PD CEN/TS 16702-2:2015

BSI Standards Publication

Electronic fee collection — Secure monitoring for autonomous toll systems

Part 2: Trusted recorder

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of CEN/TS 16702-2:2015.

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.

Published by BSI Standards Limited 2015

ISBN 978 0 580 87284 6
ICS 03.220.20; 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 April 2015.

Amendments/corrigenda issued since publication

Date	Text affected

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 16702-2

March 2015

ICS 03.220.20; 35.240.60

English Version

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

Perception du télépéage - Surveillance sécurisée pour systèmes autonomes de péage - Partie 2: Enregistreur fiabilisé

Elektronische Gebührenerhebung - Sichere Überwachung von autonomen Mautsystemen - Teil 2: Zuverlässige Datenaufzeichnung

This Technical Specification (CEN/TS) was approved by CEN on 19 January 2015 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

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

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

Ref. No. CEN/TS 16702-2:2015 E

Contents

Page

Foreword

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

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to announce this Technical Specification: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Introduction

The widespread use of tolling requires provisions for users of vehicles that are roaming through many different toll domains. Users should be offered a single contract for driving a vehicle through multiple toll domains and those vehicles require onboard equipment (OBE) that is interoperable with the toll systems in these toll domains. Thus, there is a commercial and economic justification both in respect of the OBE and the toll systems for enabling interoperability. In Europe, for example, this need has been officially recognized and legislation on interoperability has been adopted (see directive 2004/52/EC) and the associated commission decision.

The Technical Specification “Electronic fee collection – Security framework” (CEN/TS 16439) provides an overview of general security requirements of the stakeholders and provides a comprehensive threat analysis for the assets in an interoperable EFC scheme. A number of identified threats may result into less revenue of the Toll Charger, undercharging and/or not meeting required service levels between the Toll Service Provider and the Toll Charger. Some of these threats can be eliminated by implementing the security measures specified in CEN/TS 16439. However, most of the security measures necessary to combat the identified threats are to be addressed and specified in other standards.

One example of threats that cannot be mitigated by security measures specified in CEN/TS 16439 concerns the trustworthiness of Toll Declarations in autonomous toll systems. Toll declarations are statements that a vehicle has been circulating in a particular toll domain within a particular time period. In autonomous toll systems, the circulation of vehicles is measured by Toll Service Providers, using GNSS-based OBE. Toll service providers then send Toll Declarations to the Toll Charger, based on which the Toll Charger will charge the Toll Service Provider. The correctness and completeness of these declarations is obviously of paramount interest to Toll Chargers, Toll Service Providers and users alike.

The secure monitoring compliance checking concept provides a solution that allows a Toll Charger to check the trustworthiness of the Toll Declarations from a Toll Service Provider, while respecting the privacy of the user. This concept is defined in two Technical Specifications. CEN/TS 16702-1:2014 “Secure monitoring for autonomous toll systems – Part 1: Compliance checking” gives the full description of the secure monitoring compliance checking concept. The current Technical Specification, CEN/TS 16702-2 “Secure Monitoring for autonomous toll systems – Part 2: Trusted recorder” defines the Trusted Recorder, a secure element required for some of the different types of secure monitoring compliance checking defined in CEN/TS 16702-1:2014.

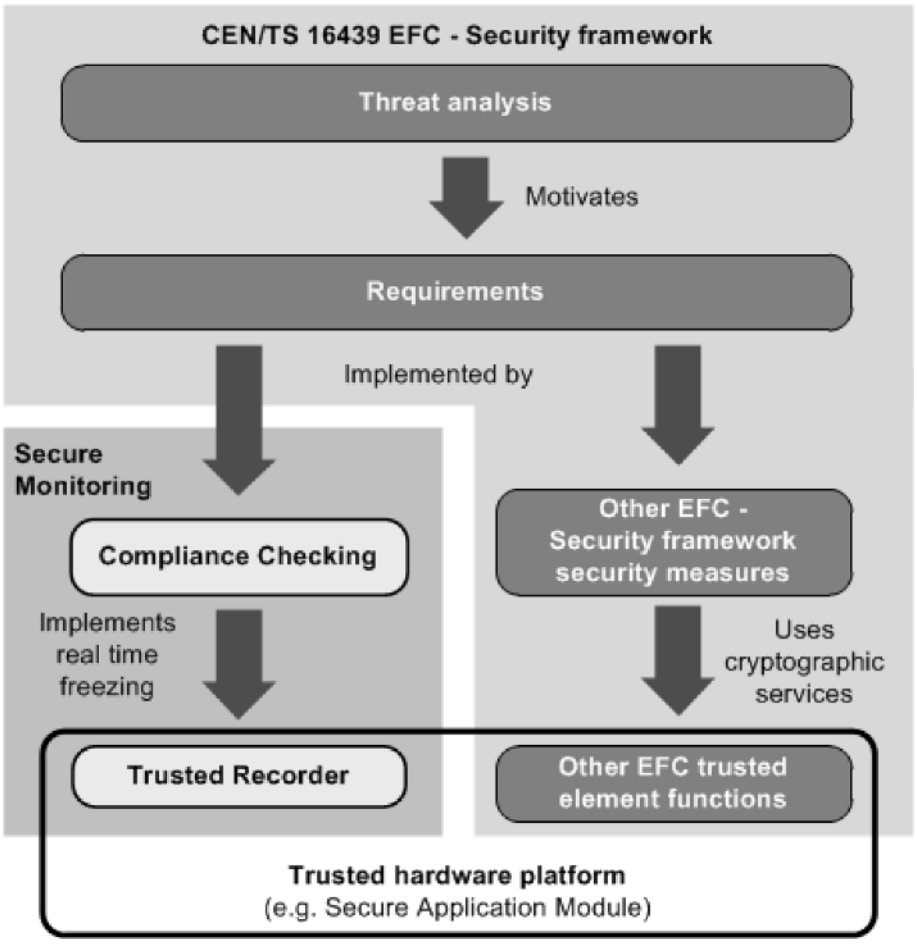

Figure 1 — Relation between EFC - Security framework and the overall secure monitoring concept

Figure 1 shows the relations between the CEN/TS 16439 EFC Security Framework and EFC Secure monitoring for autonomous toll systems, i.e. the two parts Compliance Checking and Trusted Recorder. The threat analysis in the Security Framework motivates the security requirements of an EFC system. The requirements are implemented and fulfilled by several security measures. One of these measures is Secure Monitoring, specified in “Secure Monitoring for autonomous toll systems – Part 1: Compliance checking”. The “Secure Monitoring for autonomous toll systems – Part 2: Trusted Recorder” specifies the cryptographic services necessary for the secure monitoring compliance checking concept.

Figure 1 indicates also that a Trusted Recorder will most likely be implemented on trusted hardware, e.g. on Secure Application Module (SAM), inside the OBE or on a general trusted platform of a vehicle. Such a trusted device could support more functions, which may be required for EFC or other services.

1 Scope

This Technical Specification defines the requirements for the Secure Application Module (SAM) used in the secure monitoring compliance checking concept. It specifies two different configurations of a SAM:

— Trusted Recorder, for use inside an OBE;

— Verification SAM, for use in other EFC system entities.

The Technical Specification describes

— terms and definitions used to describe the two Secure Application Module configurations;

— operation of the two Secure Application Modules in the secure monitoring compliance checking concept;

— functional requirements for the two Secure Application Modules configurations, including a classification of different security levels;

— the interface, by means of transactions, messages and data elements, between an OBE or Front End and the Trusted Recorder;

— requirements on basic security primitives and key management procedures to support Secure Monitoring using a Trusted Recorder.

This Technical Specification is consistent with the EFC architecture as defined in ISO 17573 and the derived suite of standards and Technical Specifications, especially CEN/TS 16702-1:2014 and CEN/TS 16439.

The following is outside the scope of this Technical Specification:

— The life cycle of a Secure Application Module and the way in which this is managed.

— The interface commands needed to get a Secure Application Module in an operational state.

— The interface definition of the Verification SAM.

— Definition of a hardware platform for the implementation of a Secure Application Module.

2 Normative references

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

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

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

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

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

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

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

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

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

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

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

ISO/IEC 19790:2012, *Information technology — Security techniques — Security requirements for cryptographic modules*

FIPS PUB 140-2, December 2002, *Security requirements for cryptographic modules*

Common Criteria Protection Profile BSI-PP-0035, 2007, *Security IC Platform Protection Profile, Version 1.0*

3 Terms and definitions

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

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

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

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

Note 1 to entry: In this CEN/TS either a MAC or a signature.

3.3
authenticity
property that an entity is what it claims to be

[SOURCE: ISO/IEC 27000:2009, 2.6]

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

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

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

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

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

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

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

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

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

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

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

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

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

[SOURCE: CEN/TS 16439:2013]

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

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

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

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

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

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

[SOURCE: ISO 17573:2010, 3.9]

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

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

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

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

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

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

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

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

[SOURCE: ISO 17573:2010, 3.16]

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

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

[SOURCE: ISO 17573:2010, 3.18]

3.24
toll domain ID
unique identifier of a toll domain

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

[SOURCE: ISO 17573:2010, 3.22]

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

[SOURCE: ISO 17573:2010, 3.23]

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

[SOURCE: ISO 17573:2010, 3.24]

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

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

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

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

[SOURCE: ISO 17573:2010, 3.29]

3.31
Verification SAM
Secure Application Module capable of providing cryptographic services to verify a Trusted Recorder MAC in such manner that the proof of non-repudiation is given

4 Symbols and abbreviations

ADU	Application Data Unit
AES	Advanced Encryption Standard (ISO/IEC 18033-3:2010)
BCD	Binary Coded Decimal
CA	Certification Authority
CLA	Class byte
CMAC	Cipher-based MAC
ECC	Elliptic Curve Cryptography

ECDSA	Elliptic Curve Digital Signature Algorithm
EETS	European Electronic Toll Service
ID	Identifier
INS	Instruction byte
KVC	Key Verification Code
MAC	Message Authentication Code
NTP	Network Time Protocol
OBE	On-Board Equipment
P1, P2	Parameter bytes
PKI	Public Key Infrastructure
PP	Protection Profile
RQ	Requirement
RSA	Algorithm for public-key cryptography (Rivest, Shamir and Adleman)
RSE	Roadside Equipment
SAM	Secure Application Module
SNTP	Simple Network Time Protocol
TC	Toll Charger
TDC	Toll Domain Counter
TR	Trusted Recorder
TRID	Trusted Recorder Identifier
TSP	Toll Service Provider
TTP	Trusted Third Party
TTS	Trusted Time Source
UTC	Coordinated Universal Time

5 SAM concept and scenarios

5.1 General

CEN/TS 16702-1:2014 defines requirements for a Trusted Recorder used in an OBE supporting symmetric and asymmetric algorithms. A Verification SAM (for example in the RSE) is required to achieve the same cryptographic proof of non-repudiation when using the symmetric algorithm compared to the asymmetric algorithm. 5.2 of this Technical Specification is describing the two different configurations of the Secure Application Module in the EFC context.

5.3, 5.4 and 5.5 describe the scenarios for the use of the TR and Verification SAM, motivated by CEN/TS 16702-1:2014. The scenarios in these clauses cover all possible use cases for both SAM configurations, a TR inside an OBE and a Verification SAM used in the RSE or another EFC entity.

NOTE Names and data flow elements in the diagrams in Clause 5 are symbolic and do not always give all details. For details, refer to Clause 7.

5.2 The concepts of TR and Verification SAM

The Trusted Recorder is intended for the use inside OBE. The TR is responsible for freezing itineraries by calculating an authenticator over each itinerary. This Technical Specification additionally defines the requirements for a Verification SAM, which shall be used in other EFC system entities, for example in the RSE, the TSP back office or the TC back office. The Verification SAM is responsible for the verification of symmetric authenticators over itineraries, calculated by Trusted Recorders inside OBE.

The Trusted Recorder used in OBE is a logical entity with certain security functions to support the secure monitoring compliance checking concept. If properly used, the Trusted Recorder and - if required - the Verification SAM will ensure the authenticity, integrity and non-repudiation of data produced in OBE and/or a Proxy implementing the secure monitoring compliance checking concept.

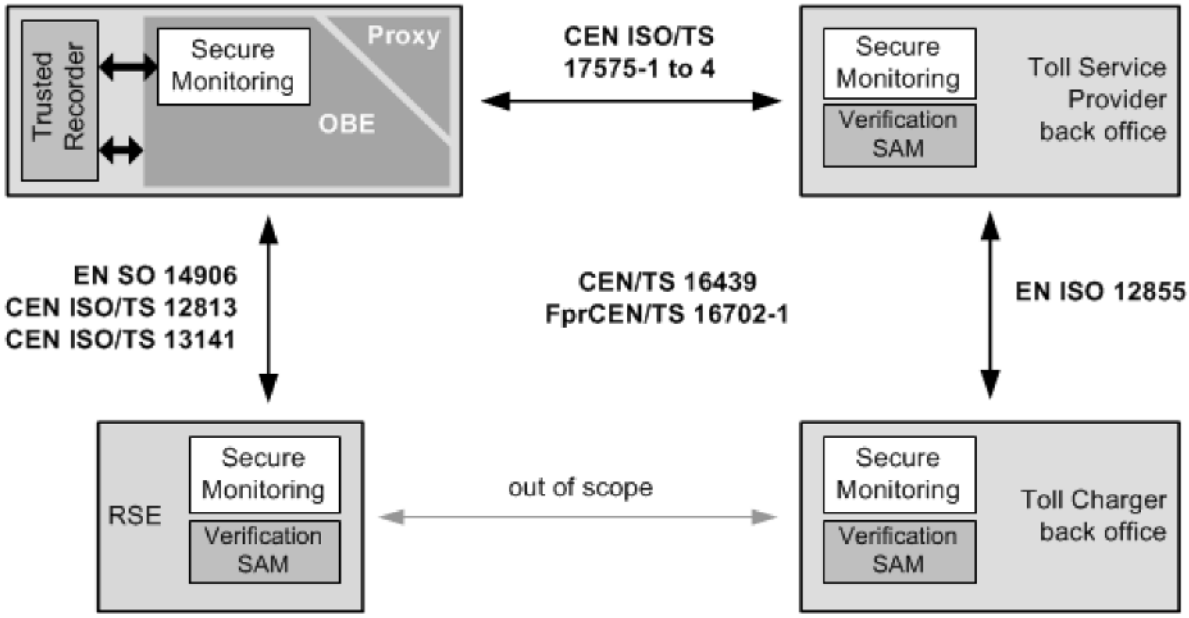

Figure 2 —Entities, standards/TS and interfaces in the context of secure monitoring compliance checking

Figure 2 shows the entities relevant in the context of EFC and the link between the Trusted Recorder, the Verification SAM and other entities and their interfaces and transactions.

Depending on its configuration (see Table 1 in 6.1.1), based on the requirements of the supported toll schemes, a Trusted Recorder provides some or all of the following features:

— data authenticity and data integrity based on asymmetric (signature) or symmetric (MAC) cryptographic algorithms;

— a Signing Time Lock to avoid that the OBE sends a request to authenticate data only in the event of an external observation by the Toll Charger;

— storage and management of counters, to ensure a correct sequence of itineraries and detect missing itineraries;

— secure storage and management of cryptographic keys.

NOTE 1 These capabilities are necessary for supporting the SM_CC-1 type of secure monitoring compliance checking defined in CEN/TS 16702–1, 0.3.

The Trusted Recorder optionally provides:

— trusted time information.

NOTE 2 This capability is necessary for supporting the SM_CC-2 type of secure monitoring compliance checking defined in CEN/TS 16702–1, 0.3.

The Verification SAM provides one specific function for the secure monitoring compliance checking concept. This is the verification of symmetric authenticators.

5.3 Scenarios for a Trusted Recorder

5.3.1 General

This clause defines the scenarios valid for a Trusted Recorder used inside OBE in a vehicle.

5.3.2 Real-Time Freezing without using a Trusted Time Source

The Trusted Recorder may be used for real-time freezing of itineraries using symmetric cryptography or asymmetric cryptography.

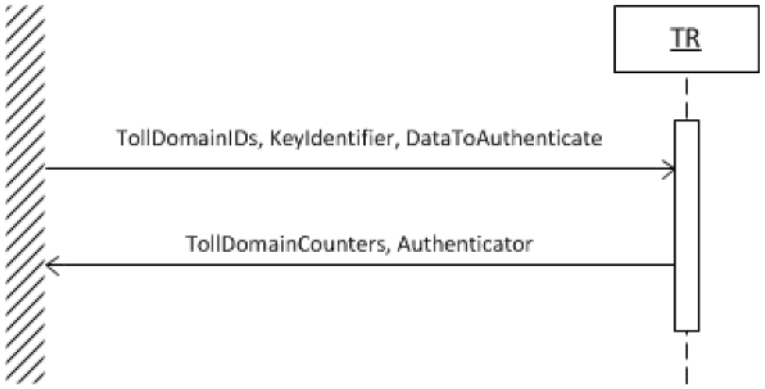

Figure 3 — Real-time freezing scenario

This scenario consists of the following steps:

1. The itinerary is sent to the Trusted Recorder. The itinerary is just data to be authenticated by the TR. A TR shall not attempt to parse or interpret this data. As indicated in Figure 3, the TR also receives the identifier of the key to be used to calculate the authenticator, and the identifier of the relevant toll domain(s). According to CEN/TS 16702–1, E.4.1, up to four toll domain identifiers may be provided.

NOTE OBE will send more than one toll domain identifier in case of overlapping toll domains. In such cases, multiple toll domain counters are used simultaneously. Detailed explanations can be found in CEN/TS 16702–1, E.4.1.

2. The TR retrieves the current value of the relevant toll domain counter(s) from its secure memory and concatenates these value(s) with the DataToAuthenticate. In case less than four toll domain identifiers are provided, for every ‘missing’ toll domain counter the TR adds a number of bytes with value zero to the concatenated data, such that the length of the data is always the same.

3. The TR calculates the authenticator over the concatenated data, using the key identified by the KeyIdentifier. The authenticator is either

    1) a. A Message Authentication Code (MAC), calculated using a symmetric key.

2) b. A signature, calculated using the private key of an asymmetric key pair.

4. The TR increments the value of the relevant toll domain counter(s) by one and stores the new value(s).

5. The TR returns the authenticator, together with the (plaintext) value of the toll domain counter(s) to the caller.

Interface and functional requirements are defined for this scenario in Clause 6 and Clause 7.

5.3.3 Real-Time Freezing using a Trusted Time Source

This is the same scenario as 5.3.2 with the following additions, as shown in Figure 4:

— In step 3, the TR also concatenates a time stamp to the DataToAuthenticate, before calculating the authenticator. The TR retrieves the value of the time stamp from its trusted time source.

— In step 5, the TR also returns the time stamp.

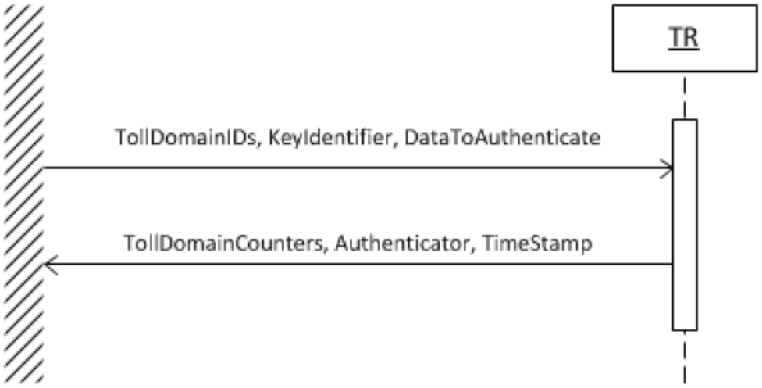

Figure 4 — Real-time freezing with TTS

Functional requirements are defined for this scenario in Clause 6. Note that no interface requirements are defined for this scenario in Clause 7.

5.4 Scenarios for a Verification SAM

5.4.1 General

This clause defines the scenarios valid for a Verification SAM used in a RSE, the TSP back office or the TC back office.

5.4.2 MAC verification

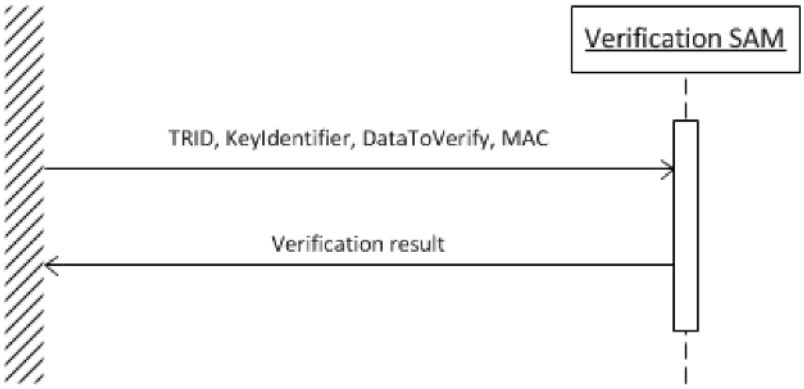

Figure 5 — MAC verification

A Verification SAM may be used to verify the authenticity of the MAC over an itinerary record. This MAC is supposed to be calculated by a Trusted Recorder inside OBE. The Verification SAM holds the same symmetric key that was used by the TR to calculate the MAC.

NOTE In case a TR uses asymmetric cryptography to freeze the itinerary record, the presence of a Verification SAM is not necessary. Any computer having access to the public key certificate of the TR is able to verify the signature. However, the methods for distributing and verifying the TR certificates are out of scope of this Technical Specification.

Verification of a MAC is done by following these steps:

a) The itinerary record is sent to the Verification SAM. From the point of view of the SAM, this is just data to be verified. A SAM shall not attempt to parse or interpret this data. As indicated in Figure 5, the SAM also receives

   1) a MAC that supposedly is valid for the data to be verified,

   2) the identifier of the Trusted Recorder that supposedly calculated the MAC,

   3) the identifier of the key supposedly used by the TR to calculate the MAC,

b) To prevent that each SAM has to contain all keys of all TRs whose outputs it may have to verify, the keys of the Trusted Recorder shall be diversified based on some predefined diversification scheme. The diversification data used shall be the TRID of the TR and the relevant key, as specified in CEN/TS 16702–1, 7.2.2. Thus, the SAM is able to calculate the key used by the TR to calculate the MAC.

c) The Verification SAM calculates the MAC over the data to be verified, using the calculated MAC key, and compares the result with the MAC provided in the call.

d) The result of the MAC verification (positive or negative) is returned to the caller

Functional requirements are defined for this scenario in Clause 6.

5.5 General Scenarios

5.5.1 General

This clause defines the general scenarios for the Trusted Recorder and the Verification SAM.

5.5.2 Assigning a Toll Domain Counter

A Trusted Recorder contains a number of Toll Domain Counters (TDCs). Each TDC is assigned to a specific toll domain by a unique toll domain ID.

Assigning a Toll Domain Counter to a specific toll domain may be done either by the TR issuer before the Trusted Recorder is issued, or by the TR itself during its lifetime. The first option may be used to ensure that the Trusted Recorder will work in a number of pre-defined toll domains. The second option allows for a dynamic, flexible allocation of Toll Domain Counters, depending on the toll domains a Trusted Recorder encounters during its lifetime.

NOTE 1 A malicious OBE could in principle easily stop a Trusted Recorder from freezing any itineraries by assigning all available Toll Domain Counters on the TR to non-existing Toll Domain IDs. To prevent this, the TR issuer could choose to assign a number of TDCs to toll domains that it knows or expects the TR will use.

The exact process to use in case of pre-issuance allocation of TDCs is out of scope of this Technical Specification.

The process to use in case the TR dynamically allocates a TDC to a specific toll domain consists of the following steps:

— The TR receives a request to freeze an itinerary in real-time, as described in 5.3.2 or 5.3.3. The request contains the ID of a toll domain for which the TR does not yet hold a Toll Domain Counter.

— The TR verifies whether it holds one or more Toll Domain Counters that are not yet assigned to a toll domain.

  — If this is the case, the TR assigns a TDC to the toll domain specified in the freezing request. It then uses the current value of this TDC (which will be zero) to calculate the authenticator over the data to be authenticated, and returns the authenticator plus the current value of the TDC to the caller, as described in 5.3.2 or 5.3.3.

  — If the TR does not hold a non-assigned Toll Domain Counter, it will deny the request to freeze the itinerary data.

NOTE 2 The 'catch-all' toll domain counter concept defined in CEN/TS 16702–1, E.4.2 need to be implemented by the OBE software based on an agreed value for the date element tollDomainId of the used TollDomainCounter. This means that the OBE implements a list of toll domain IDs that are using the same TR TollDomainCounter in case of running out of toll domain counters. The agreed identical toll domain ID of this 'catch-all' toll domain counter is also part of the frozen itinerary instead of the real toll domain ID. The ‘catch-all’ toll domain counter could be assigned before the TR is issued, as discussed in the previous Note.

5.5.3 Obtaining SAM Information

Depending on its configuration either as a TR or a Verification SAM, the TR or Verification SAM shall be able to present Device Information, Toll Domain Counter Information and Key Information:

— Device Information consists of

  — the TRID of the device as defined in Annex A. This ID will be used to derive the symmetric MAC key used by the Trusted Recorder from a master key located in e.g. the Verification SAM,

  — the Device Class identifying the capabilities of the Trusted Recorder, in accordance with Table 1 and

  — the Device Specification Version, which is the version of this Technical Specification to which the Trusted Recorder complies.

— Toll Domain Counter Information consists of the current value(s) of the Toll Domain Counter(s). Toll Domain Information shall not be present for a Verification SAM.

— The Key information contains information that in detail identifies a key. Key information may also include the CertificateID (if applicable).

Device Information and Key Information will be loaded to the TR by the Issuer. Toll Domain Counter Information is stored in the TR during its lifetime.

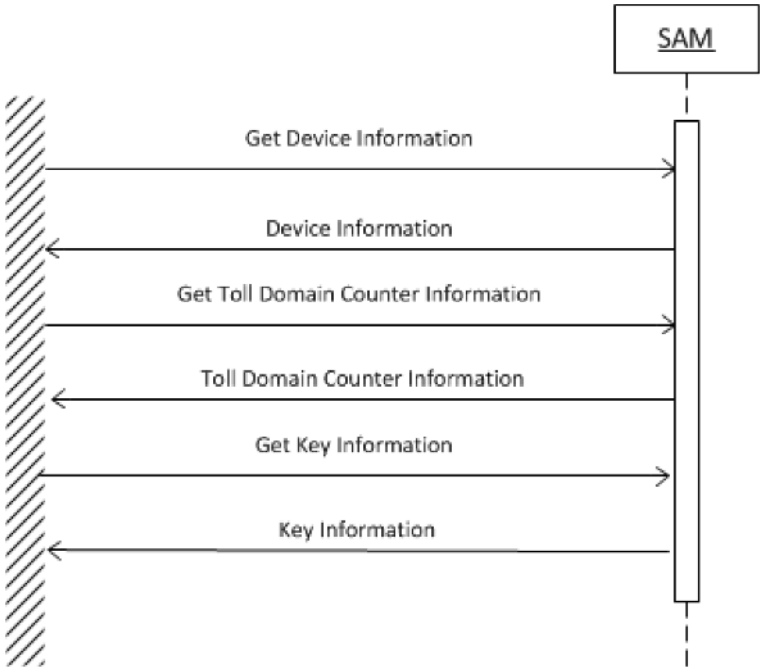

Figure 6 — SAM identification

The data flow Toll Domain Counter Information as shown in Figure 6 is only available from a Trusted Recorder but not from a Verification SAM. The interface and functional requirements for this scenario are defined in Clause 6 and Clause 7.

6 Functional requirements

6.1 General

6.1.1 SAM options

The function set implemented in a SAM is depending on its planned use. This Technical Standard defines the following options for a SAM:

a) **TR_symmetric**: The SAM is able to produce a MAC based on symmetric keys stored in the TR and to manage Toll Domain Counters.

b) **TR_asymmetric**: The SAM is able to produce a signature based on asymmetric private keys stored in the TR and to manage Toll Domain Counters.

c) **Trusted Time Source** (TTS): The SAM is able to produce time stamps based on a TTS and to include these in the data authenticated by the MAC or signature.

d) **Verification SAM**: The SAM is able to verify a MAC.

e) **Secure key import**: The SAM supports a confidential key import of a verification key, based on an asymmetric key encryption method and/or a symmetric key encryption method.

An implementation of a SAM will be a combination of several options. Table 1 shows the possible combinations of options. Other combinations of options are not allowed by this Technical Specification.

Table 1 — SAM configurations

Conf-ID	SAM configuration name	Supported options				
		a) Symmetric SM_CC	b) Asymmetric SM_CC	c) Trusted time source	d) Verification SAM	e) Confidential key import
1	Symmetric Trusted Recorder	X				
2	Trusted Recorder without TTS	X	X			
3	Full Trusted Recorder	X	X	X		
4	Verification SAM				X	X

NOTE In case a trusted recorder supports both, symmetric and asymmetric algorithms a TC or an interoperable toll scheme may limit the OBE to use only one of the supported authentication algorithms.

6.1.2 Presentation of requirements

The table below defines the format of the requirements specified in the following clauses.

Table 2 — Format of requirements

Header	Content
RQ ID (requirement identifier)	Unique requirement identifier RQ-B.x Basic requirements RQ-KM.x Key management RQ-CF.x Cryptographic functions RQ-RF.x Real-time freezing RQ-VS.x Verification SAM RQ-TD.x Toll Domain Counter RQ-TT.x Trusted time source RQ-SP.x Security protection level
Requirement	Description of the requirement
Conf-IDs	The requirement shall be fulfilled by a SAM having the indicated configuration. Possible configurations are listed in Table 1.

6.2 Basic requirements

The basic requirements are meant to ensure the ability to identify the TR or Verification SAM and its keys.

Table 3 — Basic requirements

RQ ID	Requirement	Conf-IDs
RQ-B.1	A TR or Verification SAM shall have a 16-octet worldwide unique identifier, TRID.	All
RQ-B.2	A TR or Verification SAM shall be able to present the TRID.	All
RQ-B.3	A TR or Verification SAM shall be able to present the identifiers of the keys that are located in the TR or Verification SAM.	All

6.3 Key management

The set of requirements regarding key management defines the functionality for key import, key generation, the key attributes and properties of the TR or Verification SAM.

Table 4 — Key management requirements

RQ ID	Requirement	Conf-IDs
RQ-KM.1	The TR or Verification SAM shall be able to store at least four 128-bit AES keys.	all
RQ-KM.2	The Verification SAM shall be able to confidentially import an encrypted AES master key with the key encryption method defined in CEN/TS 16439, 8.1.5 and/or encrypted with a symmetric AES key.	4
RQ-KM.3	The TR shall be able to store at least four 256-bit ECC private keys.	2/3
RQ-KM.4	The TR shall be able to generate a 256-bit ECC key pair and export the public key or to import a 256-bit private ECC key. In case a TR is capable of generating a key pair, support for key import is optional.	2/3
RQ-KM.5	The TR or Verification SAM shall not allow the export of symmetric keys.	all
RQ-KM.6	The TR shall not allow the export of asymmetric private keys.	2/3
RQ-KM.7	The input parameter used by the TR to select the key for calculation of an authenticator shall be the data element Key Reference. NOTE The data element combination of TRID and Key Reference is used in the RSE to select the corresponding key for the signature verification.	2/3
RQ-KM.8	If a TR is capable of generating asymmetric key pairs, the random bit generator it uses shall comply with the requirements defined in ISO/IEC 18031.	2/3

6.4 Cryptographic functions

The group of cryptographic functionality requirements specifies the detailed set of functions required for data authentication, integrity, confidentiality and non-repudiation based on keys stored in and managed by the TR or Verification SAM.

As the outside of the TR is not trusted, signature operations shall produce the message hashes inside the TR itself.

Table 5 — Basic cryptographic function requirements

RQ ID	Requirement	Conf-IDs
RQ-CF.1	The TR or Verification SAM shall support the CMAC algorithm according to CEN/TS 16702–1, 7.1.2.	all
RQ-CF.2	The TR shall support the elliptic curve digital signature algorithm (ECDSA) according to CEN/TS 16702–1, 7.1.3.	2/3
RQ-CF.3	The Verification SAM shall support the RSA algorithm for key encryption and decryption, according to EFC Security Framework.	4
RQ-CF.4	The Verification SAM shall support the AES algorithm for key encryption and decryption, using at least a 128-bit key according to ISO/IEC 18033-3:2010.	4

6.5 Real-time freezing

The Trusted Recorder is intended to be used for real-time freezing in the OBE. Table 6 specifies the TR requirements for the support of the real-time freezing concept defined in CEN/TS 16702–1. The real-time freezing functions shall only use the specific keys for MAC or signature calculations and shall also comply with the Signing Time Lock requirements.

Table 6 — Real-time freezing requirements

RQ ID	Requirement	Conf-IDs
RQ-RF.1	The Trusted Recorder shall be able to be used for real-time freezing in the OBE with symmetric cryptography (MAC) according to RQ-CF.1 using the symmetric keys.	1/2/3
RQ-RF.2	The Trusted Recorder shall be able to be used for real-time freezing in the OBE with asymmetric cryptography (signature) according to RQ-CF.2 using the asymmetric keys.	2/3
RQ-RF.3	The Trusted Recorder shall not accept a new request for real-time freezing of data before a minimum time, referred to as the Signing Time Lock, has elapsed since the previous request, regardless of the Toll Domain ID the previous request was related to.	1/2/3
RQ-RF.4	The TR shall have only one Signing Time Lock valid for all toll domains.	1/2/3
RQ-RF.5	The Signing Time Lock for real-time freezing shall be a configurable value in the range of 0 to 30 s.	1/2/3
RQ-RF.6	The Signing Time Lock shall only be set after authentication by a trusted party..	1/2/3
RQ-RF.7	The TR shall calculate the real-time freezing signature or MAC on the data type **IR_RTF{IRSpec}** defined in CEN/TS 16702–1, Annex A.	1/2/3
RQ-RF.8	The TR shall use individual counters for different Toll Domains but use the same key for all Toll Domains to create the authenticator.	1/2/3

6.6 Verification SAM

In case the Trusted Recorder is used with symmetric techniques for the Secure Monitoring concept, a Verification SAM with corresponding authentication verification capability is required. This Verification SAM is used in the RSE and the Toll Charger Back End to verify the MAC calculated by the TR. The requirements of this clause are only valid for such a Verification SAM.

Table 7 — Verification SAM requirements

RQ ID	Requirement	Conf-IDs
RQ-VS.1	The Verification SAM shall be able to store a minimum of 128 individual AES master keys with 256 bits key length.	4
RQ-VS.2	A Verification SAM shall not allow the export of a master key or a derived TR key.	4
RQ-VS.3	A Verification SAM shall use a master key only to internally calculate diversified TR keys.	4
RQ-VS.4	The Verification SAM shall be able to derive a TR key from themaster key identified by Key Reference (KeyRef) as described in CEN/TS 16439:2013, 8.1.3, using the TRID as key diversifier.	4
RQ-VS.5	The Verification SAM shall only use derived TR keys for the internal calculation of MACs.	4
RQ-VS.6	The Verification SAM shall compare the input MAC with an internally calculated MAC over the input message using the derived TR key. The MAC algorithm is defined in RQ-CF.1. The Verification SAM shall output the result of MAC verification. The result shall be one of the following statuses: - MAC is OK - MAC is not OK	4
RQ-VS.7	The Verification SAM shall not support the export of an internally calculated MAC using a derived TR key.	4

6.7 Toll Domain Counter

A toll domain counter (TDC) is a sequence number associated to exactly one Toll Domain. The intention of the domain counter is to be incremented for each authentication operation of a corresponding toll domain.

Table 8 — Toll domain counter requirements

RQ ID	Requirement	Conf-IDs
RQ-TD.1	The Trusted Recorder shall be able to store and maintain at least 10 and at most 255 Toll Domain Counters.	1/2/3
RQ-TD.2	A Toll Domain Counter shall consist of a Toll Domain ID and a counter value.	1/2/3
RQ-TD.3	If a TR receives a request to authenticate itinerary data for a toll domain for which it does not yet contain a Toll Domain Counter, the TR shall assign a currently non-assigned Toll Domain Counter to this toll domain by setting the Toll Domain ID of that TDC to the Toll Domain ID contained in the request.	1/2/3
RQ-TD.4	It shall not be possible to change the Toll Domain ID of a TDC once that TDC has been assigned. NOTE This implies that reassignment of a TDC to another Toll Domain is not possible.	1/2/3
RQ-TD.5	If a TR receives a request to authenticate itinerary data for a toll domain for which it does not yet contain a Toll Domain Counter and there are no non-assigned Toll Domain Counters left, the TR shall deny the request and shall not calculate an authenticator.	1/2/3

RQ-TD.6	The TR shall increment the value of a Toll Domain Counter by one when it receives an authentication request referencing the Toll Doman ID of that TDC. The TR shall first include the TDC value in the authentication operation, as specified in 5.3.2 or 5.3.3, and then increment the TDC value and store it in its memory.	1/2/3
RQ-TD.7	A Toll Domain Counter value shall not be affected by any operation other than the data authentication operation for the linked Toll Domain ID, as described in 5.3.2 or 5.3.3.	1/2/3
RQ-TD.8	When the value of a Toll Domain Counter has reached its maximum, the TR shall deny any further data authentication requests referencing this Toll Domain Counter.	1/2/3
RQ-TD.9	The TR shall be designed to prevent memory wear out caused by storing of incremented Toll Domain Counters.	1/2/3
RQ-TD.10	It shall be possible to increment a Toll Domain Counter at least 2 000 000 times.	1/2/3

6.8 Trusted time source

The trusted time source of the TR is an internal real-time clock. Real-time means that the clock time is synchronous to Coordinated Universal Time (UTC).

Table 9 — Trusted time source requirements

RQ ID	Requirement	Conf-IDs
RQ-TT.1	The Trusted Recorder with trusted time source shall have an internal real time clock.	3
RQ-TT.2	The TR shall allow an authorized and authenticated time source to set the TTS clock. The use of this function shall be access protected. Until this function has been executed, the TTS clock and time stamp function shall indicate ‘not trusted time’. The value for ‘not trusted time’ shall be [01.01.1990, 00:00:00].	3
RQ-TT.3	The TR shall have a configurable maximum allowed value for the deviation of the TTS clock from the real (UTC) time. NOTE One value for the maximum allowed deviation has to be agreed between all the relevant Toll Chargers and the issuer of the TR. The technical specifications of the TTS clock shall include its estimated average deviation per unit of time. This results in a maximum period of time the TTS can function autonomously without exceeding the allowed maximum deviation. Once this period of time has elapsed (and hence the deviation of the TTS likely has exceeded the allowed maximum deviation) the TR shall indicate ‘not trusted time’, until the moment it is (again) rest by an authorized and authenticated time source.	3
RQ-TT.4	The TR shall be able to produce a time stamp according to the data type DateAndTime defined in ISO 14906:2011 for real-time freezing.	3
RQ-TT.5	The time base for a time stamp created by the TR shall be UTC.	3
RQ-TT.6	In case the TTS clock is not able to work correctly, e.g. because of power loss, TTS clock and time stamp function shall be set to ‘not trusted time’ until an authorized and authenticated source has reset the TTS clock value.	3

NOTE 1 The DateAndTime defined in ISO 14906 covers the time period from [01.01.1990, 00:00:00] to [31.12.2117, 23:59:58].

NOTE 2 The OBE is responsible for an uninterrupted power supply to the TR for the continuous operation of the real-time clock. The TR may be able to bridge short interruptions of the external power supply.

6.9 Security protection level

Table 10 specifies the requirements for the security protection level of a TR and the Verification SAM.

Table 10 — Security requirements

RQ ID	Requirement	Conf-IDs
RQ-SP.1	The Trusted Recorder and Verification SAM shall be designed to prevent tampering.	all
RQ-SP.2	Private keys for ADU authentication and/or decryption shall be stored in a cryptographic module designed according to one of the following security specifications and protection profiles: - ISO/IEC 19790 (2012 edition or later edition), minimum level 3; - FIPS PUB 140–2 (2012–12 edition or later edition), minimum security level 3; - Common Criteria Protection Profile BSI-PP-0035 (2007 edition or later edition), minimum evaluation assurance level 4 (EAL4).	all

7 Interface requirements

7.1 General

This clause specifies the APDUs for a realization of the Trusted Recorder without trusted time source on a ISO/IEC-7816 compliant smart card. This clause does not apply for a Verification SAM.

The commands listed below are those needed in operational state of a TR. The commands which are needed to get the TR in an operational state are outside the scope of this document. It is furthermore assumed that selection of application and key files, if needed, has already been done before the commands in the following clauses are executed.

The following APDUs are compliant to ISO/IEC 7816-4:2013, Clause 5. For each command in Clause 7 there is a table for the request and one for the response which corresponds to the Command-response pair defined in ISO/IEC 7816-4:2013.

All data representations in this Clause 7 shall be Big Endian.

NOTE 1 The ASN.1 data type representing a Toll Domain Counter, i.e. TollDomainCounter which consists of the element tollDomainId and counter, is defined in CEN/TS 16702–1, Annex A.

NOTE 2 The interface of the TR is defined to avoid the need for an ASN.1/PER decoder inside the TR. Therefore all data types for input and output of the TR are defined as the required number of octets with the identical length and coding of the corresponding PER encoded ASN.1 type.

7.2 Calculate MAC for real-time freezing

7.2.1 General

This command Calculate MAC calculates a MAC over supplied data using the referenced symmetric key in the Trusted Recorder. The Trusted Recorder shall add padding according to the padding algorithm specified for CMAC in ISO/IEC 9797-1:2011.

The Calculate MAC command supports referencing up to four (4) TollDomainCounters. The supported algorithm is CMAC as defined in functional requirements in Clause 6.

The trusted recorder uses different counters for different Toll Domains but uses the same key to sign data for all Toll Domains.

NOTE The Authenticator data type defined in CEN/TS 16702-1:2014 is unknown to the TR. The MAC that is returned by the TR is used by the calling OBE to construct an element of type Authenticator. The same approach applies for TollDomainCounter.

7.2.2 Calculation of MAC

The Trusted recorder shall calculate the MAC according to the following sequence

1. Concatenate the input data according to functional requirements in Clause 6

2. Calculate the MAC according to the following:

MAC = CMAC (TollDomainID_1 | Counter_1 | TollDomainID_2 | Counter_2 | TollDomainID_3 | Counter_3 | TollDomainID_4 | Counter_4 | Data)

The input value of a not used TollDomainID shall be all bits zero.

NOTE The TollDomainID is of type ContextID which is of type Provider defined in ISO 14906, and Provider is of CountryCode and IssuerIdentifier. A valid CountryCode is never zero according to Table C.3 – ITA-2 alphabet of ISO 14816. Therefore a valid TollDomainID has never all bits zero.

The TR shall not assign a counter for a TollDomainID with all bits zero. The TR shall use the counter value zero in the concatenation with such a TollDomainID for calculating the MAC.

7.2.3 Coding of request

Table 11 — Coding of MAC request

CLA	'80’
INS	'4C'
P1	0x00 CMAC
P2	'xx' KeyRef – Reference to symmetric key to be used for MAC calculation.
Lc	Length of the subsequent data field
Data	Data – Data to be included in MAC calculation
Le	Maximum length of the data in the response

Table 12 describes the coding of the Data field of the Calculate MAC command. M/O indicates whether the data is mandatory or not.

NOTE The size of Data is not specified. It is noted that the length of the Data field needs to be a maximum of 43 bytes to ensure compliance with CEN/TS 16702-1:2014 (see CEN/TS 16702-1:2014, Table 8).

Table 12 — Coding of field Data

Description	M/O	Number of bytes
TollDomainID_1	M	3 Byte
TollDomainID_2	M	3 Byte
TollDomainID_3	M	3 Byte
TollDomainID_4	M	3 Byte
0x80: Tag for reference of the *Data*	M	1 Byte
Length N of the *Data*	M	1 Byte
Data	M	N Byte

7.2.4 Coding of response

Table 13 — Coding of MAC response

Description	M/O	Number of bytes
TollDomainID_1	M	3 Byte
Counter_1	M	4 Byte
TollDomainID_2	M	3 Byte
Counter_2	M	4 Byte
TollDomainID_3	M	3 Byte
Counter_3	M	4 Byte
TollDomainID_4	M	3 Byte
Counter_4	M	4 Byte
MAC	M	8 Byte
SW1-SW2	M	2 Byte

7.3 Calculate digital signature for real-time freezing

7.3.1 General

This command Calculate Digital Signature calculates a digital signature over supplied data using the referenced asymmetric private key in the Trusted Recorder.

The Calculate Digital Signature command supports referencing up to four (4) TollDomainCounters. The supported algorithm is ECDSA as defined in functional requirements in Clause 6.

The trusted recorder uses different counters for different Toll Domains but uses the same key to sign data for all Toll Domains.

NOTE The Authenticator data type defined in CEN/TS 16702-1:2014 is unknown to the TR. The signature that is returned by the TR is used by the calling OBE to construct an element of type Authenticator. The same approach applies for TollDomainCounter.

7.3.2 Calculation of digital signature

The Trusted recorder shall calculate the digital signature according to the following sequence

1. Concatenate the input data according to functional requirementsClause 6.

2. Calculate the hash

3. Calculate the digital signature of the Hash using the referenced Algorithm according to the following:

Hash = SHA_256 (TollDomainID_1 | Counter_1 | TollDomainID_2 | Counter_2 | TollDomainID_3 | Counter_3 | TollDomainID_4 | Counter_4 | Data)

The input value of a not used TollDomainID shall be all bits zero.

The TR shall not assign a counter for a TollDomainID with all bits zero. The TR shall use the counter value zero in the concatenation with such a TollDomainID for calculating the hash.

7.3.3 Coding of request

Table 14 — Coding of signing request

CLA	'80’
INS	'5C'
P1	0x00 ECDSA according to CEN/TS 16702–1, 7.1.3.
P2	'xx' KeyRef – Reference to asymmetric private key to be used for digital signature calculation.
Lc	Length of the subsequent data field
Data	Data – Data to be included in digital signature calculation
Le	Maximum length of the data in the response

The coding of the Data field of the Calculate Digital Signature command is the same as for Calculate MAC command, see 7.2.3.

7.3.4 Coding of response

Table 15 — Coding of signing response

Description	M/O	Number of bytes	Direction
TollDomainID_1	M	3 Byte	From the TR
Counter_1	M	4 Byte	From the TR
TollDomainID_2	M	3 Byte	From the TR
Counter_2	M	4 Byte	From the TR
TollDomainCounter_3	M	3 Byte	From the TR
TollDomainCounter_3	M	4 Byte	From the TR
TollDomainID_4	M	3 Byte	From the TR
Counter_4	M	4 Byte	From the TR
Digital signature	M	64 Byte	From the TR
SW1-SW2	M	2 Byte	From the TR

7.4 Get device information

7.4.1 General

This command is used to retrieve Device specific information. Device Specific Information consists of:

TRID	TRID as defined in Annex A.
Conf-ID	Identifies capabilities of the TR according to one of the values defined in Table 1 of this specification.
Device Specification Version	Version of CEN/TS 16702–2, i.e. the year of publication. Binary Coded Decimal (BCD) Format YYYY.

7.4.2 Coding of request

Table 16 — Coding of device information request

CLA	'80'
INS	'54'
P1	'00'
P2	'00'
Lc	Empty
Data	Empty
Le	'00' or empty

7.4.3 Coding of response

Table 17 — Coding of device information response

Description	M/O	Number of bytes	Direction
0x81: Tag for reference of the *TRID*	M	1 Byte	From the TR
0x02: Length of the *TRID*	M	1 Byte	From the TR
TRID	M	16 Byte	From the TR
0x82: Tag for reference of the *Conf-ID*	M	1 Byte	From the TR
0x01: Length of the *Conf-ID*	M	1 Byte	From the TR
Conf-ID	M	1 Byte	From the TR
0x83: Tag for reference of the *Device Specification Version*	M	1 Byte	From the TR
0x02: Length of the *Device Specification Version*	M	1 Byte	From the TR
Device Specification Version	M	2 Byte	From the TR
SW1-SW2	M	2 Byte	From the TR

7.5 Get toll domain counter information

7.5.1 General

This command is used to retrieve the number of Toll Domain Counters (maximum 255) and information of their Context ID and Counter value:

7.5.2 Coding of request

Table 18 — Coding of toll domain information request

CLA	'80'	
INS	'56'	
P1	'00'	Get Number of Toll Domain Counters
	'01'	Get Toll Domain counter
P2	'00'	in case P1 = '00'
	'XX'	in case P1 = '01 'XX is a number between 1 and N where N is the number of Toll Domain Counters in this TR
Lc	Empty	
Data	Empty	
Le	'00' or empty	

7.5.3 Coding of response

Coding of a get toll domain information response:

Table 19 — Coding of response for case "Get Number of Toll Domains"

Description	M/O	Number of bytes	Direction
Number of Toll Domains	M	1 Byte	From the TR
SW1-SW2	M	2 Byte	From the TR

Table 20 — Coding of response for case "Get Toll Domain Counter":

Description	M/O	Number of bytes	Direction
TollDomainID	M	3 Byte	From the TR
Counter	M	4 Byte	From the TR
SW1-SW2	M	2 Byte	From the TR

7.6 Get key information

7.6.1 General

This command is used to retrieve information about the keys existing within the Trusted Recorder. For each individual key the following information can be retrieved:

The sequence is to first retrieve the number of keys, using P1 = '00' for symmetric keys or P1 = '80' for asymmetric keys. In response the number of keys, and a list of KeyRefs is returned. A KeyRef is 1-byte value. After that the command is issued with either P1 set to '01' (Symmetric keys) or '81' (Asymmetric keys) to get the key information for a certain key, referenced by KeyRef.

KeyRef — Reference to the key to be used in the signature (7.3) or MAC (7.2) command.

NOTE For asymmetric keys the KeyRef (in addition with possibly other identification attributes stored in the OBE) is also used to identify the certificate.

Algorithm As defined in Annex A of CEN/TS 16702–1

The Algorithm field specifies which algorithm the key may be used for, in order to calculate the MAC or digital signature algorithm specified in Chapter 7.2 and 7.3 respectively.

7.6.2 Coding of request

Table 21 — Coding of a get key information Request

CLA	'80'
INS	'58'
P1	'00' Get Number of Symmetric Keys '80' Get Number of Asymmetric Keys '01' Get Symmetric Key Information '81' Get Asymmetric Key Information
P2	'00' in case P1 = '00' 'XX' in case P1 = '01'. 'XX' is the KeyRef of the key in the TR for which information is being retrieved.
Lc	Empty
Data	Empty
Le	'00' or empty

7.6.3 Coding of response

Coding of a Get Key Information response:

Table 22 — Coding of case "Get Number of Keys"

Description	M/O	Number of bytes	Direction
0x81: Tag for reference of the *Number of Keys*	M	1 Byte	From the TR
0x01: Length of the *Number of Keys*	M	1 Byte	From the TR
Number of Keys	M	1 Byte	From the TR
0x82: Tag for reference of the *ListofKeyRef*	M	1 Byte	From the TR
Length of the *ListofKeyRef*	M	1 Byte	From the TR
ListofKeyRef	M	x Byte	From the TR
SW1-SW2	M	2 Byte	From the TR

Table 23 — Coding of case "Get Key Information"

Description	M/O	Number of bytes	Direction
0x81: Tag for reference of the *Algorithm*	M	1 Byte	From the TR
0x01: Length of the *Algorithm*	M	1 Byte	From the TR
Algorithm	M	1 Byte	From the TR
SW1-SW2	M	2 Byte	From the TR

7.7 Error handling

The command response shall report the following results

0x9000	Success / No Error
0x9001	More data to be picked up
0x6D00	Instruction not supported – unknown command
0x6E00	Class not supported
0x6A86	Incorrect parameters P1-P2
0x6F00	No precise diagnosis
0x6985	Conditions of use not satisfied e.g. command rejected due to Signing Time Lock

Annex A
(normative)

Data type specification

A.1 General

The EFC data types and associated coding related to the EFC attributes, data elements and types described in Clauses 6, 7 and 8 are defined using the Abstract Syntax Notation One (ASN.1) technique according to ISO/IEC 8824-1.

Packed encoding rules (PER), unaligned, according to ISO/IEC 8825-2 shall be used.

A.2 Data specifications

The actual ASN.1 module is contained in the attached file “CEN 16702(2015)EfcSecMonTrV1.asn”.

Annex B
(normative)

Implementation Conformance Statement (ICS) proforma

B.1 Guidance for completing the ICS proforma

B.1.1 Purposes and structure

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

The ICS proforma is subdivided into subclauses for the following categories of information:

— guidance for completing the ICS proforma;

— identification of the implementation;

— identification of the protocol;

— global statement of conformance;

— ICS proforma tables.

B.1.2 Abbreviations and conventions

B.1.2.1 General

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

B.1.2.2 Item column

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

B.1.2.3 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?”.

B.1.2.4 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.

c.i 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.

B.1.2.5 Reference column

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

B.1.2.6 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.

B.1.2.7 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.

B.1.2.8 References to items

For each possible item answer (answer in the support column) within the ICS 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 B.5/4 is the reference to the answer of item 4 in Table 5 of Annex B.

EXAMPLE 2 B.6/3b is the reference to the second answer (i.e. in the second support column) of item 3 in Table 6 of Annex B.

B.1.2.9 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 ICS proforma

The supplier of the implementation shall complete the ICS 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 ICS proforma for Trusted Recorder

B.2.1 Identification implementation

B.2.1.1 Identification of TR supplier

Table B.1 — Identification of TR supplier form

Company	
Postal address	
Telephone	
Contact person	
E-mail address	

B.2.1.2 Identification of TR

Table B.2 — Identification of TR form

Brand	
ManufacturerID (Provider)	
TR Version	
Device Version	
Device Class	
Device Serial Number of supplied units	

B.2.2 Identification of the standard

This ICS proforma applies to the following Technical Specification:

CEN/TS 16702-2 “Electronic fee collection — Secure monitoring for autonomous toll systems — Part 2: Trusted Recorder”.

This ICS proforma applies only for TRs.

B.2.3 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 ICS, with an explanation of why the implementation is non-conforming, on pages attached to the ICS proforma.

B.2.4 ICS proforma tables for TR

B.2.4.1 TR Configurations

Table B.3 — TR Configurations

Item	Implemented TR configuration	Reference	Status	Support (Y/N)
1	Symmetric Trusted Recorder	6.1.1	o.3–1	
2	Trusted Recorder without TTS	6.1.1	o.3–1	
3	Full Trusted Recorder	6.1.1	o.3–1	
4	Verification SAM	6.1.1	n/a	

o.3-1: it is mandatory to support one of these options.

B.2.4.2 Requirements

Table B.4 — Basic requirements

Item	Requirement	Reference	Status	Support (Y/N)
1	RQ-B.1	6.2	m	
2	RQ-B.2	6.2	m	
3	RQ-B.3	6.2	m	

Table B.5 — Key management requirements

Item	Requirement	Reference	Status	Support (Y/N)
1	RQ-KM.1	6.3	m	
2	RQ-KM.2	6.3	n/a	
3	RQ-KM.3	6.3	c.5–1	
4	RQ-KM.4	6.3	c.5–1	
5	RQ-KM.5	6.3	m	
6	RQ-KM.6	6.3	c.5–1	
7	RQ-KM.7	6.3	c.5–1	
8	RQ-KM.8	6.3	c.5–1	

c.5-1: IF Table B.3/2 OR Table B.3/3 THEN m ELSE n/a

Table B.6 — Basic cryptographic function requirements

Item	Requirement	Reference	Status	Support (Y/N)
1	RQ-CF.1	6.4	m	
2	RQ-CF.3	6.4	c.6–1	
3	RQ-CF.4	6.4	n/a	

Item	Requirement	Reference	Status	Support (Y/N)
4	RQ-CF.5	6.4	n/a	

c.6-1: IF Table B.3/2 OR Table B.3/3 THEN m ELSE n/a

Table B.7 — Real-time freezing requirements

Item	Requirement	Reference	Status	Support (Y/N)
1	RQ-RF.1	6.5	m	
2	RQ-RF.2	6.5	c.7–1	
3	RQ-RF.3	6.5	m	
4	RQ-RF.4	6.5	m	
5	RQ-RF.5	6.5	m	
6	RQ-RF.6	6.5	m	
7	RQ-RF.7	6.5	m	
8	RQ-RF.8	6.5	m	

c.7-1: IF Table B.3/2 OR Table B.3/3 THEN m ELSE n/a

Table B.8 — Verification SAM requirements

Item	Requirement	Reference	Status	Support (Y/N)
1	RQ-VS.1	6.6	n/a	
2	RQ-VS.2	6.6	n/a	
3	RQ-VS.3	6.6	n/a	
4	RQ-VS.4	6.6	n/a	
5	RQ-VS.5	6.6	n/a	
6	RQ-VS.6	6.6	n/a	
7	RQ-VS.7	6.6	n/a	

Table B.9 — Toll domain counter requirements

Item	Requirement	Reference	Status	Support (Y/N)
1	RQ-TD.1	6.7	m	
2	RQ-TD.2	6.7	m	
3	RQ-TD.3	6.7	m	
4	RQ-TD.4	6.7	m	
5	RQ-TD.5	6.7	m	
6	RQ-TD.6	6.7	m	
7	RQ-TD.7	6.7	m	

Item	Requirement	Reference	Status	Support (Y/N)
8	RQ-TD.8	6.7	m	
9	RQ-TD.9	6.7	m	
10	RQ-TD.10	6.7	m	

Table B.10 — Trusted time source requirements

Item	Requirement	Reference	Status	Support (Y/N)
1	RQ-TT.1	6.8	c.10–1	
2	RQ-TT.2	6.8	c.10–1	
3	RQ-TT.3	6.8	c.10–1	
4	RQ-TT.4	6.8	c.10–1	
5	RQ-TT.5	6.8	c.10–1	
6	RQ-TT.6	6.8	c.10–1	

c.10-1: IF Table B.3/3 THEN m ELSE n/a

Table B.11 — Security requirements

Item	Requirement	Reference	Status	Support (Y/N)
1	RQ-SP.1	6.9	m	
2	RQ-SP.2 according to - ISO/IEC 19790	6.9	o.11–1	
3	RQ-SP.2 according to - FIPS PUB 140–2	6.9	o.11–1	
4	RQ-SP.2 according to - Common Criteria Protection Profile BSI-PP-0035	6.9	o.11–1	

o.11-1: it is mandatory to support at least one of these options

B.2.4.3 Interface requirements

Table B.12 — Interface specification requirements

Item	Interface specification requirement	Reference	Status	Support (Y/N)
1	Calculate MAC for real-time freezing	7.2	m	
2	Calculate digital signature for real-time freezing	7.3	c.12–1	
3	Get device information	7.4	m	

Item	Interface specification requirement	Reference	Status	Support (Y/N)
4	Get toll domain counter information	7.5	m	
5	Get key information	7.6	m	
6	Error handling	7.7	m	

c.12-1: IF Table B.3/2 OR Table B.3/3 THEN m ELSE n/a

B.3 ICS proforma for Verification SAM

B.3.1 Identification implementation

B.3.1.1 Identification of Verification SAM supplier

Table B.13 — Identification of Verification SAM supplier form

Company	
Postal address	
Telephone	
Contact person	
E-mail address	

B.3.1.2 Identification of Verification SAM

Table B.14 — Identification of Verification SAM form

Brand	
ManufacturerID (Provider)	
Device Version	
*Device Class*Class	
Device Serial Number of supplied units	

B.3.2 Identification of the standard

This ICS proforma applies to the following Technical Specification:

CEN/TS 16702-2 “Electronic fee collection — Secure monitoring for autonomous toll systems — Part 2: Trusted Recorder”.

This ICS proforma applies only for Verification SAMs.

B.3.3 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 ICS, with an explanation of why the implementation is non-conforming, on pages attached to the ICS proforma.

B.3.4 ICS proforma tables for Verification SAM

B.3.4.1 TR Configurations

Table B.15 — TR Configurations

Item	Implemented TR configuration	Reference	Status	Support (Y/N)
1	Symmetric Trusted Recorder	6.1.1	n/a	
2	Trusted Recorder without TTS	6.1.1	n/a	
3	Full Trusted Recorder	6.1.1	n/a	
4	Verification SAM	6.1.1	m	

B.3.4.2 Requirements

Table B.16 — Basic requirements

Item	Requirement	Reference	Status	Support (Y/N)
1	RQ-B.1	6.2	m	
2	RQ-B.2	6.2	m	
3	RQ-B.3	6.2	m	

Table B.17 — Key management requirements

Item	Requirement	Reference	Status	Support (Y/N)
1	RQ-KM.1	6.3	m	
2	RQ-KM.2	6.3	m	
3	RQ-KM.3	6.3	n/a	
4	RQ-KM.4	6.3	n/a	
5	RQ-KM.5	6.3	m	
6	RQ-KM.6	6.3	n/a	
7	RQ-KM.7	6.3	n/a	
8	RQ-KM.8	6.3	n/a	

Table B.18 — Basic cryptographic function requirements

Item	Requirement	Reference	Status	Support (Y/N)
1	RQ-CF.1	6.4	m	
2	RQ-CF.3	6.4	n/a	
3	RQ-CF.4	6.4	m	
4	RQ-CF.5	6.4	m	

Table B.19 — Real-time freezing requirements

Item	Requirement	Reference	Status	Support (Y/N)
1	RQ-RF.1	6.5	n/a	
2	RQ-RF.2	6.5	n/a	
3	RQ-RF.3	6.5	n/a	
4	RQ-RF.4	6.5	n/a	
5	RQ-RF.5	6.5	n/a	
6	RQ-RF.6	6.5	n/a	
7	RQ-RF.7	6.5	n/a	
8	RQ-RF.8	6.5	n/a	

Table B.20 — Verification SAM requirements

Item	Requirement	Reference	Status	Support (Y/N)
1	RQ-VS.1	6.6	m	
2	RQ-VS.2	6.6	m	
3	RQ-VS.3	6.6	m	
4	RQ-VS.4	6.6	m	
5	RQ-VS.5	6.6	m	
6	RQ-VS.6	6.6	m	
7	RQ-VS.7	6.6	m	

Table B.21 — Toll domain counter requirements

Item	Requirement	Reference	Status	Support (Y/N)
1	RQ-TD.1	6.7	n/a	
2	RQ-TD.2	6.7	n/a	
3	RQ-TD.3	6.7	n/a	
4	RQ-TD.4	6.7	n/a	
5	RQ-TD.5	6.7	n/a	
6	RQ-TD.6	6.7	n/a	
7	RQ-TD.7	6.7	n/a	
8	RQ-TD.8	6.7	n/a	
9	RQ-TD.9	6.7	n/a	
10	RQ-TD.10	6.7	n/a	

Table B.22 — Trusted time source requirements

Item	Requirement	Reference	Status	Support (Y/N)
1	RQ-TT.1	6.8	n/a	
2	RQ-TT.2	6.8	n/a	
3	RQ-TT.3	6.8	n/a	
4	RQ-TT.4	6.8	n/a	
5	RQ-TT.5	6.8	n/a	
6	RQ-TT.6	6.8	n/a	

Table B.23 — Security requirements

Item	Requirement	Reference	Status	Support (Y/N)
1	RQ-SP.1	6.9	m	
2	RQ-SP.2 according to - ISO/IEC 19790	6.9	o.23–1	
3	RQ-SP.2 according to - FIPS PUB 140–2	6.9	o.23–1	
4	RQ-SP.2 according to - Common Criteria Protection Profile BSI-PP-0035	6.9	o.23–1	

o.23-1: it is mandatory to support at least one of these options

B.3.4.3 Interface requirements

Table B.24 — Interface specification requirements

Item	Interface specification requirement	Reference	Status	Support (Y/N)
1	Calculate MAC for real-time freezing	7.2	n/a	
2	Calculate digital signature for real-time freezing	7.3	n/a	
3	Get device information	7.4	n/a	
4	Get toll domain counter information	7.5	n/a	
5	Get key information	7.6	n/a	
6	Error handling	7.7	n/a	

Annex C
(informative)

Trusted time source implementation issues

C.1 General

This annex explains some of the issues regarding the implementation of a Trusted Time Source on a Trusted Recorder. The annex contains some possible approaches to implement a TTS required by a TR.

In addition, the annex reflects technical problems based on the assumption that first TRs will be implemented on existing smartcard chip solutions. Such smartcard chips or integrated circuits do not support real time clocks (see C.2.1.2).

C.2 Possible implementations of a TTS

C.2.1 TTS based on a real time clock

C.2.1.1 General

A TTS based on a real time clock is a device that can fulfil the time accuracy requirements over the entire lifetime of the TR in complete isolation. Just the initialisation of the time at e.g. OBE personalisation is required.

C.2.1.2 Smartcard IC based TR implementations

Especially such an implementation on a smartcard chip base TR is much more unlikely because the existing clocks on smartcards have a huge deviation. The typical deviation of the internal timer on a smart card is ± 20 %, depending on many unpredictable influences like manufacturing tolerance of the internal oscillator, processor work load (is a key generated in background, non-volatile memory operation, symmetric crypto engine active). The typical maximum time span to be covered by the internal timer of a smartcard is less than 30 s. A real time clock is clearly at current time outside the scope of a smartcard.

C.2.1.3 TR with external TTS

The TTS of a TR may be implemented in an external device. Real time clocks with the required accuracy are available at the current time. The technical concept of such a combination of TR and external TTS may be prove the required protection against manipulation (maybe only “tamper resistant”, not “tamper proof”) to be accepted as a valid solution by the Toll Chargers requiring Secure Monitoring.

C.2.2 TTS with the need for external calibration

C.2.2.1 General

The TTS with the need for external calibration is a device with some internal clock that is regularly calibrated to an external time source. There are several different external time sources available for calibration. For example:

— GNSS based external calibration;

— Calibration by trusted third party;

— Network Time Protocol based calibration.

Although the TTS has an external calibration, the internal TTS shall have a guaranteed time accuracy for at least some days.

C.2.2.2 GNSS based calibration

GNSS signals, e.g. from GPS or Galileo, could be used for calibration, but these signals can easily be spoofed. A Trusted Recorder cannot differentiate between a legitimate direct signal from the sky (satellite) and a false signal sent by a perpetrator. An even easier attack is a record and playback device that may delay the GNSS signal for some time before sending them to the Trusted Recorder, thus tricking the Trusted Recorder clock to go slower than it should do. There is no concept currently in the planning for neither GPS nor Galileo to provide authenticated navigation messages. Moreover, note that even authenticated navigation messages from the satellites would not prevent record/playback tampering.

C.2.2.3 Calibration by trusted third party

Calibration by a trusted third party means that the TTS will be calibrated in a trusted environment, where an attacker has no possibility to delay the signed time information of the TTP. For using signed time stamps, it is necessary that the TTS inside the TR is able to check the signature of the time stamp.

EXAMPLE Authorized correction example protocol: The TR stores a valid certificate/public key of a Time Stamp Authority (TSA). The TR is able to make a time stamp signing request to this TSA. The TR only uses the answer if it is received within 5 s. If the received answer is correctly signed by the TSA, the TR uses the TSA time stamp plus the half time between generation of the request and receiving the answer (assuming symmetric signal transit time) as the new time. The TSA request is initiated by the OBE if a connection to the TSP back office and therefore a connection to the internet exist. The TSA used for the proposed protocol might be operated by one or more Toll Chargers or another defined TTP.

C.2.2.4 Network Time Protocol based calibration

Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. A less complex implementation of NTP, using the same protocol but without requiring the storage of state over extended periods of time is known as the Simple Network Time Protocol (SNTP). It is used in some embedded devices and in applications where high accuracy timing is not required.

There are some issues currently not solved or problematic for both protocols:

— reliability of the synchronised time (unknown attacks);

— the complete implementation of a full NTP or SNTP protocol inside the TR including an interface between TR and OBE;

— the OBE has not always connection to the internet and therefore not to a time server. Such connection breaks may last for some days.

C.3 TTS power supply

A TR with TTS requires in any case a permanent external power supply. It is assumed that an OBE has an internal power supply to gab power supply loss by the vehicle power connection. Therefore the OBE is able to permanently support the power supply for the TTS of a TR.

Annex D
(informative)

Use of this Technical Specification for the EETS

D.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.

D.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 harmonized 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 harmonized. 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.

D.3 European standardization work supporting the EETS

Many of the standards developed by CEN/TC 278 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.

D.4 Correspondence between this Technical Specification and the EETS

This Technical Specification has no direct relation to the requirements listed in EC-decision 2009/750/EC. No direct matching of requirements from the EC-decision to clauses of this Technical Specification exists. This Technical Specification supports EETS indirectly as it supports CEN/TS 16702-1 “Secure Monitoring for autonomous toll systems – Part 1: Compliance checking”.

This Technical Specification enables the secure monitoring for autonomous systems concept defined in CEN/TS 16702-1 to fulfil the EETS requirements as indicated in CEN/TS 16702-1, F.4 on Technical requirements of SM_CC in relation to 2009/750/EC.

Bibliography

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

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

[3] ISO/IEC 27000:2009, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

[4] ISO/FDIS 12813, *Electronic fee collection - Compliance check communication for autonomous systems (ISO/FDIS 12813)*

[5] EN ISO 12855, *Electronic fee collection - Information exchange between service provision and toll charging (ISO 12855)*

[6] ISO/FDIS 13141, *Electronic fee collection - Localisation augmentation communication for autonomous systems (ISO/FDIS 13141)*

[7] EN ISO 14906, *Electronic fee collection - Application interface definition for dedicated short-range communication (ISO 14906)*

[8] ISO/FDIS 17575-1, *Electronic fee collection - Application interface definition for autonomous systems - Part 1: Charging (ISO/FDIS 17575-1)*

[9] ISO/FDIS 17575-2, *Electronic fee collection - Application interface definition for autonomous systems - Part 2: Communication and connection to the lower layers (ISO/FDIS 17575-2)*

[10] ISO/FDIS 17575-3, *Electronic fee collection - Application interface definition for autonomous systems - Part 3: Context data (ISO/FDIS 17575-3)*

[11] ISO 14816, *Road transport and traffic telematics — Automatic vehicle and equipment identification — Numbering and data structure*

[12] Directive (2004/52/EC) of the European Parliament and of the Council of 29 April 2004 on the interoperability of electronic road toll systems in the Community, OJ L 166, 30.4.2004, p. 124–143

[13] 2009/750/EC: Commission Decision of 6 October 2009 on the definition of the European Electronic Toll Service and its technical elements (notified under document C(2009) 7547), OJ L 268,13.10.2009, p.11-29

[14] ISO/IEC 7812-1, *Identification cards — Identification of issuers — Part 1: Numbering system*

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.™