting a PDU while having no ability to parse a valid parameter is non-conformant. Support for a parameter on a PDU means that the semantics of that parameter are supported.

— Values allowed column

The values allowed column contains the type, the list, the range, or the length of values allowed. The following notations are used:

range of values:	< min value > .. < max value >
example:	5 .. 20
list of values:	< value1 > , < value2 > , ..., < valueN >
example:	2, 4, 6, 8, 9
example:	'1101'B, '1011'B, '1111'B
example:	'0A'H, '34'H, '2F'H
list of named values:	< name1 > (<val1 >), < name2 > (<val2 >), ..., < nameN > (<valN >)
example:	reject(1), accept(2)
length:	size (<min size > .. < max size >)
example:	size (1 .. 8)

— Values supported column

The values supported column shall be filled in by the supplier of the implementation. In this column, the values or the ranges of values supported by the implementation shall be indicated.

— References to items

For each possible item answer (answer in the support column) within the PICS proforma, a unique reference exists, used, for example, in the conditional expressions. It is defined as the table identifier, followed by a solidus character “/”, followed by the item number in the table. If there is more than one support column in a table, the columns are discriminated by letters (a, b, etc.), respectively.

EXAMPLE 1 1/4a is the reference to the first answer (i.e. contained in the first support column) of item 4 in Table B.1.

EXAMPLE 2 2/3b is the reference to the second answer (i.e. contained in the second support column) of item 3 in Table B.2.

— Prerequisite line

A prerequisite line takes the form: Prerequisite: < predicate > .

A prerequisite line after a clause or table title indicates that the whole clause or the whole table is not required to be completed if the predicate is FALSE.

B.1.3 Instructions for completing the PICS proforma

The supplier of the implementation shall complete the PICS proforma in each of the spaces provided. In particular, an explicit answer shall be entered in each of the support or supported column boxes provided, using the notation described previously.

If necessary, the supplier may provide additional comments in space at the bottom of the tables or separately.

B.2 Identification of the implementation

B.2.1 General

Identification of the Implementation Under Test (IUT) and the system in which it resides [the System Under Test (SUT)] shall be filled in so as to provide as much detail as possible regarding version numbers and configuration options.

The product supplier information and client information shall both be filled in if they are different.

A person who can answer queries regarding information supplied in the PICS shall be named as the contact person.

B.2.2 Date of the statement

.....

B.2.3 Implementation Under Test (IUT) identification

IUT name:

.....

.....

IUT version:

.....

B.2.4 System Under Test (SUT) identification

SUT name:

.....

.....

Hardware configuration:

.....

.....

.....

Operating system:

.....

B.2.5 Product supplier

Name:

.....

Address:

.....

.....

.....

Telephone number:

.....

Facsimile number:

.....

E-mail address:

.....

Additional information:

.....

.....

.....

B.2.6 Applicant (if different from product supplier)

Name:

.....

Address:

.....

.....

.....

Telephone number:

.....

Facsimile number:

.....

E-mail address:

.....

Additional information:

.....

.....

B.2.7 PICS contact person

(A person to contact if there are any queries concerning the content of the PICS)

Name:

.....

Telephone number:

.....

Facsimile number:

.....

E-mail address:

.....

Additional information:

.....

.....

.....

B.3 Identification of the protocol

This PICS proforma applies to the following standard:

WI 00278338 [1] "Electronic fee collection — Secure Monitoring for autonomous toll systems – Part 1: Compliance checking".

B.4 Global statement of conformance

Are all mandatory capabilities implemented? (Yes/No)

NOTE Answering "No" to this question indicates non-conformance to the protocol specification. Non-supported mandatory capabilities are to be identified in the PICS, with an explanation of why the implementation is non-conforming, on pages attached to the PICS proforma.

B.5 Roles

This part of the PICS proforma identifies the supported roles.

Table B.1 — Roles

Item	Supported role	Reference	Status	Support (Y/N)
1	Toll Charger	5.1	o.1–1	
2	Toll Service Provider	5.1	o.1–1	
o.1–1:It is mandatory to support at least one of these options.				

B.6 Types of Secure Monitoring

This part of the PICS proforma identifies the supported types of Secure Monitoring.

[1] Under Development

Table B.2 — Types of Secure Monitoring

Item	Supported type of Secure Monitoring	Reference	Status	Support (Y/N)
1	SM_CC-1	5.2	o.2–1	
2	SM_CC-2	5.2	o.2–1	
3	SM_CC-3a	5.2	o.2–1	
4	SM_CC-3b	5.2	o.2–1	
o.2–1: It is mandatory to support at least one of these types of Secure Monitoring. Note: It is mandatory that all roles from Table B.1 support the same type of Secure Monitoring.				

B.7 Capabilities and conditions

This part of the PICS proforma identifies technical capabilities and conditions for effective compliance checks needed to support the different types of Secure Monitoring.

Table B.3 — Capabilities and conditions

Item	Supported capability and condition for effective compliance check	Reference	Status	Support (Y/N)
1	Trusted Recorder	5.3.3	c.3–1	
2	Trusted time source	5.3.3	c.3–2	
3	High communication availability	5.4.2	c.3–3	
4	CIF via DSRC	5.4.3	c.3–4	
5	Unexpected observations	5.4.2	c.3–5	
6	Undetected observations	5.4.2	c.3–6	
c.3–1: IF Table B.1/2 AND (Table B.2/1 OR Table B.2/2) THEN m ELSE n/a. c.3–2: IF Table B.1/2 AND Table B.2/2 THEN m ELSE n/a. c.3–3: IF Table B.1/2 AND Table B.2/4 THEN m ELSE n/a. c.3–4: IF Table B.2/1 THEN m ELSE n/a. c.3–5: IF Table B.1/1 AND (Table B.2/1 OR Table B.2/2 OR Table B.2/4) THEN m ELSE n/a. c.3–6: IF Table B.1/1 AND Table B.2/3 THEN m ELSE n/a.				

B.8 Processes

This part of the PICS proforma identifies the supported processes.

Table B.4 — Processes

Item	Supported types	Reference	Status	Support (Y/N)
1	Generate Context Independent Itinerary	5.3.2	c.4–1	
2	Generate Context Dependent Itinerary	5.3.2	c.4–2	
3	Real-time freezing	5.3.3	c.4–3	
4	Freezing per declaration	5.3.4	c.4–4	
5	Observing a vehicle – Unexpected Observations	5.4.2	c.4–5	
6	Observing a vehicle – Undetected Observations	5.4.2	c.4–6	
7	Retrieving PIF in real-time	5.4.3	c.4–7	
8	Retrieving PIF data via TSP back end	5.4.3	c.4–8	
9	Checking PIF against observation	5.4.4	c.4–9	
10	Retrieve Itinerary Data	5.5.2	c.4–10	
11	Check Itinerary Consistency	5.5.3	m	
12	Checking Toll Declaration against Itinerary	5.5.4	m	
13	Claiming incorrectness	5.6	m	
14	Providing EFC context data	5.7	m	
15	Key Management	5.8	m	

c.4–1: IF Table B.1/2 THEN o.4–1 ELSE n/a.

c.4–2: IF Table B.1/2 THEN o.4–1 ELSE n/a.

o.4–1: It is mandatory to support at least one of these options.

c.4–3: IF Table B.1/2 AND (Table B.2/1 OR Table B.2/2) THEN m ELSE n/a.

c.4–4: IF Table B.1/2 AND (Table B.2/3 OR Table B.2/4) THEN m ELSE n/a.

c.4–5: IF Table B.1/1 AND (Table B.2/1 OR Table B.2/2 OR Table B.2/4) THEN m ELSE n/a.

c.4–6: IF Table B.1/1 AND Table B.2/3 THEN m ELSE n/a.

c.4–7: IF Table B.2/1 THEN m ELSE n/a.

c.4–8: IF (Table B.2/2 OR Table B.2/3 OR Table B.2/4) THEN m ELSE o.

c.4–9: IF Table B.1/1 THEN m ELSE n/a.

c.4–10: IF (Table B.2/2 OR Table B.2/3 OR Table B.2/4) THEN m ELSE o.

Annex C
(informative)

Example transactions

This annex provides example transactions for different options that can be used for Checking of Itinerary Freezing in Real-Time (CIF-1), i.e. via DSRC. The following examples are included:

— An SM_CC transaction retrieving Context Independent Itinerary data

— A combined CCC and SM_CC transaction, retrieving Context Independent Itinerary data

— An optimised combined CCC and SM_CC transaction, retrieving Context Independent Itinerary data, using a minimum number of layer-2 frames.

Table C.1 shows an example SM_CC transaction which reads out the CIIR and all data related to it. The transaction is similar for all CDIR options.

Table C.1 — Example SM_CC transaction with CIIR read-out

Phase	Roadside Equipment		On-board equipment	Remarks
Initialisation	INITIALISATION.request (BST)	→		RSE periodically sends BST.
(BST – VST)		←	INITIALISATION.response (VST) • CCC-ContextMark • AC_CR-KeyReference • RndOBE	A newly arrived OBE answers with VST. AC-CR-KeyReference is the reference to the access credential keys to be used by the RSE. RndOBE is a random number that the RSE uses when calculating the access credentials. The OBE will give access only when RSE provides the correct access credentials (AC_CR) in the subsequent phases.
Presentation	GET.request AC_CR • PaymentMeans • TrId • EquipmentOBUId Static vehicle data: • VehicleDimensions • VehicleLicensePlateNumber • VehicleWeightLimits VehicleSpecificCharacteristics Dynamic vehicle data: • VehicleAxles • VehicleClass	→		The OBE is asked to present all data necessary to check the signature on the IR.

Phase	Roadside Equipment		On-board equipment	Remarks
		←	GET.response	OBE responds with the requested data. This results in an uplink containing 75 octets of application data: 14+4+5+3+17+6+4+2+1 additional protocol overhead.
Itinerary	GET.request AC_CR • CIIR	→		The OBE is asked to send its CIIR
		←	• GET.response	OBE responds with the CIIR
Tracking	ECHO.request	→		Track OBE by exchanging dummy information.
And		←	ECHO.response	The usage of Echo is optional, at the discretion of the RSE, and may be repeated.
Closing	EVENT_REPORT.request (Release)	→		RSE closes transaction and releases OBE.

Table C.2 shows an example combined CCC and SM_CC transaction which reads out the full CCC data and the CIIR.

Table C.2 — Example combined CCC and SM_CC transaction

Phase	Roadside Equipment		On-board equipment	Remarks
Initialisation	INITIALISATION.request (BST)	→		RSE periodically sends BST.
(BST – VST)		←	INITIALISATION.response (VST) • CCC-ContextMark • AC_CR-KeyReference • RndOBE	A newly arrived OBE answers with VST. AC-CR-KeyReference is the reference to the access credential keys to be used by the RSE. RndOBE is a random number that the RSE uses when calculating the access credentials. The OBE will give access only when RSE provides the correct access credentials (AC_CR) in the subsequent phases.
Presentation	GET_STAMPED.request AC_CR • PaymentMeans (RndRSE, KeyRef_Auth) GET.request AC_CR • EquipmentOBUId • TrId Static vehicle data: • VehicleDimensions • VehicleLicensePlateNumber • VehicleWeightLimits • VehicleSpecificCharacteristics	→		The OBE is asked to present itself and its static data. Authenticated retrieval of PaymentMeans from the OBE: the OBE is asked to calculate an authenticator over PaymentMeans using the authentication key (KeyRefAuth). Retrieval of data from the OBE: remaining identification data and static vehicle data.

Phase	Roadside Equipment		On-board equipment	Remarks
		←	GET_STAMPED.response • MAC_Authentication GET.response	OBE responds with PaymentMeans, which points to the user contract/account at the Toll Service Provider plus an authenticator, providing authentication of the OBE and its data (data integrity and data origin authentication). MAC_Authentication can be directly checked by the toll charger to establish whether the OBE is authentic. OBE responds with the additional requested data.
Status	GET_STAMPED.request AC_CR • PaymentMeans Dynamic vehicle data: • VehicleAxles • VehicleAxlesHistory • VehicleClass Status Data: • ActiveContexts • OBEStatusHistory • CommunicationStatus • GnssStatus • DistanceRecordingStatus (RndRSE, KeyRef_NonRep)	→		The OBE is asked to present its dynamic status. Authenticated retrieval of a complete data package containing: PaymentMeans, VehicleAxles, VehicleClass and all Status data. The OBE is asked to calculate a signature that provides non-repudiation characteristics for the whole package using the non repudiation key (KeyRef_NonRep). MAC_NonRepudiation is stored together with the CCC data and can be used by the toll charger in the event of a dispute with the user.
		←	GET_STAMPED.response • MAC_NonRepudiation	OBE responds with the requested data, plus an authenticator, providing for non-repudiation characteristics.
Itinerary	GET.request AC_CR • CIIR	→		The OBE is asked to send its CIIR
		←	• GET.response	OBE responds with the CIIR
Tracking	ECHO.request	→		Track OBE by exchanging dummy information.
And		←	ECHO.response	The usage of Echo is optional, at the discretion of the RSE, and may be repeated.
Closing	EVENT_REPORT.request (Release)	→		RSE closes transaction and releases OBE.

Table C.3 shows an optimised combined CCC and SM_CC transaction which reads out the CCC data and the CIIR. Authentication is obtained through the CIIR signature.

Table C.3 — Example optimised combined CCC and SM_CC transaction

Phase	Roadside Equipment		On-board equipment	Remarks
Initialisation	INITIALISATION.request (BST)	→		RSE periodically sends BST.
(BST – VST)		←	INITIALISATION.response (VST) • CCC-ContextMark • AC_CR-KeyReference • RndOBE	A newly arrived OBE answers with VST. AC-CR-KeyReference is the reference to the access credential keys to be used by the RSE. RndOBE is a random number that the RSE uses when calculating the access credentials. The OBE will give access only when RSE provides the correct access credentials (AC_CR) in the subsequent phases.
Presentation	GET.request AC_CR • PaymentMeans • TrId • EquipmentOBUId Static vehicle data: • VehicleDimensions • VehicleLicensePlateNumber • VehicleWeightLimits •VehicleSpecificCharacteristics Dynamic vehicle data: • VehicleAxles • VehicleAxlesHistory • VehicleClass Status Data: • OBEStatusHistory • CommunicationStatus • DistanceRecordingStatus	→		The OBE is asked to present all CCC data This includes the TR identification data, vehicle data and status data. Note that ActiveContexts and GnssStatus are not read-out since overlapping with information contained in the IR
		←	GET.response	OBE responds with the requested data. This results in an uplink containing 102 octets of application data: 14+4+5+3+17+6+4+2+6+1+13 + 8+6 + additional protocol overhead.
Itinerary	GET.request AC_CR • CIIR	→		The OBE is asked to send its CIIR
		←	• GET.response	OBE responds with the CIIR
Tracking	ECHO.request	→		Track OBE by exchanging dummy information.
And		←	ECHO.response	The usage of Echo is optional, at the discretion of the RSE, and may be repeated.
Closing	EVENT_REPORT.request (Release)	→		RSE closes transaction and releases OBE.

Annex D
(informative)

Addressed threats (in CEN/TS 16439)

D.1 Introduction

Secure Monitoring is a concept that can provide protection against a number of attacks that could be mounted on an EFC system. This annex specifies which attacks that Secure Monitoring addresses. It is based on the threat analysis that has been carried out in CEN/TS 16439 “Electronic Fee Collection - Security Framework” and uses those references both for threats, requirements and security measures. This annex also spells out the consequences for requirements and security measures.

For an overview of the connections between threats, requirements and security measures, please refer to Figure 2.

D.2 Threats where Secure Monitoring can provide Security Measures

CEN/TS 16439:2013 “Electronic Fee Collection - Security Framework” includes two lists of threats in Annex D. The first one is the result of an attack-tree analysis, the second one of an asset-based analysis. The table below list the threats where Secure Monitoring can provide a complete or partial mitigation. Threats in *italics* have a weaker relation to Secure Monitoring but might be mitigated by it.

Table D.1 — EFC Security Framework threats where Secure Monitoring can provide Security Measures

Ref	Description
T10.1.1	Blinding the road usage sensor - The road usage sensor, for example a GNSS unit or a DSRC transponder, could be blinded, for example by covering the antenna where this is applicable.
T10.1.2	Muting the OBE - In the case where the OBE communication channel is separate from the road usage sensor itself (i.e. autonomous systems only) the communication signal might be temporarily or permanently blocked thus avoiding the reporting of road usage data rendering the OBE “mute”.
T10.1.3	Removing or destroying the OBE - One of the simplest yet most effective attacks is to destroy or remove the OBE. Removal could be permanent or temporal. Unless some counter measure is designed this will render the vehicle “invisible” for the system.
T10.1.4	Disconnect the OBE power supply temporarily or permanently. The simplest attack is to remove the OBE power supply. That can be done permanently or only temporary, e.g. insert a switch in the power supply.
T10.1.5	Jamming the GNSS road usage sensor (e.g. with a portable device).
T10.2.1	Manipulating the input to the usage sensors - This attack is typically relevant in system where road usage is continually recorded (such as in GNSS-based systems) and involves spoofing the signal that goes into the sensor. It does not require any modifications to the OBE since it is directed at the road usage signal before it enters the OBE.
T10.2.2	Manipulating the usage sensors - This attack involves modifying the road usage sensors, for example replacing them or filtering their output to generate data that results in a lower toll. It is performed in real-time and modifies road usage data as it is collected.
T10.2.3	Manipulating the usage data collection software - The software calculating the road usage based on the sensor inputs is altered in such a way that a lower road usage will be resulting and stored and

Ref	Description
	transmitted to the back-office (only possible in autonomous systems).
T10.2.4	Manipulating the usage data after collection stored in the OBE - In the case where several items of road usage data remains under the control of the user before being reported to another party the User has the possibility of modifying the road usage data taking the whole data set into account.
T10.2.5	Manipulating the usage data in transit from the OBE - Road usage data can be manipulated as it is communicated from the OBE.
T10.2.6	Use an OBE simulator to produce the required road usage “toll declaration” - Prevent the OBE from sending the road usage to the back-office and produce a fake data set with OBE simulation equipment that is send instead.
T102.1	*A Charge Report could be changed during transmission between Front End and TSP back-office.*
T102.6	*The authenticity of sent Charge Reports cannot be proven and/or its origin is repudiated.*
T107.1	*Manipulation of stored data – Due to manipulation the correct functionality of the OBE is no longer guaranteed*
T107.7	An attacker tries to change the compliance check attributes inside the OBE to a proper value for an enforcement authority.
T107.9	*An attacker tries to manipulate or exchange hardware components to pay lower toll.*
T112.2	*Alteration of charge report in an autonomous system.*
T112.4	*Data transfer corruption in an autonomous system*
T114.1	*A User Identification could be changed during transmission between OBE and RSE*
T20.1	Faking road use - The Toll Service Provider could charge a customer for road usage that has never taken place. He calculates the fake charge based on the toll context data and tariffs of a Toll Charger without involving them.
T20.2	Using incorrect toll context data - The Toll Service Provider could use faulty toll context data to inflate the toll charged to the road customer while use the correct data that results in a lower toll in communication with the Toll Charger and thus being able to keep the difference.
T20.3	Overcharging the Customer - The Toll Service Provider charges the customer a higher amount as calculated by himself or by the Toll Charger(s) based on the billing details. The Toll Service Provider changes the invoice data received from the Toll Charger to increase the charge.
T23.1	Modifying usage data reported from the OBE - The Toll Service Provider could modify the road usage data so to be sent to the Toll Charger that the toll is deflated, for example slightly shifting the time values to put the trip in another, cheaper, time class, while using the correct data to charge the customer.
T23.2	Suppressing reporting of road use - The Toll Service Provider could refrain from reporting road usage to the Toll Charger, while using the correct data to charge the customer.
T23.3	Faulty interpretation of usage data - In certain set-ups the Toll Service Provider will have the ability to interpret the road usage data in a way that inflates the toll that is due to the Toll Charger, while using the correct data to charge the use. An example could be if map matching is under the control of the Toll Service Provider and road usage sensor data are intentionally misinterpreted to mean a faulty, less expensive, route.
T23.4	Using incorrect toll context data - If the Toll Service Provider is in control of computing the final toll or some data on which the final toll is computed it could use faulty toll context data to deflate the toll to be paid to the Toll Charger while use the correct data that results in a higher toll in communication

Ref	Description
	with the customer and thus being able to keep the difference.
T23.5	Manipulate Charge Data during enrichment. A Toll Service Provider which has been requested by a Toll Charger to enrich determined charge data, may manipulate them to reduce the final toll, while using the correct data to charge the customer.
T40.1	Fake an input signal from the vehicle and have it accepted as valid. In this attack a signal, that is required for the operation of the system, is emulated or modified to modify its semantics. Typical sources of signals are CAN bus, tachograph or odometer.
T40.2	Induce noise on Power Supply Lines to cause system misoperation. Excessive power supply noise can induce system misoperation and/or system restarts with corresponding data loss.
T40.3	Remove system from the vehicle while maintaining PSU connections. Maintaining the power supply unit (PSU) avoids the anti-tamper circuitry being triggered and allows the device to be removed from the vehicle.
T40.4	Fake input signal from GNSS - Create a ‘fake’ GNSS signal which swamps the ‘real’ one and gives a different position for the OBE.
T40.5	Provide false configuration data to the OBE/Proxy - Adjust the OBE so that it is inappropriately set (for example telling it that it is in a car rather than a truck).
T40.6	To fake User Input according to sensed external state. For example, to automatically update the class of a vehicle before an audit-check event takes place.

D.3 Related Requirements

In CEN/TS 16439 “Electronic Fee Collection - Security Framework” different threats are connected to requirements. If a threat is considered to be important in the specific case of an EFC system, then the related requirements should be applied. Making the connection from all the threats in the preceding section to the related requirement, the list in the following table is produced. Requirements in *italics* are related to those threats that have a weaker connection to the Secure Monitoring concept (also *italicized* in the preceding section).

Table D.2 — EFC Security Framework Requirements related to Secure Monitoring relevant threats

Ref	Description
RQ.DS.01	*Access to stored data shall only be granted after authorisation.*
RQ.DS.02	*Access to store data shall only be granted via defined interfaces and defined procedures.*
RQ.IF.11	*Data exchange shall guarantee data integrity.*
RQ.IF.13	*Data exchange shall guarantee non-repudiation with proof of origin.*
RQ.IF.14	*Data exchange shall guarantee non-repudiation with proof of delivery.*
RQ.SU.01	The TSP and TC shall enable the User to check the correctness of an invoice.
RQ.TC.01	The Toll Charger shall determine if factual road usage is represented by a corresponding set of toll declarations (enabled by RQ.TSP.51).
RQ.TC.02	The Toll Charger shall be able to determine if a toll declaration is based on correct and complete road usage data (enabled by RQ.TSP.52).
RQ.TC.03	The TC shall determine, in a spot check, if an OBE is in an OK operational state.

Ref	Description
RQ.TC.04	The TC shall check the integrity and authenticity of the received data as compared to the data sent from the Front End.
RQ.TC.05	The TC shall determine if toll declarations are based on data originating from a legitimate Front End and/or TSP back-office (enabled by RQ.TSP.55).
RQ.TC.06	The Toll Charger shall periodically audit invoices of customers for tolls of his toll domain (enabled by RQ.TSP.56).
RQ.TSP.01	The Toll Service Provider shall determine if factual road usage is represented by a corresponding set of toll declarations.Note: This means that toll declarations are not altered and completely transmitted.
RQ.TSP.02	The Toll Service Provider shall determine if a toll declaration is based on correct and complete road usage data.Note: This means that tolling related events are correctly collected.
RQ.TSP.04	The TSP shall check the integrity and authenticity of the received data as compared to the data sent from the Front End.
RQ.TSP.05	The TSP shall determine if toll declarations are based on data originating from a legitimate Front End.
RQ.TSP.09	The TSP shall notify the driver if the OBE is not working correctly.
RQ.TSP.16	The OBE shall detect signal input inconsistencies and in such case signal not OK to the User and send an indication to TSP.
RQ.TSP.40	The OBE shall not allow change of internal data via the user interface, except the data allowed to be changed.
RQ.TSP.51	The TSP shall enable the TC to determine if factual road usage is represented by a corresponding set of Toll Declarations (required to enable RQ.TC.01).
RQ.TSP.52	The TSP shall enable the TC to determine if a toll declaration is based on correct and complete road usage data (required to enable RQ.TC.02).
RQ.XX.02	*Prevent from manipulating equipment hardware; especially prevent OBE from HW manipulation. Such a requirement can only be fulfilled by developing a tamper resistant OBE which is not cost efficient feasible. This is out of scope of this Technical Specification.*

D.4 Related Security Measures

In CEN/TS 16439 “Electronic Fee Collection - Security Framework” requirements are related to Security Measures. Making the connection from all the requirements in the preceding section to the related security measure, the list in the following table is produced. Excluded from this list are security measures which are implemented directly in the CEN/TS 16439. Those security measures that are implemented by this technical specification are listed in **bold**.

Table D.3 — EFC Security Framework Security Measures related to Secure Monitoring relevant requirements

Ref	Description
SM211	The RSE shall request the OBE to calculate and provide a MAC_TSP over at least the EN ISO 14906 attributes PaymentMeans, using a key known only to the Toll Service Provider
SM213	**The RSE shall read, increment and write a transaction counter to the OBE. The OBE shall support this.**

Ref	Description
SM223	**The OBE shall provide an undeniable proof of correct registration of usage data for the given location and moment in time of the CCC transaction.**
SM230	The RSE shall provide a MAC_TC over the LAC data send to the OBE calculated with a key known only to the Toll Charger and the IACtime.
SM240	**The authenticator in the ChargeReport shall guarantee its authenticity and integrity.**
SM257	**The Toll Service Provider shall provide data underlying a specific toll declaration acquired through his system, on demand of the Toll Charger (ChargeReport and/or more detailed road usage data).**
SM310	The Front End shall be designed as a clearly distinguished entity with a defined interface to the TSP Back-office. The Front End's functionality shall be tested to guarantee its functionality and it shall be auditable according to a procedure agreed between Toll Charger and Toll Service Provider.
SM311	The correct and trustworthy Front End functionality shall be periodically audited by the Toll Service Provider and optionally by the Toll Charger or an independent entity on his behalf. NOTE An audit process can compare charge data of sample vehicles equipped with the OBE with well known independent trip data.
SM312	**The Toll Charger and/or Toll Service Provider shall perform plausibility and completeness checks on toll declarations acquired by the Toll Service Provider. Those checks comprise the verification of the physical feasibility of trips on the Toll Domain compared with the actual toll declarations.**
SM313	**The Toll Charger shall compare the toll declarations with his own observations, in accordance with privacy regulations.**
SM314	**The Toll Charger shall verify if toll declaration(s) acquired by the Toll Service Provider correctly correspond(s) to ChargeReport(s) and/or usage data.**
SM316	**The Toll Charger shall determine if the ChargeReport has been produced by a trusted Front End by a MAC or signature.**
SM317	**The Toll Charger shall verify the integrity of the ChargeReport based on the Front End MAC or signature.**
SM318	**The registration of usage data by the Toll Service Provider shall be based on a minimum set of functions in the Front End trusted by both the Toll Service Provider and the Toll Charger. These functions shall directly or indirectly ensure the integrity of the toll declarations incl. non-repudiation with proof of origin.**
SM319	**The Toll Service Provider shall provide an undeniable proof of correct registration of usage data for a defined location and moment in time, or for a defined range of time, on demand to the Toll Charger.**
SM320	**The Toll Charger shall compare the proof of correct registration of usage data with his own observations, in accordance with privacy regulations.**
SM410	**The OBE shall support a Compliance Checking Communication transaction over an interface.**
SM412	In case of Localisation Augmentation received via DSRC, the Toll Service Provider shall store the value of the MAC_TC, KeyRef and IACtime as part of the charge data and provide them as part of the ChargeReport.

Ref	Description
SM414	The driver shall be notified by the OBE about the correct OBE working status. For example the following status shall result in OBE not ok indication:- no collection of road usage data - OBE unable to communicate with the back end - no external power supply - out of OBE memory
SM420	The Toll Service Provider shall verify if toll declaration(s) correctly correspond(s) to ChargeReport(s) and/or usage data.
SM421	**Toll Service Provider shall determine if the ChargeReport has been produced by a trusted Front End.**
SM422	**Toll Service Provider shall verify the integrity of the ChargeReport.**
SM510	In case of toll declarations acquired via the DSRC interface, the Toll Charger shall check the value of the MAC_TC using the key addressed by KeyRef and the RndRSE.
SM512	In case of toll declarations acquired via the DSRC interface, the Toll Charger shall store the value of the authenticated AttributeList, MAC_TC, MAC_TSP, KeyRef and RndRSE as part of the billing Details.
SM513	In case of toll declarations provided by the Toll Service Provider, the RSE shall perform a Compliance Checking Communication transaction.
SM514	In case of compliance checking via DSRC, the Toll Charger shall check the value of the MAC_TC using the key addressed by KeyRef and the RndRSE.
SM520	**The Toll Charger shall perform plausibility and completeness checks on toll declarations acquired by himself. Those checks comprise the verification of the physical feasibility of trips on the Toll Domain compared with the actual toll declarations.**
SM521	If the charge data provided by the TSP are based on LAC data, the TC shall verify the MAC_TC.
SM530	**The Toll Charger shall compare the toll declarations acquired by himself with his own observations, in accordance with privacy regulations.**

Annex E
(informative)

Essentials of the SM_CC concept

E.1 Introduction

This informative annex provides additional background information on the rationale and purpose of SM_CC and motivates a number of choices and options in the concept. In addition, a few related issues are addressed that may appear when implementing SM_CC.

E.2 The SM_CC concept – FAQs

What is the purpose of SM_CC?

The main purpose of SM_CC is to provide the Toll Charger and the Toll Service Provider with improved means to detect manipulation, fraud or OBE malfunction for EFC schemes using autonomous OBE. The use of SM_CC does not guarantee that no fraud (by the Service User or the TSP) can take place. It does neither guarantee that all misuse will be detected by the TC or TSP. A proper implementation and use of SM_CC will however significantly reduce effective 'modes of attack' for the SU and TSP, and increase the probability that an attempt will be detected. This has a strong impact on the 'business case' for fraud, and is as a result likely to lead to higher user compliance. The effectiveness will be influenced by the intensity and thoroughness of checks, possible penalties for fraud and the related perceptions of the SU.

How does it work?

There are a number of different options within SM_CC that work in a slightly different way. The basic idea is however similar.

When travelling in an EFC domain, an autonomous OBE generates a stream of GNSS data (and possibly additional sensor data). These data are processed and compressed in some form before being sent as *charge data* to the TSP Backoffice (proxy). The format and content of the charge data may vary, depending on OBE capabilities, technical choices of the TSP as well as reporting rules imposed by the TC. The TSP Backoffice takes care of further processing of the charge data into a Toll Declaration to be submitted to the TC. Generic threats consist of manipulating the GNSS input to the OBE and modifying or deleting charge data before they are sent to the backoffice.

When using Secure Monitoring, apart from the charge data an additional stream of data, called *itinerary data* is produced. In the process of SM_CC, itinerary data are checked for consistency with data from a roadside observation.

The itinerary data originate from the same source as the charge data. Obviously, if a fraudulent user can manipulate the charge data, he could in principle also manipulate the corresponding itinerary data. The main added value of SM_CC is however that the itinerary data are committed to ('frozen') *before* the fraudulent SU or TSP would know whether, where and when the TC performed or will perform a roadside check. At the point the TC requests the itinerary data to perform the check, the itinerary data are already frozen: it is no longer possible to modify the data without detection by the TC. As a result, a manipulation strategy in which the OBE or backoffice is only to produce truthful data around the roadside checks of the TC will be ineffective: the SU or TSP does not know where/when a roadside check will take place or has taken place at the point the corresponding itinerary data are to be committed to.

Why is a separate stream of data necessary for SM_CC?

In principle, it is possible to freeze (detailed) charge data and use such data for similar roadside checks as well as for toll declaration checking. Indeed, in some situations the frozen itinerary data may actually be identical to the charge data, which simplifies the solution. However, this would not be a practical solution for all toll contexts and possible TSP front ends. As the content, format and periodicity of charge data records depends on choices of the TSP / the front-end supplier (the OBE-proxy interface is not standardized), the TC would possibly have to deal with a variety of contents and formats. The structure and content of *itinerary data* on the other hand is fully defined in this TS. This guarantees that syntax and semantics of itinerary records do not depend on the TSP. When using context-independent itinerary records (CIIR), the syntax and semantics are even identical across toll domains.

This leads to the question: why is it feasible to 'standardize' itinerary data when we take for granted that it is not possible or desirable to standardize charge data? One reason is that severe requirements are imposed on the accuracy and reliability of the charging process. Different approaches exist that optimize accuracy, within constraints of e.g. maintainability and bandwidth. This is deemed a domain of innovation and competition. For compliance checking on the other hand, it is generally not necessary that the data collected would enable to achieve the ultimate charging accuracy. The purpose is only to detect fraud and anomalies. As a simplified example, a charging algorithm for 'travelled distance' may use 1 position sample per second as input, while 1 sample per 30 s would be used as itinerary data for compliance checking. The itinerary data would in this case not allow reconstruction of the exact charge, but still be adequate to check against roadside observations, to check for consistency with items in the toll declaration and for internal consistency checks (does a set of itinerary records constitute a complete and possible trip section based on distance/time evaluations).

An important advantage of using a separate stream of data are that it provides the flexibility to forward or request the data only on a spot-check basis: the data are not needed for the primary process of calculating the charge. Compliance checking is typically done on a sample of the use of the tolled domain. The data are only required if a check is actually performed. For the TSP this means that itinerary records may – as an option – be kept on the OBE provided they are kept for sufficient time to be submitted on request. On the interface between TSP and TC it means that the level of detail in the toll declaration can be kept low, given that the TC may ask for details ('evidence') on a spot-check basis at a later point in time. In general, such mechanisms also provide more flexibility to comply with local privacy requirements: decentralization of data, automatic deletion after a certain amount of time has passed and access to details only in case of need.

We already have a standard for CCC. What does SM_CC add?

CEN/ISO 12813 specifies compliance checking communication for EFC systems based on autonomous OBE. CCC is intended to perform checks from the roadside, using DSRC communication, usually combined with vehicle (number plate) registration. The mode of use is therefore comparable to one of the SM_CC options, i.e. SM_CC_1. In the CCC transaction, the OBE indicates its status (OK or NOK), location and some additional data. To a certain extent this allows the TC to assess whether the OBE is operating properly. CCC has however some limitations where SM_CC provides additional assurance:

— In the CCC communication, the OBE will normally indicate that it is OK and send plausible position and time data. The TC can only believe this statement, as he has no independent means to verify that the OBE is working correctly and reporting charge data correctly. In other words the effectiveness of the check relies on the integrity of the OBE. In the concept of SM_CC_1, the basic assumption is that the OBE and its input cannot be trusted. Trust is only required for the aspect that the authenticator can only be generated by an authentic TR, and only over previously submitted itinerary data.

— With a roadside check based on CCC, there is no guarantee that the corresponding charge data are actually sent to the back end. Even if the OBE reports OK status and viable position data to the roadside, it may not report correct or complete charge data to the backoffice. With SM_CC_1 there is also no guarantee that the charge data are reported correctly and completely, but the backoffice has tools to make sure that itinerary records are reported completely and correctly. Any itinerary record that is sent to the RSE in the process of SM_CC_1, will also be available for the TSP (and TC). As a result of the freezing process, alteration or deletion of records can be detected. And finally, in the process of Checking of Toll Declarations, the consistency between Toll Declaration and itinerary data can be verified.

It is noted that SM_CC also offers modes of compliance checking where no DSRC communication is used. The scope of SM_CC is therefore broader than for CCC.

Will SM_CC replace CCC?

No. In the first place the use of SM_CC is a choice of the TC. Obviously, SM_CC has implications for the system and operations of the TC. Support for SM_CC will lead to additional development and costs that have to be justified by the expected benefits. Some TCs may decide that they do not (yet) need SM_CC and will continue to use CCC as the sole means for compliance checking.

A similar consideration is made by the TSP: if in a given interoperable domain there is no requirement from any of the TCs within the supported toll contexts, and the TSP has no business case for SM_CC for his own operations, he may choose not to use it.

It should be noted that a DSRC transaction in accordance with SM_CC_1 implies that the CCC-data are read out as well, see Annex C for examples.

E.3 SM_CC options

E.3.1 SM_CC_1

The process of itinerary freezing in real-time

The process of freezing in real-time is the basis of SM_CC_1. Figure E.1 illustrates the concept. The OBE generates data that are used for the charging process: time and position, possibly complemented with other data (from GNSS or sensors) and/or derived data from e.g. an on-board map, segment or object matching process. The idea of freezing in real-time is that a relevant subset of these data, an itinerary record, is periodically submitted to and ‘stamped’ by the Trusted Recorder. The TR generates a sequential number and freezes (produces an Authenticator over the data, a digital signature or a MAC) the submitted data. The Authenticator is stored as part of the itinerary record on the OBE.

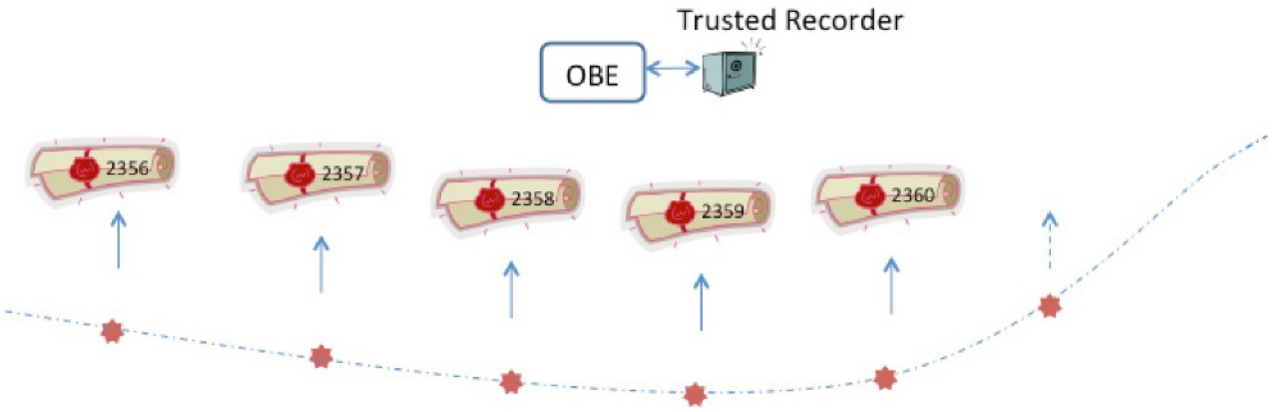

Figure E.1 — Illustration of the concept of itinerary freezing in real-time

As a result of this process:

— The content of the itinerary record cannot be changed without invalidating the Authenticator.

— Records cannot be deleted without trace: the toll domain counter value obviously allows detection of missing records.

Note that the freezing process does not guarantee that the contents of the itinerary records are correct. The GNSS input or the OBE itself may have been tampered with. The TR may even communicate with a fake OBE – it is assumed to have no means or intelligence to verify the source or content.

In other words: the freezing process provides reliable means to verify that itinerary data, which provide a reasonable indication of the chargeable road use, have not been changed or partially deleted afterwards. When changes are detected or data appear to be missing, this is a clear indication of equipment malfunction, sabotage or fraud.

Trust that the contents of the itinerary records are correct is also essential. This is where ‘observing the vehicle’ and ‘checking of itinerary freezing’ come in.

Observing the vehicle and checking of itinerary freezing

At certain points on the tolled network, the TC will use roadside compliance checking equipment to check passing vehicles. Such equipment may take the form of a fixed, gantry-mounted installation, temporary stationary installations or even mobile equipment operated from a moving vehicle.

The compliance checking equipment identifies the passing vehicle, usually using ANPR, and possibly determines other characteristics of the vehicle. (Almost) At the same time, SM_CC communication with the OBE mounted in the vehicle takes place via DSRC. In this exchange the compliance checking equipment retrieves the last (or at least a recently) frozen itinerary record. The itinerary record contains a time and position and other information relating to the chargeable road use. The roadside compliance checking process will primarily compare the position and time with the current time and location where the check takes place, as illustrated in Figure E.2.

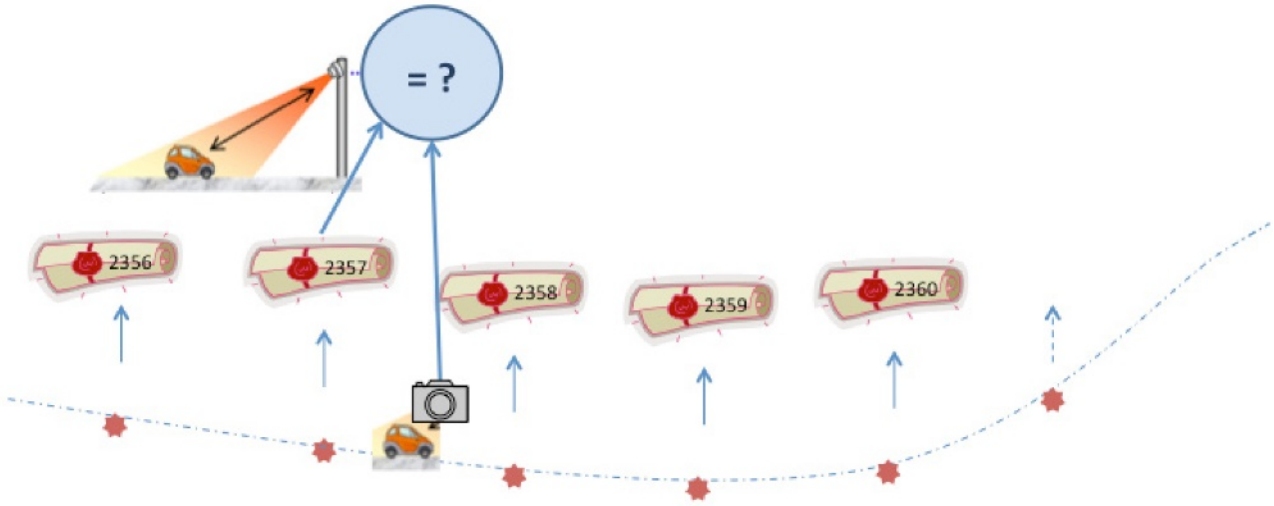

Figure E.2 — Illustration of the concept of checking of itinerary freezing in real-time

Taking into account that a record may be generated some time earlier (depending on the periodicity of the itinerary records as defined in the EFC Context Data), and allowing for some inaccuracy of the GNSS, the compliance checking algorithm will apply a certain threshold in time and place to determine whether the record is classified as OK or NOK. Image and DSRC-data pertaining to a check producing ‘OK’ can be deleted on the spot. In other cases a file is produced for follow-up, enforcement or otherwise.

It is obvious that roadside compliance checking is only done on a spot check basis. The number of itinerary records that are checked through this process is consequently only a very small fraction of all itinerary records produced. As was noted above, a manipulated or fake OBE may feed correct or incorrect data to the TR to produce a valid itinerary record. If a fraudulent SU would be able to programme his (fake) OBE in such a way that it feeds correct data to the TR in case of a roadside check, and incorrect data (leading to a lower charge)

everywhere else, he would easily avoid enforcement. This attack will not work however if - at the point that the record that will be sent to the RSE is submitted to the TR - the SU/OBE is not yet aware that the check is going to take place. This is meant with the requirement of '*unexpected observation*' in Table 1. With current state-of-the art it shall be assumed that RSE with ANPR cameras and DSRC can be observed from some distance. To counter the attack described, it is therefore to be arranged that the record used in the check, has to be created before the RSE would reasonably be possible to observe by an upcoming driver. Two mechanisms are helpful in this respect:

— The TR implements a time lock to frustrate attempts to freeze data at a (much) higher frequency than specified for normal use.

— The RSE is to be provided with an older than the last frozen record (this time offset T is specified in the EFC Context Data). This means the record that is evaluated is always created between T and T + the sampling interval before. Of course, the tolerances for the plausible time and position in the check have to be adapted accordingly.

It is noted that for effective checking, it is not necessary that all checks are unexpected. The business case for fraud may sufficiently be reduced if there is a considerable risk for the SU to detect the RSE too late.

Choice of a type of Itinerary Record

In the process described above only position and time are used for the check. The itinerary records contain other data that may or may not be used in the roadside check. For all toll contexts, the Context Independent Itinerary Record is suitable. Apart from the position and time, it includes the (Euclidian) distance between that position and the position in the previous itinerary record. It also includes the counter value of the Toll Domain Counter.

A TC may nevertheless prefer one of the context-dependent record types (CDIR) if the additional data that CDIR provides are deemed to increase the effectiveness of the checks. The preferred type of CDIR is to be specified in the EFC Context Data. In general, the use of CDIR requires a level of intelligence / toll-context specific data that cannot be assumed for all OBEs in an interoperable domain. As a consequence, the TC shall always be able to handle the CIIR as well.

Checking of Toll Declaration

Even if the checking of itinerary freezing in real-time is done intensively and fully effective in being 'unexpected', there is a need for another process called Checking of Toll Declaration. This is a result of the fact that the itinerary records are not directly used for calculation of the charge. The fraudulent SU / manipulated OBE may e.g. generate fully correct itinerary data and consequently all roadside checks may render the 'OK' result. Meanwhile the OBE may generate false charge data, leading to a false (lower) Toll Declaration.

Through the Checking of Toll Declaration process, the TC can therefore request the itinerary records that relate to the chargeable road use on which the Toll Declaration (or items of it) reports. The TC can consequently check if the Toll Declaration and the corresponding itinerary records are consistent. The concept is illustrated in Figure E.3.

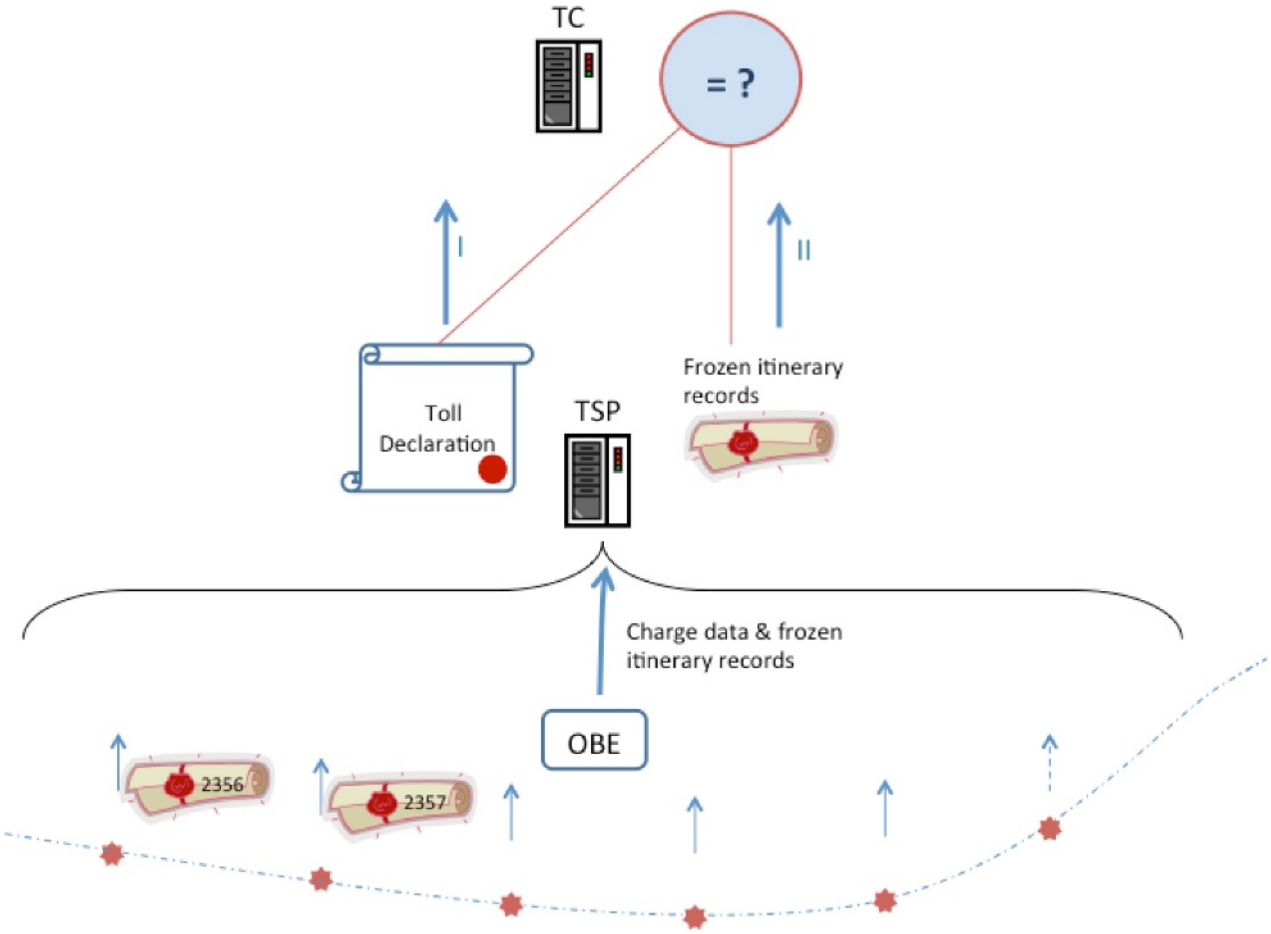

Figure E.3 — Illustration of the concept of checking of toll declaration

E.3.2 SM_CC_2

The process of itinerary freezing in real-time with a TR with a trusted time source

This process is similar to itinerary freezing in real-time as described for SM_CC_1. The main difference is that the timestamp in the itinerary records is – contrary to the process of freezing as described for SM_CC_1 – not submitted by the (in principle not trusted) OBE, but internally generated in the TR and can be trusted to represent the actual time of freezing. In other words, it is not possible (very difficult, not economically viable) to tamper with the timestamp in the record. This process of itinerary freezing is illustrated in Figure E.4.

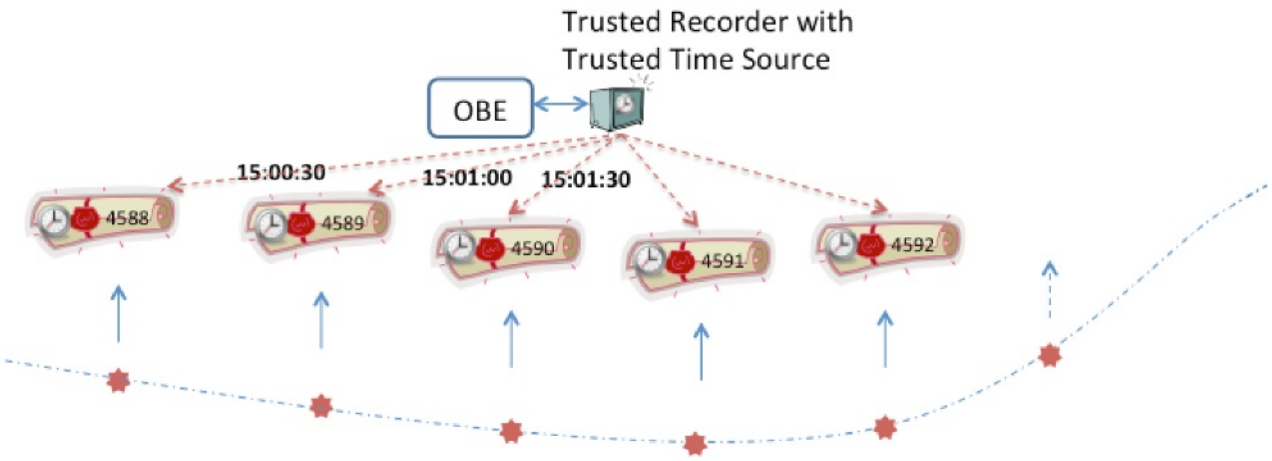

Figure E.4 — Illustration of the concept of itinerary freezing in real-time using a TR with trusted time source

Implementation

It is noted that a simple and suitable implementation for a TR with trusted time source is not known to exist today. SM_CC_2 should be regarded as a possibly interesting option in the future when such solutions might become available. Obviously, an externally powered chip card – the straightforward solution for a 'normal' TR – cannot feature a trusted time source. An integrated crystal oscillator is generally not able to keep accurate time over years without some form of external synchronisation. If external synchronisation is added to the solution, the authenticity of the external clock signal has to be verified by the TR and mechanisms are needed that eliminate the possibility of feeding a replayed or delayed signal.

Observing the vehicle and checking of itinerary freezing

Similar to SM_CC_1, an itinerary record is checked for consistency with a roadside observation of the passing vehicle. Because the timestamp can be trusted, it is possible to disconnect the retrieval of observation data with the retrieval of the itinerary record(s) used for the check. Consequently, it is possible to retrieve the itinerary record(s) through the Toll Service Provider.

First, the TC takes an image of passing vehicles on a selected location on the tolled network. The image is stored with date, time and location. As a next step the TC sends a specific request to the TSP of the SU to receive the records for that vehicle on a certain date and around a certain point in time. After reception of the itinerary record, the TC can check whether the location included in the itinerary record(s) is within a

reasonable range from the observation location. If the result is OK, no further action is required and the data can be deleted. The concept is illustrated in Figure E.5.

As to the effectiveness of the check, similar considerations apply as for SM_CC_1: *unexpected observations* are required. Also in this case, it is assumed that the OBE and thus the input to the TR can be tampered with. A main attack scenario is that correct input is provided to the TR in case a compliance checking observation is expected, and manipulated data are provided at all other points in time. This attack is rendered ineffective if there is a good chance that the SU/OBE is not aware that an observation is about to take place at the moment the itinerary record(s) that will later be compared to the observation data, is frozen.

It is noted that in order to request the itinerary records, the relevant TSP shall be found using the vehicle registration mark (number plate). This can be done through whitelisting of the vehicle registration marks or, alternatively, through an initial request addressed to all possible TSPs. Of course there is no guarantee that there is a valid contract for this vehicle with any of the TSPs. Therefore, occasional CCC or DSRC-based SM_CC might add value to the effectiveness of enforcement, as it allows identification of a vehicle without OBE/valid contract in real-time.

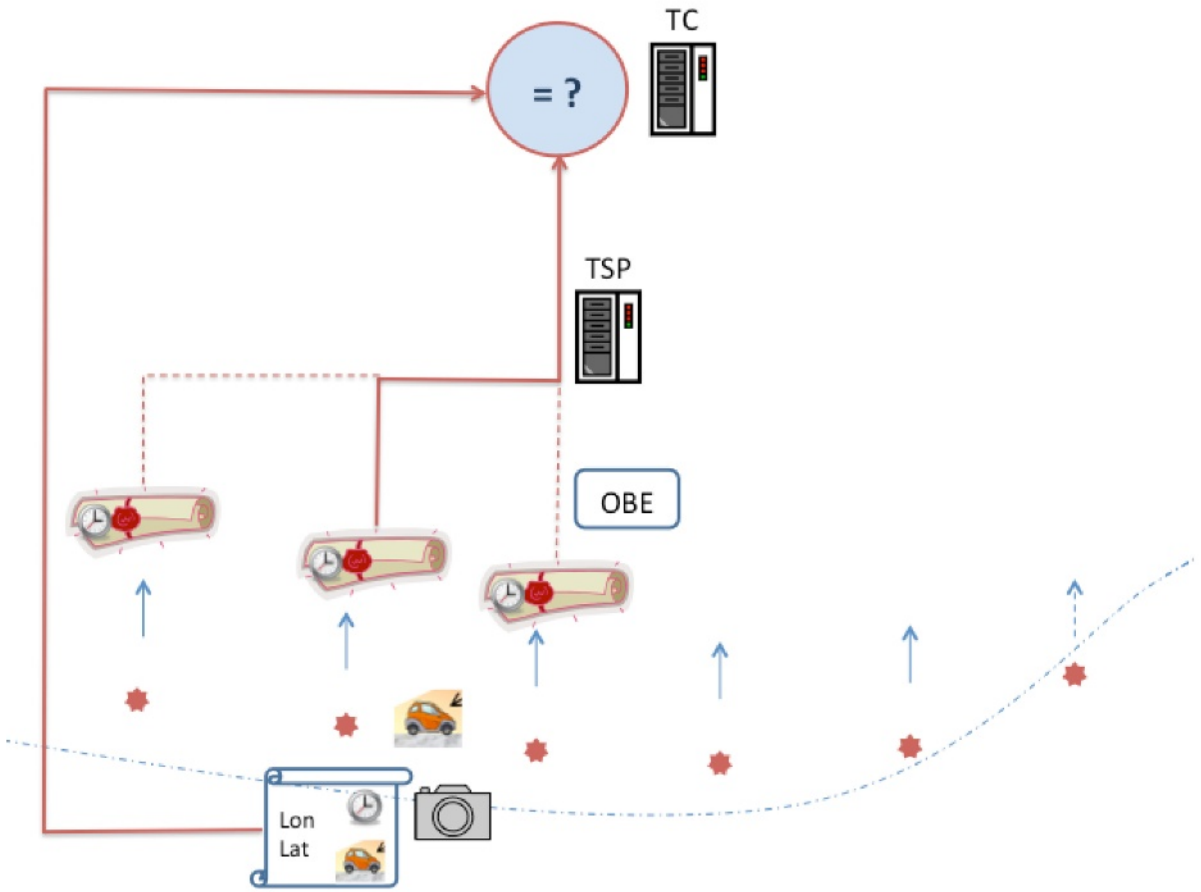

Figure E.5 — Illustration of the concept of delayed checking of itinerary freezing using a TR with trusted time source

Checking of Toll Declaration

Checking of Toll Declaration is needed as a complementary process. This process is the same as described in Checking of Toll Declaration for SM_CC_1.

E.3.3 SM_CC_3a

The process of itinerary freezing per declaration

In this case, just as for SM_CC_1 itinerary records are generated by the OBE. The main difference is that no Trusted Recorder is used and the records cannot be frozen by the OBE. The OBE sends the itinerary records to the TSP. When sending a (signed) Toll Declaration to the TC, the TSP includes a hash over the itinerary records that correspond to the Toll Declaration. From that point the itinerary records can be considered frozen: changing or deleting records will lead to another hash. The TC can detect such change when subsequently retrieving itinerary records (on request). The concept is illustrated in Figure E.6.

For simplicity, the description above does not include the complexity of the two-level freezing which is specified in Clause 6.

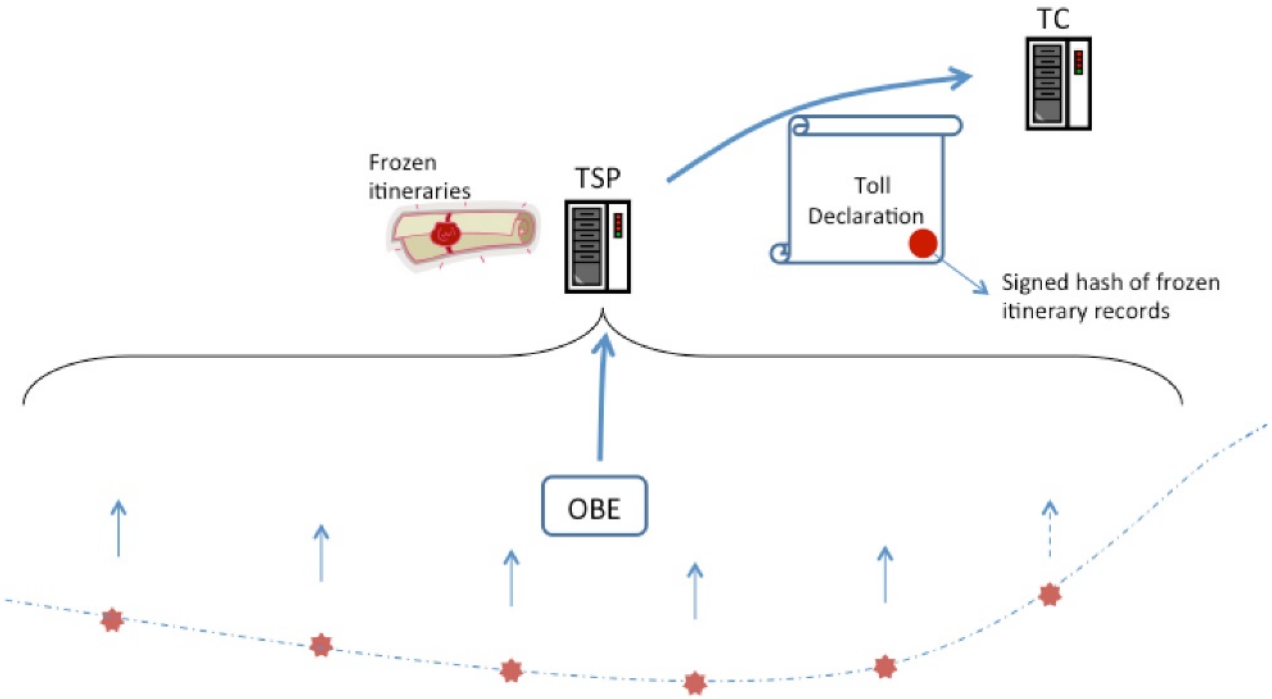

Figure E.6 — Illustration of the concept of freezing per declaration

Observing the vehicle and checking of itinerary freezing

The concept is illustrated in Figure E.7. The TC captures an image of a passing vehicle on a selected location on the tolled network. The image is stored with date, time and location. The TC now waits for the Toll Declaration from the corresponding TSP.

Once the Toll Declaration is received by the TC, the TSP is committed to the complete set of underlying itinerary records through the included hash, even if the itinerary records are not included. It is noted that the hash in the Toll Declaration connects to the underlying itinerary batches.

As a next step the TC sends a specific request to the TSP to receive a set of itinerary records for that vehicle (based on its vehicle registration mark), on a certain date and around a certain point in time. After reception of the itinerary records, the TC can check whether at the recorded time of observation, a matching record is included in itinerary record(s), i.e. within a reasonable range from the observation location. Some other data may be checked, depending on the type of itinerary record. If the result of the check is OK, no further action is required and the data can be deleted.

Just as described for the other SM_CC options, it is considered of importance for the effectiveness of the check that neither the SU nor the TSP are in a position to submit correct itinerary data for freezing *only* at the moments/locations where a roadside observation takes place. With freezing per declaration, the SU is still able to modify records until the itinerary data are sent to the TSP and the TSP is even able to modify itinerary records without detection until the Toll Declaration is sent to the TC. It can be concluded that a requirement for an effective check is in this case that the SU and the TSP do not know where roadside observations have taken place. The condition for effectiveness is therefore: *undetected observations* – neither known before nor after the observation took place. The observation should be undetected by SUs as well as by the TSP.

Undetectable observations equipment may be difficult to achieve with current state-of-the-art technology. ANPR-cameras cannot yet be fit in miniature housings and require good line of sight to the vehicle's number plate. It can be expected that the sizes will further reduce in the future, making discovery more and more challenging. Another factor that may help to make 'undetected observations' a feasible concept is the increase in the number of cameras at the roadside that are installed for other purposes: if the fraudulent SU has no clue which of the cameras is used for EFC compliance checking he would have to produce truthful itinerary records around any camera encountered. This would obviously make the task of creating false itineraries more difficult and less profitable. Another relevant development is the progress of real-time traveller information services. Just as for speed traps downstream, motorists / in-vehicle equipment may receive information on locations of EFC compliance checks. This may lead to a situation where undetected observations will only be feasible with mobile or transportable equipment that is moved around regularly.

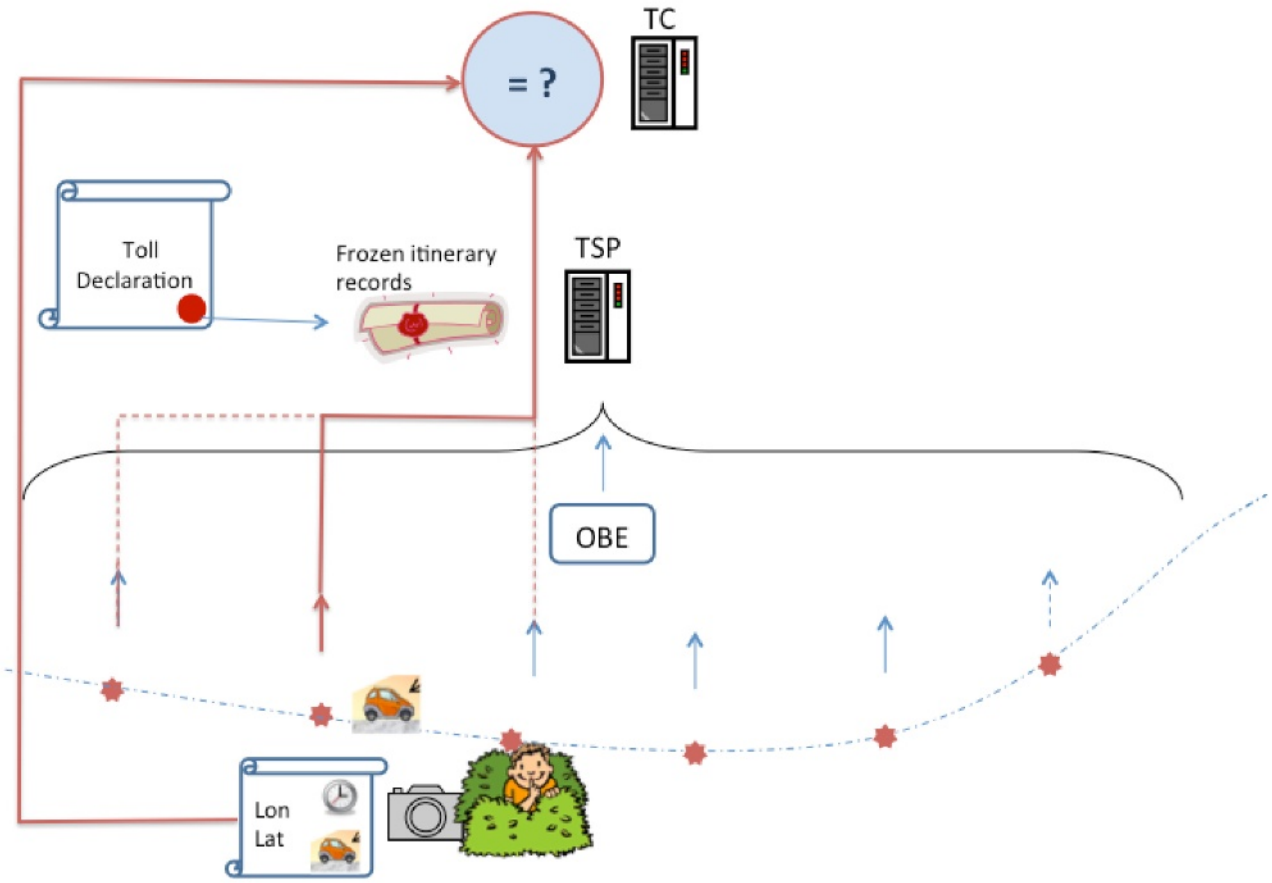

Figure E.7 — Illustration of the concept of checking of itinerary freezing in case of itinerary freezing per declaration

Checking of Toll Declaration

Checking of Toll Declaration is needed as a complementary process. This process is similar to SM_CC_1 regarding purpose and effect. Note that – in comparison with freezing in real-time as used in SM_CC_1 and SM_CC_2, there are differences in the implementation of the two-level freezing mechanism.

E.3.4 SM_CC_3b

The process of itinerary freezing

Also in this option, freezing per declaration is applied. The process is as illustrated in Figure E.6 and as described in the previous section. The only difference is the frequency of Toll Declarations. In this scenario it is assumed that the OBE uploads itinerary and charge data in (almost) real-time through the mobile network. In addition, the TSP is supposed to submit Toll Declarations with minimal delay to the TC.

Observing the vehicle and checking of itinerary freezing

The process is essentially similar to SM_CC_3a. However, because the TC receives the declaration in almost real-time, the TSP, SU and the OBE do not have the opportunity to modify an itinerary record after noticing that an observation for compliance checking took place – as the corresponding itinerary batch is already committed to. The situation is somewhat comparable to SM_CC_1. If the OBE is not yet able to detect the upcoming check at the point where the itinerary batch relevant for the check is frozen, the condition for

effectiveness is satisfied. In this case, freezing means that the itinerary data are sent to the TSP back-office *and* the corresponding Toll Declaration is sent to the TC. It is concluded that *unexpected observations* are required, but undetected observations are not necessary.

It is emphasised that in this scenario the requirements on the frequency and speed of declarations are high.

E.4 Managing multiple toll domains

E.4.1 Overlapping toll domains

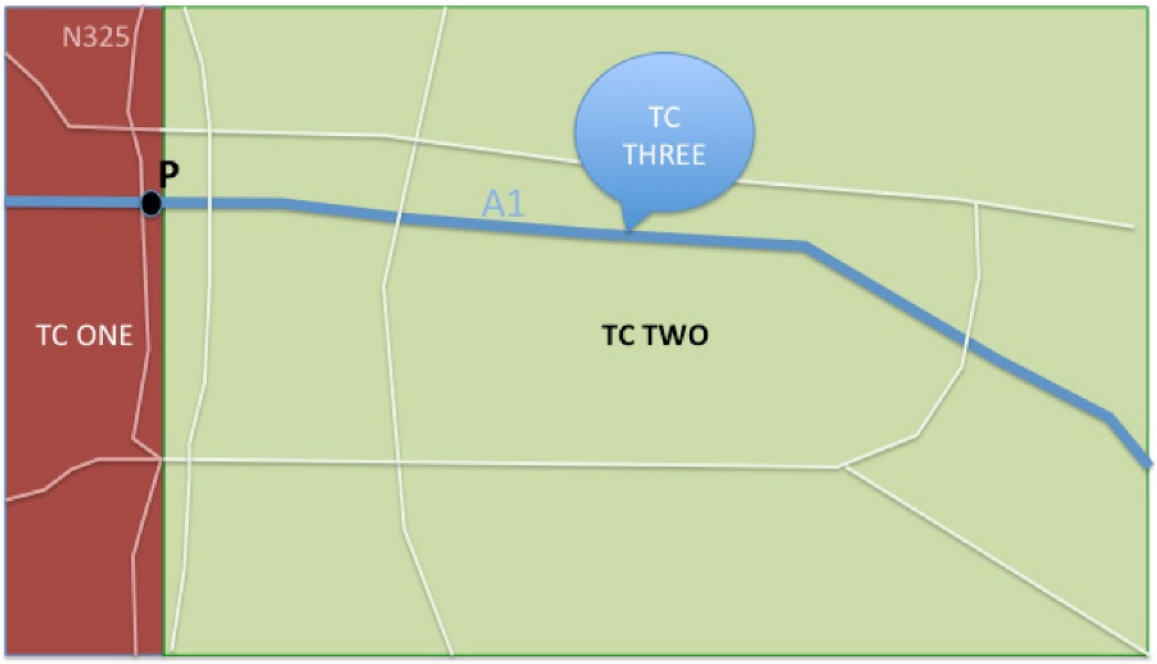

Figure E.8 — Illustration of neighbouring and overlapping toll domains

It is undesirable both from a privacy and commercial point of view, that a TC would have unrestricted access to itinerary data relating to travel in the domain of other TCs. For that reason an identification of the toll domain is included in the itinerary record which allows to sort and allocate the records. It is also important that a TC can easily verify that no itinerary records were deleted or left out. This is achieved with a sequence number (the toll domain counter) using a secure counter in the TR. Combining the two requirements, the straightforward solution is a separate counter per toll domain. This solution is specified in SM_CC. Some specific behaviour is required for situations of overlapping toll domains or where the determination of the toll domain cannot be done by the OBE with high reliability. This is addressed in the following paragraphs.

Using toll domain counters simultaneously

In case of freezing in real-time, the toll domain (and the corresponding toll domain counter) has to be determined by the OBE. As a minimum, it is required that a rudimentary definition of the geographic toll domains is present in the OBE. Depending on the front end of the TSP however, the OBE may not have a detailed definition of the tolled road network or of the boundaries between domains of different TCs. As a result, determining the toll domain is not unambiguous under all circumstances. See Figure E.8: when a vehicle travelling on the N325, the OBE might be able to determine that the vehicle is travelling in the domain of TC ONE or TC TWO domain, but not with sufficient probability which of the two. In such cases, the OBE shall create records for both domains, using the corresponding toll domain counters. Another example is the situation near point P. Main road A1 is surrounded by the ONE and TWO domains, but operated by TC THREE. The OBE may not be able to tell in which domain the vehicle is travelling. To make sure that each TC can be provided with the records they might ask for, itinerary records are created for the ONE, TWO and THREE domain.

It is noted that apart from the situation described above, where the toll domain boundary definitions in the OBE are not sufficiently precise to allocate the itinerary record with certainty, the simultaneous creation of records for different domains also applies when:

— Toll domains are actually overlapping (as could e.g. be the case with domains TWO and THREE in the figure). In this case records for both TCs should be created anyway.

— Roads in adjacent toll domains are very close, and back office functionality (e.g. complex map matching or use of trip logic) is required to match the trip to the right road segment with sufficient reliability. Also in this case both (or each of the) TCs should receive itinerary records.

A maximum of 4 simultaneous toll domain counters

In the previous paragraph it was discussed that under certain circumstances it is needed to generate itinerary records for different toll domains simultaneously. In such cases mostly two toll domains will be involved. An example was also given for three toll domains. The SM_CC specification limits the number of simultaneous toll domain counters to 4.

This limitation is driven by the constraints of the available bandwidth on the DSRC interface: in order to keep the GET.response with the requested itinerary record (e.g. CiirRtf or CdirEventsRtf), within the maximum frame size of 128 bytes, a maximum of 4 **tollDomainCounters** (each including the toll context identification and the counter value) can be included. This is regarded sufficient for all cases that might occur in practice.

Harmonization of real-time freezing parameters between adjacent domains

A limitation is that on the DSRC interface there is only one itinerary record available of a certain type, although it may include up to 4 **tollDomainCounters.** As a consequence, all involved TCs have to be able to handle the record when applying SM_CC_1. Therefore, in situations where records are frozen for more than one domain simultaneously, some harmonization between the respective TCs is required. The relevant parameters are the *freezing interval* and the *minimum delay* for the record to be available on the DSRC interface (see discussion on unexpected observation in E.3.1). Both parameters depend on the selected compliance checking strategy of the TC, influenced by the specifics of the toll domain. The following default rules can be used for the situation in which itinerary records are created for more than one toll domain at the same time:

— The OBE uses the highest frequency (shortest interval) of all of the involved toll domains.

— The OBE uses the longest minimum delay of all of the involved toll domains.

If needed, other approaches can be agreed between adjacent TCs and the involved TSPs in specific cases.

It is noted that the need for harmonization will always apply to the CiirRtf, as the RSE shall always be capable to handle this type of record. Recall that some TCs/OBEs may only support this type of itinerary record. It may

also apply to one of the context-dependent itinerary record types, in case more than one of the TCs in an ‘area of overlap’ use this type of itinerary record.

E.4.2 The ‘catch-all’ toll domain counter

As a starting point, each toll context has an own toll domain counter. As discussed above this is a solution to limit the access of TCs to the detailed travel data only in (or near to) their toll domain, while at the same time providing a straightforward mechanism to verify the completeness of relevant itinerary records.

In this Technical Specification it is stated that a minimum number of 10 toll domain counters is to be supported. However, the number of different toll contexts in an interoperable domain could possibly be much larger, e.g. considering the scope of the EETS. A low-cost chip card solution for a TR has limitations in available user memory. It is also kept in mind that a TR is required to have a long life cycle, and counters may have to incremented millions of times. In order to avoid wear-out of memory cells, memory management techniques may be needed that multiply the memory requirement. As a consequence, the number of counters available in a TR implementation may not be sufficient for the number of toll contexts to be supported. We note that there is a general trend of smaller and cheaper memory, and it will also take some time before interoperable domains with large numbers of TCs using SM_CC will be a reality. It is therefore not certain that the problem will occur in practice. Anyhow, a work-around is available in the form of a ‘catch-all’ toll domain counter.

When using the ‘catch-all’ toll domain counter mechanism, one of the counters is allocated for shared use. It is sensible to use this counter for the domains that are likely to be used only scarcely (for a given group of OBEs or users, depending on their location of issue or expected usage characteristics). If the vehicle is travelling in a domain that is allocated to the ‘catch-all’ counter, itinerary records will be generated using this counter. The itinerary data are available for all TCs that share this counter. This implies a compromise with the privacy requirement that a TC only has access to detailed data he actually needs for his operations. Privacy risks may be acceptable if the mechanism is indeed only used for rare cases.

Annex F
(informative)

Use of this Technical Specification for the EETS

F.1 General

In 2004 an EU Directive 2004/52/EC of the European parliament and of the council “on the interoperability of electronic road toll systems in the community” was adopted. This EU-Directive calls for the establishment of a European Electronic Toll Service (EETS).

In 2009 an EC-decision 2009/750/EC “on the definition of the European Electronic Toll Service and its technical elements” was adopted. It sets out the necessary technical specifications and requirements for that purpose, and contractual rules relating to EETS provision. The decision lays down rights and obligations on EETS Providers, Toll Chargers and EETS Users.

NOTE Other requirements and other EU Directives may be applicable to the product(s) falling within the scope of this technical specification.

F.2 Overall relationship between European standardization and the EETS

The EU Directive 2004/52/EC also triggered the establishment of a standardization mandate (M/338, “Standardisation mandate to CEN, CENELEC and ETSI in support of Interoperability of electronic road toll systems in the Community”) that called for development of technical standards in support of the EETS. Activities under m/338 is supervised by the “ITS co-ordination group” (ITS-CG, previously ICTSB/ITSSG).

The M/338 does not explicitly call for the provision of harmonised standards (according to Directive 98/34/EC on the new approach to technical harmonization and standards), which means that this possibility is not available for the European standards that are developed in support of the EETS. Instead, this brief informative annex provides an outline how this standard could be used in the context of the EETS.

EC-Decisions can point out the use of specific standards, even if they are not formally harmonised. This is also done in EC-decision 2009/750/EC for a few standards (i.e. those that were available at the time of its approval). In case there will be more EC-decisions in support of the EC-Directive, further European standards could be referenced there as well.

The European Commission has also published in 2011 a “Guide for the Application of Directive on the Interoperability of Electronic Road Toll Systems ” (ISBN 978-92-79-18637-0). This guide is intended to be a reference manual for all parties directly or indirectly concerned by Directive 2004/52/EC and Decision 2009/750/EC. It aims at providing help for the implementation of the EETS, including a list of standards that might be of use. The guide is only informative (e.g. the document cannot notify certain standards as “mandatory” for use in the EETS) and is intended to be updated on regular basis.

F.3 European standardization work supporting the EETS

Many of the standards developed by CEN/TC278 have been drafted with the EETS-requirements in mind (including the use of the results from European projects such as CARDME, PISTA, CESARE and RCI). CEN-representatives have also taken part as observers in working groups etc. initiated by the EC for the EETS. Hence, some work has been done in close co-operation between CEN working groups and the EC.

It should be noted that no CEN/ISO standards are “turnkey” solutions for the EETS. They are to be used as “building blocks” for the EETS, supporting the EETS legal framework and agreements between the parties

concerned by the EETS. A precise EETS-specification is not within the scope of CEN/ISO standards, but remains that task of the owners of the EETS-scheme.

It should also be noted that CEN/ISO has a wider scope than the EETS, which is a complementary service to the national services of the Members States and optional for the users, whereas CEN/ISO standards should be applicable to all EFC-services worldwide.

F.4 Correspondence between this technical specification and the EETS

This technical specification defines technical requirements that correspond to the requirements being listed in EC-decision 2009/750/EC, as indicated in Table F.1 below.

Table F.1 — Technical requirements of SM_CC in relation to 2009/750/EC

Clause(s) / sub-clause(s) of this TS	**Essential Requirements (ERs) of EC Decision 2009/750/EC**	**Qualifying remarks/Notes**
5.2, 5.4, 5.5, 6.3, 6.4, 6.5	Annex III, Article 2.1.1.3	SM_CC defines a means for EETS Providers to provide secured information for enforcement to Toll Chargers via two interoperable communication channels, namely one based on CEN DSRC according to the EN 15509 protocol, and one based on the interoperable back-office interface definition according to EN ISO 12855.
5.2, 5.4, 5.5, 6.3, 6.4, 6.5	Annex III, Article 2.1.1.4	SM_CC defines a mechanism for Toll Chargers to detect if a vehicle is actually equipped with a validated and properly functioning EETS OBE providing truthful information.
6.3.3, 6.4	Annex III, Article 2.1.1.5	SM_CC defines a mechanism for Toll Chargers to identify the responsible EETS Provider.
5, 6, 7 (1.3)	Annex III, Article 2.1.1.6	EETS equipment implementing SM_CC is designed utilising open standards.
(0.4), 5.3, 5.4, 5.5, 6.3, 6.4, 6.5	Annex III, Article 2.2	SM_CC provides the Toll Charger and EETS Provider with a means to check users thereby minimizing the processing of data in accordance with Directive 95/46/EC.

Bibliography

[1] ISO/IEC 9646-7, *Information technology — Open Systems Interconnection — Conformance testing methodology and framework — Part 7: Implementation Conformance Statements*

[2] ISO/IEC/TR 10000-1:1998, *Information technology — Framework and taxonomy of International Standardized Profiles — Part 1: General principles and documentation framework*

[3] ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

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

[5] ISO 17573:2010, *Electronic fee collection — Systems architecture for vehicle-related tolling*

[6] CEN ISO/TS 17444-1, *Electronic fee collection - Charging performance - Part 1: Metrics (ISO/TS 17444-1)*

[7] ISO/IEC 19505-1:2012, *Information technology — Object Management Group Unified Modeling Language (OMG UML) — Part 1: Infrastructure*

[8] ISO/IEC 19505-2:2012, *Information technology — Object Management Group Unified Modeling Language (OMG UML) — Part 2: Superstructure*

[9] FprCEN/TS 16702-22, *Electronic Fee Collection – Secure Monitoring for autonomous toll systems – Part 2: Trusted Recorder*

[10] IEEE 1609.11 *IEEE Standard for Wireless Access in Vehicular Environments (WAVE) — Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transportation Systems (ITS)*

[11] FIPS PUB 180-4, March 2012, Secure Hash Standard (SHS)

[12] FIPS PUB 186-3, June 2009, Digital Signature Standard (DSS)

[13] IETF RFC 4648, October 2006, The Base16, Base32, and Base64 Data Encodings

[14] IETF RFC 5280, January 2013, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[15] FprCEN ISO/TS 19299 Electronic Fee Collection – Security Framework

[2] WI00278338 under development

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™