

DIN CEN/TS 16702-1

ICS 03.220.20; 35.240.60

Ersatz für
DIN CEN/TS 16702-1
(DIN SPEC 74123):2015-02

**Elektronische Gebührenerhebung –
Sichere Überwachung von autonomen Mautsystemen –
Teil 1: Einhaltungsprüfung;
Englische Fassung CEN/TS 16702-1:2020**

Electronic fee collection –
Secure monitoring for autonomous toll systems –
Part 1: Compliance checking;
English version CEN/TS 16702-1:2020

Perception de télépéage –
Surveillance sécurisée pour systèmes autonomes de péage –
Partie 1: Contrôle de conformité;
Version anglaise CEN/TS 16702-1:2020

Gesamtumfang 93 Seiten

DIN-Normenausschuss Automobiltechnik (NAAutomobil)
DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Nationales Vorwort

Dieses Dokument (CEN/TS 16702-1:2020) wurde vom Technischen Komitee CEN/TC 278 „Intelligente Verkehrssysteme“ ausgearbeitet, dessen Sekretariat von NEN (Niederlande) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Gemeinschaftsarbeitsausschuss NA 052-00-71 GA „Gemeinschaftsarbeitsausschuss NAAutomobil/DKE: Intelligente Verkehrssysteme“ des DIN-Normenausschusses Automobiltechnik (NAAutomobil).

Das Präsidium des DIN hat mit seinem Beschluss 1/2004 festgelegt, dass von dem in den Regeln der europäischen Normungsarbeit von CEN/CENELEC verankerten Grundsatz, wonach Europäische Normen in den drei offiziellen Sprachen Deutsch, Englisch und Französisch veröffentlicht werden, in begründeten Ausnahmefällen abgewichen und auf die Deutsche Sprachfassung verzichtet werden kann.

Dieses Dokument enthält unter Berücksichtigung des DIN-Präsidialbeschlusses 1/2004 nur die Englische Fassung von CEN/TS 16702-1:2020.

Technische Spezifikationen sind nicht Bestandteil des Deutschen Normenwerks.

Eine Technische Spezifikation ist das Ergebnis einer Normungsarbeit, das wegen bestimmter Vorbehalte zum Inhalt oder wegen des gegenüber einer Norm abweichenden Aufstellungsverfahrens von DIN noch nicht als Norm herausgegeben wird.

Zur vorliegenden Technischen Spezifikation wurde kein Entwurf veröffentlicht.

Erfahrungen mit dieser Technischen Spezifikation sind erbeten:

- vorzugsweise als Datei per E-Mail an NAAutomobiltechnik@din.de in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter <http://www.din.de/stellungnahme> abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Automobiltechnik (NAAutomobil), 10004 Berlin, Postfach 80462, Behrenstr. 35, 10117 Berlin.

Diese Technische Spezifikation ist der erste Teil von zwei Dokumenten, die zusammen die sichere Überwachung für autonome Mautsysteme festlegen. Dieser Teil für sichere Überwachung – Einhaltungsprüfung legt die Transaktionen zwischen Straßenrandeinheiten (RSE) des Mauterhebers über DSRC fest, sowie die Transaktionen zwischen den Mauterhebern und den Backend-Systemen der Mautdienstleister zur sicheren Überwachung fest.

Diese Technische Spezifikation bietet Mautdienstleistern die Möglichkeit geeignete Konsistenzprüfungen der Abbuchungsberichte durchzuführen.

Änderungen

Gegenüber DIN CEN/TS 16702-1 (DIN SPEC 74123):2015-02 wurden folgende Änderungen vorgenommen:

- a) Verkürzung der Einführung;
- b) Ergänzung von Begriffen im Zuge der übergreifenden Harmonisierung von Begriffen in Normen der Domain elektronische Gebührenerhebung;
- c) Änderung und Aufteilung verschiedener Parameter;
- d) der ASN.1 Code wird in einem separaten File bereitgestellt und in Anhang A nur noch referenziert.

Frühere Ausgaben

DIN CEN/TS 16702-1 (DIN SPEC 74123): 2015-02

Nationaler Anhang NA (informativ)

Begriffe

Die Benummerungen der folgenden Begriffe sind identisch mit den Benummerungen in der Englischen Fassung.

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- ISO Online Browsing Platform: verfügbar unter <http://www.iso.org/obp>
- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>

3.1

Attribut

(en: attribute)

adressierbares Datenpaket, welches aus einem einzelnen Datenelement oder aus strukturierten Sequenzen von Datenelementen besteht

3.2

Authentifikator

(en: authenticator)

Daten, wenn möglich verschlüsselt, die zur Authentifizierung verwendet werden

3.3

Back-End

Teil eines Back-Office-Systems, welches mit einem oder mehreren Front-End(s) gekoppelt ist

3.4

Abrechnungsbericht

(en: charge report)

Informationen, die für das Front-End hervorgebrachte Straßennutzungs- und Zusatzinformationen beinhalten

3.5

Kontextdaten

Maut Kontextdaten

(en: context data, toll context data)

Informationen, die von dem verantwortlichen Mauterheber festgelegt wurden und notwendig sind, um die Mautgebühr für die Nutzung eines Fahrzeugs in einem bestimmten Mautgebiet festzuschreiben und die Mauttransaktion abzuschließen

3.6

kontextabhängiger Programmablauf

(en: context dependent itinerary)

Programmablauf, dessen Syntax und Semantik abhängig von Kontextdaten des Mautgebietes ist

3.7

kontextunabhängiger Programmablauf

(en: context independent itinerary)

Programmablauf, dessen Syntax und Semantik unabhängig von Kontextdaten des Mautgebietes ist

3.8

elektronische Gebührenerhebung

(en: electronic fee collection)

Mauterhebung mittels Elektronik

3.9

Einfrieren mittels Deklaration

(en: freezing per declaration)

Prozess, der den Programmablauf bezogen auf die Mautdeklaration durch Senden einer kryptografischen Bestätigung oder den gesamten Programmablauf zum Mauterheber, einfriert

3.10

Front-End

Teil eines Mautsystems, bestehend aus einer fahrzeuginternen Einrichtung (en: OBE) und möglicherweise einem Proxy, mit dem Straßenmautinformationen und Nutzungsdaten gesammelt und zur Lieferung an das Back-End verarbeitet werden

3.11

Programmablauf

(en: itinerary)

Reisetagebuch, welches in Einträgen eines Programmablaufs oder mehreren Programmabläufen organisiert ist und eine Bewertung der Richtigkeit einer Mautdeklaration ermöglicht

3.12

Programmablaufblatt

(en: itinerary leaf)

Sequenz von fortlaufenden Programmablaufeinträgen vom selben Typ, die alle eine definierte Menge von Mautdomain betreffen

3.13

Programmablauf einfrieren

(en: itinerary freezing)

Registrierung eines Programmablaufs sowie eine unbestreitbare Bestätigung desselben

3.14

Programmablaufstamm

(en: itinerary trunk)

Sequenz gesammelter Daten bezogen auf eine Anzahl untergeordneter Programmablaufstapel

3.15

Programmablaufeintrag

(en: itinerary record)

grundlegendes Datenelement, welches die Benutzung des Straßennetzes oder die Benutzung eines Fahrzeugs beschreibt

3.16

MAC

Nachrichtenauthentifizierungscode

(en: MAC, message authentication code)

festе Länge einer Kette von Bits, die zur Überprüfung der Authentizität einer Botschaft verwendet wird, die vom Sender der Botschaft generiert, zusammen mit der Botschaft übertragen und vom Empfänger der Botschaft überprüft wurde

3.17**fahrzeuginterne Einrichtung**

(en: on-board equipment)

alle notwendigen Einrichtungen innerhalb eines Fahrzeugs, um die notwendigen Funktionen und Kommunikationsdienste für die elektronische Gebührenerhebung auszuführen

3.18**Echtzeit Einfrierung**

(en: real-time freezing)

Einfrierung jedes Programmablaufeintrages unter Verwendung von zuverlässiger Datenaufzeichnung sobald dessen Aufzeichnung abgebrochen wurde

3.19**Einhaltungsprüfung der sicheren Überwachung**

(en: secure monitoring compliance checking)

Konzept, welches einem Mauterheber ermöglicht, sich auf die Vertrauenswürdigkeit der Mautdeklaration zu verlassen, die vom Mautdienstanbieter erstellt wurde

3.20**Zeitschloss**

(en: time lock)

Mechanismus der sicherstellt, dass eine neue Operation erst nach einer konfigurierbaren Zeitdauer oder Prozessortaktzeiten seit der letzten Operation bevollmächtigt wird

3.21**Mauterklärung**

(en: toll declaration)

Aussage, dass die Nutzung eines gegebenen Dienstes an einen Mauterheber vereinbart wurde

3.22**Mautgebiet**

(en: toll domain)

Bereich oder Teil eines Straßennetzes, in dem ein bestimmtes Mautregime angewendet wird

3.23**zuverlässige Datenaufzeichnung**

(en: trusted recorder)

lokale Einheit, die für kryptografische Funktionen geeignet ist und eine OBE mit Sicherheitsdiensten, inklusive Datenvertraulichkeit, Datenintegrität, Authentifizierung und Nachweisbarkeit unterstützt

3.24**unentdeckte Überwachung**

(en: undetected observation)

Überwachung der Straßennutzung, die vom Mauterheber durchgeführt wird und weder dem Fahrer oder der OBE vor, noch nach der Überwachung bekannt ist

3.25**unerwartete Überwachung**

(en: unexpected observation)

Überwachung der Straßennutzung, die vom Mauterheber durchgeführt wird und dem Fahrer, oder der OBE vor der Überwachung nicht bekannt, danach aber bekannt werden könnte

— Leerseite —

English Version

Electronic fee collection —
Secure monitoring for autonomous toll systems —
Part 1: Compliance checking

Perception du télépéage —
Surveillance sécurisée pour systèmes autonomes
de péage —
Partie 1: Contrôle de conformité

Elektronische Gebührenerhebung —
Sichere Überwachung von autonomen Mautsystemen —
Teil 1: Einhaltungsprüfung

This Technical Specification (CEN/TS) was approved by CEN on 25 November 2019 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, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, 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: Rue de la Science 23, B-1040 Brussels

Contents

Page

European foreword.....	4
Introduction	5
1 Scope	7
2 Normative references.....	7
3 Terms and definitions	9
4 Abbreviations	12
5 Processes.....	13
5.1 Overview	13
5.2 Profiles	15
5.3 Itinerary Freezing.....	20
5.3.1 Introduction.....	20
5.3.2 Generate Itinerary	21
5.3.3 Real-time freezing.....	22
5.3.4 Freezing per declaration	23
5.4 Checking of Itinerary Freezing.....	23
5.4.1 Introduction.....	23
5.4.2 Observing a vehicle	24
5.4.3 Retrieving Proof of Itinerary Freezing (PIF)	24
5.4.4 Checking PIF against Observation.....	25
5.5 Checking of Toll Declaration.....	26
5.5.1 Introduction.....	26
5.5.2 Retrieve Itinerary Data	26
5.5.3 Check Itinerary Consistency.....	26
5.5.4 Checking Toll Declaration against Itinerary	27
5.6 Inconsistency report.....	27
5.7 Providing EFC Context Data.....	27
5.8 Key Management.....	28
5.8.1 Introduction.....	28
5.8.2 Requirements	28
6 Transactions	29
6.1 Introduction.....	29
6.2 Description of Itinerary Data.....	31
6.2.1 Introduction.....	31
6.2.2 Itinerary Leaf.....	32
6.2.3 Itinerary Record Data Elements	33
6.3 Retrieving PIF in real-time (DSRC Transaction).....	35
6.3.1 Transactional Model	35
6.3.2 Syntax and Semantics	36
6.3.3 Security	38
6.4 Toll Declaration	38
6.4.1 Transactional Model	38
6.4.2 Syntax and semantics.....	39

6.4.3	Itinerary Trunk	39
6.4.4	Security.....	41
6.5	Back end data checking.....	41
6.5.1	Introduction	41
6.5.2	Transactional model.....	41
6.5.3	Checks of the Itinerary.....	43
6.5.4	Syntax and semantics.....	44
6.5.5	Security.....	44
6.6	Inconsistency Report.....	44
6.6.1	Transactional model.....	44
6.6.2	Syntax and semantics	45
6.6.3	Security.....	46
6.7	Providing EFC Context Data	46
6.7.1	Transactional model.....	46
6.7.2	Syntax and semantics	47
6.7.3	Security.....	47
7	Security.....	47
7.1	Security functions and elements.....	47
7.1.1	Hash functions	47
7.1.2	MAC.....	47
7.1.3	Digital signatures.....	48
7.1.4	Public Keys, Certificates and CRL.....	48
7.2	Key Management.....	48
7.2.1	Key Exchange between Stakeholders.....	48
7.2.2	Key generation and certification	49
7.3	Trusted Recorder and SM_CC Verification SAM characteristics	49
7.3.1	Introduction	49
7.3.2	Trusted Recorder.....	50
7.3.3	SM_CC Verification SAM.....	51
	Annex A (normative) Data type specification.....	52
	Annex B (normative) Protocol Implementation Conformance Statement Proforma	53
	Annex C (informative) Example transactions.....	62
	Annex D (informative) Relationships to other standards.....	69
	Annex E (informative) Essentials of the SM_CC concept	71
	Annex F (informative) Use of this document for the EETS.....	85
	Bibliography	87

European foreword

This document (CEN/TS 16702-1:2020) 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 shall not be held responsible for identifying any or all such patent rights.

This document supersedes CEN/TS 16702-1:2014.

This second edition of CEN/TS 16702-1 incorporates the following main modifications compared to the previous one:

- amendment of terms, in order to reflect harmonization of terms across electronic fee collection (EFC) standards;
- renaming SmccClaimADU to InconsistencyReportAdu;
- breaking up the Checking Itinerary transaction into Checking Itinerary Trunk and Checking Itinerary Leaf transactions;
- renaming itinerary sequence and itinerary batch to itinerary leaf and itinerary trunk;
- shortening the Introduction;
- presenting the ASN.1 code as a separate electronic file referenced from Annex A.

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 organisations of the following countries are bound to announce this Technical Specification: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Introduction

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 EN ISO 12813 provides useful indications to a TC of whether the on-board equipment (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 document 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. An operational EFC System can use a combination of the CCC and SM_CC tools to keep misuse under control effectively.

This document is the first part in a set of two that together specify Secure Monitoring for Autonomous Toll Systems: This document, "**Secure Monitoring - Compliance Checking**", specifies the transactions between roadside equipment (RSE) of the TC over dedicated short-range communication (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.

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 EN ISO 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).

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 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 checking of itinerary freezing (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

This document specifies transactions and data for Compliance Checking - Secure Monitoring. The Scope of this document consists of:

- the concept and involved processes for Secure Monitoring;
- the definition of transactions and data;
- the use of the OBE compliance checking transaction as specified in EN ISO 12813, for the purpose of Compliance Checking - Secure Monitoring;
- the use of back end transactions as specified in EN ISO 12855, 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 organizational 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.

NOTE Outside the Scope of this document is: The 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 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.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN ISO 12813:2019, *Electronic fee collection – Compliance check communication for autonomous systems (ISO 12813:2019)*

EN ISO 12855:2015, *Electronic fee collection – Information exchange between service provision and toll charging (ISO 12855:2015)*

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

EN ISO 17575-1:2016, *Electronic fee collection – Application interface definition for autonomous systems – Part 1: Charging (ISO 17575-1:2016)*

EN ISO 17575-3:2016, *Electronic fee collection – Application interface definition for autonomous systems – Part 3: Context data (ISO 17575-3:2016)*

CEN ISO/TS 19299:2015, *Electronic fee collection – Security framework (ISO/TS 19299:2015)*

ISO 15628:2013, *Intelligent transport systems – Dedicated short range communication (DSRC) – DSRC application layer*

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

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) – Part 1*

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

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

ISO/IEC 9594-8, *Information technology – Open Systems Interconnection – The Directory – Part 8: Public-key and attribute certificate frameworks*

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

ISO/IEC 11770-3:2015, *Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques*

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

IETF RFC 4648, *October 2006, The Base16, Base32, and Base64 Data Encodings*

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

FIPS PUB 180-4, *Secure Hash Standard (SHS)*

FIPS PUB 186-3, *June 2009, Digital Signature Standard (DSS)*

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.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at <https://www.iso.org/obp>

— IEC Electropedia: available at <http://www.electropedia.org/>

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

part of a back office system interfacing to one or more front ends

3.4

charge report

information containing road usage and related information originated at the front end

3.5

context data

toll 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

part of a tolling system consisting of on-board equipment (OBE) and possibly a proxy where road tolling information and usage data are collected and processed for delivery 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 leaf

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 trunk

sequence of aggregated data committing to a number of underlying itinerary leaves

3.15

itinerary record

atomic data element describing use of the road network or use of the vehicle

3.16

MAC

message authentication code

fixed-length string of bits used to verify the authenticity of a message, generated by the sender of the message, transmitted together with the message, and verified by the receiver of the message

3.17

on-board equipment

all required equipment on-board a vehicle for performing required electronic fee collection (EFC) functions and communication services

3.18

real-time freezing

freezing of each itinerary record as soon as its acquisition has terminated using a trusted recorder

3.19

secure monitoring compliance checking

concept that allows a Toll Charger to rely on the trustworthiness of toll declarations produced by Toll Service Providers

3.20

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

3.21

toll declaration

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

3.22

toll domain

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

3.23

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

3.24

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

3.25

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.

AES	Advanced Encryption Standard
CA	Certification Authority
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
MAC	Message Authentication Code
OBE	On-Board Equipment
OBU	On-Board Unit
PICS	Protocol Implementation Conformance Statement
PIF	Proof of Itinerary Freezing
RSE	Roadside 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 Modelling Language

5 Processes

5.1 Overview

This clause introduces the conceptual framework of Secure Monitoring Compliance Checking in terms of requirements to a system or devices implementing it. It also describes the relations between different processes and information classes. An overview of the main stakeholders and processes of Secure Monitoring can be found in Figure 1.

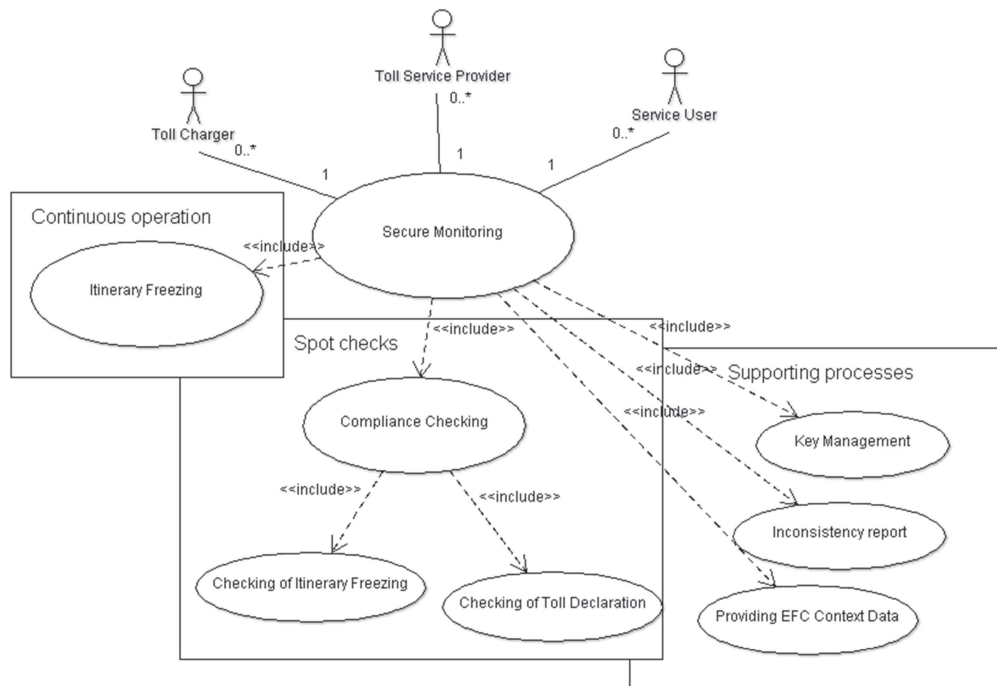


Figure 1 — The main stakeholders and processes of Secure Monitoring (UML use case diagram)

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

- Itinerary Freezing: generate and freeze the itinerary;
 - Checking of Itinerary Freezing: check the frozen itinerary for correctness against the observation;
 - Checking of Toll Declaration: check the correctness of the Toll Declaration against the itinerary;
- and the following supporting processes:
- Inconsistency Report: information from TC to TSP about a negative outcome of Checking of Itinerary Freezing and/or Checking of Toll Declaration;
 - 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.

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 12855:2015 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)**. The sub-processes of Compliance Checking are illustrated in Figure 2.

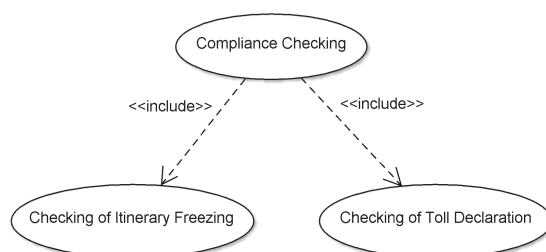


Figure 2 — The sub-processes of Compliance Checking (UML use case diagram)

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 checking of toll (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.

Annex E provides further background information on the use of and the rationale for these processes. Annex F describes how this document can be used for the EETS.

5.2 Profiles

For an overview of the different types of Secure Monitoring from the available options, see Table 1.

Table 1 — Different types of Secure Monitoring

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.

Table 1 — Different types of Secure Monitoring (*continued*)

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.

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 unauthorized 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 roadside 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. This option is intended to provide support for non-dedicated EFC OBE (such as e.g. smart phone-based solutions).

The choice of a type of Secure Monitoring is translated into requirements for the TSP via options described in Table 2.

Table 2 — Processes to be implemented by the TSP

Type of Secure Monitoring	Processes to be supported by the TSP					
	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 Real-time Freezing using a Trusted Recorder without trusted time source	X				X	OPTIONAL
SM_CC-2 Real-time Freezing using a Trusted Recorder with trusted time source	X	X				X
SM_CC-3a Freezing per Declaration			X			X
SM_CC-3b Freezing with High Frequency			X	X		X

NOTE Profile SM_CC-3b is intended to provide support for non-dedicated EFC OBE (such as e.g. smart phone-based solutions).

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).

The choice of a type of Secure Monitoring is translated into requirements for the TC via options described in Table 3.

Table 3 — Processes to be implemented by the TC

Type of Secure Monitoring	Processes to be supported by the TC				
	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 Real-time Freezing using a Trusted Recorder without trusted time source	X		X		OPTIONAL
SM_CC-2 Real-time Freezing using a Trusted Recorder with trusted time source				X	OPTIONAL
SM_CC-3a Freezing per Declaration		X		X	OPTIONAL
SM_CC-3b Freezing per Declaration with High Frequency	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), Inconsistency Report (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. The sub-processes of Itinerary Freezing are illustrated in Figure 3.

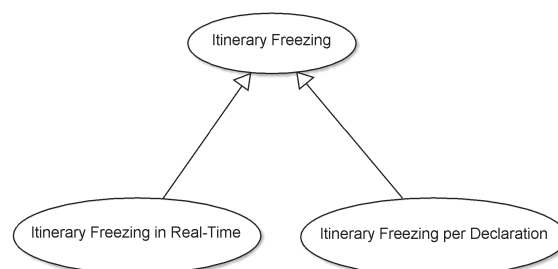


Figure 3 — The sub-processes of Itinerary Freezing (UML use case diagram)

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, 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 EN ISO 17575-1:2016, 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 is 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

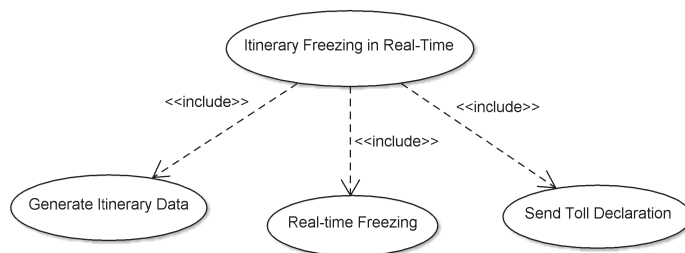


Figure 4 — The sub-processes of Itinerary Freezing in Real-Time (UML use case diagram)

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. The sub-processes of Itinerary Freezing in Real-Time is illustrated in Figure 4. 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 worth noting 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 leaves defined in 6.2 according to a first in - first out (FIFO) principle.

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

NOTE 3 Itinerary records are organized in leaves which in turn are organized in trunks. The terminology of "leaf" and "trunk" refers to the tree like data structure similar to so-called hash trees or Merkle trees (https://en.wikipedia.org/wiki/Merkle_tree).

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 as specified in EN ISO 12855:2015. 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 document.