TECHNICAL SPECIFICATION

ISO/TS 19299

First edition
2015-10-01

Electronic fee collection — Security framework

Perception de télépéage — Cadre de sécurité

Reference number
ISO/TS 19299:2015(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

ISO/TS 19299 was prepared by European Committee for Standardization (CEN) in collaboration with ISO/TC 204, *Intelligent transport systems*, in accordance with the agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This first edition of ISO/TS 19299 cancels and replaces CEN/TS 16439:2013.

Introduction

Reader's guide

The development process for a security concept and implementation to protect any existing electronic fee collection (EFC) system normally includes several steps as follows:

— definition of the security objectives and policy statements in a security policy;

— threat analysis with risk assessment to define the security requirements;

— development of the security measures followed by the development of security test specifications.

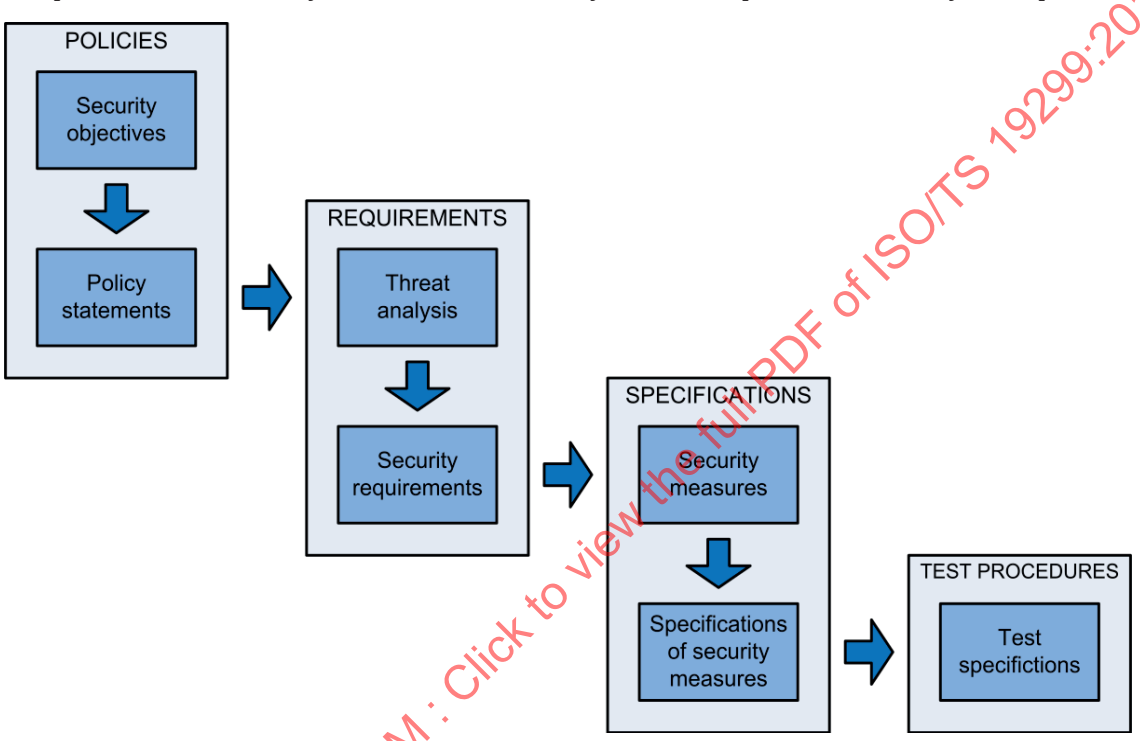

Figure 1 — Development path for the security documents

In the second step, each actor in an existing EFC system has to implement the defined security measures and supervise the effectiveness. Security measures which do not work or work incorrectly need to be improved. The development of the EFC security framework follows this approach as closely as possible. The used methodology needs to consider following limitations:

— No security policy exists: The security policy can only be defined by the responsible stakeholders and its freedom is only limited by laws and regulations. Nonetheless, this Technical Specification provides basic examples of possible security policies (in Annex E to Annex F).

— No risk assessment possible: The risk assessment compares the possible loss for the stakeholder and the required resources (e.g. equipment, knowledge, time, etc.) to perform an attack. It is the trade-off evaluation of the cost and benefit of each countermeasure which is only possible for an implemented system.

— No specific system design or configuration during the development of this Technical Specification was considered to keep it universally applicable. Only the available EFC base standards and the comments received by the CEN/TS 16439:2013 (i.e. the previous edition of the EFC security framework) were taken as references. Specific technical details of a particular system (e.g. servers, computer centres, and de-central elements like road side equipment) need to be taken into consideration during the implementation in addition to the present EFC security framework.

The selection of requirements and the respective security measures for an existing EFC system is based on the security policy and the risk assessment of several stakeholders systems. Due to the fact that there is neither an overall valid security policy, nor the possibility to provide a useful risk assessment, the EFC security framework provides a toolbox of requirements and security measures covering as many threats as possible without claiming to provide an exhaustive list.

There is one limitation though to be compliant to this Technical Specification that is, if a requirement is selected, the associated security measure(s) have to be implemented.

To understand the content of this Technical Specification, the reader should be aware of the methodological assumptions used to develop it. The security of an (interoperable) EFC scheme depends on the correct implementation and operation of a number of processes, systems, and interfaces. Only a reliable end-to-end security ensures the accurate and trustworthy operation of interacting components of toll charging environments. Therefore, this security framework also covers systems or interfaces which are not EFC specific like back office connections. The application independent security framework for such system parts and interfaces, the Information Security Management System (ISMS), is provided in the ISO 2700x family of standards.

The development process of this Technical Specification is described briefly in the steps below:

a) Definition of the stakeholder objectives and generic requirements as the basic motivation for the security requirements (Annex C). A possible security policy with a set of policy statements is provided in Annex E, and an example of an European electronic toll service (EETS) security policy is given in Annex F.

b) Based on the EFC role model and further definitions from the EFC architecture standard (ISO 17573), the specification defines an abstract EFC system model as the basis for a threat analysis, definition of requirements, and security measures.

c) The threats on the EFC system model and its assets are analysed by two different methods: an attack-based analysis and an asset-based analysis. The first approach considers a number of threat scenarios from the perspective of various attackers. The second approach looks in depth on threats against the various identified assets (tangible and intangible entities). This approach, although producing some redundancy, ensures completeness and coverage of a broader range of risks (see Annex D).

d) The requirements specification (see Clause 6) is based on the threats identified in Annex D. Each requirement is at least motivated by one threat and at least one requirement covers each threat.

e) The definition of security measures (see Clause 7) provides a high-level description of recommended possible methods to cover the developed requirements.

f) The security specifications for interoperable interface implementation (Clause 8) provide detailed definitions, e.g. for message authenticators. These specifications represent an add-on for security to the corresponding relevant interface standards.

g) Basic key management requirements that support the implementation of the interoperable interfaces are described in Clause 9. The toll charging environment uses cryptographic elements (keys, certificates, certificate revocation lists, etc.) to support security services like confidentiality, integrity, authenticity, and non-repudiation. This section of the specification covers the (initial) setup of key exchange between stakeholders and several operational procedures like key renewal, certificate revocation, etc.

h) A general trust model (see Clause 5) is defined to form the basis for the implementation of cryptographic procedures to ensure confidentiality, integrity, and authenticity of exchanged data. In this context, the security framework references approved international standards for the implementation of cryptographic procedures enhanced by EFC specific details where needed.

A stakeholder of an EFC scheme who wants to use this security framework needs to do the following:

— define a security policy for the EFC scheme (may involve more than one stakeholder in an interoperable EFC scheme). Some examples for a security policy and its elements are provided (in

Annex E and Annex F) as an aid for using this Technical Specification to build up a secure system for a concrete interoperability framework (including the European electronic toll service).

— identify the relevant processes, systems and interfaces, and match them to the EFC security framework;

— select the corresponding security requirements according to the security policy;

— implement the security measures associated to the selected requirements;

— provide evidence of compliance of its systems, processes, and interfaces with the requirements set forth in this Technical Specification. Evidence can be provided by a self-declaration, an internal or external audit, or other certifications.

EFC role model

This Technical Specification complies with the role model defined in ISO 17573. According to this role model, the toll charger (TC) is the provider of the tolled infrastructure or transport service and hence, the recipient of the road usage fees. The TC is the actor associated with the toll charging role (see Figure 2).

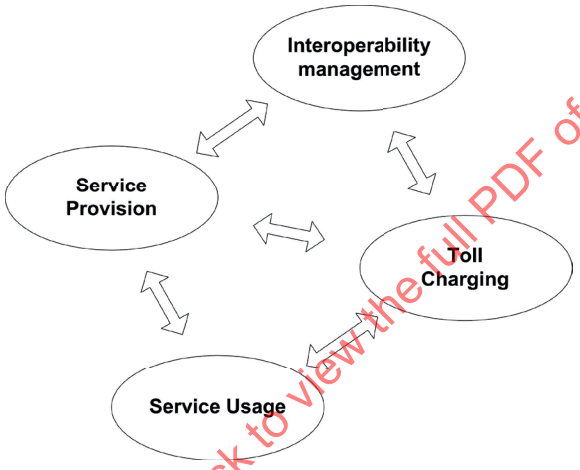

Figure 2 — The role model underlying this Technical Specification

Toll service providers (TSP) issue on-board equipment (OBE) to the users of the tolled infrastructure or transport service. TSPs are responsible for providing the OBE that will be used for collecting data, enabling the TC to send a claim to the TSP for the use of the infrastructure or transport service by their service users (SU). In autonomous systems, each TSP delivers toll declarations to the TC who operates the autonomous system. Such a TC possibly receives toll declarations from more than one TSP. In dedicated short-range communication (DSRC)-based systems, the TC receives the main toll declarations from its own RSE which communicates with the TSP's OBE and only supplementary charging data, if required, from the TSP. Interoperability management (IM) in Figure 2 comprises all specifications and activities that in common define and maintain a set of rules that govern the overall toll charging environment.

The trust model defined in this Technical Specification is based on the role model above and it is also the technical base for the protection of the data communication between the entities of the role model. Besides this communication security, trust in the secure implementation and management of the back end and other equipment for the EFC framework is required. A toll charger or toll service provider compliant to this Technical Specification needs to be able to give evidence of security management as required. Such evidence is the basis of trust relations between the involved entities.

Figure 3 below illustrates the abstract EFC system model used to analyse the threats, define the security requirements and associated security measures for this Technical Specification. This Technical Specification is based on the assumption of an OBE which is dedicated to EFC purposes only and neither considers value added services based on EFC OBE, nor more generic OBE platforms (also called in-vehicle ITS Stations) used to host the EFC application. The OBE may either be connected to a central

account or use a payment medium such as ICC or mobile payment for on-board-account EFC system. Any financial transactions to the payment medium are out of scope of this Technical Specification.

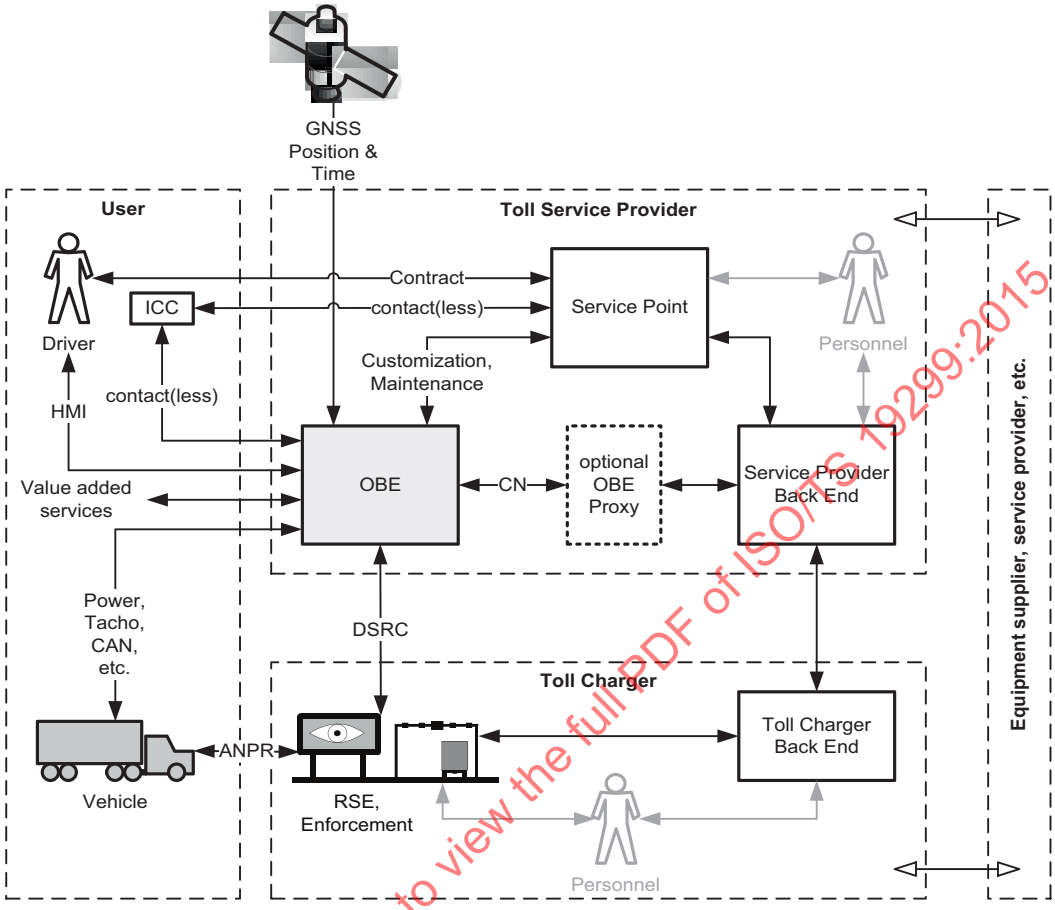

Figure 3 — EFC system model of the EFC Security framework

Relation to other security standards

Several generic and specific standards and Technical Reports concerning security issues for information technology already exist. This Technical Specification uses these existing standards and expands their usability for EFC applications. The framework references and tailors the security techniques and methodologies from these standards.

Figure 4 illustrates the context of the EFC security framework to other security standards. It is not an exhaustive description as only the most relevant standards are shown, i.e. the standards that gave most input to this Technical Specification. Standards that are directly used and referenced are highlighted in black (as opposed to grey). Other standards that may provide other security related input are given for information and completeness only, but are not further used.

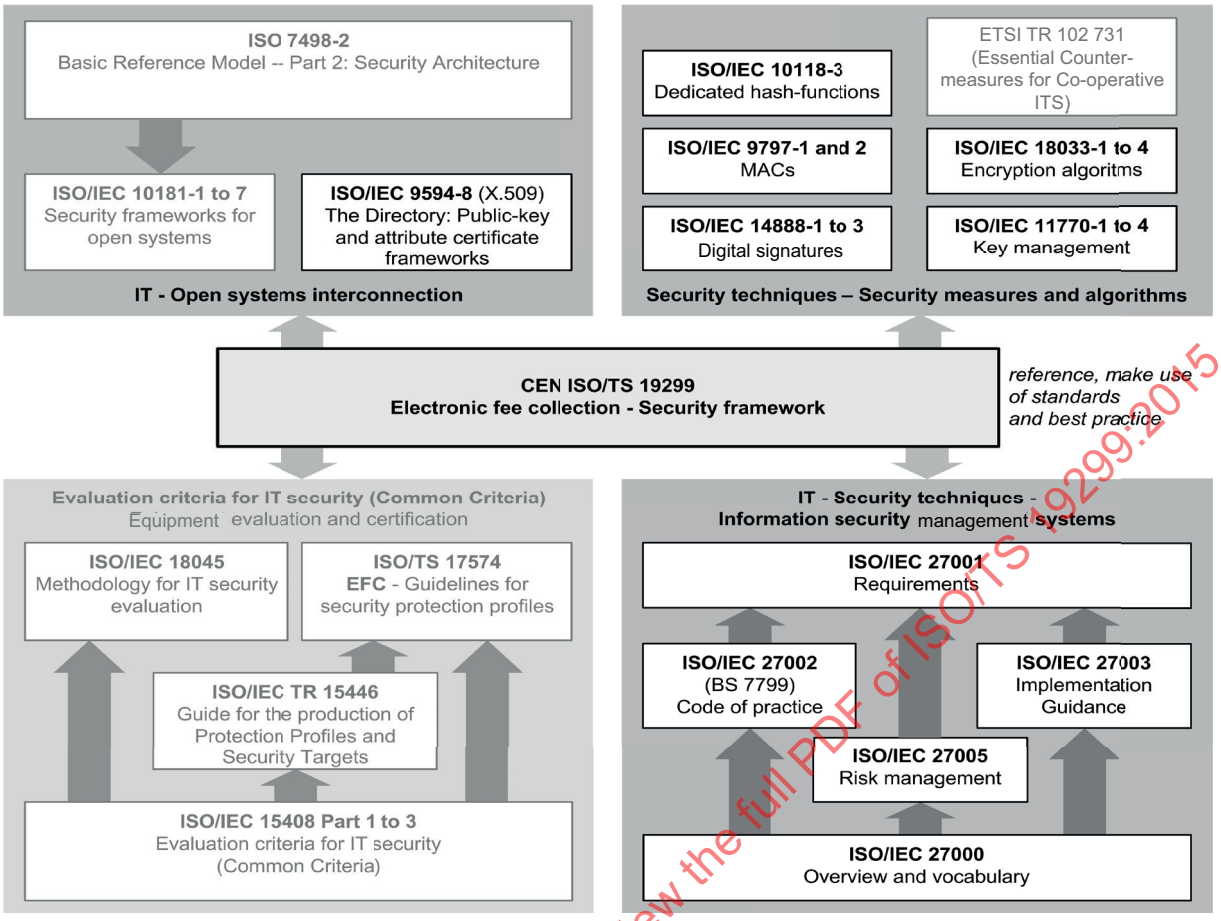

Figure 4 — Relevant security standards in the context of the EFC — Security framework

Each group of standards in Figure 4 provides the following features:

— **Security techniques — Security measures and algorithms**: The group is a collection of essential security measures and recommended cryptographic algorithms including the guidelines for accurate use.

— **IT — Open system interconnection**: This group of standards provides mechanisms for the secure communications between open systems. The standards address some of the security requirements in the areas of authentication and other security services through the provision of a set of frameworks.

— **Evaluation criteria for IT security (common criteria)**: This standard group defines methodologies and processes for the security evaluation and certification for most categories of products used in the EFC environment. The arrows inside the group indicate the relation between the standards in a bottom-up direction.

— **IT — Security techniques — Information security management system**: This standard family defines requirements and guidelines for the implementation of security management systems for all types of organizations. The standards are well suited for the security solutions of the back end and other fixed or installed equipment including software of EFC systems.

A corresponding ISO/IEC 27001 certification of a toll charger (TC) or toll service provider (TSP) organization may be used to demonstrate fulfilment of this Technical Specification provided that the scope and the Statements of Applicability (SoA) include the EFC business processes specified in ISO 17573 and the selected security requirements and their associated security measures provided by this Technical Specification are applied, e.g. by using them as part of the so-called catalogues containing the security measures and control objectives. Figure 5 below illustrates how this approach works in parallel. The first step of both paths is analysing the business processes followed by a threat analysis.

A common risk analysis combines the generic and the EFC related analysis and results in the respective security measures and controls.

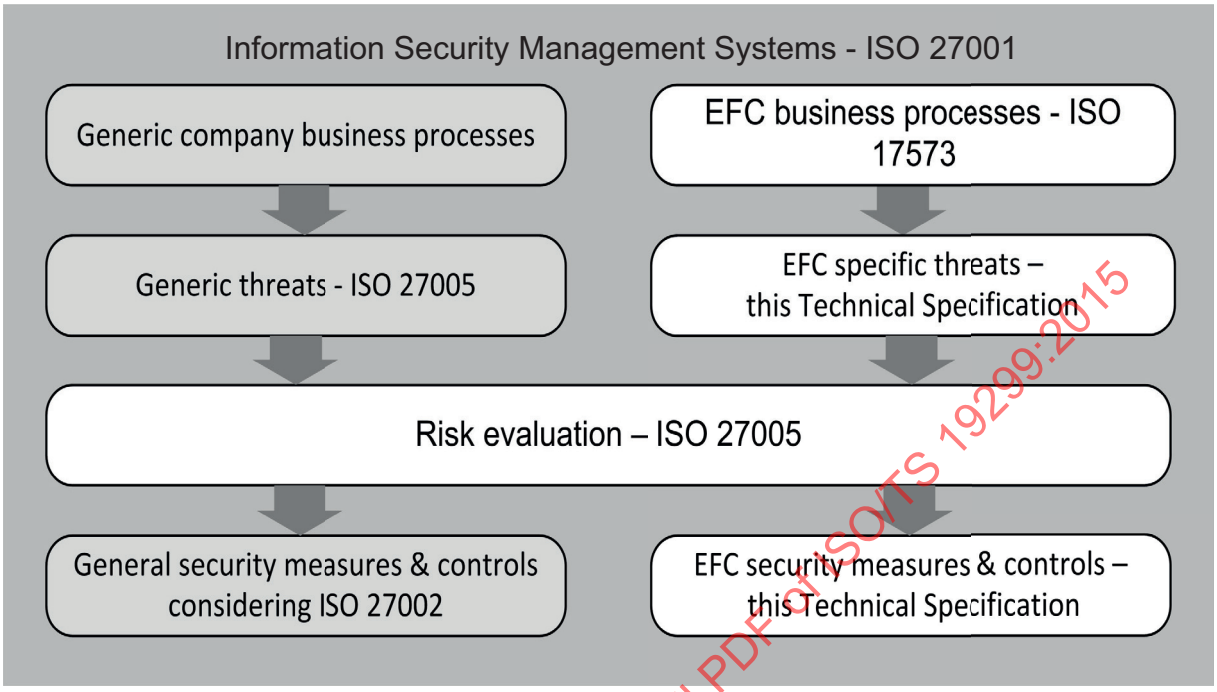

Figure 5 — Scope in relation to the Information Security Management System

In addition, the EFC security framework makes use of existing threat analysis methods and also uses existing threat analysis with relation to EFC or ITS [e.g. ETSI/TR 102 893 (intelligent transport systems; security; threat, vulnerability and risk analysis)].

Electronic fee collection — Security framework

1 Scope

The overall scope of this Technical Specification is an information security framework for all organizational and technical entities of an EFC scheme and in detail for the interfaces between them, based on the system architecture defined in ISO 17573. The security framework describes a set of requirements and associated security measures for stakeholders to implement and thus ensure a secure operation of their part of an EFC system as required for a trustworthy environment according to its security policy.

The scope of this Technical Specification comprises the following:

— definition of a trust model (Clause 5);

  Basic assumptions and principles for establishing trust between the stakeholders.

— security requirements (Clause 6);

— security measures — countermeasures (Clause 7);

  Security requirements to support actual EFC system implementations.

— security specifications for interface implementation (Clause 8);

  These specifications represent an add-on for security to the corresponding standards. Figure 5 above shows the relevant interfaces and the corresponding relevant interface standards, as illustrated in Figure 6.

— key management (Clause 9);

  Covering the (initial) setup of key exchange between stakeholders and several operational procedures like key renewal, certificate revocation, etc.

— security profiles (Annex A);

— implementation conformance statement (Annex B) provides a checklist to be used by an equipment supplier, a system implementation, or an actor of a role declaring his conformity to this Technical Specification;

— general information security objectives of the stakeholders (Annex C) which provide a basic motivation for the security requirements;

— threat analysis (Annex D) on the EFC system model and its assets using two different complementary methods, an attack-based analysis, and an asset-based analysis;

— security policy examples (Annex E and Annex F);

— recommendations for privacy-focused implementation (Annex G);

— proposal for end-entity certificates (Annex H).

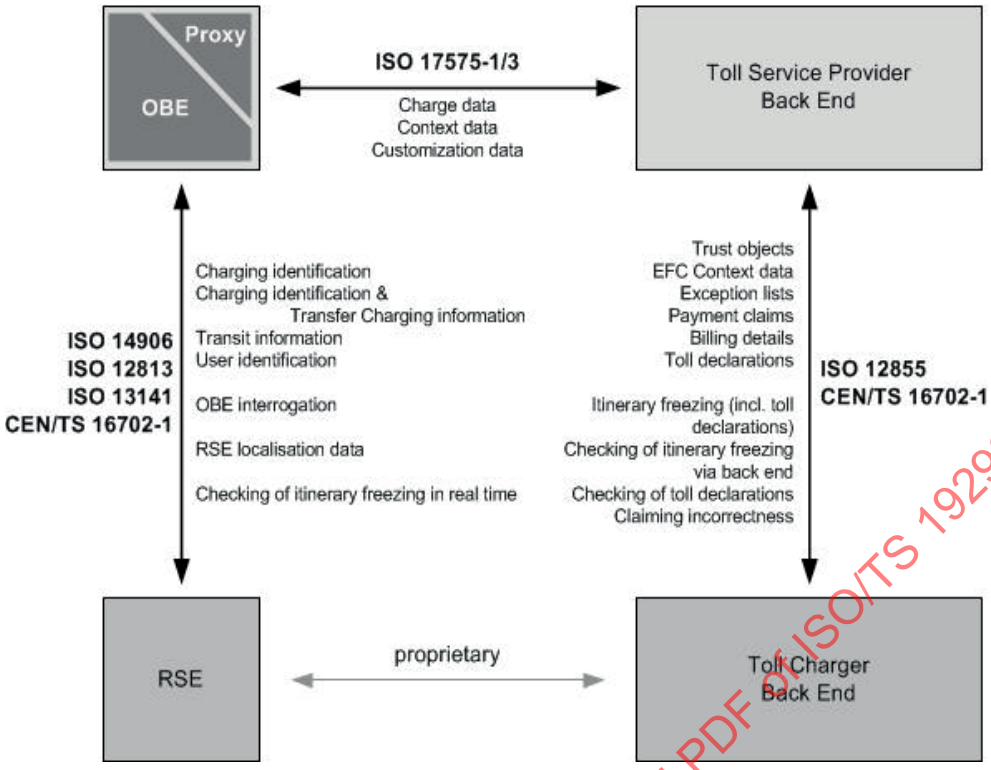

Figure 6 — Scope of EFC security framework for secure communication

The following are outside the scope of this Technical Specification:

— a complete risk assessment for an EFC system;

— security issues rising from an EFC application running on an ITS station;

NOTE Security issues associated with an EFC application running on an ITS station are covered in CEN/TR 16690.

— entities and interfaces of the interoperability management role;

— the technical trust relation between TSP and service user;

— concrete implementation specifications for implementation of security for EFC system [e.g. European electronic toll service (EETS)];

— detailed specifications required for privacy-friendly EFC implementations;

— any financial transactions between the payment service provider and the payment medium issued by the latter (e.g. ICC).

2 Normative references

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

ISO 12813:2015, *Electronic fee collection — Compliance check communication for autonomous systems*

ISO 12855:2015, *Electronic fee collection — Information exchange between service provision and toll charging*

ISO 13141:2015, *Electronic fee collection — Localization augmentation communication for autonomous systems*

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

EN 15509:2014, *Electronic fee collection — Interoperability application profile for DSRC*

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

ISO 17575-1:2015, *Electronic fee collection — Application interface definition for autonomous systems — Part 1: Charging*

ISO/IEC 7816-3, *Identification cards — Integrated circuit cards — Part 3: Cards with contacts — Electrical interface and transmission protocols*

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 9594-8:2014, *Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks — Part 8*

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

ISO/IEC 11770-1:2010, *Information technology — Security techniques — Key management — Part 1: Framework*

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

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

ISO/IEC 18033-2, *Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers*

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

ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

IETF Request for Comments (RFC) 4301:2005-12, *Security Architecture for the Internet Protocol*

IETF Request for Comments (RFC) 4347:2006-04, *Datagram Transport Layer Security*

IETF Request for Comments (RFC) 4648:2006-10, *The Base16, Base32, and Base64 Data Encodings*

IETF Request for Comments (RFC) 5035:2007-08, *Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility*

IETF Request for Comments (RFC) 5246:2008-08, *The Transport Layer Security (TLS) Protocol, Version 1.2*

IETF Request for Comments (RFC) 5280:2008-05, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

IETF Request for Comments (RFC) 5746:2010-02, *Transport Layer Security (TLS) Renegotiation Indication Extension*

Federal Information Processing Standards (FIPS) PUB 140-2, December 2002, *Security requirements for cryptographic modules*

3 Terms and definitions

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

3.1
accountability
property that ensures that the actions of an entity may be traced uniquely to the entity

[SOURCE: ISO 7498-2:1989, 3.3.3]

3.2
activist
especially active, vigorous advocate of a cause, especially a political cause

3.3
asset
anything that has value to a stakeholder

Note 1 to entry: An asset may be tangible or intangible.

3.4
attack
attempt to destroy, expose, alter, disable, steal, or gain unauthorized access to or make unauthorized use of an *asset* (3.3)

[SOURCE: ISO/IEC 27000:2014, 2.3]

3.5
authenticity
property that an entity is what it claims to be

[SOURCE: ISO/IEC 27000:2014, 2.8]

3.6
availability
property of being accessible and usable upon demand by an authorized entity

[SOURCE: ISO 7498-2:1989, 3.3.11]

3.7
back end
part of the back office system interfacing to one or more *front ends* (3.17)

3.8
certificate revocation list
signed list indicating a set of certificates that are no longer considered valid by the certificate issuer

[SOURCE: ISO/IEC 9594-8:2014, 3.5.12]

3.9
key certification authority
CA
authority trusted by one or more users to create and assign public-key certificates

[SOURCE: ISO 15782-1:2009, 3.15]

3.10
communication provider
provider of communication services used for the transmission of information

3.11
confidentiality
prevention of information leakage to non-authenticated individuals, parties, and/or processes

[SOURCE: ISO/TS 17574:2009, 3.7]

3.12
data protection commissioner
data privacy commissioner
person responsible for the enforcement and monitoring of compliance with the applicable data protection legislation

3.13
data subject's consent
any freely given specific and informed written indication of his wishes by which the data subject signifies his agreement to *personal data* (3.30) relating to him being processed

3.14
electronic money
value having its equivalence in real money, electronically stored e.g. on a bank account or an IC-card, which thus can be used by the user for payments

[SOURCE: ISO/TR 19639:—, 3.5]

3.15
enforcement
measures or actions performed to achieve compliance with laws, regulations, or rules

Note 1 to entry: In this context, the process of compelling observance of a *toll regime* (3.46).

3.16
foreign state agency
any agency of any state except the state under whose jurisdiction a particular *toll scheme* (3.47) is operated

3.17
front end
part of a tolling system consisting of OBE and possibly, a proxy where tolling information and usage data are collected and processed for delivery to the *back end* (3.7)

3.18
domestic state agency
government or any agency of the state or nation under whose jurisdiction a particular toll schema is being operated

3.19
hacker
person who attempts or succeeds to gain unauthorized access to protected resources

3.20
information asset
knowledge or data that has value to the stakeholder

[SOURCE: ISO/IEC 27032:2012, 4.27, modified]

3.21
information security
preservation of *confidentiality* (3.11), *integrity* (3.24), *availability* (3.6), *authenticity* (3.5), *accountability* (3.1), *non-repudiation* (3.27), and reliability of information

[SOURCE: ISO/IEC 27000:2014, 2.33, modified]

3.22
information security event
identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant

[SOURCE: ISO/IEC 27000:2014, 2.35]

3.23
information security incident
unwanted *information security* (3.21) events that have a significant probability of compromising business operations and threatening information security

[SOURCE: ISO/IEC 27000:2014, 2.36, modified]

3.24
integrity
property that data has not been altered or destroyed in an unauthorized manner

[SOURCE: ISO/TS 17574:2009, 3.11, modified]

3.25
interoperability
ability of systems to exchange information and to make mutual use of the information that has been exchanged

[SOURCE: ISO/IEC/TR 10000-1:1998, 3.2.1, modified]

3.26
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]

3.27
non-repudiation
ability to prove the occurrence of a claimed event or action and its originating entities

[SOURCE: ISO/IEC 27000:2014, 2.55]

3.28
on-board equipment
OBE
equipment located on-board a vehicle including nomadic devices with the function of exchanging information with external systems

3.29
payment medium
carrier of payment means, such as paper ticket, IC-card, smart phone or on-board unit (OBU)

3.30
personal data
information relating to an identified or identifiable natural person

Note 1 to entry: In relation to EFC, an identified or identifiable natural person is equivalent to the role service user (ISO 17573:2010).

3.31
policy
overall intention and direction as formally expressed by management

[SOURCE: ISO/IEC 27000:2014, 2.60, modified]

3.32
data privacy
rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure and disposal of personal information

[SOURCE: ISO/TS 14441:2013, 3.26]

3.33
processing of personal data
operation or set of operations which is performed upon *personal data* (3.30), whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction

3.34
roadside equipment
RSE
equipment located along the road ether fixed or mobile

3.35
secure application module
SAM
physical module that securely executes cryptographic functions and stores keys

3.36
security policy
set of rules that regulate how to handle security threats or define the appropriate security level

[SOURCE: ISO/TS 17574:2009, 3.23]

3.37
security service
service provided by communicating systems which ensures adequate security of the systems or of data transfers

[SOURCE: ISO 7498-2:1989, 3.3.51, modified]

3.38
digital signature
one or more data elements resulting from the digital signature process

3.39
threat
potential cause of an unwanted information security incident, which may result in harm

[SOURCE: ISO/IEC 27000:2014, 2.83, modified]

3.40
threat agent
entity that has the intention to act adversely on an *asset* (3.3)

3.41
threat analysis
systematic detection, identification, and evaluation of *threats* (3.39)

3.42
toll
any charge, tax, or duty levied in relation with using a vehicle in a *toll domain* (3.45)

[SOURCE: CEN/TR 16092:2011, 3.6, modified]

3.43
toll charger
TC
entity which levies *toll* (3.42) for the use of vehicles in a *toll domain* (3.45)

[SOURCE: ISO 17573:2010, 3.16, modified]

3.44
toll declaration
statement to declare the usage of a given toll service to a *toll charger* (3.43)

[SOURCE: ISO 17573:2010, 3.17, modified]

3.45
toll domain
area or a part of a road network where a certain *toll regime* (3.46) is applied

[SOURCE: ISO 17573:2010, 3.18, modified]

3.46
toll regime
set of rules, including enforcement rules, governing the collection of *toll* (3.42) in a *toll domain* (3.45)

[SOURCE: ISO 17573:2010, 3.20]

3.47
toll scheme
organizational view of a *toll regime* (3.46) including the actors and their relationships

[SOURCE: ISO/TS 17575-3:2011, 3.35, modified]

3.48
toll service provider
TSP
entity providing toll services in one or more *toll domains* (3.45)

[SOURCE: ISO 17573:2010, 3.23, modified]

3.49
trusted third party
TTP
security authority or its agent trusted by other entities with respect to security-related activities

[SOURCE: ISO/IEC 10181-1:1996, 3.3.30 modified]

3.50
service user
SU
generic term used for the customer of a *toll service provider* (3.48), one liable for *toll* (3.42), the owner of the vehicle, a fleet operator, a driver, etc. depending on the context

[SOURCE: ISO 17573:2010, 3.29, modified]

3.51
vulnerability
weakness of an *asset* (3.3) or control that can be exploited by an attacker

[SOURCE: ISO/IEC 27000:2014, 2.89, modified]

4 Symbols and abbreviated terms

AC_CR	Access Credentials (EN 15509:2014)
ADU	Application Data Unit
CA	Certification Authority (ISO 15782-1:2009)
CCC	Compliance Check Communication (ISO 12813:2015)
CN	Cellular Network
CRL	Certificate Revocation List
DES	Data Encryption Standard
DSRC	Dedicated Short-Range Communication (ISO 14906:2011)
EETS	European Electronic Toll Service
EFC	Electronic Fee Collection (ISO 17573:2010)
GNSS	Global Navigation and Satellite System (ISO 17573:2010)
HTTP	HyperText Transfer Protocol
HTTPS	HTTP over Secure socket layer
ICC	Integrated Chip Card (IC card)
ICS	Implementation Conformance Statement (ISO/TS 14907-2:2011)
IETF	Internet Engineering Task Force
IM	Interoperability Management
IPsec	Internet Protocol Security
ISMS	Information Security management system (ISO/IEC 27000:2014)
LAC	Localization Augmentation Communication (ISO 13141:2015)
MAC	Message Authentication Code
MAC_TC	DSRC Message Authentication Code for toll charger
MAC_TSP	DSRC Message Authentication Code for toll service provider

OBE	On-Board Equipment (ISO 14906:2011)
OID	Object Identifier
PAN	Personal Account Number
PER	Packed Encoding Rules (ISO/IEC 8825-2)
PKI	Public Key Infrastructure
RQ	Requirement
RSA	Rivest, Shamir and Adleman

NOTE RSA is an algorithm for public-key cryptography also referred to as asymmetrical cryptographic technique.

RSE	Roadside Equipment (ISO 14906:2011)
SAM	Secure application module
SHA-1	Secure hash algorithm (ISO/IEC 10118-3)
SM	Security Measure (countermeasure)
SU	Service User
TC	Toll Charger (ISO 17573:2010)
TLS	Transport Layer Security
TSP	Toll Service Provider
TTP	Trusted Third Party
VPN	Virtual Private Network
XER	XML Encoding Rules (ISO/IEC 8825-4)

5 Trust model

5.1 Overview

The trust model provides the basic trust and functionality for the implementation of authenticated and secured communication channels between TSP and TC.

The trust model has two different levels, the contractual framework between the stakeholders (TC, TSP, and SU) and the technical trust model between the IT infrastructure of the TC and TSP.

The trust model is based on the assumption that no initial technical trust relation between any of the stakeholders exists or will be generated by a predefined third party.

5.2 Stakeholders trust relations

Three kinds of bidirectional contract-based peer-to-peer trust relations are present in the underlying EFC role model. The following are the peer-to-peer trust relations:

— between toll charger and toll service provider;

— between toll service provider and service user;

— between toll charger or toll service provider and interoperability management.

There is no direct trust relation between toll charger and service user, as illustrated in Figure 7. The obligation of the service user is to pay for the transport service (e.g. road use) according to laws and regulations of the respective toll domain by using the OBE issued by the TSP.

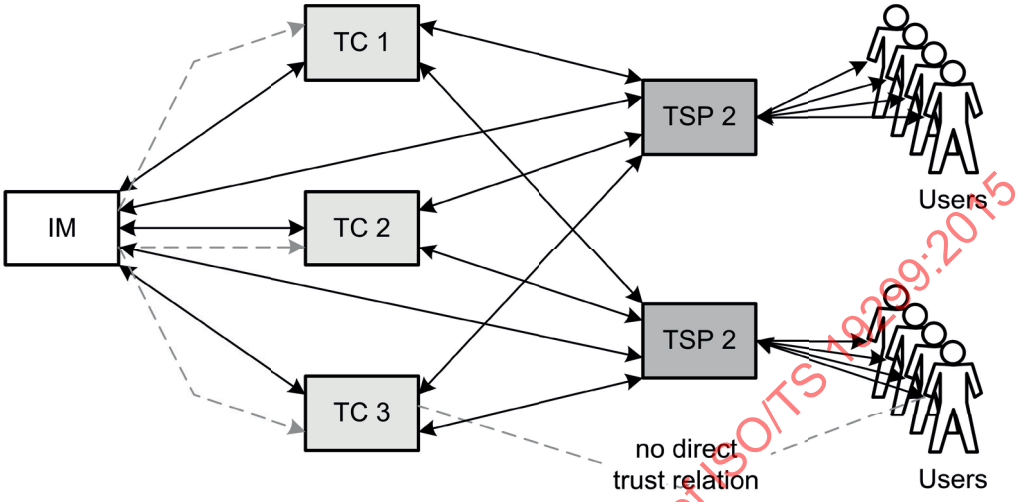

Figure 7 — Stakeholder trust relations

The interoperability management can be a single organization or a construct of several entities performing different tasks. Issuing rules, regulations, and general user information by the interoperability management (IM) is done using a trust relation outside of the scope of this Technical Specification (dotted arrows in Figure 7). Trust relations between IM and TC or TSP inside the scope are among others used for certification of organization or equipment and TTP functions in case this is performed by the IM.

One supported model is an agreement between TC and TSP to use a Trusted Third Party (TTP) (e.g. for issuing public-key root certificates). Such a hierarchical trust relation supported by a TTP can include the IM relations to TC and TSP. The TTP could either be performed as a part of the IM or external TTP(s) could be used to issue the root certificates. This Technical Specification does not require a mandatory TTP in a hierarchical trust model, but supports the use of it.

Another supported model is an agreement between TC and TSP to directly trust them by exchanging self-signed root certificates. Such a peer-to-peer trust relation can also include the IM relations to TC and TSP. This Technical Specification does not require a mandatory peer-to-peer trust model, but supports the use of it.

The technical trust relation of any chosen trust model between TSP and service user (SU) as well as the indirect trust relation between TC and SU are outside the scope of this Technical Specification.

5.3 Technical trust model

5.3.1 General

The technical trust model defines a solution for the trust relations between the different stakeholders. The technical trust model is dependent on the requirements of the concerned stakeholders with respect to support an interoperable EFC system.

5.3.2 Trust model for TC and TSP relations

The technical trust model uses the ISO/IEC 9594-8, (X.509) version 3 public-key and attribute certificate frameworks for establishing secure communication channels. These secure communication channels

ensure confidentiality, integrity, authenticity, and non-repudiation (only with proof of origin) of the messages exchanged between TC and TSP.

The use of ISO/IEC 9594-8, i.e. using the possibility to import and use in parallel different (self-signed) root certificates in the trust model, enables the support of both a peer-to-peer approach and a hierarchical approach using a trusted third party. In addition, it also allows a mixed approach with peer-to-peer relations between TC and TSP on one hand and a TTP certification authority (CA) approach on the other hand.

EXAMPLE Figure 8 illustrates an example of a trust model approach which is supported by this Technical Specification.

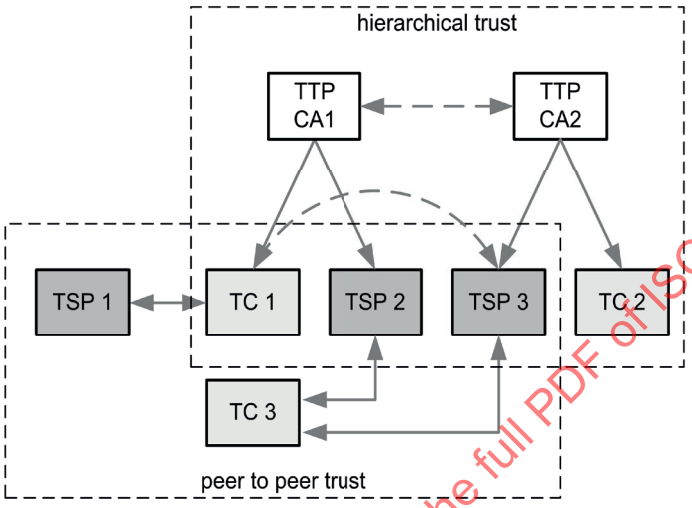

Figure 8 — Example of a mixed trust model environment

Figure 8 indicates the possibility of the trust model allowing an entity to participate at the same time in a mixed environment with both approaches. The dotted box marked as "hierarchical trust" shows the trusted third parties in their roles as certification authorities (CA1 and CA2) issuing certificates for each entity based on its self-signed root certificate imported by the entities. It is also possible that the TTP CAs directly issue certificates for the technical entities communicating with each other. In this case, no root certificate would exist and securing all interfaces would be established by bilaterally accepting self-signed certificates.

A trust relation can also be established across different TTP CAs as indicated by the dotted connections TC1 trusts TTP CA1 and TSP3 trusts TTP CA2. TTP CA1 also trusts TTP CA2 and vice versa. Thererefore, there is also a trust relation between TC1 and TSP3.

The dotted box "peer-to-peer trust" shows entities generating self-signed root certificates for exchange and import of these certificates. Entities in the overlapping part of the boxes (i.e. TC1, TSP2, and TSP3) import both the certificates issued by the TTP CAs and the connected peer-to-peer trust partner (i.e. TC3, TSP1) self-signed root certificates.

The use of the ISO/IEC 9594-8 framework and certificates also enables hierarchical CA structures with a root CA and subordinate level CAs. To limit implementation complexity and to support interoperability, the set of allowed certification levels shall be limited as indicated in 5.4.3.

The used type and structure of the model for the trust relation between the involved stakeholders is a decision of their contractual framework and depends on their technical requirements as well as the legal framework. The IM in an interoperable EFC system shall develop and maintain a suitable trust model. An example for EETS can be found in Annex F.

5.3.3 Trust model for TSP and service user relations

A standardized trust relation mechanism for the trust between TSP and service user is not required for interoperability. The solution for a trusted and secured communication between TSP and service user is a decision taken by the TSP based on the legal requirements for the contract between TSP and service user.

According to ISO 17573, the operation of the OBE and the provision of toll declarations in a secure way as required for toll charging is part of the toll service provider role. Requirements for achieving end-to-end security from the OBE to the toll chargers systems is therefore considered to be an internal interface of the TSP and then between TSP and TC. If security requirements for end-to-end security are imposed by the security policy, appropriate measures need to be implemented (e.g. usage of CEN/TS 16702-1 or CEN/TS 16702-2).

5.3.4 Trust model for Interoperability Management relations

The interoperability management may issue rules, regulations, and standards for the EFC system via commonly recognized channels. Communication between IM and TC or TSP (e.g. for certification of organizations or equipment) can be done with legacy methods such as physical mail and face to face meetings. No technical trust model is required for either of these communications.

For all other cases where electronic data exchange channels are required, the same technical trust model as defined in 5.3.2 shall be used.

5.4 Implementation

5.4.1 Setup of trust relations

After TC and TSP have agreed on the trust relation to be used and have signed a contract, they shall setup the technical trust relation.

The initial step for the setup of the trust relation is the import of a root certificate. This can be either the CA root certificate of an agreed TTP acting as a root CA or a (self-signed) root certificate of the TC or TSP respectively as already explained in 5.3.2.

If using a TTP, the retrieval of the CA root certificate shall be done according to mechanism 3 of ISO/IEC 11770-3:2015, Clause 12 or an equivalent. Several procedures might be used such as the following:

— downloading the certificate from a recognized and secure website;

— retrieving it per courier, if supported by the TTP;

— receiving it through signed e-mail, etc.

In the case of a peer-to-peer trust model, the exchange of the CA root certificates between TC and TSP shall be done using a secure communication channel which ensures the authenticity of the issuer and sender (proof of origin). The exchange of the root certificates shall be done with one of the public key transport mechanisms 1 or 2 as defined in ISO/IEC 11770-3:2015, Clause 12 (Public key transport).

— Mechanism 1: This mechanism shall fulfil the requirements and implement the measures of mechanism 1 of ISO/IEC 11770-3:2015, Clause 12, but using a certificate instead of a public key. As an example, it may be implemented by a physical meeting when both stakeholders (representatives of the TC and TSP, respectively) exchange valid identification tokens (e.g. passport) and documents proving the relationship with their organization.

  ISO/IEC 11770-3 public key transport mechanism 1 may be implemented as a part of the contract signing process to guarantee the certificate and public key authenticity.

— Mechanism 2: This mechanism shall fulfil the requirements and implement the measures of mechanism 2 of ISO/IEC 11770-3:2015, Clause 12, but using a certificate instead of a public key. As an example, it may be implemented by sending the root certificate through signed e-mail (using

another certificate, e.g. issued by a TTP) and then checking the fingerprint through telephone, or sending the certificate through courier which authenticates the sender.

The key token verification shall be done using fingerprint of the root certificate based on the algorithms defined in ISO 12855:2015 if ISO/IEC 11770-3 public key transport mechanism 2 is used.

5.4.2 Trust relation renewal and revocation

The root certificate shall have a validity and key length recommended for the use during the planned contract duration between TC and TSP.

NOTE For recommended key length and validity periods, see, for example, https://www.bsi.bund.de/DE/Themen/weitereThemen/ElektronischeSignatur/TechnischeRealisierung/Kryptoalgorithmen/kryptoalgorithmen_node.html (German only).

The trust relation shall automatically end when a root certificate is not replaced by the date of expiry.

The replacement of a root certificate shall be done in the same way as already defined in 5.4.1. All issued end-entity certificates of this root certificate shall be renewed according to the process defined in 5.4.3.

It shall be possible to revoke a root certificate by its issuer before the expiry of the validity for any reason. The revocation of a root certificate shall be done by a procedure similar to the early termination of the contract and results in a termination of the trust relation. The trust relation shall automatically end when a root certificate is revoked.

The information about revocation of a root certificate shall be distributed issuing a Certificate Revocation List (CRL) defined in ISO/IEC 9594-8 signed by the private-key of the root certificate. The digital signature of the message shall be verified with the public key of the originally imported root certificate.

Further activities that are necessary to handle compromised root certificates are beyond the scope of this Technical Specification because they usually require certain organizational measures.

5.4.3 Issuing and revocation of sub CA and end-entity certificates

The corresponding private-key of the root certificate shall only be used for signing end-entity or sub CA certificates. The purpose and usage of the end-entity certificate (e.g. TC to TSP communication) shall be defined by using the extended key usage extension in the ISO/IEC 9594-8 certificate.

The implementation of the certificate verification process shall support a certificate chain starting from a root certificate and contain at least up to four certificate levels (i.e. Root > CA1 > CA2 > CA3 > End-Entity) signed by a sub CA or end-entity private key.

Each entity shall have at least three different end-entity certificates to be used for

— secure communication channels,

— message signing, and

— message or key encryption purposes.

It is recommended that these end-entity certificates have a validity period of less than two years.

The information about revocation of an end-entity certificate shall be distributed issuing a Certificate Revocation List (CRL) defined in ISO/IEC 9594-8 signed by the private-key of the root certificate. The digital signature of the message shall be verified with the public key of the originally imported root certificate.

Exchange of certificates and CRLs is defined in Clause 9.

5.4.4 Certificate and certificate revocation list profile and format

The issued ISO/IEC 9594-8 certificates version 3 and CRL version 2 shall be according to the profile defined in IETF RFC 5280 with the update specified in RFC 6818. A compliant implementation to this specification to import and use the certificates and CRLs shall at least support all possible critical certificate and CRL extensions as defined in IETF RFC 5280 profile with the update specified in RFC 6818.

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

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

All certificates and CRL shall have a fingerprint in hexadecimal format based on the algorithms defined in ISO 12855:2015.

5.4.5 Certificate extensions

Considering IETF RFC 5280:2008, 4.2 and clarifications in ISO/IEC 9594-8:2014, Clause 7, the processing of critical extensions is delicate and shall be clearly agreed between the stakeholders (TC and TSP) to avoid implementation problems when the involved PKI platform technologies do not support the processing of certificates with certain extensions marked as critical.

Each extension used in a certificate shall be designated as either critical or non-critical. A certificate-using system shall reject the certificate if it encounters a critical certificate extension it does not recognize or a critical certificate extension that contains information it cannot process. A non-critical extension may be ignored if it is not recognized, but shall be processed if it is recognized.

NOTE Any extension that is flagged non-critical can cause inconsistent behaviour between certificate-using systems that will process the extension and certificate-using systems that do not recognize the extension and will ignore it.

A root certificate shall only use the certificate extensions listed below marked as critical:

a) key usage;

b) basic constraints.

An end-entity certificate shall use the certificate extensions listed below marked as critical:

a) key usage;

   The values in Table 1 shall be used.

b) Extended key usage with object identifier (OID) for the following:

— TC to TSP interface certificate;

— Front end to TSP back end interfaces certificate.

The following extensions may be present in root certificates as non-critical:

a) CRL distribution points;

b) authority information access.

The following extensions may be present in end-entity certificates as non-critical:

a) basic constraints;

b) CRL distribution points;

c) authority information access.

Table 1 — Values for key usage

Value	Meaning
0	Digital signature
1	Content commitment
2	Key encipherment
3	Data encipherment
4	Key agreement
5	Key certificate signing
6	CRL signing
7	Encipher only
8	Decipher only

6 Security requirements

6.1 General

A security requirement is a functional or non-functional requirement that needs to be satisfied in order to mitigate the threats to an EFC system or reducing its consequences.

Security requirements can be motivated by different sources. The following list presents some of the most relevant sources for EFC systems:

— generic information technology security requirements can be found in ISO Information Security Management System family of standards (e.g. in ISO/IEC 27001);

— security requirements for the protection of payment card data can be found in the Payment Card Industry Data Security Standard (PCI DSS),[12] if applicable;

— system-specific security requirements based on a threat analysis of the EFC system as presented in this Technical Specification in Annex D.

Mainly motivated by the threat analysis in Annex D, the following section specifies a basic set of information security requirements to protect the threatened assets in an EFC system.

The security policy for an EFC scheme or for an EFC operators system may consider additional security requirements driven by the mentioned standards or other relevant sources.

NOTE A general and complete IT security guideline for an information security management system is provided in the ISO 2700x family of standards (see 1.2 and 6.2).

In order to be compliant with this Technical Specification, an implementation shall fulfil all requirements selected in accordance with the applicable security policy. Any security measures from Clause 7 that are associated to the security requirements listed in this Clause shall be implemented when the relevant requirement is selected to be fulfilled.

If a requirement is not selected, it is also not mandatory to implement the associated security measure. In addition to the security policy, there are also some security profiles defined in Annex A to ease the implementation of a common set of security requirements. If an entity states compliance with one or more of the defined security profiles, all mentioned requirements are mandatory and the associated security measures have to be implemented.

Table 2 explains the notation of the requirements defined in this clause.

Table 2 — Notation of requirements

Table header	Meaning
No.	Unique number for every requirement to enable a later matching with the security measures.
Requirement	Definition of the requirement or recommendation.
DSRC	Marked with an X if this requirement is relevant for a DSRC system.
GNSS	Marked with an X if this requirement is relevant for an autonomous system.

Annex D provides a reference to the requirement(s) that is (are) driven by a given threat.

6.2 Information security management system

This Technical Specification provides measures to address potential EFC specific risks by defining requirements and detailed security measures which take into consideration the specific nature of EFC systems including their interoperable interfaces and specific assets. Those security measures have been designed based on an analysis of possible threats specifically applicable to EFC systems, without evaluating the real associated risks, which are system specific.

TCs and TSPs shall analyse and evaluate the risks associated with those threats and should also identify and analyse more generic information and communication technology risks applicable to organizations operating EFC systems, by performing a comprehensive risk analysis according to ISO/IEC 27005.

In order to effectively ensure information security in a holistic approach, TCs and TSPs shall establish, implement, operate, monitor, review, maintain, and continuously improve an Information Security Management System (ISMS) according to ISO/IEC 27001. The ISMS shall consider the EFC business processes specified in ISO 17573 within its scope and consider, among others, the risks identified in this Technical Specification. The security measures defined in this Technical Speciation shall be used while defining and implementing the controls for minimizing the impact of the identified risks.

The ISMS should also consider the generic companies business processes as part of its scope.

Table 3 — ISMS requirements

No.	Requirement	DSRC	GNSS
RQ.ISMS.1	An Information Security Management System (ISMS) according to ISO/IEC 27001 shall be established, implemented, operated, maintained, and continuously improved.	X	X
RQ.ISMS.2	Non-EFC specific threats shall be covered by a security measure or security control defined by the ISO/IEC 27002 or equivalent standard.	X	X

6.3 Communication interfaces

Communication interfaces are some of the most threatened links in the security chain of the EFC system as shown in the threat analysis in Annex D. Protecting interfaces against all threats without a basic risk analysis results in unreasonably high implementation costs. Table 4 lists all requirements identified in the threat analysis.

Table 4 — General interface requirements

No.	Requirement	DSRC	GNSS
RQ.IF.02	Data exchange shall be done using transmission channels with reliable availability.	X	X
RQ.IF.10	Data exchange shall guarantee data confidentiality.	X	X
RQ.IF.11	Data exchange shall guarantee data integrity.	X	X

Table 4 *(continued)*

No.	Requirement	DSRC	GNSS
RQ.IF.12	Data exchange shall guarantee the authenticity of the data originator.	X	X
RQ.IF.13	Data exchange shall guarantee non-repudiation with proof of origin.	X	X
RQ.IF.14	Data exchange shall guarantee non-repudiation with proof of delivery.	X	X
RQ.IF.20	Data exchange shall only be done between authenticated entities for the respective data exchange.	X	X
RQ.IF.30	Data exchange shall allow the detection of resent messages (protection against replay attacks).	X	X
RQ.IF.31	Data exchange shall allow the detection of mass rejection of toll declarations (protection against interface errors).	X	X
RQ.IF.32	Data exchange shall allow the detection of mass rejection of billing details (protection against interface errors).	X	X

6.4 Data storage

Data storage shall fulfil the following requirements independently of the state of data processing.

Table 5 — Data storage requirements

No.	Requirement	DSRC	GNSS
RQ.DS.01	Access to stored data shall only be granted after authorization.	X	X
RQ.DS.02	Access to stored data shall only be granted via defined interfaces and defined procedures.	X	X
RQ.DS.03	Stored data shall have an independent backup storage.	X	X
RQ.DS.05	Data storage shall guarantee data integrity.	X	X
RQ.DS.06	Access to data storage shall guarantee data confidentiality.	X	X
RQ.DS.07	Data storage shall guarantee non-repudiation with proof of origin for applicable data.	X	X
RQ.DS.08	Data storage shall guarantee non-repudiation with proof of delivery for applicable data.	X	X

6.5 Toll charger

The following clauses list requirements for protection of the TCs assets.

Table 6 — Toll charger requirements

No.	Requirement	DSRC	GNSS
RQ.TC.01	The TC shall determine if factual road usage is represented by a corresponding set of correct and complete toll declarations either acquired directly through the TCs RSE or through a TSP (enabled by RQ.TSP.51 for autonomous systems).	X	X
RQ.TC.02	In case the TC performs spot checks, he shall be able to determine the OBE working status (enabled by RQ.TSP.53 for autonomous systems).	X	X
RQ.TC.03	In case the TC performs spot checks, he shall be able to determine the ICC working status in the OBE.	X	X
RQ.TC.04	The TC shall check the integrity and authenticity of the received data as compared to the data sent from the OBE.	X	X
RQ.TC.05	The TC shall determine if toll declarations are based on data originating from a legitimate OBE or TSP back end (enabled by RQ.TSP.55).	X	X

Table 6 *(continued)*

No.	Requirement	DSRC	GNSS
RQ.TC.06	The TC shall make sure that any invoices generated in his name and on his behalf are conformant to the invoicing rules of his country (enabled by RQ.TSP.56).	X	X
RQ.TC.07	The TC shall ensure that the TSPs OBE is suitable for use in his toll.	X	X
RQ.TC.08	The TC shall check the model and make of OBE during a vehicle check (enabled by RQ.TSP.58) to identify the use of OBE versions not certified by the TC.	X	X
RQ.TC.10	The TC shall implement all necessary technical and organizational mechanisms for a correct implementation of a keyset for OBE communication provided by the TSP.	X	X
RQ.TC.12	The TC shall make sure that his back end system can cope with a sudden change of the customization information of an OBE (e.g. change of license plate over the air).	X	X
RQ.TC.13	The TC shall verify the correctness of billing details received from the TSP. NOTE This requirement is not applicable where the billing details are provided by the TC (this is covered by RQ.TSP.12).	n.a.	X
RQ.TC.20	The TC shall detect RSE damaging and recover the RSE functionality within an agreed time frame.	X	X
RQ.TC.21	The TC shall detect theft of RSE parts and recover the RSE functionality by a replacement of the stolen part within an agreed time frame.	X	X
RQ.TC.22	The TC shall implement RSE authentication measures for DSRC communication based upon security level 1 as defined in EN 15509:2014 or equivalent national standards/regulations.	X	X
RQ.TC.23	The TC shall detect RSE malfunction or underperformance and correct it within an agreed time frame.	X	X
RQ.TC.24	The RSE shall not allow unauthorized access to software and data.	X	X
RQ.TC.25	The TC shall guarantee confidentiality, integrity, and non-repudiation with proof of origin of a keyset for OBE communication during transfer to the RSE.	X	X
RQ.TC.30	The TC shall implement all necessary technical and organizational measures to avoid an enforcement case when a correct toll declaration was received.	X	X
RQ.TC.31	The TC shall make sure that the correct service user is charged for an enforcement case.	X	X
RQ.TC.32	The TC shall make sure that the enforcement case data are court proof.	X	X
RQ.TC.50	A data protection commissioner or delegate shall have the possibility to audit the system for compliance with data privacy regulations. NOTE Such audits shall be used to prove the data protection concept.	X	X
RQ.TC.51	The TC shall publish his procedures of collecting and processing personal data or register with the responsible data protection authorities.	X	X
RQ.TC.70	The TC shall exhaustively test all features of an RSE update before it is implemented.	X	X
RQ.TC.71	The TC shall have a rollback scenario ready before an RSE update is implemented.	X	X
RQ.TC.90	The TCs systems shall be designed in a way that access to stored or processed data is only possible within the legal context of the respective country (e.g. lawful interception).	X	X
RQ.TC.91	The TC shall provide non-repudiation with proof of origin for distributed toll context data.	X	X

Table 6 *(continued)*

No.	Requirement	DSRC	GNSS
RQ.TC.92	The TC shall only accept an OBE after detecting if an OBE belongs to a trusted TSP and that the TSP guarantees payment for that specific OBE (enabled by RQ.TSP.62).	X	X
RQ.TC.93	The TC shall only accept an OBE after detecting if the ICC in the OBE belongs to a trusted TSP and that the TSP guarantees payment for that specific ICC.	X	X
RQ.TC.94	The TC shall only accept an exception list after verification of non-repudiation with proof of origin.	X	X
RQ.TC.95	The TC shall be responsible for the availability of his back office interfaces according to agreed service levels.	X	X
RQ.TC.96	The TC shall be responsible for the availability of his RSE interfaces to an OBE according to agreed service levels.	X	X
RQ.TC.97	The TC shall verify the provided non-repudiation with proof of delivery in the TSPs acknowledge for distributed toll context data.	X	X
RQ.TC.98	The TC shall implement all necessary technical and organizational measures to guarantee the distribution of correct toll context data to the TSP.	X	X
RQ.TC.99	The TC shall acknowledge a received exception list and provide non-repudiation with proof of delivery to the TSP.	X	X

6.6 Toll service provider

The following clauses list requirements for the protection of the TSPs assets.

Table 7 — Toll service provider requirements

No.	Requirement	DSRC	GNSS
RQ.TSP.01	The TSP shall determine if factual road usage is represented by a corresponding set of correct and complete toll declarations.	n.a.	X
RQ.TSP.03	The TSP shall check the integrity and authenticity of the received road usage data sent from the OBE.	n.a.	X
RQ.TSP.04	The TSP shall determine if toll declarations are based on data originating from a legitimate OBE or ICC.	X	X
RQ.TSP.05	The OBE shall prevent or detect illegal modification of parameters through its external interfaces.	X	X
RQ.TSP.06	The ICC shall prevent or detect illegal modification of parameters through its external interfaces.	X	X
RQ.TSP.07	The OBE shall not allow the service user to modify fixed vehicle parameters.	X	X
RQ.TSP.08	The TSP shall detect duplicate or false OBE or ICC identities and block such OBE or ICC identities by placing them on the exception list.	X	X
RQ.TSP.09	The TSP shall notify the service user if the OBE or ICC is not working correctly.	X	X
RQ.TSP.10	The TSP shall determine if billing details are based on correct and complete road usage data.	n.a.	X
RQ.TSP.11	The TSP shall determine if factual road usage is represented by a corresponding set of billing details.	n.a.	X
RQ.TSP.12	The TSP shall verify the correctness of billing details received from the TC. NOTE This requirement is not applicable where the billing details are provided by the TSP (this is covered by RQ.TC.13).	X	X

Table 7 *(continued)*

No.	Requirement	DSRC	GNSS
RQ.TSP.13	The TSP shall accept received toll context data only after verification of non-repudiation with proof of origin.	X	X
RQ.TSP.14	The TSP shall provide exception lists including non-repudiation with proof of origin to the TC.	X	X
RQ.TSP.16	The OBE shall detect signal input inconsistencies.	n.a.	X
RQ.TSP.17	The TSP shall acknowledge received toll context data and provide non-repudiation with proof of delivery to the TC.	X	X
RQ.TSP.18	The TSP shall verify the provided non-repudiation with proof of delivery in the TCs acknowledge for a distributed exception list.	X	X
RQ.TSP.19	The TSP shall notify the TC about stolen or cloned OBE or ICC.	X	X
RQ.TSP.20	The TSP shall accept reports of stolen OBE or ICC by service users.	X	X
RQ.TSP.21	The TSP shall detect cloned OBE or ICC and block them by placing them on the exception list.	X	X
RQ.TSP.40	The OBE shall not allow change of internal data through the user interface except the data allowed to be changed.	X	X
RQ.TSP.41	The OBE shall only present intended data by the user interface.	X	X
RQ.TSP.42	The TSPs implementation of the front end and gathering and processing of data should be in compliance with the privacy requirements of the toll domain.	X	X
RQ.TSP.50	The TSP shall ensure that only authenticated service users have access to systems that manage their personal data.	X	X
RQ.TSP.51	The TSP shall enable the TC to determine if actual road usage is represented by a corresponding set of correct and complete toll declarations sent either directly from the OBE to the TCs RSE (in a DSRC system) or through a back office data exchange (required to enable RQ.TC.01 for autonomous systems).	X	X
RQ.TSP.53	The TSP shall enable the TC to perform spot checks through CCC (required to enable RQ.TC.02 for autonomous systems).	X	X
RQ.TSP.55	The TSP shall enable the TC to determine if toll declarations are based on data originating from a legitimate front end (required to enable RQ.TC.05 for autonomous systems) or OBE (in a DSRC system).	X	X
RQ.TSP.56	The TSP shall enable the TC to audit invoices to service users for tolls of his toll domain (required to enable RQ.TC.06).	X	X
RQ.TSP.57	The TSP shall enable the service user to check the correctness of an invoice.	X	X
RQ.TSP.58	The TSP shall enable the TC to check the model and make of OBE during a vehicle check (required to enable RQ.TC.08). NOTE The data in the relevant fields are set by the manufacturer during production. The responsibility of the TSP is to provide the TC with the different possible values for these fields to distinguish between the different OBE models and makes.	X	X
RQ.TSP.59	The TSP shall publish his procedures of collecting and processing personal data or register with the responsible data protection authorities.	X	X
RQ.TSP.60	The TSP shall only use equipment that passed certification by the TC and delivers the agreed quality of service.	X	X
RQ.TSP.62	The TSP shall enable the TC to detect if an OBE belongs to the TSP (required to enable RQ.TC.92).	X	X
RQ.TSP.70	The TSP shall exhaustively test all features of an OBE update before it is implemented (e.g. distributed over the air).	X	X

Table 7 *(continued)*

No.	Requirement	DSRC	GNSS
RQ.TSP.71	The TSP shall have a rollback scenario ready before an OBE update is implemented (e.g. distributed over the air).	X	X
RQ.TSP.80	The TSP shall implement all necessary technical and organizational quality control mechanisms for all OBE before they are distributed to the service users.	X	X
RQ.TSP.81	The TSP shall implement all necessary technical and organizational quality control mechanism for the provision of a key set for OBE communication to the TC.	X	X
RQ.TSP.82	The TSP shall implement all necessary technical and organizational quality control mechanism for the maintenance or exchange of OBE with low performance.	X	X
RQ.TSP.89	The TSP shall take protective measures against repudiation of invoices and its underlying confirmation data by service users.	X	X
RQ.TSP.90	The TSPs systems should be designed in a way that access to stored or processed data is only possible within the legal context of the respective countries (lawful interception).	X	X
RQ.TSP.91	The data communication between front end (OBE) and back end (TSP) shall be protected against interception in a way that access to stored or processed data is only possible within the legal context of the respective country (lawful interception).	n.a.	X
RQ.TSP.92	Customization of OBE shall be done in a secure way to guarantee data integrity and non-repudiation with proof of origin.	X	X
RQ.TSP.96	The TSP shall guarantee the availability of its POS network according to agreed service levels.	X	X
RQ.TSP.97	The TSP shall implement all necessary technical and organizational measures that an update of the customization information is correct.	X	X

6.7 Interoperability Management

The main security requirement for an interoperability management is to ensure the trust of all stakeholders in the interoperability scheme.

Table 8 — Interoperability management requirements

No.	Requirement	DSRC	GNSS
RQ.IM.01	The interoperability management shall issue an EFC security policy. NOTE Examples explaining the content of such a security policy are given in Annex E and Annex F.	X	X
RQ.IM.02	The interoperability management shall have or define one or more auditing bodies supervising the security implementation of the TSP and TC involved in the interoperable EFC scheme.	X	X

6.8 Limitation of requirements

The following requirements are included to document the limitation of security measures against some threats. This means that either no required security measure exists to protect against the threat, or the security measure is not really feasible because it is much too expensive. The requirements in Table 9 are not further treated in this Technical Specification.

Table 9 — Denial of service and hardware integrity threats

No.	Requirement	DSRC	GNSS
RQ.XX.01	Prevent denial of service attack. Prevent message transmission delay. This requirement covers attacks against a communication interface or against a whole service. A simple and/or cheap security measure does not exist due to the fact that long distance communication interfaces cannot be protected against all kinds of imaginable attacks.	X	X
RQ.XX.02	Prevent manipulating equipment; especially prevent OBE from HW manipulation. Such a requirement can be fulfilled by developing a tamperproof OBE, which is not deemed viable from a cost efficiency perspective.	X	X

7 Security measures — countermeasures

7.1 Overview

A security measure describes actions to be taken by the addressed entity to satisfy one or more security requirements. The actual implementation of the action is up to the entity. A security measure describes one possible solution to satisfy one or more security requirements.

In order to be compliant with this Technical Specification, an implementation shall fulfil all security measures that are associated to the security requirements in Clause 6 which are selected in accordance with the applicable security policy.

The table below explains the notation and relations of the security measures defined in this Clause.

Table 10 — Notation and relations of security measures

Table header	Meaning
No.	Unique number for every security measure
Security measure	Description of the security measure (countermeasure)
DSRC	Marked with an X if this security measure is relevant for a DSRC system
GNSS	Marked with an X if this security measure is relevant for an autonomous system
Fulfilled RQ	List of requirements that the security measure fulfils

NOTE For a detailed definition for the implementation of communication interface security measure, see Clause 8.

7.2 General security measures

This Technical Specification provides measures to address potential EFC specific risks by defining requirements and detailed security measures which take into consideration the specific nature of EFC systems including their interoperable interfaces and specific assets. Those security measures have been designed based on an analysis of possible threats specifically applicable to EFC systems, without evaluating the real associated risks, which are system specific.

Table 11 — General security measures

No.	Security measure	DSRC	GNSS
		Fulfilled RQ	
SM.101	The TC shall register the data processing application of the EFC system with the national data protection commissioner or authority for compliance with national data protection regulations if required by law.	X	X
		RQ.TC.50 RQ.TC.51 RQ.TSP.42 RQ.TSP.59 RQ.TSP.90 RQ.TSP.91	
SM.102	The TC and the TSP shall sign a Personal Data Assistant Agreement to be compliant to the national data protection regulations of the TC. In this agreement, the duties and rights of the TSP are stated in regard to the data processing.	X	X
		RQ.TSP.42 RQ.TSP.90 RQ.TSP.91	
		RQ.TC.06 RQ.TSP.56 RQ.TSP.89	
SM.103	The contracting parties of communication providers shall sign a Personal Data Assistant Agreement or equivalent to be compliant to the national data protection regulations of the TC. In this agreement, the duties and rights of the communication provider are stated in regard to the processing of personal data.	X	X
		RQ.TSP.42 RQ.TSP.90 RQ.TSP.91	
SM.104	The TC shall have the possibility to perform audit(s) of the TSP systems and procedures to proof the adherence to the registered data processing application and the Personal Data Assistant Agreement.	X	X
		RQ.TSP.42 RQ.TSP.90 RQ.TSP.91	
SM.105	The contracting parties of communication providers shall have the possibility to perform audit(s) of the communication providers systems and procedures to prove the adherence to the registered data processing application and the Personal Data Assistant Agreement or equivalent.	X	X
		RQ.TSP.42 RQ.TSP.90 RQ.TSP.91	
SM.106	The TSP shall establish a quality control process for the maintenance or exchange of low performing OBE within an agreed time frame. This process may be initiated by the detection of a low performing OBE by the TSP or by a report of such an OBE by the TC.	X	X
		RQ.TSP.82	
SM.107	The TSP shall enable the TC to audit invoices generated in his name. The TC shall periodically audit invoices to service users for tolls of his toll domain.	X	X
		RQ.TC.06 RQ.TSP.56 RQ.TSP.89	

7.3 Communication interfaces security measures

7.3.1 General

Security measures for the protection of data exchanged between entities using the different interfaces.

Table 12 — General interface security measures

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.200	The contracting parties of communication providers shall have proper service levels agreed and monitoring procedures in place that are able to detect any non-compliant behaviour of the communication provider.	X	X
		RQ.IF.02 RQ.TSP.60	

Table 12 *(continued)*

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.201	The TC and the TSP shall agree on defined interfaces and procedures for the access to stored data. These interfaces should be based on European or International Standards whenever possible.	X	X
		RQ.DS.02 RQ.DS.06 RQ.IF.20 RQ.IF.31 RQ.IF.32 RQ.TC.24 RQ.TC.90	
SM.202	The TC and the TSP shall only allow access to stored data for an authorized and authenticated entity.	X	X
		RQ.DS.01 RQ.IF.20 RQ.TC.24 RQ.TC.90 RQ.TSP.50	
SM.203	Implement the security measure or security control defined by ISO/IEC 27002 or equivalent.	X	X
		RQ.DS.03 RQ.DS.05 RQ.ISMS.2	
SM.204	The TC and TSP shall agree on a service level agreement defining quality goals and response times.	X	X
		RQ.TC.07 RQ.TC.20 RQ.TC.21 RQ.TC.23 RQ.TC.95 RQ.TC.96 RQ.TSP.60 RQ.TSP.96	
SM.205	Implement an Information Security Management System (ISMS) according to ISO/IEC 27001 or an equivalent.	X	X
		RQ.ISMS.1	
SM.207	Proof of origin authenticators shall be stored together with the data received.	X	X
		RQ.DS.07	
SM.208	Proof of delivery authenticators shall be stored together with the data delivered.	X	X
		RQ.DS.08	

7.3.2 DSRC-EFC interface

Table 13 — DSRC-EFC interface security measures

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.210	If toll declarations are acquired through the DSRC interface, the RSE shall request the OBE to calculate and provide a DSRC Message Authentication Code for TC (MAC_TC) over at least the ISO 14906 attribute PaymentMeans using a key known only to the TC and the TSP during an EFC transaction. The OBE shall respond accordingly.	X	n.a.
		RQ.IF.11 RQ.IF.12 RQ.IF.13 RQ.TC.01 RQ.TSP.55 RQ.TSP.89	

Table 13 *(continued)*

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.211	If toll declarations are acquired through the DSRC interface, the RSE shall request the OBE to calculate and provide a DSRC Message Authentication Code for TSP (MAC_TSP) over at least the ISO 14906 attribute PaymentMeans using a key known only to the TSP during an EFC transaction. The OBE shall respond accordingly.	X	n.a.
		RQ.IF.11 RQ.IF.12 RQ.IF.13 RQ.TSP.04 RQ.TSP.89	
SM.212	The OBE shall implement an access control mechanism for an EFC command addressing its EFC data attributes. The RSE shall implement the calculation of the corresponding access codes.	X	n.a.
		RQ.IF.20 RQ.TC.22 RQ.TSP.05 RQ.TSP.07 RQ.TSP.40 RQ.TSP.41	
SM.213	The RSE shall read, increment, and write a transaction counter to the OBE. The OBE shall support this.	X	n.a.
		RQ.TSP.21	
SM.214	The TSP shall implement a MAC_TSP authenticator in the OBE to prove its authenticity and integrity.	X	n.a.
		RQ.IF.11 RQ.IF.12 RQ.IF.13 RQ.TSP.03 RQ.TSP.04 RQ.TSP.62	
SM.215	The TSP shall implement a MAC_TC authenticator in the OBE to prove its authenticity and integrity.	X	X
		RQ.IF.11 RQ.IF.12 RQ.IF.13 RQ.TSP.62	

7.3.3 CCC interface

Table 14 — CCC interface security measures

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.220	If compliance checking is performed through the DSRC interface, the RSE shall request the OBE to calculate and provide a DSRC Message Authentication Code for TC (MAC_TC) over at least the ISO 14906 attribute PaymentMeans using a key known only to the TC and the TSP during a CCC transaction. The OBE shall respond accordingly.	n.a.	X
		RQ.IF.11 RQ.IF.12 RQ.IF.13 RQ.TSP.53	
SM.221	If compliance checking is performed through the DSRC interface, the RSE shall request the OBE to calculate and provide a DSRC Message Authentication Code for TSP (MAC_TSP) over at least the PaymentMeans attribute, using a key known only to the TSP during a CCC transaction. The OBE shall respond accordingly.	n.a.	X
		RQ.IF.11 RQ.IF.12 RQ.IF.13	

Table 14 *(continued)*

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.222	The OBE shall implement an access control mechanism for an EFC command addressing its CCC data attributes. The RSE shall implement the calculation of the corresponding access codes.	n.a.	X
		RQ.IF.20 RQ.TC.22 RQ.TSP.05 RQ.TSP.07 RQ.TSP.40 RQ.TSP.41 RQ.TSP.53	
SM.223	If toll declarations are acquired by the TSP, the OBE shall provide an undeniable proof of correct registration of road usage data for the given location and moment in time of the CCC transaction.	n.a.	X
		RQ.TC.01 RQ.TSP.51 RQ.TSP.53 RQ.TSP.89	

7.3.4 LAC interface

Table 15 — LAC interface security measures

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.230	If localization augmentation communication is performed through the DSRC interface, the RSE shall provide a MAC_TC over the LAC data sent to the OBE calculated with a key known only to the TC and the lacTime.	n.a.	X
		RQ.IF.11 RQ.IF.12 RQ.IF.13	
SM.231	The OBE shall implement an access control mechanism for an EFC command addressing the LAC data attributes. The RSE shall implement the calculation of the corresponding access codes.	n.a.	X
		RQ.IF.20 RQ.TC.22 RQ.TSP.05 RQ.TSP.07 RQ.TSP.40 RQ.TSP.41	

7.3.5 Front End to TSP back end interface

Table 16 — Front end to TSP back end interface security measures

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.240	The TSP shall implement an authenticator in the charge report which guarantees its authenticity and integrity.	n.a.	X
		RQ.TC.04 RQ.TSP.03	
SM.241	The bidirectional Front End to TSP back end communication shall be implemented using a secure connection.	n.a.	X
		RQ.IF.10 RQ.IF.11	

7.3.6 TC to TSP interface

Table 17 — TC to TSP interface security measures

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.250	The bidirectional TC to TSP back office data exchange shall be implemented using a secure connection with authentication.	X	X
		RQ.IF.10 RQ.IF.11 RQ.IF.31 RQ.IF.32	
SM.251	The TC shall link the billing details to a set of toll declarations provided by the TSP or include the associated event data for those toll declarations which have been acquired by him.	X	X
		RQ.TSP.10 RQ.TSP.11 RQ.TSP.12	
SM.252	If the TSP receives billing details from the TC, he shall compare them against the sent toll declarations to detect modifications and/or missing or additional toll declarations not sent to the TC in a GNSS environment.	n.a.	X
		RQ.TSP.10 RQ.TSP.11 RQ.TSP.12 RQ.TSP.89	
SM.253	Distribution of toll context data shall be undeniably signed by the TC and confirmed by the TSP in an agreed time frame with an authenticated response.	X	X
		RQ.IF.12 RQ.IF.13 RQ.IF.14 RQ.TC.91 RQ.TC.97 RQ.TSP.13 RQ.TSP.17	
SM.254	Distribution of the exception list shall be undeniably signed by the TSP and confirmed by the TC in an agreed time frame with an authenticated response.	X	X
		RQ.IF.12 RQ.IF.13 RQ.IF.14 RQ.TC.94 RQ.TC.99 RQ.TSP.14 RQ.TSP.18	
SM.255	The front end and/or the TSP back end shall undeniably sign charge reports and/or toll declarations.	n.a.	X
		RQ.IF.12 RQ.IF.13 RQ.TSP.55 RQ.TSP.89	
SM.256	The originator of a trust object shall undeniably sign it.	X	X
		RQ.IF.12 RQ.IF.13 RQ.TC.25 RQ.TSP.81	
SM.257	The TSP shall provide data underlying a specific toll declaration acquired through his system on demand of the TC (charge report and/or more detailed road usage data).	n.a.	X
		RQ.TSP.51	
SM.258	The TC shall provide the tariff table and all the relevant toll context data to the TSP to allow him to calculate the amount given in the billing details. NOTE Other means than ISO/TS 17575-3 could be used, e.g. publication on a website.	X	X
		RQ.TC.98 RQ.TSP.12	

Table 17 *(continued)*

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.259	The TSP shall be able to perform plausibility and completeness checks on received billing details. NOTE Those checks could be performed by the verification of the physical feasibility of trips in the toll domain.	X	X
		RQ.TSP.10 RQ.TSP.11 RQ.TSP.12	
SM.260	The TSP shall establish a control mechanism to ensure a correct provision of a key set for OBE communication to the TC.	X	X
		RQ.TSP.84	
SM.261	The TC and the TSP shall establish a data transfer protocol that allows the detection of duplicate messages as a protection against replay attacks.	X	X
		RQ.IF.30	
SM.262	The TSP shall provide the TC with the data about all valid OBE issued by him.	X	X
		RQ.TSP.55 RQ.TSP.58 RQ.TSP.62	
SM.263	The TC shall verify that an OBE is listed as valid by the TSP who issued it.	X	X
		RQ.TC.08 RQ.TC.92	
SM.264	The TC shall guarantee the correct manual entry or automatic processing of a keyset for OBE communication provided by the TSP.	X	X
		RQ.TC.10	
SM.265	The TC shall compare the billing details received from the TSP against the sent toll declarations to detect modifications, missing, or additional toll declarations not sent to the TC in a GNSS environment.	n.a.	X
		RQ.TC.13 RQ.TSP.89	
SM.266	The TC shall always acquire the correct and current service user details before starting an enforcement procedure.	X	X
		RQ.TC.31	

7.3.7 ICC interface

Table 18 — ICC interface security measures

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.270	The OBE shall calculate an authentication code to ICC complying with ISO/IEC 7816-3 command/response using a key known only to the ICC issuer.	X	X
		RQ.IF.11 RQ.IF.12	

7.4 End-to-end security measures

End-to-end security means front end to TSP to TC security measures.

Table 19 — End-to-end security measures

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.310	The OBE shall be designed as a clearly distinguished entity with a defined interface to the TC RSE. The OBE's functionality shall be tested to guarantee its functionality and it shall be auditable according to suitability for use procedure.	X	n.a.
		RQ.TC.01 RQ.TC.07 RQ.TC.12 RQ.TSP.51 RQ.TSP.60 RQ.TSP.70	
SM.311	The correct and trustworthy OBE functionality shall be periodically audited by the TSP and optionally by the TC or an independent entity on his behalf. NOTE An audit process can compare charge data of sample vehicles equipped with the OBE with known independent trip data.	X	X
		RQ.TC.01 RQ.TC.07 RQ.TSP.51 RQ.TSP.60	
SM.312	The TC shall perform plausibility and completeness checks on toll declarations acquired by the TSP in a GNSS environment.	n.a.	X
		RQ.TC.01 RQ.TC.12	
SM.313	The TC shall compare toll declarations acquired by the TSP with his own observations in accordance with privacy regulations.	n.a.	X
		RQ.TC.01	
SM.314	The TC shall verify if toll declaration(s) acquired by the TSP correctly correspond(s) to charge report(s) and/or road usage data.	n.a.	X
		RQ.TC.01	
SM.315	The TSP shall prepare a fall back scenario before any OBE update and initiate a rollback of the update when needed.	X	X
		RQ.TSP.71	
SM.316	The TC shall determine if the toll declarations have been produced by a trusted OBE by a message authentication code (MAC) or digital signature.	X	X
		RQ.IF.12 RQ.IF.13 RQ.TC.01 RQ.TC.04 RQ.TC.05	
SM.317	The TSP shall undeniably sign any update package before it is distributed over the air to ensure its integrity. The OBE shall check the integrity of the received update before the update is started.	X	X
		RQ.TSP.70	
SM.318	If toll declarations are acquired by the TSP, the registration of road usage data shall be based on a minimum set of functions in the OBE trusted by both the TSP and the TC. These functions shall directly or indirectly ensure the integrity of the toll declarations including non-repudiation with proof of origin.	n.a.	X
		RQ.TC.01 RQ.TC.04 RQ.TC.05 RQ.TSP.51 RQ.TSP.55 RQ.TSP.89	
SM.319	The TSP shall provide an undeniable proof of correct registration of road usage data for a defined location and moment in time or for a defined range of time and for a specified set of OBE(s) on demand to the TC.	n.a.	X
		RQ.TSP.51	
SM.320	The TC shall compare proof of correct registration of road usage data acquired by the TSP with his own observations in accordance with privacy regulations.	n.a.	X
		RQ.TC.01	
SM.322	The OBE shall be designed as a clearly distinguished entity with a defined interface to the proxy or TSPs back end. The OBE's functionality shall be tested to guarantee its functionality and it shall be auditable according to a defined procedure.	n.a.	X
		RQ.TC.07 RQ.TSP.01 RQ.TSP.60 RQ.TSP.70	

Table 19 *(continued)*

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.323	The TSP shall perform plausibility and completeness checks on toll declarations acquired by him. Those checks comprise the verification of the physical feasibility of trips in the toll domain compared with the actual toll declarations.	n.a.	X
		RQ.TSP.01 RQ.TSP.51	
SM.324	The TC shall prepare a fall back scenario before any RSE update and initiate a rollback of the update when needed.	X	X
		RQ.TC.71	
SM.330	The TSP shall provide the service user with the detailed transaction data upon request.	X	X
		RQ.TSP.57 RQ.TSP.89	

7.5 Toll service provider security measures

7.5.1 Front end security measures

Table 20 — Front end/OBE interface security measures

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.410	If compliance checking is performed through the DSRC interface, the OBE shall support a Compliance Checking Communication transaction over an interface with security as defined in ISO 12813:2015 when it passes such a RSE or use secure monitoring-compliance checking.	n.a.	X
		RQ.TC.01 RQ.TC.02 RQ.TSP.51 RQ.TSP.53	
SM.411	The TSP shall test a significant percentage of OBE delivered to him to achieve an accepted quality level according to ISO 2859 or equivalent.	X	X
		RQ.TSP.80	
SM.412	If localization augmentation communication is performed through the DSRC interface, the TSP shall store the value of the MAC_TC, KeyRef, and lacTime as part of the charge data and provide them as part of the charge report.	n.a.	X
		RQ.IF.12 RQ.IF.13 RQ.TSP.51	
SM.413	The OBE shall implement a role based access control mechanism for its DRSC interface. Any commands reserved to the TSP (i.e. other than those for DSRC-EFC, CCC, and LAC) shall be usable only by the TSP.	X	X
		RQ.IF.20 RQ.TC.22 RQ.TSP.05 RQ.TSP.07 RQ.TSP.40 RQ.TSP.41	
SM.414	The service user shall be notified about the OBE or ICC working status.	X	X
		RQ.TC.02 RQ.TC.03 RQ.TSP.09	
SM.415	The communication between OBE and proxy shall guarantee confidentiality, integrity, and authenticity.	n.a.	X
		RQ.IF.10 RQ.IF.11	
SM.416	The OBE shall prevent any illegal modification of parameters through its external interfaces or switch to a “NOT OK” state if it detects it.	X	X
		RQ.TSP.05 RQ.TSP.07	

Table 20 *(continued)*

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.417	The OBE shall switch to a "NOT OK" state if it detects signal input inconsistencies and the TSP shall be informed by the GNSS OBE.	n.a.	X
		RQ.TSP.16	
SM.418	The OBE shall not allow the service user to modify any data in the OBE except the data allowed to be changed through the user interface.	X	X
		RQ.TSP.05 RQ.TSP.07 RQ.TSP.40	
SM.419	The ICC shall not allow the service user to modify any data in the ICC.	X	X
		RQ.TSP.06	

7.5.2 Back end security measures

Table 21 — TSP back end security measures

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.420	The TSP shall verify if toll declaration(s) correctly correspond(s) to charge report(s) and/or road usage data.	n.a.	X
		RQ.TSP.51	
SM.421	The TSP shall determine if the charge report has been produced by a trusted front end.	n.a.	X
		RQ.TSP.01 RQ.TSP.04 RQ.TSP.08	
SM.422	The TSP shall verify the integrity of the charge report.	n.a.	X
		RQ.TSP.01	
SM.423	The TSP shall include stolen or cloned OBE or ICC in an exception list.	X	X
		RQ.TSP.08 RQ.TSP.19 RQ.TSP.20 RQ.TSP.21	
SM.424	The TSP shall detect a cloned OBE or ICC by using the transaction counter or by detecting multiple locations for the same OBE or ICC at the same time.	X	X
		RQ.TSP.08 RQ.TSP.21	
SM.425	The TSP shall use cryptographic measures to encrypt the sending of customization data to the OBE to guarantee data integrity and non-repudiation with proof of origin.	X	X
		RQ.TSP.92 RQ.TSP.97	
SM.426	The TSP shall verify the integrity of the charge report based on the MAC_TSP or digital signature.	n.a.	X
		RQ.IF.11 RQ.IF.12 RQ.IF.13 RQ.TSP.01 RQ.TSP.03 RQ.TSP.04	

7.6 Toll charger security measures

7.6.1 RSE security measures

Table 22 — RSE security measures

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.510	If toll declarations are acquired through the DSRC interface, the TC shall check the value of the MAC_TC using the key addressed by KeyRef and the RndRSE.	X	n.a.
		RQ.IF.11 RQ.IF.12 RQ.IF.13 RQ.TC.01 RQ.TC.04 RQ.TC.05	
SM.511	If toll declarations are acquired through the DSRC interface, the TC shall store the value of the transaction counter read-out of the OBE as part of the billing details.	X	n.a.
		RQ.TSP.21	
SM.512	If toll declarations are acquired through the DSRC interface, the TC shall store the value of the authenticated AttributeList, MAC_TSP, KeyRef, and RndRSE as part of the billing details.	X	n.a.
		RQ.IF.12 RQ.IF.13 RQ.TSP.21	
SM.513	If toll declarations are acquired by the TSP, the dedicated compliance checking RSE of the TC shall perform a Compliance Checking Communication transaction over an interface with security as defined in ISO 12813:2015 when an OBE passes it or use secure monitoring-compliance checking.	n.a.	X
		RQ.TC.01 RQ.TC.02 RQ.TC.05 RQ.TSP.53	
SM.514	If compliance checking is performed through the DSRC interface, the TC shall check the value of the MAC_TC using the key addressed by KeyRef and the RndRSE.	n.a.	X
		RQ.IF.11 RQ.IF.12 RQ.IF.13 RQ.TC.01 RQ.TC.04	
SM.515	If compliance checking is performed through the DSRC interface, the TC shall store the value of the authenticated AttributeList, MAC_TC, MAC_TSP, KeyRef, and RndRSE as part of the compliance check record.	n.a.	X
		RQ.IF.12 RQ.IF.13	
SM.516	The RSE's functionality shall be tested to guarantee its functionality.	X	X
		RQ.TC.70	

7.6.2 Back end security measures

Table 23 — TC Back end security measures

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.520	The TC shall perform plausibility and completeness checks on toll declarations acquired by him through the DSRC interface.	X	n.a.
		RQ.TC.12	

Table 23 *(continued)*

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.521	If toll declarations are acquired by the TSP and these are based on LAC data, the TC shall check the value of the MAC_TC using the key addressed by KeyRef and the RndRSE.	n.a.	X
		RQ.IF.11 RQ.IF.12 RQ.IF.13 RQ.TC.04 RQ.TC.05	
SM.522	The TC shall check the exception list to ensure a valid payment guarantee of the TSP for the existing service user.	X	X
		RQ.TC.92 RQ.TC.93	
SM.523	The TC shall use cryptographic measures to guarantee confidentiality, data integrity, and non-repudiation with proof of origin of a keyset for OBU communication during transfer to the RSE.	X	X
		RQ.TC.25	
SM.524	The TC shall make sure that all relevant toll declarations are considered before initiating enforcement procedures against a service user.	X	X
		RQ.TC.30	
SM.525	The TC shall use cryptographic measures to guarantee data integrity and non-repudiation with proof of origin for all recorded data regarding an enforcement case.	X	X
		RQ.TC.32	

7.6.3 Other TC security measures

Table 24 — Other TC security measures

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.530	If toll declarations are acquired through the DSRC interface, the TC shall compare them with his own observations in accordance with privacy regulations.	X	n.a.
		RQ.TC.01	

8 Security specifications for interoperable interface implementation

8.1 General

8.1.1 Subject

This subclause defines the detailed Technical Specifications supplementing the definitions in other standards that shall be implemented to fulfil the security measures defined in Clause 7 which are directly related to an application data unit (ADU) specification of an interoperable interface.

8.1.2 Signature and hash algorithms

The signature and hash algorithms for proof of message authenticity, integrity, and non-repudiation are defined in the following standards:

— security specifications for TC to TSP back office interface: ISO 12855:2015;

— security specifications for front end to TSP interface: ISO 17575-1:2015;

— non-DSRC MAC algorithm: CEN/TS 16702-1:2014;

— security specifications for CCC: ISO 12813:2015;

— security specifications for LAC: ISO 13141:2015.

8.2 Security specifications for DSRC-EFC

8.2.1 Subject

This subclause provides the implementation of security measures SM.210, SM.211, SM.212, SM.214, and SM215.

8.2.2 OBE

The OBE shall comply with the security measures of EN 15509:2014 security level 1 or equivalent national standards/regulations Europe.

8.2.3 RSE

The RSE shall comply with the security measures of EN 15509:2014 security level 1 or equivalent national standards/regulations outside Europe. The RSE may additionally support OBE complying with EN 15509:2014 security level 0 or equivalent national standards/regulations.

NOTE Security level 0 will provide compatibility with legacy OBE not supporting this Technical Specification.

The RSE shall request MAC_TC and MAC_TSP by addressing at least the PaymentMeans attribute. The RSE shall use one of the values of KeyRef corresponding to AuthenticationKey 1 to 4 to obtain the MAC_TC. The RSE shall use one of the values of KeyRef corresponding to AuthenticationKey 5 to 8 to obtain the MAC_TSP.

The exact values of KeyRef to be used shall be subject of agreement between toll charger and toll service provider.

9 Key management

9.1 Overview

Keys are a critical part of any security system that relies on cryptographic techniques. The appropriate protection of keys depends on a number of factors such as the type of application for which the keys are used, the threats they face, the different states the keys may assume, etc. Primarily, depending upon the cryptographic technique, they have to be protected against disclosure, modification, destruction and replay.

NOTE ISO/IEC 11770-1:2010, Annex A provides a list of threats to key management.

The objective of key management is the secure administration and use of key management services and therefore, the protection of keys is extremely important. Key management procedures depend on the underlying cryptographic mechanisms, the intended use of the key, and the security policy in use. Key management also includes those functions that are executed in cryptographic devices.

Key management is the administration and use of the services of generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation, and destruction of keying material.

9.2 Asymmetric keys

9.2.1 Key exchange between stakeholders

The exchange of root public keys, i.e. CA root certificates is defined in 5.4.1.

The exchange of entity public keys, i.e. end-entity certificates, shall be according to the public key transport mechanism 3 defined in ISO/IEC 11770-3.

In case of public key transport mechanism 3, the certificate verification procedure shall include the check of the certificate attribute "Extended Key Usage" with OID for the following:

— TC to TSP interface certificate;

— Front End to TSP Back End interfaces certificate.

9.2.2 Key generation and certification

Key generation and certification including certificate life cycle management (including, among others, key generation and certification processes) shall be performed at least according to Annex D of ISO/IEC 11770-1:2010.

Random bit generators (e.g. for the generation of session keys) shall comply with the requirements defined in ISO/IEC 18031.

NOTE Additional information and guidance for asymmetric key management and PKIs is provided for example in Reference [16].

9.2.3 Protection of keys

Private keys for ADU authentication and/or decryption shall be stored in a cryptographic module designed according to one of the following example security standards and protection profiles:

— ISO/IEC 19790 (minimum level 3);

— FIPS PUB 140-2 (minimum security level 3);

— common criteria protection profile BSI-PP-0002 (minimum EAL4).

9.2.4 Application

Each TSP shall have at least the following certificates for different uses:

— an ADU message signing certificate for ISO 12855:2015 messages;

— a certificate used for establishing secure communication channels (an IPsec/TLS certificate securing ISO 12855:2015 communication);

— if applicable a certificate used for establishing secure communication between front end to TSP back end in an autonomous system.

In case of charge report authentication by a signature according to SM.240, each OBE should have its own certificate.

Each TC shall have at least the following certificates for different uses:

— an ADU message signing certificate for ISO 12855:2015 messages;

— a key encryption certificate for message and/or key encryption purposes from the TSP;

— a certificate used for establishing secure communication channels (an IPsec/TLS certificate securing ISO 12855:2015 communication).

9.3 Symmetric keys

9.3.1 General

The following are three different applications for symmetric keys in an EFC system:

— the DSRC communication keys with two different characteristics, the DSRC master key, and the derived OBE DSRC key;

— the MAC keys with two different characteristics, the MAC master key and the derived OBE MAC key;

— the communication session keys to encrypt data of a communication channel between two entities.

9.3.2 Key exchange between stakeholders

9.3.2.1 General

Symmetric keys shall be exchanged by using the secured and authenticated channel. Such a channel is, for example, a VPN connection or a transfer using a courier, registered mail, etc. where the key message is stored on a memory device. The keys inside the message shall be additionally encrypted unless a cryptographic module with active key access authentication for the exchange is used.

The key encryption algorithm (including padding/encoding method) for the data element key below shall be performed according the following definitions.

9.3.2.2 Key encryption algorithm

The RSA algorithm with the RSA encoding method (REM1) according to ISO/IEC 18033-2 shall be used for key encryption.

RSA-2048 as defined in ISO/IEC 18033-2 shall be used for key encryption.

NOTE The required key encryption algorithm (REM1) according to ISO/IEC 18033-2 is equal to RSAES-OAEP in PKCS#1 v2.1 when KDF1 is applied.

9.3.2.3 Padding algorithm

If not otherwise defined, the padding algorithm used in this Technical Specification shall be the padding method 2 defined in ISO/IEC 9797-1:2011, 6.3.3.

For non-DSRC messages authenticated by a signature or MAC, the padding algorithm defined in this Clause shall be used, but the padding shall not be added to the message for transmission.

NOTE 1 Adding these padding bits to an ASN.1, encoded message is not supported by the ASN.1 compiler.

NOTE 2 The padding method 2 for hashes defined in ISO 10118-1:2000, A.2 is technically the same method.

9.3.2.4 Key transfer

The keys shall be signed by its originator and sent in the TrustObjectADU if an ISO 12855:2015 compatible back office data exchange is used.

The specific ASN.1 module TrustObjectCode has been defined in ISO 12855:2015 to verify the decryption of sent encrypted data (e.g. the DSRC master keys).

9.3.3 Key lifecycle

9.3.3.1 General

Random bit generators for the generation of symmetric keys shall comply with the requirements defined in ISO/IEC 18031.

Destroying of a key shall be done by overwriting the original key and any copy of the key in the memory and other backup data storages.

9.3.3.2 DSRC keys

DSRC master keys for DSRC-EFC, CCC, and LAC are generated and stored by the TSP at start-up and any time it is deemed necessary by the TSP or the interoperability management. DSRC master keys are associated to one or more values of the EFC-Context Mark, CCC-Context Mark, or LAC-Context Mark respectively as specified in Table 25.

Table 25 — Overview of DSRC keys

DSRC AID	Identified by	Applicable standard	Key usage	KeyType	Resulting authentication code
1	EFC_ContextMark + KeyRef	EN 15509:2014	Authentication key1 ... Authentication key4	0	MAC_TC
1	EFC_ContextMark + KeyRef	EN 15509:2014	Authentication key5 ... Authentication key8	0	MAC_TSP
1	EFC_ContextMark	EN 15509:2014	Access Key	1	AC_CR
20	CCC_ContextMark + KeyRef	ISO 12813:2015	Authentication key1 ... Authentication key4	2	MAC_TC
20	CCC_ContextMark + KeyRef	ISO 12813:2015	Authentication key5 ... Authentication key8	2	MAC_TSP
20	CCC_ContextMark	ISO 12813:2015	Access Key	3	AC_CR
21	LAC_ContextMark	ISO 13141:2015	Access Key	4	AC_CR
21	LAC_ContextMark + keyRefMAC_TC_LAC	ISO 13141:2015	LAC_Authentication-Key_TC	n.a.	MAC_TC

The derived DSRC keys shall be transmitted to and stored in the OBE.

The OBE may store additional DSRC keys for purposes beyond the mentioned DSRC applications:

— for writing of the EFC or CCC attributes which are marked as read-only. This is often referred to as personalization;

— for other DSRC applications hosted by the OBE like ERI/AVI.

Only the DSRC master keys are required to check the value of MAC_TC and the master keys to calculate the AC_CR are needed by the TC. Such master keys for DSRC EFC, CCC, and LAC shall be transmitted to the TC in accordance with 9.3.2.1.

DSRC master keys can be archived only if there is no OBE with a corresponding context mark active in the EFC system anymore.

DSRC master keys can only be destroyed if all data related to OBE with a corresponding context mark have been deleted.

9.3.3.3 MAC keys

MAC master keys are generated and stored by the TSP. Derived MAC keys are transmitted to and stored in the OBE.

MAC master keys shall be transmitted to the TC in accordance with 9.3.2.1.

In case the MAC of a ChargeReport should provide the same evidence compared to a signature based on a PKI (e.g. may be required by the secure monitoring concept), other requirements for MAC master key management will apply. For example, in such case, a MAC master key should be provided in a cryptographic module with limited functions (MAC verification with OK/NOK output only, no access to the key itself) to the TC.

9.3.4 Key storage and protection

9.3.4.1 Master keys

DSRC master keys and MAC master keys stored and used in the TC and TSP back end and in RSE shall be protected against unauthorized access.

DSRC master keys and MAC master keys, when stored for non-operative purposes (e.g. back-up or offline storage) or transferred internally in the system, shall be encrypted with an algorithm considered strong enough. The corresponding encryption key shall be stored in the same manner as described for the DSRC master keys and access to it shall be protected at least by a passphrase.

When stored in the clear and used for cryptographic operations, DSRC master keys and MAC master keys shall be kept in a secure environment and implemented by either of the following:

— a dedicated cryptographic HW module (e.g. a SAM);

— defined procedures, hardware provisions, and software security functions to address the threats in the specific environment as evaluated by the toll charger with reasonable measures.

Either solution shall fulfil the following security requirements and objectives:

a) manage secure key distribution, i.e. reception of encrypted keys and subsequent decryption for operational storage;

b) protect the cryptographic functions from unauthorized operation or use, including physical protection against unauthorized operation and/or deactivation to prevent unauthorized operation;

c) prevent unauthorized disclosure of the keys, including physical protection against disclosure and/or deletion to prevent disclosure (e.g. storage in volatile memory);

d) prevent use of keys with prohibited algorithms (e.g. prevent that encryption keys are used for authentication);

e) prevent unauthorized modification of the cryptographic algorithms, including unauthorized modification, substitution, insertion, and deletion of keys

f) provide indications about the operational state of the environment;

g) ensure that the implemented module solution performs properly when operating in an approved mode of operation;

h) detect errors in the operation of the implemented module solution and to prevent the compromise of keys resulting from these errors.

A certified cryptographic hardware module for storage of DSRC master keys and execution of key functions is recommended.

9.3.4.2 OBE keys

The OBE shall only store derived keys.

9.3.5 Session keys

Session keys used in the TC and TSP back end and in RSE shall be protected against unauthorized access during their lifetime. Session keys that are no more used shall be destroyed securely (e.g. overwriting of any copy of the key in memory and other data storages).

Annex A
(normative)

Security profiles

A.1 General

The profile definition uses the following pattern:

Risk assessment: Simplified risk assessment description.

Requirement profile: Defines the mandatory and recommended requirements to be fulfilled for profile compliance.

In order to claim conformance with a profile, all listed mandatory requirements shall be fulfilled.

A.2 Communication interface profiles

A.2.1 DSRC profile

The DSRC profile includes the requirements for the charging (EFC), the compliance check (CCC), and the localization (LAC) transactions.

Risk assessment: OBE charging transaction data received by the RSE contains all relevant information for the payment claim. Read out of OBE data by a fake RSE is possible without service user notice. This requires the authentication of the OBE access by the RSE.

Manipulation of such data and/or replay by a fake OBE is in principle simple even if technically difficult. This requires authentication mechanisms for OBE and RSE. Proof of message integrity is also required.

A service user may deny a certain road use (charging or CCC event). A faked LAC event can be used to prove, deny, or claim a cheaper road use. Faking or denying unprotected data is simple. Non-repudiation with proof of origin is required.

Communication eavesdropping is technically difficult and requires either access or a close location to the OBE or RSE and does not provide an attacker with substantial new data of the service user, vehicle, or RSE. Confidentiality is not required.

Requirement profile: Mandatory: RQ.IF.11 + RQ.IF.12 + RQ.IF.13 + RQ.IF.20 + RQ.IF.30

Recommended: -

A.2.2 TC to TSP profiles

The profile covers the not-secured communication between TC and TSP for back office data exchange according to ISO 12855:2015.

Profile A

Risk assessment: Communication eavesdropping and interception by third parties on a non-protected communication channel is easy and most likely. Modification of information as man in the middle and sending fake messages are also serious threats. Protection of sensitive service user data is also an issue. Message confidentiality, integrity, and authenticity shall be ensured.

The TSP or its service user may deny a toll declaration or billing detail. Therefore, non-repudiation with proof of origin is required.

The back office interface shall be protected against replay attacks.

Requirement profile: Mandatory: RQ.IF.02 + RQ.IF.10 + RQ.IF.11 + RQ.IF.13 + RQ.IF.30

Recommended: RQ.IF.12 + RQ.IF.20

Profile B (extended profile A)

Risk assessment: For a TSP, it is crucial that a TC receives exception lists. For a TC, it is crucial that a TSP uses valid and up-to-date toll context data. Therefore, this communication channel shall provide non-repudiation with proof of delivery.

Requirement profile: Mandatory: RQ.IF.02 + RQ.IF.10 + RQ.IF.11 + RQ.IF.13 + RQ.IF.14 + RQ.IF.30

Recommended: RQ.IF.12 + RQ.IF.20

A.2.3 Communication provider profile

This profile covers TC or TSP system internal interfaces using communication services of a third party. This includes, but is not limited to, the use of a telecommunication provider for the following:

— RSE to TC back end communication;

— OBE to proxy/TSP back end communication;

— TC or TSP internal back end communication.

Communication protection according to this profile can be used as proof for trustworthy data handling by a TSP or TC.

Risk assessment: Standard communication channels offered by communication providers can have some security mechanisms providing confidentiality, integrity, and authenticity against third party attacks. These possible security measures do not protect against communication eavesdropping and interception by insiders, e.g. personnel of the communication provider. Communication eavesdropping and interception by third parties is possible, but in most cases less likely. Protection of sensitive service user data is also an issue.

The risk is high enough to require additional from the communication provider independent, confidentiality, integrity, and authenticity measures for exchanged messages.

Requirement profile: Mandatory: RQ.IF.02 + RQ.IF.10 + RQ.IF.11

Recommended: -

A.2.4 ICC interface profile

The ICC interface profile includes the requirements for the reading account data and charging.

Risk assessment: ICC reading account data and ICC charging transaction data received by RSE through OBE contains all relevant information for the payment claim. Read out of ICC data by a fake RSE and/or OBE is possible without service user notice. This requires authentication of the RSE and/or OBE.

This requires authentication mechanisms for ICC and RSE and/or OBE.

Proof of message integrity is also required.

A user may deny a certain road use (charging). A faked ICC may be used to deny road use or claim a cheaper road use. Faking or denying unprotected data is simple. Non-repudiation with proof of origin is required.

Communication eavesdropping is technically difficult and requires either access or a close location to the ICC or OBE and does not provide an attacker with substantial new data of the service user. Confidentiality is not required.

Requirement profile: Mandatory: RQ.IF.11 + RQ.IF.12 + RQ.IF.13 + RQ.IF.20 + RQ.IF.30

Recommended: -

A.3 Data storage profiles

A.3.1 OBE data storages profile

This profile considers an OBE in the service user environment, i.e. a personalized OBE mounted in a vehicle.

Risk assessment: An illegal manipulation of data stored in the OBE may result in lower charge for the service user and loss of income for TC and TSP or even an interruption in the registration of road usage. An unauthorized read out of data stored in the OBE can result in a privacy violation of the service user.

Requirement profile: Mandatory: RQ.DS.01 + RQ.DS.02 + RQ.DS.05 + RQ.DS.07 + RQ.DS.06 if applicable (e.g. for keys)

Recommended: -

EXAMPLE 1 For an OBE mounted Inside of a vehicle, RQ.DS.02 is fulfilled for the HMI. An existing CN or DSRC interface requires additional access credentials covered by RQ.DS.01.

EXAMPLE 2 RQ.DS.02 + RQ.DS.05 + RQ.DS.06 + RQ.DS.07 can be guaranteed by a tamper evident OBE.

A.3.2 ICC data storage profile

This profile considers an ICC in the service user environment, i.e. an issued ICC inserted into an OBE.

Risk assessment: Not allowed manipulation of data stored in the ICC can result in lower charge for the service user and loss of income for TC or in an increase of stored values without paying. Not authorized read out of data stored in the ICC can result in a privacy violation to the service user.

Requirement profile: Mandatory: RQ.DS.01 + RQ.DS.02 + RQ.DS.05 + RQ.DS.07 + RQ.DS.06 if applicable (e.g. for keys)

Recommended: -

A.3.3 RSE data storage profile

The profile covers RSE at a publicly available location without any additional external protection measure (e.g. surveillance camera).

Risk assessment: An illegal manipulation of data stored in the RSE (before transmitted to the TSPs back end) may result in loss of income for TC and TSP. An unauthorized read out of data stored in the RSE (e.g. enforcement data) can result in a privacy violation to the service user and/or loss of reputation of the TC. Changing of the data originator identity (i.e. OBE identity) can result in charging a wrong service user. Access to the communication keys can allow the faking of OBE or the personalization of OBE without a TSP contract.

Requirement profile: Mandatory: RQ.DS.01 + RQ.DS.02 + RQ.DS.05 + RQ.DS.07 + RQ.DS.06 if applicable (e.g. for keys)

Recommended: -

A.3.4 Back end data storage profile

This profile is given for completeness only. A detailed method for the evaluation of security requirements can be found in ISO/IEC 27001. The requirement profile below does not apply to all kind of data stored in a back end, but each requirement will apply to a certain kinds of data.

Requirement profile: Mandatory: RQ.DS.01 + RQ.DS.02 + RQ.DS.03 + RQ.DS.05 + RQ.DS.07 + RQ.DS.08 + RQ.DS.06 if applicable (e.g. for keys)

Recommended: -

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 or an actor taking a role according to the requirements defined in this Technical Specification can 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;

— global statement of conformance;

— ICS proforma tables.

B.1.2 Abbreviations and conventions

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

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

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

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

m mandatory - The capability is required to be supported.

o optional - The capability may be supported or not.

n/a not applicable - In the given context, it is impossible to use the capability.

x prohibited (excluded) - There is a requirement not to use this capability in the given context.

o.i qualified optional - For mutually exclusive or selectable options from a set. "i" is an integer which identifies a unique group of related optional items and the logic of their selection which is defined immediately following the table.

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.

— Reference column: The reference column makes reference to this Technical Specificaton except where explicitly stated otherwise.

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

Y or y supported by the implementation.

N or n not supported by the implementation.

N/A, n/a or - no answer required (allowed only if the status is n/a directly or after evaluation of a conditional status).

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

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

range of values: < min value > .. < max value >

EXAMPLE 1: 5 .. 20

list of values: < value1 > , < value2 > , ..., < valueN >

EXAMPLE 1: 2, 4, 6, 8, 9

EXAMPLE 2: '1101'B, '1011'B, '1111'B

EXAMPLE 3: '0A'H, '34'H, '2F'H

list of named values: < name1 > (<val1 >), < name2 > (<val2 >), ..., < nameN > (<valN >)

EXAMPLE 1: reject(1), accept(2)

length: size (<min size > .. < max size >)

EXAMPLE 1: size (1 .. 8)

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

— References to items: For each possible item answer (answer in the support column) within the 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 "/" and 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 B.5.

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

— 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 or an actor taking a role 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.

Additional comments may be provided in the space at the bottom of the tables or separately, if necessary.

B.2 Identification of the implementation

B.2.1 General

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

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

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

B.2.2 Date of the statement

.....

B.2.3 Implementation Under Test (IUT) identification

IUT name:

.....

.....

IUT version:

.....

B.2.4 System Under Test (SUT) identification

SUT name:

.....

.....

Hardware configuration:

.....

.....

.....

Operating system:

.....

B.2.5 Supplier

Name:

.....

Address:

.....

.....

.....

Telephone number:

.....

Facsimile number:

.....

E-mail address:

.....

Additional information:

.....

.....

.....

B.2.6 Actor (if different from supplier)

Name:

.....

Address:

.....

.....

.....

Telephone number:

.....

Facsimile number:

.....

E-mail address:

.....

Additional information:

.....

.....

B.2.7 ICS contact person

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

Name:

.....

Telephone number:

.....

Facsimile number:

.....

E-mail address:

.....

Additional information:

.....

.....

.....

B.3 Identification of the standard

This ICS proforma applies to the following Technical Specification:

— ISO/TS 19299 *Electronic fee collection — Security framework*.

B.4 Global statement of conformance

Are all mandatory capabilities implemented? (Yes/No) .....

Answering "No" to this question indicates non-conformance to this Technical 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.5 Roles

Table B.1 — Roles

Item	Implemented role	Reference	Status	Support (Y/N)
1	Toll charger	5.2	o.1–1	
2	Toll service provider	5.2	o.1–1	
3	Interoperability management	5.2	o.1–1	

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

B.6 Trust model

Table B.2 — Trust model basics

Item	Supported functionality	Reference	Status	Support (Y/N)
1	Support for a trust model	5.4.1	m	
2	Use of ISO/IEC 9594-8 certificates	5.3.2	c.2–1	
3	Use of a hierarchical trust model (using a TTP)	5.2	o.2–1	
4	Use of a peer-to-peer trust model	5.2	o.2–1	
5	Root CA is performed by IM	5.2	c.2–2	
6	Root CA is performed by external TTP	5.2	c.2–3	
7	Use of trust model for all electronic data exchange channels between IM and TC/TSP	5.3.4	c.2–4	

o.2-1: It is mandatory to support at least one of these options.

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

c.2-2: IF Table B.1/3 and Table B.2/3 THEN o ELSE n/a.

c.2-3: IF (Table B.1/1 or Table B.1/2) and Table B.2/3 and not Table B.2/4 THEN m ELSE n/a.

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

Table B.3 — Trust relation setup

Item	Supported functionality	Reference	Status	Support (Y/N)
1	Importing CA root certificate from a TTP according to method 3 of ISO/IEC 11770-3:2015, Clause 12 or an equivalent	5.4.1	c.3–1	
2	- downloading the certificate from a recognized and secure website	5.4.1	o.3–1	
3	- retrieving it per courier, if it is supported by the TTP	5.4.1	o.3–1	
4	- receiving it via signed e-mail	5.4.1	o.3–1	
5	- other method, please describe	5.4.1	o.3–1	
6	Exchanging root certificates according to method 1 or 2 of ISO/IEC 11770-3:2015, Clause 12 or an equivalent	5.4.1	c.3–2	
7	- using mechanism 1 of ISO/IEC 11770-3:2015, Clause 12 or an equivalent	5.4.1	o.3–2	
8	- using mechanism 2 of ISO/IEC 11770-3:2015, Clause 12 or an equivalent	5.4.1	o.3–2	

Table B.3 *(continued)*

Item	Supported functionality	Reference	Status	Support (Y/N)
9	Key verification using a fingerprint based on the algorithms defined in ISO 12855:2015	5.4.1	c.3–3	

o.3-1: IF Table B.2/3 THEN it is mandatory to support at least one of these options.

o.3-2: IF Table B.2/4 THEN it is mandatory to support at least one of these options.

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

c.3-2: IF Table B.2/4 THEN m ELSE n/a.

c.3-3: IF Table B.3/8 THEN m ELSE n/a.

Table B.4 — Trust relation renewal and revocation

Item	Supported functionality	Reference	Status	Support (Y/N)
1	Length of private key of root certificate sufficient for duration of use	5.4.2	m	
2	Validity of root certificate according to the length of the private key	5.4.2	m	
3	Automatic termination of trust relation after expiration date of root certificate	5.4.2	m	
4	Replacement of a root certificate according to Table B.3	5.4.2	m	
5	Replacement of derived sub-CA or end-entity certificates according to Table B.5	5.4.2	m	
6	Support for revocation of root certificates	5.4.2	m	
7	Automatic termination of trust relation after revocation of root certificate	5.4.2	m	
8	Use of Certificate Revocation List as defined in ISO/IEC 9594-8	5.4.2	m	
9	Signing of revocation message for a root certificate	5.4.2	m	
10	Verification of the signature of revocation message for a root certificate	5.4.2	m	

Table B.5 — Issuing and revocation of sub-CA and end-entity certificates

Item	Supported functionality	Reference	Status	Support (Y/N)
1	Private key of root certificate only used for signing end-entity or sub CA certificates	5.4.3	m	
2	Extended Key Usage extensions according to ISO/IEC 9594-8 used	5.4.3	m	
3	Certificate validation process can handle at least four certificate levels	5.4.3	m	
4	End-entity certificate for securing communication channels	5.4.3	m	
5	End-entity certificate for message signing	5.4.3	m	
6	End-entity certificate for message/key encryption	5.4.3	m	
7	Use of Certificate Revocation List as defined in ISO/IEC 9594-8	5.4.3	m	
8	Signing of revocation message for a root certificate	5.4.3	m	
9	Verification of the signature of revocation message for a root certificate	5.4.3	m	

Table B.6 — Certificate and certificate revocation list profile and format

Item	Supported functionality	Reference	Status	Support (Y/N)
1	ISO/IEC 9594-8 certificates version 3 issued according to ISO/IEC 9594-8 with the update specified in RFC 6818	5.4.4	m	
2	ISO/IEC 9594-8 CRL version 2 issued according to ISO/IEC 9594-8 with the update specified in RFC 6818	5.4.4	m	
3	All certificates DER encoded and Base64 encoded (PEM certificate)	5.4.4	m	
4	All CRL DER encoded and Base64 encoded (PEM CRL)	5.4.4	m	
5	Key verification using a fingerprint based on the algorithms defined in ISO 12855:2015	5.4.4	m	

Table B.7 — Certificate and certificate revocation list profile and format

Item	Supported functionality	Reference	Status	Support (Y/N)
1	Agreement on the use of critical certificate extensions	5.4.5	m	
2	All certificate extensions defined either as critical or non-critical	5.4.5	m	
3	Rejection of unrecognized critical certificate extensions	5.4.5	m	
4	Rejection of critical certificate extensions with information unable to process	5.4.5	m	
5	Ignoring unrecognized non-critical certificate extensions	5.4.5	m	
6	Process recognized non-critical certificate extensions	5.4.5	m	
7	Only use key usage and basic constraints as critical certificate extensions in a root certificate	5.4.5	m	
8	Only use key usage with allowed values as critical certificate extensions in an end-entity certificate	5.4.5	m	
9	Only use extended key usage with OID for the TC to TSP back end interface	5.4.5	c.7–1	
10	Only use Extended Key Usage with OID for the TSP Front End to Back End interface	5.4.5	c.7–2	
11	Only use allowed non-critical certificate extensions in a root certificate	5.4.5	m	
12	Only use allowed non-critical certificate extensions in an end-entity certificate	5.4.5	m	

c.7.1: IF Table Table B.1/1 or Table B.1/2 THEN m ELSE n.a.

c.7.1: IF Table B.1/2 THEN m ELSE n.a.

B.7 Profiles

Table B.8 — Profiles

Item	Requirement	Reference	Status	Support (Y/N)
1	DSRC profile	A.2.1	o	
2	TC to TSP profile A	A.2.2	o	
3	TC to TSP profile B	A.2.2	o	

Table B.8 *(continued)*

Item	Requirement	Reference	Status	Support (Y/N)
4	Communication provider profile	A.2.3	o	
5	ICC interface profile	A.2.4	o	
6	OBE data storage profile	A.3.1	o	
7	ICC data storage profile	A.3.2	o	
8	RSE data storage profile	A.3.3	o	
9	Back end data storage profile	A.3.4	o	

B.8 Requirements

Table B.9 — Information system security requirements

Item	Requirement	Reference	Status	Support (Y/N)
1	RQ.ISMS.01	6.2	m	
2	RQ.ISMS.02	6.2	o	

Table B.10 — General interface requirements

Item	Requirement	Reference	Status	Support (Y/N)
1	RQ.IF.02	6.3	c.10–1	
2	RQ.IF.10	6.3	c.10–1	
3	RQ.IF.11	6.3	c.10–2	
4	RQ.IF.12	6.3	c.10–3	
5	RQ.IF.13	6.3	c.10–4	
6	RQ.IF.14	6.3	c.10–5	
7	RQ.IF.20	6.3	c.10–3	
8	RQ.IF.30	6.3	c.10–4	
9	RQ.IF.31	6.3	o	
10	RQ.IF.32	6.3	o	

c.10-1: IF Table B.8/2 or Table B.8/3 or Table B.8/4 THEN m ELSE o.

c.10-2: IF Table B.8/1 or Table B.8/2 or Table B.8/3 or Table B.8/4 THEN m ELSE o.

c.10-3: IF Table B.8/1 THEN m ELSE o.

c.10-4: IF Table B.8/2 or Table B.8/3 THEN m ELSE o.

c.10-5: IF Table B.8/3 THEN m ELSE o.

Table B.11 — Data Storage requirements

Item	Requirement	Reference	Status	Support (Y/N)
1	RQ.DS.01	6.4	c.11–1	
2	RQ.DS.02	6.4	c.11–1	
3	RQ.DS.03	6.4	c.11–3	
4	RQ.DS.05	6.4	c.11–1	
5	RQ.DS.06	6.4	c.11–2	
6	RQ.DS.07	6.4	c.11–1	
7	RQ.DS.08	6.4	c.11–3	

c.11-1: IF Table B.8/5 or Table B.8/6 or Table B.8/7 THEN m ELSE o.

c.11-2: IF Table B.8/5 or Table B.8/6 THEN m ELSE o.

c.11-3: Table B.8/7 THEN m ELSE o.

Table B.12 — Toll charger requirements

Item	Requirement	Reference	Status	Support (Y/N)
1	RQ.TC.01	6.5	c.12–1	
2	RQ.TC.02	6.5	c.12–1	
3	RQ.TC.03	6.5	c.12–1	
4	RQ.TC.04	6.5	c.12–1	
5	RQ.TC.05	6.5	c.12–1	
6	RQ.TC.06	6.5	c.12–1	
7	RQ.TC.07	6.5	c.12–1	
8	RQ.TC.08	6.5	c.12–1	
9	RQ.TC.10	6.5	c.12–1	
10	RQ.TC.12	6.5	c.12–1	
11	RQ.TC.13	6.5	c.12–1	
12	RQ.TC.20	6.5	c.12–1	
13	RQ.TC.21	6.5	c.12–1	
14	RQ.TC.22	6.5	c.12–1	
15	RQ.TC.23	6.5	c.12–1	
16	RQ.TC.24	6.5	c.12–1	
17	RQ.TC.25	6.5	c.12–1	
18	RQ.TC.30	6.5	c.12–1	
19	RQ.TC.31	6.5	c.12–1	
20	RQ.TC.32	6.5	c.12–1	
21	RQ.TC.50	6.5	c.12–1	
22	RQ.TC.51	6.5	c.12–1	
23	RQ.TC.70	6.5	c.12–1	
24	RQ.TC.71	6.5	c.12–1	
25	RQ.TC.90	6.5	c.12–1	

Table B.12 *(continued)*

Item	Requirement	Reference	Status	Support (Y/N)
26	RQ.TC.91	6.5	c.12–1	
27	RQ.TC.92	6.5	c.12–1	
28	RQ.TC.93	6.5	c.12–1	
29	RQ.TC.94	6.5	c.12–1	
30	RQ.TC.95	6.5	c.12–1	
31	RQ.TC.96	6.5	c.12–1	
32	RQ.TC.97	6.5	c.12–1	
33	RQ.TC.98	6.5	c.12–1	
34	RQ.TC.99	6.5	c.12–1	

c.12-1: IF Table B.1/1 THEN o ELSE n/a.

Table B.13 — Toll service provider requirements

Item	Requirement	Reference	Status	Support (Y/N)
1	RQ.TSP.01	6.6	c.13–1	
2	RQ.TSP.03	6.6	c.13–1	
3	RQ.TSP.04	6.6	c.13–1	
4	RQ.TSP.05	6.6	c.13–1	
5	RQ.TSP.06	6.6	c.13–1	
6	RQ.TSP.07	6.6	c.13–1	
7	RQ.TSP.08	6.6	c.13–1	
8	RQ.TSP.09	6.6	c.13–1	
9	RQ.TSP.10	6.6	c.13–1	
10	RQ.TSP.11	6.6	c.13–1	
11	RQ.TSP.12	6.6	c.13–1	
12	RQ.TSP.13	6.6	c.13–1	
13	RQ.TSP.14	6.6	c.13–1	
14	RQ.TSP.16	6.6	c.13–1	
15	RQ.TSP.17	6.6	c.13–1	
16	RQ.TSP.18	6.6	c.13–1	
17	RQ.TSP.19	6.6	c.13–1	
18	RQ.TSP.20	6.6	c.13–1	
19	RQ.TSP.21	6.6	c.13–1	
20	RQ.TSP.40	6.6	c.13–1	
21	RQ.TSP.41	6.6	c.13–1	
22	RQ.TSP.42	6.6	c.13–1	
23	RQ.TSP.50	6.6	c.13–1	
24	RQ.TSP.51	6.6	c.13–1	
25	RQ.TSP.53	6.6	c.13–1	

Table B.13 *(continued)*

Item	Requirement	Reference	Status	Support (Y/N)
26	RQ.TSP.55	6.6	c.13–1	
27	RQ.TSP.56	6.6	c.13–1	
28	RQ.TSP.57	6.6	c.13–1	
29	RQ.TSP.58	6.6	c.13–1	
30	RQ.TSP.59	6.6	c.13–1	
31	RQ.TSP.60	6.6	c.13–1	
32	RQ.TSP.62	6.6	c.13–1	
33	RQ.TSP.70	6.6	c.13–1	
34	RQ.TSP.71	6.6	c.13–1	
35	RQ.TSP.80	6.6	c.13–1	
36	RQ.TSP.81	6.6	c.13–1	
37	RQ.TSP.82	6.6	c.13–1	
38	RQ.TSP.89	6.6	c.13–1	
39	RQ.TSP.90	6.6	c.13–1	
40	RQ.TSP.91	6.6	c.13–1	
41	RQ.TSP.92	6.6	c.13–1	
42	RQ.TSP.96	6.6	c.13–1	
43	RQ.TSP.97	6.6	c.13–1	

c.13-1: IF Table B.1/2 THEN o ELSE n/a.

Table B.14 — Interoperability Management requirements

Item	Requirement	Reference	Status	Support (Y/N)
1	RQ.IM.01	6.8	c.14–1	
2	RQ.IM.02	6.8	c.14–1	

c.14-1: IF Table B.1/3 THEN o ELSE n/a.

B.9 Security measures

Table B.15 — General security measures

Item	Requirement	Reference	Status	Support (Y/N)
1	SM.101	7.2	c.15–1	
2	SM.102	7.2	c.15–1	
3	SM.103	7.2	c.15–1	
4	SM.104	7.2	c.15–1	
5	SM.105	7.2	c.15–1	
6	SM.106	7.2	c.15–1	
7	SM.107	7.2	c.15–1	

c.15-1: IF any requirement listed in Table 11 for this security measure is selected in Table B.9, Table B.10, Table B.11, Table B.12, Table B.13, or Table B.14, THEN m ELSE n/a.

Table B.16 — General interface security measures

Item	Measure	Reference	Status	Support (Y/N)
1	SM200	7.3.1	c.16–1	
2	SM201	7.3.1	c.16–1	
3	SM202	7.3.1	c.16–1	
4	SM203	7.3.1	c.16–1	
5	SM204	7.3.1	c.16–1	
6	SM205	7.3.1	c.16–1	
7	SM207	7.3.1	c.16–1	
8	SM208	7.3.1	c.16–1	

c.16-1: IF any requirement listed in Table 12 for this security measure is selected in Table B.9, Table B.10, Table B.11, Table B.12, Table B.13, or Table B.14, THEN m ELSE n/a.

Table B.17 — DSRC-EFC interface security measures

Item	Measure	Reference	Status	Support (Y/N)
1	SM210	7.3.2	c.17–1	
2	SM211	7.3.2	c.17–1	
3	SM212	7.3.2	c.17–1	
4	SM213	7.3.2	c.17–1	
5	SM214	7.3.2	c.17–1	
6	SM215	7.3.2	c.17–1	

c.17-1: IF any requirement listed in Table 13 for this security measure is selected in Table B.9, Table B.10, Table B.11, Table B.12, Table B.13, or Table B.14, THEN m ELSE n/a.

Table B.18 — CCC interface security measures

Item	Measure	Reference	Status	Support (Y/N)
1	SM220	7.3.3	c.18–1	
2	SM221	7.3.3	c.18–1	
3	SM222	7.3.3	c.18–1	
4	SM223	7.3.3	c.18–1	

c.18-1: IF any requirement listed in Table 14 for this security measure is selected in Table B.9, Table B.10, Table B.11, Table B.12, Table B.13, or Table B.14, THEN m ELSE n/a.

Table B.19 — LAC interface security measures

Item	Measure	Reference	Status	Support (Y/N)
1	SM230	7.3.4	c.19–1	

Table B.19 *(continued)*

Item	Measure	Reference	Status	Support (Y/N)
2	SM231	7.3.4	c.19–1	

c.19-1: IF any requirement listed in Table 15 for this security measure is selected in Table B.9, Table B.10, Table B.11, Table B.12, Table B.13, or Table B.14, THEN m ELSE n/a.

Table B.20 — Front end to TSP back end interface

Item	Measure	Reference	Status	Support (Y/N)
1	SM240	7.3.5	c.20–1	
2	SM241	7.3.5	c.20–1	

c.20-1: IF any requirement listed in Table 16 for this security measure is selected in Table B.9, Table B.10, Table B.11, Table B.12, Table B.13, or Table B.14, THEN m ELSE n/a.

Table B.21 — TC to TSP interface security measures

Item	Measure	Reference	Status	Support (Y/N)
1	SM250	7.3.6	c.21–1	
2	SM251	7.3.6	c.21–1	
3	SM252	7.3.6	c.21–1	
4	SM253	7.3.6	c.21–1	
5	SM254	7.3.6	c.21–1	
6	SM255	7.3.6	c.21–1	
7	SM256	7.3.6	c.21–1	
8	SM257	7.3.6	c.21–1	
9	SM258	7.3.6	c.21–1	
10	SM259	7.3.6	c.21–1	
11	SM260	7.3.6	c.21–1	
12	SM261	7.3.6	c.21–1	
13	SM262	7.3.6	c.21–1	
14	SM263	7.3.6	c.21–1	
15	SM264	7.3.6	c.21–1	
16	SM265	7.3.6	c.21–1	
17	SM266	7.3.6	c.21–1	

c.21-1: IF any requirement listed in Table 17 for this security measure is selected in Table B.9, Table B.10, Table B.11, Table B.12, Table B.13, or Table B.14, THEN m ELSE n/a.

Table B.22 — End-to-end security measures

Item	Measure	Reference	Status	Support (Y/N)
1	SM310	7.4	c.22–1	

Table B.22 *(continued)*

Item	Measure	Reference	Status	Support (Y/N)
2	SM311	7.4	c.22–1	
3	SM312	7.4	c.22–1	
4	SM313	7.4	c.22–1	
5	SM314	7.4	c.22–1	
6	SM315	7.4	c.22–1	
7	SM316	7.4	c.22–1	
8	SM317	7.4	c.22–1	
9	SM318	7.4	c.22–1	
10	SM319	7.4	c.22–1	
11	SM320	7.4	c.22–1	
12	SM322	7.4	c.22–1	
13	SM323	7.4	c.22–1	
14	SM324	7.4	c.22–1	
15	SM330	7.4	c.22–1	

c.22-1: IF any requirement listed in Table 19 for this security measure is selected in Table B.9, Table B.10, Table B.11, Table B.12, Table B.13, or Table B.14, THEN m ELSE n/a.

Table B.23 — Front end/OBE interface security measures

Item	Measure	Reference	Status	Support (Y/N)
1	SM410	7.5.1	c.23–1	
2	SM411	7.5.1	c.23–1	
3	SM412	7.5.1	c.23–1	
4	SM413	7.5.1	c.23–1	
5	SM414	7.5.1	c.23–1	
6	SM415	7.5.1	c.23–1	
7	SM416	7.5.1	c.23–1	
8	SM417	7.5.1	c.23–1	
9	SM418	7.5.1	c.23–1	
10	SM419	7.5.1	c.23–1	

c.23-1: IF any requirement listed in Table 20 for this security measure is selected in Table B.9, Table B.10, Table B.11, Table B.12, Table B.13, or Table B.14, THEN m ELSE n/a.

Table B.24 — TSP back end security measures

Item	Measure	Reference	Status	Support (Y/N)
1	SM420	7.5.2	c.24–1	
2	SM421	7.5.2	c.24–1	
3	SM422	7.5.2	c.24–1	

Table B.24 *(continued)*

Item	Measure	Reference	Status	Support (Y/N)
4	SM423	7.5.2	c.24–1	
5	SM424	7.5.2	c.24–1	
6	SM425	7.5.2	c.24–1	
7	SM426	7.5.2	c.24–1	

c.24-1: IF any requirement listed in Table 21 for this security measure is selected in Table B.9, Table B.10, Table B.11, Table B.12, Table B.13, or Table B.14, THEN m ELSE n/a.

Table B.25 — RSE security measures

Item	Measure	Reference	Status	Support (Y/N)
1	SM510	7.6.1	c.25–1	
2	SM511	7.6.1	c.25–1	
3	SM512	7.6.1	c.25–1	
4	SM513	7.6.1	c.25–1	
5	SM514	7.6.1	c.25–1	
6	SM515	7.6.1	c.25–1	
7	SM516	7.6.2	c.25–1	

c.25-1: IF any requirement listed in Table 22 for this security measure is selected in Table B.9, Table B.10, Table B.11, Table B.12, Table B.13, or Table B.14, THEN m ELSE n/a.

Table B.26 — TC Back End security measures

Item	Measure	Reference	Status	Support (Y/N)
1	SM520	7.6.2	c.26–1	
2	SM521	7.6.2	c.26–1	
3	SM522	7.6.2	c.26–1	
4	SM523	7.6.2	c.26–1	
5	SM524	7.6.2	c.26–1	
6	SM525	7.6.2	c.26–1	

c.26-1: IF any requirement listed in Table 23 for this security measure is selected in Table B.9, Table B.10, Table B.11, Table B.12, Table B.13, or Table B.14, THEN m ELSE n/a.

Table B.27 — Other TC security measures

Item	Measure	Reference	Status	Support (Y/N)
1	SM530	7.6.1	c.27–1	

c.27-1: IF any requirement listed in Table 24 for this security measure is selected in Table B.9, Table B.10, Table B.11, Table B.12, Table B.13, or Table B.14, THEN m ELSE n/a.

B.10 Specifications for interoperable interfaces security

Table B.28 — Security specifications for DSRC-EFC

Item	Specification	Reference	Status	Support (Y/N)
1	Security level 1 OBE for EFC	8.2.2	c.28–1	
2	Security level 1 RSE for EFC	8.2.3	c.28–2	
3	RSE requests MAC_TC	8.2.3	c.28–2	
4	RSE requests MAC_TC	8.2.3	c.28–2	
5	Agreement with TC/TSP on KeyRef	8.2.3	C.28–3	

c.28-1: IF Table B.1/2 THEN m ELSE n/a.

c.28-2: IF Table B.1/1 THEN m ELSE n/a.

c.28-3: IF Table B.1/1 or Table B.1/2 THEN m ELSE n/a.

Annex C
(informative)

Stakeholder objectives and generic requirements

C.1 General

For the motivation of this Technical Specification and for proper identification of the assets to be protected and possible threats, it is necessary to identify the various security objectives and generic requirements of the different stakeholders in an interoperability scheme.

Stakeholders are:

— toll chargers;

— toll service providers;

— service users;

— interoperability management entities like EETS member states or other third parties.

NOTE Either party may use subcontractors and/or delegate parts of their task/responsibility to third parties. However, with regard to the relation with the other party, the full responsibility and liability is assumed to remain completely with the subcontracting party. More specifically, this Technical Specification assumes, in this respect, for both a toll service provider and a toll charger that

1) subcontracting/delegation by one party shall have no consequences for the security measures required for another party, and

2) nevertheless, a (subcontracting/delegating) party may require that another party will use dedicated addresses and/or keys for specific purposes (messages).

EXAMPLE 1 A toll service provider may use a subcontractor for all his tasks up to issuing the declarations to the toll chargers. In such a case, the toll service provider may require a toll charger to use different addresses and keys for declaration related communication and charging (invoice) related communication.

EXAMPLE 2 A toll charger may (have to) entrust enforcement/compliance checking to a third party. In such a case, the toll charger may require a toll service provider to deal with dedicated addresses and dedicated keys for any communication related with these parties.

Security might not only be required by the stakeholder, but also imposed by regulations. This Clause presents the security requirements imposed by legislation and regulation in one or more toll charging environments.

The security framework specified in this Technical Specification is suitable to adhere to the following legal requirements in a toll charging environment:

a) the toll service shall provide security features relative to the protection of data stored, handled, and transferred between stakeholders in the toll service environment. The security features shall protect the interests of toll service stakeholders from harm or damage caused by lack of availability, confidentiality, integrity, authentication, non-repudiation, and access protection of sensitive user data appropriate to a multi-user toll service environment;

   EXAMPLE 3 For Europe, see Reference [7], Annex III, Article 1.5.2.

b) the toll service shall provide means for toll chargers to easily and unambiguously detect whether a vehicle circulating on their toll domain and allegedly using the toll service is actually equipped with a validated and properly functioning OBE providing truthful information;

EXAMPLE 4 For Europe, see Reference [7], Annex III, article 2.1.1.4.

c) the toll service shall provide means to protect toll chargers, toll service providers, and toll service users against fraud/abuse;

EXAMPLE 5 For Europe, see Reference [7], Annex III, article 1.5.1.

d) the toll service shall fulfil the requirements of legislation on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

EXAMPLE 6 For Europe, see Reference [6], article 2.7 and in Reference [7], Annex III, article 2.2, and Reference [9].

This list of regulatory requirements for the EETS may be supplemented, if applicable, with additional regulatory requirements for other toll charging environments. Nevertheless, this security framework is also suitable for countries with less stringent legal requirements.

C.2 Toll chargers

C.2.1 Toll chargers and their main interests

A toll charger is a legal entity that charges toll for vehicles in a toll domain.

See ISO 17573 for details.

The main asset for a toll charger to be protected is its income.

The main security requirements for a toll charger to protect its assets are the following:

— prevention of loss of income due to incorrect toll declarations, high collection costs, and/or irrecoverable debts;

— confidentiality of commercial details;

— adherence to the regulatory security requirements in the toll charging environments he is operating in.

A toll charger can operate in more than one toll charging environment. For Scandinavia, one may think, e.g. on a local system, EasyGo, and the EETS.

C.2.2 Security service requirements for a toll charger

Security requirements for a toll charger can be fulfilled with the following security services:

a) non-repudiation services for data received from external entities particularly from toll service providers (including acknowledgements);

NOTE These services are needed in order to prevent losses due to the denial of having sent charging related data.

EXAMPLE Toll declarations, compliance checking data, blacklists, etc.

b) accountability of toll declarations (for autonomous toll charging environments).

In an autonomous toll charging environment, a toll charger shall have the possibility to check for any vehicle observed in the toll charger domain,

1) whether or not the vehicle is equipped with a valid OBE,

2) the identity of the toll service provider responsible for this OBE, and

3) whether or not the vehicle's OBE behaves correctly,

4) whether or not the presence of this vehicle is correctly accounted for in the toll service provider's toll declaration.

C.3 Toll service providers

C.3.1 Toll service providers and their main interests

A toll service provider is a legal entity providing to his service users toll service(s) on one or more toll domains for one or more classes of vehicles.

See ISO 17573 for details.

The main asset for a toll service provider to protect is his business as an intermediary between his service users and the toll chargers.

The main security requirements for a toll service provider to protect its assets are the following:

— provide a secure toll service and trustworthy toll declarations for his service users;

NOTE 1 It is in the interest of the toll service provider that a service user can easily check the correctness of the toll declarations issued on his behalf.

— provide the toll chargers with trustworthy toll declarations;

NOTE 2 It is in the interest of the toll service provider that a toll charger can easily check the correctness of the toll declarations issued by a toll service provider.

— confidentiality of commercial details;

— adherence to the regulatory security requirements in the toll charging environments the devices provided by the toll service provider are operating;

— being able to check the correctness of the tolling operations and the behaviour of the toll service provider devices involved therein and to provide evidence of that to the other stakeholders;

— being able to protect his business from fraud and unjustified claims.

C.3.2 Security service requirements for a toll service provider

Security requirements for a toll service provider can be fulfilled with the following security services:

a) non-repudiation services for data received from external entities, particularly from toll chargers (including acknowledgements);

NOTE These services are needed in order to prevent losses due to the denial of having sent charging related data.

b) accountability for toll declarations (for autonomous toll charging environments) towards his service users. A service user shall be given the possibility to check any toll declaration that has been sent for his vehicle by the toll service provider to a toll charger;

c) confidentiality services for

1) communications between the toll service provider's central equipment and the toll charger's central equipment, and

2) communications between the toll service provider's central equipment and the service user's central equipment.

C.4 Service users

C.4.1 Service users and their main interests

The main interests of a service user are

— protection against unfair charging, and

— all involved entities ensuring the protection of user privacy.

See Annex G for detailed explanation about user privacy.

C.4.2 Service users requirements

The main objectives and security related requirements of a service user are the following:

a) possibility to check and control that the toll service provider is charging fairly;

EXAMPLE For Europe, see Reference [3], article 4.8.

b) ensuring that nobody (neither TC, nor TSP) collects data that is not absolutely necessary (data not required for tolling and not required by law);

c) protection of user data held by toll chargers and toll service providers against misuse;

d) protection of user privacy by toll chargers and toll service providers;

e) easy fulfilment of the obligation to pay the usage of road network.

C.5 Interoperability management

C.5.1 Interoperability management and its main interests

Interoperability management includes all actors responsible for ensuring interoperability, particularly for the interoperability requirements of the equipment to be used by toll chargers and toll service providers.

The main security requirements for an interoperability management actor to protect its assets are

— to ensure the trust of all stakeholders in the interoperability scheme, and

EXAMPLE To ensure that fraud or breach of any security measure have minimum impact on the whole schema.

— to avoid disputes between stakeholders and ensure interoperability.

C.5.2 Security service requirements for interoperability management

No specific security services are identified for the exchange of information with interoperability management actors.

Communication with an interoperability actor could be based on conventional information interchange such as registered letters, recorded letters signed for, recorded letters with proof of delivery signed by the addressee, and/or bailiff's notifications and so on.

Annex D
(informative)

Threat analysis

D.1 General

D.1.1 General approach

This informative part of the Technical Specification is the basic motivation for the security requirements which are normative.

The threat analysis is carried out using two different approaches. The first approach is based on the attack tree methodology (see D.2) where the attack driver is the intention and benefit of the attacker. This threat analysis has one weakness: that unintended threats by user and equipment which caused accidents or which had natural causes (e.g. climatic phenomenon) are not covered. Therefore, the second approach, an asset based threat analysis (see D.2, D.3) in parallel is required. A parallel threat analysis will also result in a more complete list of existing threats.

D.1.2 Naming conventions

The threat numbering scheme is based on the format TH.XXX.MG.NU where

— TH describes that the number is referring to a threat;

— XXX is the attacker class or the event causative entity or object class. The class enables the attack tree threats and asset based threats to have the same numbering scheme. The coding covers the following definitions:

  — SU – Service user;

  — TSP – Toll service provider;

  — TC – Toll charger;

  — HA – Hacker;

  — ACT – Activist;

  — CP – Communication provider;

  — EN – Enterprise;

  — GOV – Government;

  — FSA – Foreign state agency;

  — IM – Interoperability management;

  — OUT – Outsider;

  — DT – Data Transmission equipment;

  — IT – IT equipment;

— MG is the numeric equivalent of the main goal of the attacker or the asset at risk, e.g. avoid to pay toll, profile service users (attack tree goals being numbered 1xx), and billing details, service user

contract information, and OBE (assets at risk being numbered 2xx). The total sum of attacker goals and assets at risk are supposed to be less than 999 each. Each attacker class or asset at risk could then have allocated a number series enabling each attacker class or asset at risk to have up to 999 different goals or events;

— NU is the threat number within each main goal of the attacker or asset at risk.

D.1.3 Statement of completeness

The list of threats contained in this Annex is not a comprehensive all-encompassing list of all possible threats to an EFC system. Such a list can never be complete as there will always be threats to a specific implementation not included here and will always contain threats not applicable to a specific implementation. This list should just cover the most common threats to an EFC system. It will be the responsibility of the implementer of this Technical Specification to select the threats applicable to his specific implementation.

D.2 Attack trees based threat analysis

D.2.1 Overview

These attack trees are based on the approach proposed on the attack tree methodology introduced by Bruce Schneier (for detailed information, see Reference [26]). Attack trees provide a formal, methodical way of describing the security of systems based on varying attacks. Essentially, attacks are represented against a system in a tree structure with the goal as the root node and different ways of achieving that goal as leaf nodes.

A threat exists only if an attacker has a benefit from the attack. Threats without any benefit for an attacker are not considered threats in the current approach. It is possible that attacks are executed only for fun, but then the fun is the attacker's benefit. The main driver of a threat analysis is the benefit of the attack. A strong relationship between the threat, the attacker, and the goal of the attack exists. If there is no benefit, no attack will be performed and no threat exists which requires security measures.

The concept of an attack tree is that it is rooted in the class of user attempting the attack. The attacker is characterized by a primary motivation which defines the types of attack they perform and the exploitations of the outcomes of those attacks.

It is fully expected that the attacks that different classes of attackers will perform will overlap and a single attack can be attempted by several classes of attackers with differing motivations. The purpose of the attack tree is simply to maximize the coverage of the attack space by means of a structured approach, not to constrain or mandate specific solutions to these attacks based on the originating community.

D.2.2 System model

The system model shown below is used for the attack tree based threat analysis and the asset based threat analysis.

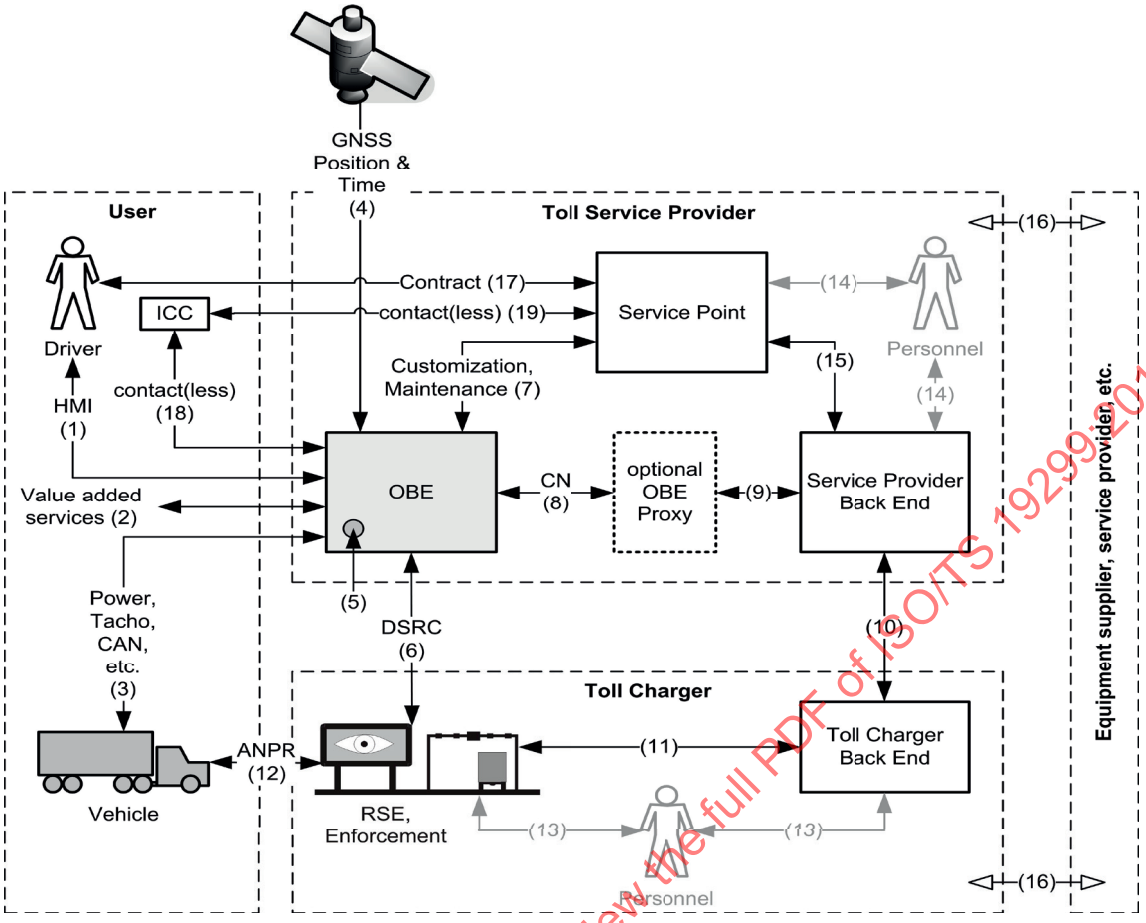

Figure D.1 — Attack trees — Assumed system model

The arrangement of components in the system is largely irrelevant to the attack tree approach since it is focused on the external elements of an attack. It does, however, provide a common terminology for the components within the system and also an enumeration of the externally visible attack surfaces (some of which are visible to certain attackers and not to others).

The interfaces and therefore, the most likely attack points are the following:

1) OBE user interface;
2) OBE data interface(s) for value added services (out of scope for this Technical Specification);
3) OBE vehicle interface: Connections to the vehicle, e.g. power supply, CAN bus, tachograph signal, etc.;
4) GNSS interface;
5) OBE tampering;
6) DSRC interface;
7) OBE customization and maintenance interface;
8) OBE cellular network interface;
9) OBE proxy to toll service provider interface (optional);
10) Toll service provider to toll charger Back End connection;
11) RSE interface to toll charger back end;

12) RSE compliance check interface for license/number plate recognition (ANPR);

13) TC personnel HMI and access to equipment;

14) TSP personnel HMI and access to equipment;

15) OBE distribution to TSP Back End communication;

16) delivering of equipment (e.g. OBE) and service provision (e.g. communication services) by suppliers and subcontractors. This is not a real interface, but attacks to be considered could be performed during equipment development, equipment manufacturing, service implementation, or service operation;

17) the service user declares all contractual parameters from the vehicle and for invoicing, used to customize the OBE;

18) physical or contactless interface from the OBE to the IC card;

19) physical or contactless interface for the loading of the IC card (out of scope for this Technical Specification).

D.2.3 Presentation of attack trees

The table below explains the template used for the attack tree based threat analysis.

Table D.1 — Notation and relations of threats

Table header	Meaning
No.	Unique number for every threat according to the numbering scheme described in D.1.2.
Threat	Description of the threat.
DSRC	Marked with an X if this requirement is relevant for a DSRC system.
GNSS	Marked with an X if this requirement is relevant for an autonomous system.
Related RQ	Reference to the requirement(s) driven by the threat..

D.2.4 Attacker class 1: Service user

D.2.4.1 General

The service user is defined as the person who is liable to pay the toll in the EFC-system and as such, can be a physical person, a company, or another legal entity. The service user class also includes the driver even when someone else pays the toll. Publicity is not an objective of the service user (this is dealt with under the activist attacker).

D.2.4.2 Goal 101: Avoiding payment of toll

The primary goal from a service user is his intention to avoid paying the toll. The effect of the attack is two-fold.

— Firstly, it represents a loss of income for the entity collecting the toll (i.e. toll charger).

— Secondly, if it becomes a wide-spread practice, it undermines the belief that the EFC system is correct and fair.

D.2.4.2.1 Sub goal: Manipulating the system to not register road usage

Table D.2 — SU goal: Avoiding payment of toll — Manipulating the system to not register road usage

No.	Threat	DSRC	GNSS
		Related RQ	
TH.SU.101.11	Blinding the road usage sensor The road usage sensor in a GNSS or a DSRC OBE could be blinded, for example, by covering the antenna where this is applicable.	X	X
		RQ.TC.01 RQ.TC.02 RQ.TSP.01 RQ.TSP.09 RQ.TSP.51	
TH.SU.101.12	Muting the OBE In the case where the OBE communication channel is separate from the road usage sensor itself (i.e. autonomous systems only), the communication signal might be temporarily or permanently blocked, thus avoiding the reporting of road usage data rendering the OBE "mute".	n.a.	X
		RQ.TC.01 RQ.TC.02 RQ.TSP.01 RQ.TSP.51 RQ.TSP.09	
TH.SU.101.13	Removing or destroying the OBE One of the simplest, yet most effective attacks is to destroy or remove the OBE. Removal could be permanent or temporal. Unless some counter measure is designed, this will render the vehicle "invisible" for the system.	X	X
		RQ.TC.02	
TH.SU.101.14	Disconnect the OBE power supply temporarily or permanently The simplest attack is to remove the OBE power supply. That can be done permanently or only temporarily, e.g. by inserting a switch in the power supply.	X	X
		RQ.TC.01 RQ.TC.02 RQ.TSP.01 RQ.TSP.09 RQ.TSP.51	
TH.SU.101.15	Jamming the GNSS road usage sensor e.g. with a portable jamming device	n.a.	X
		RQ.TC.01 RQ.TC.02 RQ.TSP.01 RQ.TSP.09 RQ.TSP.51	
TH.SU.101.16	Jamming the DSRC road usage sensor e.g. with a portable jamming device or an ITS-system	X	n.a.
		RQ.TC.01 RQ.TC.02 RQ.TSP.01 RQ.TSP.09 RQ.TSP.51	
TH.SU.101.17	Destroying the ICC One of the simplest, yet most effective attacks is to destroy the ICC and deny responsibility for the malfunction.	X	X
		RQ.TC.02	
TH.SU.101.18	Jamming the ICC interface e.g. with a portable jamming device Jamming the ICC interface during charging transactions would look like a malfunction.	X	X
		RQ.TC.01 RQ.TC.02 RQ.TSP.01 RQ.TSP.09 RQ.TSP.51	

D.2.4.2.2 Sub goal: Manipulating the system to register the wrong road usage

Table D.3 — SU goal: Avoiding payment of toll — Manipulating the system to register the wrong road usage

No.	Threat	DSRC	GNSS
		Related RQ	
TH.SU.101.21	Manipulating the input to the road usage sensors This attack is typically relevant in systems where road usage is continually recorded (such as in GNSS-based systems) and involves spoofing the signal that goes into the sensor. It does not require any modifications to the OBE since it is directed at the road usage signal before it enters the OBE.	n.a.	X
		RQ.TC.01 RQ.TSP.01 RQ.TSP.16 RQ.TSP.51	
TH.SU.101.22	Manipulating the road usage sensors This attack involves modifying the road usage sensors, for example, by replacing them or filtering their output to generate data that results in a lower toll. It is performed in real time and modifies road usage data as it is collected.	n.a.	X
		RQ.TC.01 RQ.TSP.01 RQ.TSP.51	
TH.SU.101.23	Manipulating the road usage data collection software The software calculating the road usage based on the sensor inputs is altered in such a way that a lower road usage will be recorded, stored, and transmitted to the back end (only possible in autonomous systems).	n.a.	X
		RQ.TC.01 RQ.TSP.01 RQ.TSP.51	
TH.SU.101.24	Manipulating the road usage data after collection in the OBE or ICC In the case where several items of road usage data remain under the control of the service user, before being reported to another party, the service user has the possibility of modifying the road usage data taking the whole data set into account.	n.a.	X
		RQ.TC.01 RQ.TC.04 RQ.TSP.01 RQ.TSP.03 RQ.TSP.07 RQ.TSP.40 RQ.TSP.51	
TH.SU.101.25	Manipulating the road usage data in transit from the OBE or ICC Road usage data can be manipulated as it is communicated from the OBE or ICC.	n.a.	X
		RQ.TC.01 RQ.TC.04 RQ.TSP.01 RQ.TSP.03 RQ.TSP.51	
TH.SU.101.26	Use an OBE simulator to produce the required road usage “toll declaration” Prevent the OBE from sending the road usage to the back end and produce a fake data set with OBE simulation equipment that is sent instead.	n.a.	X
		RQ.TC.01 RQ.TC.05 RQ.TSP.01 RQ.TSP.04 RQ.TSP.51 RQ.TSP.55	
TH.SU.101.27	Change user input according to sensed or known external audit-checks Update the tariff relevant settings of an OBE before known audit-check event (CCC or camera equipment) takes place.	X	X
		RQ.TC.02 RQ.TSP.05 RQ.TSP.40 RQ.TSP.53	
TH.SU.101.28	Use an ICC simulator to produce the required data for an OBE at the time of road usage Use ICC simulation equipment instead of a real ICC.	n.a.	X
		RQ.TC.01 RQ.TC.05 RQ.TSP.01 RQ.TSP.04 RQ.TSP.51 RQ.TSP.55	

D.2.4.2.3 Sub goal: Faking toll parameters

Table D.4 — SU goal: Avoiding payment of toll — Faking toll parameters

No.	Threat	DSRC	GNSS
		Related RQ	
TH.SU.101.31	Faking vehicle parameters The service user sets vehicle parameters to a value that does not reflect reality, but that lowers the toll.	X	X
		RQ.TC.02 RQ.TSP.05 RQ.TSP.40 RQ.TSP.53	
TH.SU.101.32	Faking identity The service user sets OBE, ICC or user identity parameters to a value that does not reflect reality and that lowers the toll (e.g. reduced tariff for disabled person) or charges the toll to another (or a fake) user.	X	X
		RQ.TC.02 RQ.TSP.05 RQ.TSP.06 RQ.TSP.08 RQ.TSP.40 RQ.TSP.53	

D.2.4.2.4 Sub goal: Manipulating the system to loose road usage data

Table D.5 — SU goal: Avoiding payment of toll — Manipulating the system to loose road usage data

No.	Threat	DSRC	GNSS
		Related RQ	
TH.SU.101.41	Force insufficient OBE data buffer Preventing the OBE from sending data to the back end for as long as possible to produce insufficient memory that results in road usage no longer being collected or overwriting old road usage not taken in account in the back end.	n.a.	X
		RQ.TC.01 RQ.TC.02 RQ.TSP.01 RQ.TSP.09 RQ.TSP.51 RQ.TSP.53	
TH.SU.101.42	Bribing TC or TSP employee to manipulate the service user account The service user influences (e.g. bribes, as family or friend) an employee to manipulate his account to pay lower toll to avoid a penalty, etc.	X	X
		RQ.ISMS.2	
TH.SU.101.43	Denying presence in toll domain The service user denies the presence in a toll domain at a given time and thus, denies payment of invoice.	X	X
		RQ.TSP.89	
TH.SU.101.44	Using an OBE without a valid contract with a TSP SU uses an OBE without a valid contract with a TSP to avoid payment to the TSP.	X	X
		RQ.TC.92	
TH.SU.101.45	Using an ICC without a valid contract with a TSP SU uses an ICC without a valid contract with a TSP to avoid payment to the TSP.	X	X
		RQ.TC.93	

D.2.4.3 Goal 102: Undermining the system

A secondary goal is to undermine the system out of discontent with its design or plain existence. This secondary threat might cause the service user to perform attacks that due to their costs are not justifiable from an economic perspective. The effect of the attack is two-fold:

— Firstly, it represents a loss of income for the entity that is collecting the toll (i.e. toll charger).

— Secondly, if it becomes a wide-spread practice, it undermines the belief that the EFC system is correct and fair.

All the attacks described in Goal 102 might also be performed without the economic incentive, but be motivated by spite.

D.2.4.4 Goal 103: Protecting the service users own privacy

A service user might be discontent with the privacy protection features of a mandatory EFC system causing her/him not to disclose data that is crucial for the functioning of the system. The effect of the attack is two-fold.

— Firstly, it represents a loss of income for the entity that is collecting the toll (i.e. toll charger).

— Secondly, if it becomes a wide-spread practice, it undermines the belief that the EFC system is correct and fair.

All the attacks described in Goal 103 might also be performed without the economic incentive, but be motivated by a concern for the service user's own privacy.

D.2.5 Attacker class 2: Toll service provider

D.2.5.1 General

The toll service provider is the legal entity providing toll services to his service users in one or more toll domains for one or more classes of vehicles.

D.2.5.2 Goal 104: Increase revenue from service user/overcharge service user

In order for this to be considered an attack, the way to increase revenue from the user shall involve overcharging, that is, charging a toll that is larger than what is motivated by the actual road usage. The motivation is short-term financial gain.

Table D.6 — TSP goal: Increase revenue from service user/overcharge service user

No.	Threat	DSRC	GNSS
		Related RQ	
TH.TSP.104.01	Faking road use The TSP could charge a service user for road usage that has never taken place. He calculates the fake charge based on the toll context data and tariffs of a TC without involving them.	X RQ.TC.13 RQ.TSP.57	X
TH.TSP.104.02	Using incorrect toll context data The TSP could use faulty toll context data to inflate the toll charged to the service user while also using the correct data that results in a lower toll declared to the TC and thus, be able to keep the difference.	n.a. RQ.TSP.17 RQ.TSP.57	X
TH.TSP.104.03	Overcharging the service user The TSP charges the service user a higher amount as calculated by himself or by the TC(s) based on the billing details. The TSP changes the invoice data received from the TC to increase the charge.	X RQ.TSP.57	X
TH.TSP.104.04	Modify toll declarations The TSP modifies toll declarations acquired and reported by him to increase his remuneration.	n.a. RQ.TC.13 RQ.TSP.12	X

D.2.5.3 Goal 105: Profiling of service user(s)

The toll service provider could perform profiling for its own gain or could be pressurized by a third party (e.g. a repressive government or a criminal organization) to collect and provide service user profiles.

The attack could be directed towards the whole service user collective or an individual service user. When the whole collective is profiled, it could be used to target commercial offerings [own or others; in the second case, probably in combination with reselling of data about tolled service users (see Goal 106)] to a suitable service user. Yet, political or criminal motives are also possible.

If a single service user is profiled, the motivations could, in addition, also be of a personal nature, stalking of celebrities, jealous spouses, etc.

Table D.7 — TSP goal: Profiling of service user(s)

No.	Threat	DSRC	GNSS
		Related RQ	
TH.TSP.105.01	Accessing and compiling information on the service users	X	X
	The TSP collects and compiles service user profiles, based on the collected vehicle position data and/or vehicle mileage, in a way that is not allowed according to law or contract.	RQ.TSP.59	

D.2.5.4 Goal 106: Reselling of data about service user(s)

The toll service provider could gain financially from reselling confidential and sensitive data about the service user(s) to other commercial parties operating data mining systems, for example, to an insurance company, advertising industry, or governmental agencies which are active in anti-terrorism, etc.

Table D.8 — TSP goal: TSP's reselling of data about service user(s)

No.	Threat	DSRC	GNSS
		Related RQ	
TH.TSP.106.01	Resell service user data to third party	X	X
	The collected service user and vehicle position data are sold and transmitted to an external party without the knowledge of the SU.	RQ.TSP.59	
TH.TSP.106.02	Allow service user tracking by third parties	X	X
	The collected service user and vehicle position data, maybe more data than is required for charging purposes, is sold and transmitted "in real time" to third parties without the permission of the service user for service user and vehicle tracking. The attack is either performed by the TSP or by his staff without the knowledge of TSP.	RQ.ISMS.1 RQ.ISMS.2 RQ.TSP.59	
TH.TSP.106.03	Provide specific data mining based on road usage data	X	X
	Perform specific data mining and statistics on demand and distribute the (even anonymous) results to commercially interested parties.	RQ.TSP.59	

D.2.5.5 Goal 107: Reduction of payments to toll charger

The intention is to pay the toll charger less than it is entitled to due to the road usage of the service user. The motivation is short-term financial gain.

Table D.9 — TSP goal: Reselling of data about service user(s)

No.	Threat	DSRC	GNSS
		Related RQ	
TH.TSP.107.01	Modifying road usage data reported from the OBE The TSP could modify the road usage data to be sent to the TC so that the toll is deflated, for example, slightly shifting the time values to put the trip in another, cheaper, time class, while using the correct data to charge the service user.	n.a.	X
		RQ.TC.01 RQ.TSP.51	
TH.TSP.107.02	Suppressing reporting of road use The TSP could refrain from reporting road usage to the TC while using the correct data to charge the service user.	n.a.	X
		RQ.TC.01 RQ.TSP.51	
TH.TSP.107.03	Faulty interpretation of road usage data In certain set ups, the TSP will have the ability to interpret the road usage data in a way that inflates the toll that is due to the TC while using the correct data to charge the use. An example could be if map matching is under the control of the TSP and road usage sensor data are intentionally misinterpreted to mean a faulty, less expensive, route.	n.a.	X
		RQ.TC.01 RQ.TSP.51	
TH.TSP.107.04	Using incorrect toll context data If the TSP is in control of computing the final toll or some data on which the final toll is computed, it could use faulty toll context data to deflate the toll to be paid to the TC while using the correct data that results in a higher toll requested from the service user and thus, be able to keep the difference.	n.a.	X
		RQ.TC.01 RQ.TC.17 RQ.TSP.51	
TH.TSP.107.05	Manipulate charging data during enrichment A TSP which has been requested by a TC to enrich determined charging data may manipulate them to reduce the final toll while using the correct data to charge the service user.	n.a.	X
		RQ.TC.01 RQ.TSP.51	
TH.TSP.107.06	Issuing OBE without a valid contract A TSP issues an OBE to the SU without a valid contract between TC and TSP to get paid by the SU without paying the TC.	n.a.	X
		RQ.TC.92	
TH.TSP.107.07	Issuing ICC without a valid contract A TSP issues an ICC to the SU without a valid contract between TC and TSP to get paid by the SU without paying the TC.	n.a.	X
		RQ.TC.93	

D.2.5.6 Goal 108: Use of cheaper (substandard) equipment

The toll service provider may have an advantage if it can lower its investment costs for equipment (primarily OBE).

Table D.10 — TSP goal: Use of cheaper (substandard) equipment

No.	Threat	DSRC	GNSS
		Related RQ	
TH.TSP.108.01	Using substandard equipment The TSP could use equipment that does not fulfil agreed certifications or that cannot deliver the agreed quality of service.	X	X
		RQ.TC.07 RQ.TC.08 RQ.TSP.58 RQ.TSP.60	

D.2.5.7 Goal 109: Neglect maintenance of equipment

The toll service provider may have an advantage if it can lower its operational costs by neglecting the maintenance of equipment (primarily OBE).

NOTE For example, using an OBE longer than its intended battery life or not replacing poorly performing OBE.

Table D.11 — TSP goal: Neglect maintenance of equipment

No.	Threat	DSRC	GNSS
		Related RQ	
TH.TSP.109.01	Using an OBE longer than its guaranteed battery life The TSP could use an OBE longer than its guaranteed battery life which leads to a lower quality of service and additional cost/loss of income to the TC.	X RQ.TSP.82	X
TH.TSP.109.02	Not exchanging OBE with low performance The TSP avoids the exchange of OBE even if he has knowledge of its low performance prolonging a lower quality of service and additional cost/loss of income to the TC.	X RQ.TSP.82	X

D.2.5.8 Goal 110: Delaying payment to TC

The toll service provider can have an advantage if it can delay its payment to the TC. Especially when a TSP goes bankrupt, this can lead to damage to the TC if the unpaid amount is higher than the payment security provided.

D.2.6 Attacker class 3: Toll charger

D.2.6.1 General

The toll charger is a legal entity charging toll for vehicles in a toll domain. The motivation of the toll charger can be to reduce the complexity of his operations or to make charges against a toll service provider or service user which are not appropriate and thus, to increase his revenue. He can also attempt to resell or otherwise, profit from the data collected from toll service providers or service users.

D.2.6.2 Goal 111: Increase revenue

The malicious intention of a toll charger to increase the revenue received from toll service providers and/or service users for the usage of the toll domain.

Table D.12 — TC goal: Increase revenue

No.	Threat	DSRC	GNSS
		Related RQ	
TH.TC.111.01	Modify toll declarations acquired by the TC The TC modifies the toll declarations he has acquired himself (e.g. with its road side equipment) and reports it as billing details.	X RQ.TSP.10 RQ.TSP.11	n.a.
TH.TC.111.02	Insert toll declarations acquired by the TC The TC adds fake toll declarations to the genuine toll declarations he has acquired himself and reports them as billing details.	X RQ.TSP.10 RQ.TSP.11	n.a.
TH.TC.111.03	Replay toll declarations The TC replays genuine toll declarations he has acquired himself and reports them again as billing details.	X RQ.TSP.10 RQ.TSP.11	n.a.

Table D.12 *(continued)*

No.	Threat	DSRC	GNSS
		Related RQ	
TH.TC.111.04	Modify toll declarations reported by the TSP The TC modifies the toll declarations acquired and reported by the TSP and reports them as billing details back to the TSP.	n.a. RQ.TSP.12	X
TH.TC.111.05	Insert toll declarations reported by the TSP The TC inserts fake toll declarations into the list of toll declarations acquired and reported by the TSP and reports them as billing details back to the TSP.	n.a. RQ.TSP.12	X
TH.TC.111.06	Repudiate the origin of toll context data The TC repudiates the origin (or the update of a new version) of the toll context data and claims payment for service users according to the old toll context data.	X RQ.TC.91 RQ.TC.97 RQ.TSP.13 RQ.TSP.17	X
TH.TC.111.07	Repudiate reception of exception list The TC denies or repudiates the reception of an exception list and claims payment for service users which were on the denied or repudiated list at the time of acquisition of the toll declaration(s) by him.	X RQ.TC.94 RQ.TC.99 RQ.TSP.14 RQ.TSP.18	X

D.2.6.3 Goal 106: Reselling of data about service users

The toll charger could gain financially from reselling confidential and sensitive data about the service users to other commercial parties operating data mining systems, for example, to an insurance company, advertising industry, or governmental agencies which are active in anti-terrorism, etc.

Table D.13 — TC goal: TC's reselling of data about service users

No.	Threat	DSRC	GNSS
		Related RQ	
TH.TC.106.01	Resell service user data to third party The collected service user and vehicle position data are sold and transmitted to an external party without the knowledge of the SU.	X RQ.TC.51	X
TH.TC.106.02	Allow service user tracking by third parties The collected service user and vehicle position data, maybe more data than is required for charging purposes, are sold and transmitted "in real time" to third parties without the permission of the service user for service user and vehicle tracking. The attack is either performed by the TC or by his staff without knowledge of the TC.	X RQ.ISMS.1 RQ.ISMS.2 RQ.TC.51	X
TH.TC.106.03	Provide specific data mining based on road usage data Perform specific data mining and statistics on demand and distribute the (even anonymous) results to commercially interested parties.	X RQ.TC.51	X

D.2.6.4 Goal 112: Neglect maintenance of equipment

The toll charger can have an advantage if it can lower its operational costs by neglecting the maintenance of equipment (primarily RSE).

NOTE For example, using RSE longer than its intended life span does not replace poorly performing RSE.

Table D.14 — TC goal: Neglect maintenance of equipment

No.	Threat	DSRC	GNSS
		Related RQ	
TH.TC.112.01	Avoiding a regular maintenance of RSE equipment in free flow systems The TC could avoid a regular maintenance of RSE equipment which leads to a lower quality of service and possible claims of low OBE performance to the TSP.	X RQ.TC.20 RQ.TC.96	n.a.
TH.TC.112.02	Not exchanging DSRC beacons with low performance in free flow systems The TC does not exchange DSRC beacons even if he has knowledge of their low performance prolonging lower quality of service and possible claims of low OBE performance to the TSP.	X RQ.TC.20 RQ.TC.96	n.a.
TH.TC.112.03	Avoiding a regular maintenance of RSE equipment in barrier based DSRC systems The TC could avoid a regular maintenance of RSE equipment which leads to the use of manual payment instead of handling through the TSP harming the business case of the TSP.	X RQ.TC.20 RQ.TC.96	n.a.
TH.TC.112.04	Not exchanging DSRC beacons with low performance in barrier based DSRC systems The TC does not exchange DSRC beacons even if he has knowledge of their low performance prolonging the use of manual payment instead of the handling through the TSP harming the business case of the TSP.	X RQ.TC.20 RQ.TC.96	n.a.

D.2.6.5 Goal 113: Poor management of toll context data

The toll charger can have an advantage if it can lower its operational costs by neglecting the management of toll context data.

NOTE For example, using wrong names in toll station descriptions and using wrong prices for charging points.

Table D.15 — TC goal: Poor management of toll context data

No.	Threat	DSRC	GNSS
		Related RQ	
TH.TC.113.01	Poor quality of toll context data The TC could provide toll context data with a poor quality causing additional costs to the TSP for service user complaint handling.	X RQ.TC.98	X
TH.TC.113.02	Using incorrect toll context data The TC could provide faulty toll context data to inflate the toll charged to the service user.	X RQ.TC.98	X

D.2.6.6 Goal 114: Delaying payment of TSP remuneration

The toll charger can have an advantage if it can delay its payment to the TSP.

NOTE This is considered to be out of scope and only kept to document the boundaries of the current EFC security framework.

D.2.7 Attacker class 4: Hacker

D.2.7.1 General

A hacker is defined as an attacker who is attempting to penetrate the system without direct financial motivation. A hacker is characterized by capable intellect, high tenacity, and a desire to demonstrate

relatively publicly the results of his efforts. This class of attacker can find the results of their actions exploited for commercial or criminal benefit by attackers in other classes. Their effects cannot be considered benign, but are likely to be technically sophisticated and can be time consuming in implementation.

D.2.7.2 Goal 115: Demonstrate system vulnerability

This class of attacks shows that the system is vulnerable, but does not necessarily achieve a perceivable benefit for the attacker.

Table D.16 — Hacker goal: Demonstrate system vulnerability

No.	Threat	DSRC	GNSS
		Related RQ	
TH.HA.115.01	Fake an input signal from the vehicle and have it accepted as valid In this attack, a signal required for the operation of the system is emulated or modified to change its semantics. Typical sources of signals are CAN bus, tachograph, or odometer.	X	X
		RQ.TSP.16	
TH.HA.115.02	Induce noise on power supply lines to cause system misoperation Excessive power supply noise can induce system misoperation and/or system restarts with corresponding loss of data.	X	X
		RQ.TC.01 RQ.TC.02 RQ.TSP.01 RQ.TSP.53	
TH.HA.115.04	Fake input signal from GNSS Create a 'fake' GNSS signal which overrules the 'real' one and gives a different position for the OBE.	n.a.	X
		RQ.TC.01 RQ.TC.02 RQ.TSP.01 RQ.TSP.16 RQ.TSP.53	
TH.HA.115.05	Provide false configuration data to the OBE/proxy Adjust the OBE so that it is inappropriately set (for example, telling it that it is in a passenger car rather than a truck).	X	X
		RQ.TSP.05 RQ.TSP.07 RQ.TSP.97	
TH.HA.115.06	Fake user input according to sensed or known external audit checks For example, to automatically update the class of a vehicle before an audit check event takes place to generate problems for the service users.	X	X
		RQ.TC.01 RQ.TSP.01 RQ.TSP.05 RQ.TSP.07	

D.2.7.3 Goal 116: Obtain respect amongst their peers

This class of attack is characterized by innate "cleverness" or complexity. Again, it does not necessarily have a malevolent intent or result, but can be exploited by others for commercial gain.

NOTE No protection requirements are defined for these threats as there is no possible damage to the system, except for perhaps, "loss of repudiation". These threats are considered to be out of scope and only kept to document the boundaries of the current EFC security framework.

Table D.17 — Hacker goal: Obtain respect amongst their peers

No.	Threat	DSRC	GNSS
		Related RQ	
TH.HA.116.01	Replace the secure element with a fake secure element Allowing the modification of the data that is recorded by the secure element (secure storage in OBE, e.g. HSM).	X -	X
TH.HA.116.02	Extract private keys from the OBE Allowing the falsification of an OBE to act as the OBE for the purpose of charge manipulation.	X -	X
TH.HA.116.03	Extract secret keys from the RSE Allowing a fake RSE to act as the RSE for the purpose of charge manipulation.	X -	n.a.
TH.HA.116.04	Act as an OBE communication peer to extract information from it	n.a. -	X
TH.HA.116.05	Providing an additional service which interferes with the tolling application An additional application could be installed on an OBE which supports secondary applications to prevent the OBE from operating correctly by — using system resources (memory, CPU, etc.), — compromising input signals, and — compromising output state registration.	X -	X
TH.HA.116.06	Act as the maintenance and customization functionality Enabling elevated access to the system for the purpose of modifying its configuration.	X -	X
TH.HA.116.07	Open the OBE and observe communication between two components on printed circuit board To gain knowledge about the communication and being able to manipulate it.	X -	X
TH.HA.116.08	Replace component on the printed circuit board Removal of a component (ROM, FPGA, etc.) and replacement with a similar component which offers new/different functionality.	X -	X
TH.HA.116.09	Invalidate/incapacitate a component on the printed circuit board For example, by using a JTAG interface to switch a component into test mode or destroying the antenna without interfering with the rest of the functionality.	X -	X
TH.HA.116.10	Act as a RSE for the purpose of extracting data from the OBE	X -	n.a.
TH.HA.116.11	Get access to central system of a TC or TSP Allowing the big scale manipulation of service user data and road usage data.	X -	X
TH.HA.116.12	Access to OBE through back door Gaining access to the OBE data for the purpose of manipulation, data collection, and/or further investigation.	X -	X
TH.HA.116.13	Access to OBE for manipulation of sensor data Modify the input signals that are received by the charging application with an intention of getting it to miscalculate the result.	X -	X

Table D.17 *(continued)*

No.	Threat	DSRC	GNSS
		Related RQ	
TH.HA.116.14	Access to OBE for manipulation of output state Modifying the information that is recorded in the OBE as a charge event (trail).	n.a. -	X

D.2.7.4 Goal 117: Improve understanding of the system or to research its operation

This class of attack leads to information leakage from the system or an increased level of knowledge outside of the implementer community which was never intended.

Table D.18 — Hacker goal: Improve understanding of the system or to research its operation

No.	Threat	DSRC	GNSS
		Related RQ	
TH.HA.117.01	Intercept the communication between the OBE (front end) and the TSP back end.	n.a. RQ.IF.10 RQ.IF.11 RQ.TSP.90 RQ.TSP.91	X
TH.HA.117.02	Intercept internal communications between the OBE and Proxy.	n.a. RQ.IF.10 RQ.IF.11 RQ.TSP.90	X
TH.HA.117.03	Intercept internal communications between any two elements within the OBE.	X RQ.XX.02	Y
TH.HA.117.04	Intercept communications between the OBE and RSE.	X RQ.IF.10 RQ.IF.11 RQ.TC.90	n.a.

D.2.7.5 Goal 118: Provide fake OBE or ICC

This class of attack demonstrates the cleverness and engineering capabilities of the hacker and can also lead to financial profit by selling faked OBE or ICC or the knowledge of how to fake them.

Table D.19 — Hacker goal: Fake an OBE or ICC

No.	Threat	DSRC	GNSS
		Related RQ	
TH.HA.118.01	Clone an OBE Clone an existing OBE and its private key on an original OBE or an also-cloned hardware.	X RQ.TSP.08 RQ.TSP.10 RQ.TSP.19 RQ.TSP.21	X
TH.HA.118.02	Build a fake OBE Design and build a fake OBE which is not (easily) detectable by RSE and enforcement equipment.	X RQ.TSP.08 RQ.TSP.10	X

Table D.19 *(continued)*

No.	Threat	DSRC	GNSS
		Related RQ	
TH.HA.118.03	Clone an ICC Clone an existing ICC and its private key on an original ICC or also, on an also-cloned hardware.	X RQ.TSP.08 RQ.TSP.10 RQ.TSP.19 RQ.TSP.21	X
TH.HA.118.04	Build a fake ICC Design and build a fake ICC which is not (easily) detectable by RSE and enforcement equipment.	X RQ.TSP.08 RQ.TSP.10	X

D.2.8 Attacker class 5: Activist

D.2.8.1 General

An activist is defined as an especially active, vigorous advocate of a cause, especially a political cause which may use violence, civil disobedience, or criminal activities to achieve his goals. Terrorists are included in this attacker class. An activist may be interested in abusing or manipulating the system in order to highlight or realize his political objective even though that objective might not have any relation to the system as such. To an activist, publicity is one of the main goals; therefore, he is interested in large scale disruptions of the systems that cannot be easily reconciled or hidden by the authorities. The activist might not be interested in hiding his identity.

NOTE Most of the threats are covered by other requirements and security measures. An activist has possibly more resources than the other attackers and can break the security measures defined by the EFC security framework. Yet, such specific threats and the respective intention of an activist (e.g. terrorist, etc.) are out of scope of the EFC security framework. This subclause is kept to document the boundaries of the current EFC security framework.

D.2.8.2 Goal 119: Societal destabilization

Manipulation of tolling systems might have destabilizing effects on society as a whole. This can be the intention of activists motivated by anger or resentment against the political regime or the way of living in one or more countries. Manipulation of tolling systems could have the following effects:

— reducing the trust of service users in the correct functioning of tolling systems and, by extension, of any high-tech system;

— reducing trust of service users in toll chargers, toll service providers or toll charging environment management, and, by extension, in any authority;

— endangering the financial stability of toll chargers or local or national governments by reducing revenues from tolling operations;

— disrupting the maintenance of infrastructure due to lack of funds.

Table D.20 — Activist goal: Societal destabilization

No.	Threat	DSRC	GNSS
		Related RQ	
TH.ACT.119.01	Large-scale disruption of GNSS signal By jamming or otherwise, disrupting the GNSS signal in large areas, the OBE of a large number of service users of autonomous EFC systems will stop functioning correctly.	n.a. -	X

Table D.20 *(continued)*

No.	Threat	DSRC	GNSS
		Related RQ	
TH.ACT.119.02	Breach of data integrity/non-repudiation	X	X
	Break into the system or into data communication between parts of the system and change the contents of messages and possibly the associated message authenticators.	-	
TH.ACT.119.03	Manipulating the exception list by, for example, deleting entries or inserting new entries	X	X
		-	
TH.ACT.119.04	Breach of data confidentiality/privacy	X	X
	Break into the system and get access to personal data of service users. By publishing the attack and the data, a major loss of trust in the system can be achieved in the general public.	-	
TH.ACT.119.05	Denial of service	X	X
	The whole or parts of the charging system may be prevented from operation.	-	
		-	
TH.ACT.119.06	Manipulate the status of a large population of OBE	X	X
	Cause OBE malfunction which leads to inability to access the system or unjustified enforcement to service users.	-	

D.2.8.3 Goal 120: Raise in profile of the activists cause

Activists may try to manipulate the system for the sole purpose of drawing the attention of the public at large to the activists cause. This will often be achieved by claiming responsibility for a successful attack afterwards.

In general, there will not be very much difference in the attack methods employed compared with the attacks described in D.2.8.2.

D.2.8.4 Goal 121: Direct furthering of activists cause

Activists may try to manipulate the system in order to directly further their cause. This might, for example, be a reduction in the number of total driven kilometres in the case of an activist motivated by green issues. A key factor here is to influence the behaviour of any party in the system, but especially that of the service users. One of the ways to achieve this is to reduce the trust of service users in the system, so that they will be less inclined to use it.

In general, there will not be very much difference in the attack methods employed compared with the attacks described in D.2.8.2.

D.2.8.5 Goal 122: Reduction in credibility of the system

The activists cause may be the toll charging environment itself, for example, if he is opposed to the idea of tolling as such. By trying to discredit the system in the eyes of users or politicians, he might try to end the use of existing tolling systems or to prevent the establishing of new ones.

In general, there will not be very much difference in the attack methods employed compared with the attacks described in D.2.8.2.

D.2.9 Attacker class 6: Communication provider

D.2.9.1 General

The communication provider is the entity providing the communications infrastructure for the operation of the EFC system. The different communication services of the system are provided by several providers, for example, CN services, internet, etc. Using one specific service can involve several toll service providers at the same time (e.g. internet).

D.2.9.2 Goal 123: Increase network utilization

The communication provider is trying to optimize network utilization for the purpose of achieving higher remuneration from toll service providers or toll chargers.

Table D.21 — Communication provider goal: Increase network utilization

No.	Threat	DSRC	GNSS
		Related RQ	
TH.CP.123.01	Data corruption	X	X
	Deliberately, corrupting the data flow leading to retransmission of packets and thus, increased aggregate data flow.	RQ.IF.02	

D.2.9.3 Goal 124: Decrease network utilization

The communication provider is trying to reduce the use of the network by flat rate communication user (it is assumed that EFC systems have flat rate contracts for all OBE) to increase income from time or volume metered communication users.

Table D.22 — Communication provider goal: Decrease network utilization

No.	Threat	DSRC	GNSS
		Related RQ	
TH.CP.124.01	Prevent data transfer	n.a.	X
	By preventing data transfer from the OBE for an extended period of time, it is possible to make the OBE data buffer overflow and the data to be lost, thus, not being transferred over the network with a resulting decrease in network utilization.	RQ.IF.02	

D.2.9.4 Goal 125: Collecting travel behaviour

The communication provider establishes individual user tracking profiles and sells them to interested third parties.

Table D.23 — Communication provider goal: Collecting travel behaviour

No.	Threat	DSRC	GNSS
		Related RQ	
TH.CP.125.01	Data communication interception	X	X
	The attack collects the usage data (e.g. vehicle position and mileage) by data communication interception to generate service user tracking profiles.	RQ.IF.02 RQ.IF.10 RQ.TC.90 RQ.TSP.90 RQ.TSP.91	

Table D.23 *(continued)*

No.	Threat	DSRC	GNSS
		Related RQ	
TH.CP.125.02	Data traffic analysis The attack analyses the data communication traffic, i.e. the connection, location, duration, and frequency of the communications to generate service user tracking profiles.	n.a. RQ.IF.10	X

D.2.10 Attacker class 7: Enterprise

D.2.10.1 General

The attacker class enterprise contains all kind of organizations with certain financial, technical, and personnel resources. This class includes general organized commercial enterprises of either a legitimate or illegitimate nature using their resources to make profit performing the attack against the tolling system.

D.2.10.2 Goal 126: Movement tracking

The aim of movement tracking is to know where a vehicle at a certain time is or what trips a vehicle make over a certain time. This might have several reasons, for example:

— knowing the position of a vehicle or its freight of special value (e.g. steal the vehicle);

— tracking an individual (the driver);

— tracking the vehicle to discover business behaviour of a competitor.

Table D.24 — Enterprise goal: Movement tracking

No.	Threat	DSRC	GNSS
		Related RQ	
TH.EN.126.01	Bribing TSP or TC employee to get data A main attack avenue may be to get access to data by bribing an employee to act like a 'spy'. The bribed employee may install a bypass data connection to allow online access for the (criminal) enterprise or manually download data from the system. In principle, all kinds of data can be collected such as the movement and mileage data of targeted vehicles and service user personal data.	X RQ.ISMS.2	X
TH.EN.126.02	Data communication interception on the communication provider to TSP interface To intercept all data sent from the communication provider to the TSP and use it for own purposes.	X RQ.IF.10 RQ.TC.90 RQ.TSP.90 RQ.TSP.91	X
TH.EN.126.03	Data communication interception on the TSP to TC interface To intercept all data sent between the TC and the TSP and use it for own purposes.	X RQ.TC.90 RQ.TSP.90	X
TH.EN.126.04	Data communication interception on the air interface (e.g. OBE CN interface) To intercept all data sent from a specific OBE to the TSP over the air interface and use it for own purposes.	n.a. RQ.IF.10 RQ.TSP.90 RQ.TSP.91	X

D.2.10.3 Goal 127: Creation and distribution of cloned equipment

A (criminal) enterprise clones OBE or ICC and sells them to service users.

Table D.25 — Enterprise goal: Creation and distribution of cloned equipment

No.	Threat	DSRC	GNSS
		Related RQ	
TH.EN.127.01	Cloning or faking of OBE and sell it to other service users	X	X
	Cloning or faking an existing OBE and its credentials or accounts (trusted objects), on original OBE or on an also-cloned hardware, and selling the OBE to service users allowing them to avoid paying toll.	RQ.TSP.08 RQ.TSP.10 RQ.TSP.19 RQ.TSP.21	
TH.EN.127.02	Cloning or faking of ICC and sell it to other service users	X	X
	Cloning or faking an existing ICC and its credentials or accounts (trusted objects), on original ICC or on an also-cloned hardware, and selling the ICC to service users allowing them to avoid paying toll.	RQ.TSP.08 RQ.TSP.10 RQ.TSP.19 RQ.TSP.21	

D.2.10.4 Goal 128: Disable/compromise system encryption

An enterprise demonstrates the vulnerability of the system encryption to discredit a competitor's implementation.

NOTE An enterprise has possibly more resources than other attackers and can break the cryptographic algorithms. Yet, this is out of scope of the EFC security framework. This subclause is kept to document the boundaries of the current EFC security framework.

Table D.26 — Enterprise goal: Disable/compromise system encryption

No.	Threat	DSRC	GNSS
		Related RQ	
TH.EN.128.01	Compromise the system by exploiting weaknesses in the encryption algorithms for recovery of diversified keys.	X	X
		-	
TH.EN.128.02	Disable receiving of information	X	X
	Intercept data communication and replace data, certificates, hashes, or other key information to disable data decryption or verification of signatures.	-	
TH.EN.128.03	Disable correct encryption and/or data signing	X	X
	Exchange receiver certificate and/or encryption session key with a fake or a wrong (not from the appointed receiver) one.	-	

D.2.10.5 Goal 129: Steal equipment

A (criminal) enterprise steals OBE, road side, or other equipment either for analysing and cloning or for reselling the equipment.

Table D.27 — Enterprise goal: Steal equipment

No.	Threat	DSRC	GNSS
		Related RQ	
TH.EN.129.01	Steal an OBE (analysing, cloning, or reselling)	X	X
	Steal one or more OBE from service user vehicles or from a TSP stock.	RQ.TSP.19 RQ.TSP.20	

Table D.27 *(continued)*

No.	Threat	DSRC	GNSS
		Related RQ	
TH.EN.129.02	Steal an ICC (analysing, cloning, or reselling) Steal one or more ICC from service user vehicles or from a TSP stock.	X RQ.TSP.19 RQ.TSP.20	X
TH.EN.129.03	Steal roadside equipment Steal installed roadside equipment or equipment from a TC stock or premise.	X RQ.TC.21	X

D.2.10.6 Goal 130: Extortion

A (criminal) enterprise could try to break into several parts of an EFC system to obtain sensitive data. It can use this data either to extort money from targeted individuals, or to extort money from the involved toll service provider or toll charger by threatening to disclose this information about their clients.

Table D.28 — Enterprise goal: Extortion

No.	Threat	DSRC	GNSS
		Related RQ	
TH.EN.130.01	Bribing TSP or TC employee to get data A main attack avenue may be to get access to data by bribing an employee to act like a 'spy'. The bribed employee may install a bypass data connection to allow online access for the (criminal) enterprise or manually download data from the system. In principle, all kinds of data can be collected such as the movement and mileage data of targeted vehicles and service user personal data.	X RQ.ISMS.2	X
TH.EN.130.02	Data communication interception on the communication provider to TSP interface To intercept all data sent from the communication provider to the TSP and use it for own purposes.	X RQ.IF.10 RQ.TC.90 RQ.TSP.90 RQ.TSP.91	X
TH.EN.130.03	Data communication interception on the TSP to TC interface To intercept all data sent between the TC and the TSP and use it for own purposes.	X RQ.TC.90 RQ.TSP.90	X
TH.EN.130.04	Data communication interception on the air interface (e.g. OBE CN interface) To intercept all data sent from a specific OBE to the TSP over the air interface and use it for own purposes.	n.a. RQ.IF.10 RQ.TSP.90 RQ.TSP.91	X

D.2.11 Attacker class 8: Government

D.2.11.1 General

The sovereign entity within whose domain the toll charger operates. That includes all government departments and governmental organizations, for example, police and military forces, intelligence services, etc. The government is characterized by significant resources and significant technical and financial capability.

D.2.11.2 Goal 131: In theatre commercial advantage

This class of attack gives a commercial advantage to companies of the tolling scheme (e.g. toll service providers and OBE manufactures) or other business in the domain of the government. The main target is to collect information outside the legal framework that provides an advantage to the local companies. If this is done within the legal framework, it is not a threat.

Examples are the following:

— collecting information about using an OBE may be interesting for OBE manufacturers and toll service providers

— tracking commercial vehicles to discover business behaviour and relationships that may give local service users an advantage

— tracking private vehicles to discover their commercial behaviour and whereabouts which may give local companies an advantage

NOTE Attacks not related to data collected and exchanged in the EFC system are out of scope of the current threat analysis.

Table D.29 — Government goal: In theatre commercial advantage

No.	Threat	DSRC	GNSS
		Related RQ	
TH.GOV.131.01	Access targeted information at the TC's system The targeted information is obtained through direct contact with the (state-owned) TC which provides the data on request of the Government after appropriate data mining.	X RQ.TC.90	X
TH.GOV.131.02	Access detailed charge/location data at the TSP system The targeted information is obtained through direct contact with the (state-owned) TSP which provides the data on request of the Government after appropriate data mining.	X RQ.TSP.90	X

D.2.11.3 Goal 132: Political targeting of individuals and organizations

Governmental organizations are able to control movements and/or discrediting individuals or organizations based on their travelling behaviour. This will be done by collecting travelling data of visited locations or travelled distance of individuals or members of organizations outside of the legal framework by collecting travelling data of their vehicles. If this is done within the legal framework, it is not a threat.

Table D.30 — Government goal: Political targeting of individuals and organizations

No.	Threat	DSRC	GNSS
		Related RQ	
TH.GOV.132.01	Data communication interception on the communication provider to TSP interface The same attack as TH.GOV.133.01.	X RQ.IF.10 RQ.TC.90 RQ.TSP.90 RQ.TSP.91	X
TH.GOV.132.02	Data communication interception on the TSP to TC interface The same attack as TH.GOV.133.02.	X RQ.TC.90 RQ.TSP.90	X

Table D.30 *(continued)*

No.	Threat	DSRC	GNSS
		Related RQ	
TH.GOV.132.03	Data communication interception on the air interface (e.g. OBE CN interface) The same attack as TH.GOV.133.03.	n.a.	X
		RQ.IF.10 RQ.TSP.90 RQ.TSP.91	
TH.GOV.132.04	Identify the vehicle/OBE at relevant locations Use an appropriate installation to obtain an identifier of the vehicle or OBE's.	X	X
		RQ.TSP.90	

D.2.11.4 Goal 133: Tracking of Individuals by interception of data communication

This class of attacks allows the Government the tracking of individuals by interception of data communication outside the legal framework for several reasons.

NOTE For example, to catch criminals, supervise suspicious individuals, collecting traffic information, etc.

The tracking of users and vehicles is realized by data collected by data communication interception. If this is done within the legal framework, it is not a threat.

Table D.31 — Government goal: Tracking of individuals by interception of data communication

No.	Threat	DSRC	GNSS
		Related RQ	
TH.GOV.133.01	Data communication interception on the communication provider to TSP interface To intercept all data sent from the communication provider to the TSP and use it for own purposes.	X	X
		RQ.IF.10 RQ.TC.90 RQ.TSP.90 RQ.TSP.91	
TH.GOV.133.02	Data communication interception on the TSP to TC interface To intercept all data sent between the TC and the TSP and use it for own purposes.	X	X
		RQ.TC.90 RQ.TSP.90	
TH.GOV.133.03	Data communication interception on the air interface (e.g. OBE CN interface) To intercept all data sent from a specific OBE to the TSP over the air interface and use it for own purposes.	n.a.	X
		RQ.IF.10 RQ.TSP.90 RQ.TSP.91	

D.2.11.5 Goal 134: Tracking of individuals by direct access to data through power of authority

This class of attacks allows the Government the tracking of individuals by direct access to data through power of authority outside the legal framework for several reasons.

NOTE For example, to catch criminals, supervise suspicious individuals, collecting traffic information, etc.

If this is done within the legal framework, it is not a threat.

Table D.32 — Government goal: Tracking of individuals by direct access to data through power of authority

No.	Threat	DSRC	GNSS
		Related RQ	
TH.GOV.134.01	Access detailed charge/location data at the TC system The targeted charge/location data are obtained through direct contact with the (state-owned) TC which provides the data on request of the government.	X RQ.TC.90	X
TH.GOV.134.02	Access detailed charge/location data at the TSP system The targeted charge/location data are obtained through direct contact with the (state-owned) TSP which provides the data on request of the government.	X RQ.TSP.90	X

D.2.12 Attacker class 9: Foreign state agency

D.2.12.1 General

A foreign state agency is defined as any agency of any state except the state under whose jurisdiction a particular toll scheme is operated. The foreign state agency is characterized by significant resources both technical and financial.

NOTE Most of the threats are covered by other requirements and security measures. A foreign state agency has possibly more resources than the other attackers and can break the security measures defined by the EFC security framework. Yet, such specific threats and the respective intention of a foreign state agency (e.g. terrorist, etc.) are out of scope of the EFC security framework. This subclause is kept to document the boundaries of the current EFC security framework.

D.2.12.2 Goal 119: Societal destabilization

Manipulation of tolling systems might have destabilizing effects on society as a whole. This may be the intention of activists motivated by anger or resentment against the political regime or the way of living in one or more countries. Manipulation of tolling systems could have the following effects:

— reducing the trust of service users in the correct functioning of tolling systems and, by extension, of any high-tech system;

— reducing trust of service users in toll chargers, toll service providers or toll charging environment management, and, by extension, in any authority;

— endangering the financial stability of toll chargers or local or national governments by reducing revenues from tolling operations;

— disrupting the maintenance of infrastructure due to lack of funds.

Table D.33 — Hacker goal: Societal destabilization

No.	Threat	DSRC	GNSS
		Related RQ	
TH.FP.119.01	Large-scale disruption of GNSS signal By jamming or otherwise disrupting the GNSS signal in large areas, the OBE of a large number of service users of autonomous EFC systems will stop functioning correctly.	n.a. -	X

Table D.33 *(continued)*

No.	Threat	DSRC	GNSS
		Related RQ	
TH.FP.119.02	Breach of data integrity/non-repudiation	X	X
	Break into the system or into data communication between parts of the system and change the contents of messages and possibly the associated message authenticators.	-	
TH.FP.119.03	Manipulating the exception list by, e.g. deleting entries or inserting new entries.	X	X
		-	
TH.FP.119.04	Breach of data confidentiality/privacy	X	X
	Break into the system and get access to personal data of service users. By publishing the attack and the data, a major loss of trust in the system can be achieved in the general public.	-	
TH.FP.119.05	Denial of service	X	X
	The whole or parts of the charging system may be prevented from operation.	-	
TH.FP.119.06	Manipulate the status of a large population of OBE	X	X
	OBE will be caused to malfunction which causes inability to access the system or unjustified enforcement to service users.	-	

D.2.12.3 Goal 135: Movement tracking

The foreign state agency may be interested in tracking certain persons (e.g. political activists or government officials) in the toll domain.

Table D.34 — Hacker goal: Movement tracking

No.	Threat	DSRC	GNSS
		Related RQ	
TH.FP.135.01	Bribing TSP or TC employee to get data	X	X
	The same attacks as TH.EN.126.01. A main attack avenue for foreign state agencies could be to get access to data by bribing an employee to act like a "spy". The bribed employee may install a bypass data connection to allow online access for the (criminal) enterprise or manually download data from the system. In principle, all kinds of data can be collected, such as the movement and mileage data of targeted vehicles and service user personal data. A major reason why a foreign state agency can use this attack (where, e.g. activists cannot) is that it potentially has large sums of money at its discretion.	RQ.ISMS.2	
TH.FP.135.02	Hire hackers	X	X
	Another way of attacking the system to obtain the desired data is by hiring hackers using the money in the possession of a foreign state agency. Although these hackers then cease to be "ethical" hackers, many of the attacks listed in D.2.6, especially those related to the interception of communication, will still be usable.	-	

D.2.12.4 Goal 136: Extortion

A foreign state agency could try to break into several parts of an EFC system to obtain sensitive data or to gain control over the system. It could use this data either to extort targeted individuals or to extort the involved government by threatening to disclose information about their citizens on a large scale. This is very close to the intention of movement tracking described above.

Alternatively, the foreign state agency could extort the government, toll service providers, or toll chargers by showing its control over (some part of) the EFC system and threatening to use this power in a way disadvantageous to the party involved. In contrast to extortion by a (criminal) enterprise, its object will usually not be money, but some form of collaboration with the foreign state agency's goal. This does, however, not change the methods used by the foreign state agency.

Table D.35 — Hacker goal: Extortion

No.	Threat	DSRC	GNSS
		Related RQ	
TH.FP.136.01	Switching off satellite system	n.a.	X
	If the foreign state agency in question is in control of the satellite system used by the EFC system in question, it might threaten to disable the use of the system for that particular EFC system (if possible).	-	
TH.FP.136.02	Jamming the satellite signal	n.a.	X
	The foreign state agency might threaten to jam the satellite signal used by the EFC in question on a large scale.	-	
TH.FP.136.03	Bribing TSP or TC employee to get data	X	X
	The same attack as TH.FP.135.01.	RQ.ISMS.2	
TH.FP.136.04	Hire hackers	X	X
	The same attack as TH.FP.135.02.	-	

D.2.12.5 Goal 137: International prestige

A foreign state agency could seek to enhance its own internal prestige by showing it is able to disrupt large-scale EFC systems operation by other governments. Alternatively, it could seek to diminish the prestige of other governments by disrupting their EFC systems. In this respect, the foreign state agency comes very close to the motives of a hacker described in goals 115 to 118 (see D.2.7.2 to D.2.7.5).

D.3 Asset based threat analysis

D.3.1 General

For every identified asset, the possible threats will be listed with a description on possible damages. The threat analysis does not assume any existing security measure. Therefore, an attack can exploit any imaginable vulnerability.

One of the main targets is the identification of realistic threats without a benefit for the threat agent, especially if the threat agent is not a person or organization. Nevertheless, the current threat analysis does not include threats by hardware, software, or other implementation faults. This includes malfunction of equipment caused by inconsistent data received through an interface.

D.3.2 Threatened Assets

This section identifies objects subject to attacks in an EFC system called 'threatened assets'. Threatened assets require protection by certain security measures. The main types of threatened assets in the current analysis are the following:

— important information objects such as described in ISO 17573;

— software such as OBE, ICC, and computer software;

— physical entities, e.g. OBE, ICC, RSE, and back end equipment;

— privacy of service users;

— intangibles such as toll chargers and toll service providers reputation and image.

Not all of the information objects as described in ISO 17573 are in the scope of the current Technical Specification, i.e. the information objects in the EFC rules class are out of scope.

While this security architecture covers all information objects and interfaces, it has to be mentioned that not all interfaces fully rely on technical implementations. Furthermore, technical standards are not available for every interface.

D.3.3 Compliance matrix

Most of the interface-related assets have been derived from the EFC architecture standard which describes information objects. The following matrix matches the interfaces and assets from the system model (see Figure D.1) to the analysed assets in the asset-based threat analysis.

Table D.36 — Compliance matrix of the asset based threat analysis

Interface	Covered in
1) OBE user interface	— Asset 209: OBE
2) OBE data interface(s) for value added services	— Out of scope of this Technical Specification
3) OBE vehicle interface: Connections to the vehicle, e.g. power supply, CAN bus, tachograph signal, etc.	— Asset 209: OBE
4) GNSS interface	— Asset 209: OBE
5) OBE tampering	— Asset 209: OBE — Asset 213: TC and TSP central system — Asset 219: Limited autonomy
6) DSRC interface	— Asset 201: Information assets — Asset 202: Infrastructure assets — Asset 205: Customization information — Asset 209: OBE — Asset 211: RSE — Asset 214: Road usage data — Asset 216: Service user identification
7) OBE customization and maintenance interface	— Asset 205: Customization information — Asset 213: TC and TSP central system — Asset 216: Service user identification
8) OBE cellular network interface	— Asset 201: Information assets — Asset 202: Infrastructure assets — Asset 204: OBE Charge report — Asset 205: Customization information — Asset 209: OBE — Asset 213: TC and TSP central system — Asset 214: Road usage data — Asset 217: Toll context data
9) OBE proxy to toll service provider interface (optional)	— Asset 201: Information assets — Asset 202: Infrastructure assets — Asset 204: OBE Charge report — Asset 205: Customization information — Asset 209: OBE — Asset 213: TC and TSP central system — Asset 214: Road usage data — Asset 217: Toll context data — Asset 219: Limited autonomy

Table D.36 *(continued)*

Interface	Covered in
10) Toll service provider to toll charger back end connection	— Asset 201: Information assets — Asset 203: Billing Details — Asset 207: Exception list — Asset 213: TC and TSP central system — Asset 215: Trust Objects — Asset 217: Toll context data — Asset 221: Contractual conditions — Asset 222: Operational rules
11) RSE interface to toll charger back end	— Asset 207: Exception list — Asset 213: TC and TSP central system — Asset 214: Road usage data
12) RSE compliance check interface for license/number plate recognition (ANPR)	— Asset 211: RSE — Asset 226: Enforcement data
13) TC personnel HMI and access to equipment	— Asset 213: TC and TSP central system — Asset 226: Enforcement data
14) TSP personnel HMI and access to equipment	— Asset 213: TC and TSP central system
15) OBE distribution to TSP back end communication	— Asset 213: TC and TSP central system
16) Delivering of equipment (e.g. OBE) and service provision (e.g. communication services) by suppliers and subcontractors. This is not a real interface, but attacks to be considered may be performed during equipment development, equipment manufacturing, service implementation, or service operation.	— Asset 209: OBE — Asset 213: TC and TSP central system
17) The service user declares all contractual parameters from the vehicle and for invoicing used to customize the OBE.	— Asset 206: Service user contract information — Asset 208: Customer service — Asset 210: Service user privacy — Asset 213: TC and TSP central system — Asset 223: Complaints
18) Physical or contactless interface between OBE and IC card	— Asset 228: ICC
19) Physical or contactless interface for the loading of the IC card	— Out of scope of this Technical Specification

D.3.4 Presentation of threats

The table below explains the template used for the asset based threat analysis.

Table D.37 — Notation and relations of threats

Table header	Meaning
No.	Unique number for every threat according to the numbering scheme described in D.1.2.
Threat	A description of the actual threat (without having a concrete vulnerability in mind) Description of the possible cause and damage of execution of the threat.
DSRC	Marked with an X if this requirement is relevant for a DSRC system.
GNSS	Marked with an X if this requirement is relevant for an autonomous system.
Related RQ	Reference to the requirement(s) driven by the threat.

D.3.5 Generic threats

D.3.5.1 Asset 201: Information assets

Information assets are, in general, information objects representing some value (possibly representing money) for an organization or person. These information objects have a generating process stored in and exchanged between equipment (e.g. OBE, RSE, and back end). The table below contains the generic threats for these information assets.

Table D.38 — Generic threats to information assets

No.	Threat	DSRC	GNSS
		Related RQ	
TH.DT.201.01 TH.OUT.201.01 TH.SU.201.01	Modify the data during transmission. Possible damage: — violation of data integrity (loss of income).	X	X
		RQ.IF.11	
TH.OUT.201.02 TH.SU.201.02 TH.TC.201.02 TH.TSP.201.02	Modify the data stored in any equipment or Back End including a central cluster equipment. Possible damage: — violation of data integrity (loss of income).	X	X
		RQ.DS.01 RQ.DS.02 RQ.DS.05	
TH.OUT.201.03 TH.SU.201.03	Deleting a message during transmission. Possible damage: — no availability of data (loss of income).	X	X
		RQ.XX.01	
TH.OUT.201.03 TH.SU.201.03	Prevent data communication (denial of service attack). Possible damage: — no availability of data (loss of income).	X	X
		RQ.XX.01	
TH.DT.201.05 TH.IT.201.05	Loss of data caused by accident, environmental incident, or equipment failure. Possible damage: — no availability of data (loss of income).	X	X
		RQ.XX.01	
TH.OUT.201.06 TH.SU.201.06	Modify the identification of the data originator Possible damage: — violation of authenticity (loss of income).	X	X
		RQ.DS.07 RQ.IF.12	
TH.OUT.201.07 TH.SU.201.07	The originator of the data is a not an authorized person or entity. Possible damage: — violation of authenticity (loss of income).	X	X
		RQ.DS.07 RQ.IF.20	
TH.OUT.201.08 TH.TC.201.08 TH.TSP.201.08	Replaying of a data communication message. Possible damage: — violation of authenticity (loss of income).	X	X
		RQ.IF.30	
TH.OUT.201.09	Eavesdropping of data communication. Possible damage: — breach of confidentiality (disclosure of information to unauthorized individuals or systems, violation of service user privacy).	X	X
		RQ.IF.10	
TH.OUT.201.10 TH.SU.201.10 TH.TC.201.10 TH.TSP.201.10	Read access to data stored in any equipment or back end. Possible damage: — breach of confidentiality (disclosure of information to unauthorized individuals or systems, violation of service user privacy).	X	X
		RQ.DS.01	
		RQ.IM.01 RQ.IM.02	

Table D.38 *(continued)*

No.	Threat	DSRC	GNSS
		Related RQ	
TH.OUT.201.11	Intercept a communication with fake recipient identification. Data are sent to an unauthorized recipient. Possible damage: — violation of authenticity; — no availability of data (loss of income); — breach of confidentiality (disclosure of information to unauthorized individuals or systems, violation of service user privacy).	X	X
		RQ.IF.20	
TH.SU.201.12 TH.TC.201.12 TH.TSP.201.12	Deny being the originator of an information or message. Possible damage: — loss of non-repudiation (loss of income).	X	X
		RQ.IF.13	
TH.SU.201.13 TH.TC.201.13 TH.TSP.201.13	Deny having received an information or message. Possible damage: — loss of non-repudiation (loss of income).	X	X
		RQ.IF.14	
TH.IM.201.14 TH.TC.201.14 TH.TSP.201.14	Missing global security rules The TCs and TSPs do not have a globally valid set of security rules (possibly defined by an interoperability management). This leads to unaligned security implementations with different levels of security at the various TCs and TSPs and possible security holes. Possible damage: — undermine trust in the toll charging environment; — no or incorrect tolling; — loss of income; — breach of confidentiality (disclosure of information to unauthorized individuals or systems, violation of service user privacy) — violation of data integrity (loss of income); — violation of authenticity (loss of income); — no availability of data (loss of income).	X	X
		RQ.IM.01 RQ.IM.02	

D.3.5.2 Asset 202: Infrastructure assets

Infrastructure assets are any kind of equipment used for the EFC system (e.g. OBE, RSE, or back end equipment) not covered as a specific asset. This class of asset consists of two parts namely the physical hardware and the software of the equipment. The table below contains the generic threats for these infrastructure assets.

Table D.39 — Generic threats to infrastructure assets

No.	Threat	DSRC	GNSS
		Related RQ	
TH.DT.202.01 TH.IT.202.01	Environmental incident. Possible damage: — damage of the equipment; — data processing failure; — loss of data (no availability of data, loss of income).	X	X
		RQ.TC.20 RQ.TC.23	
TH.OUT.202.02 TH.SU.202.02	Vandalism. Possible damage: — damage of the equipment; — data processing failure; — loss of data (no availability of data, loss of income).	X	X
		RQ.TC.20 RQ.TC.23 RQ.TSP.09	

Table D.39 *(continued)*

No.	Threat	DSRC	GNSS
		Related RQ	
TH.OUT.202.03 TH.SU.202.03	Traffic accidents (only OBE and RSE). In GNSS only relevant for CCC and LAC. Possible damage: — damage of the equipment; — data processing failure; — loss of data (no availability of data, loss of income).	X	X
		RQ.TC.20 RQ.TC.23 RQ.TSP.09	
TH.OUT.202.04 TH.SU.202.04	Theft of equipment. Possible damage: — loss of equipment; — loss of data (no availability of data, loss of income) and possibly; —breach of confidentiality (disclosure of information to unauthorized individuals or systems, violation of service user privacy).	X	X
		RQ.TC.21 RQ.TSP.20	
TH.OUT.202.05 TH.SU.202.05	Software modification. Possible damage: — violation of data integrity (loss of income); — loss of data (no availability of data, loss of income) and possibly; — breach of confidentiality (disclosure of information to unauthorized individuals or systems, violation of service user privacy).	X	X
		RQ.TC.24 RQ.TSP.05 RQ.TSP.40	
TH.OUT.202.06 TH.SU.202.06	Denial of service attack against data communication interfaces or internal software processes or services. Possible damage: — loss of data (no availability of data, loss of income).	X	X
		RQ.XX.01	

D.3.6 Asset 203: Billing details

Refined charge report of the OBE up to the level of details requested in the user bill including the payment claim.

Table D.40 — Threats to billing details

No.	Threat	DSRC	GNSS
		Related RQ	
TH.DT.203.01	Billing details could be changed during transmission between TSP and TC back end. Possible damage: — billing detail data no longer usable for billing the service user or for making a proper claim from the TC to the TSP; — wrong data could lead to wrong invoices and TC claims.	X	X
		RQ.IF.11	
TH.IT.203.02 TH.OUT.203.02 TH.TSP.203.02	Billing details could be transmitted to an unauthorized party. Possible damage: — undermine trust in the toll charging environment; — violation of service users privacy; — loss of Billing details for further processing and billing.	X	X
		RQ.IF.20	
TH.IT.203.03 TH.OUT.203.03	Billing details could be sent from an unauthorized party. Possible damage: — undermine trust in the toll charging environment; — charging the service user for non-existing usage of the toll domain.	X	X
		RQ.IF.20	

Table D.40 *(continued)*

No.	Threat	DSRC	GNSS
		Related RQ	
TH.IT.203.04 TH.OUT.203.04 TH.TC.203.04 TH.TSP.203.04	The content of Billing details could be revealed to an unauthorized party. Possible damage: — undermine trust in the toll charging environment; — violation of service users privacy.	X	X
		RQ.ISMS.2 RQ.TC.90	
TH.DT.203.05 TH.IT.203.05 TH.OUT.203.05 TH.TSP.203.05	The transmission of billing details could be disturbed and delayed. Possible damage: — undermine trust in the toll charging environment; — denial of service; — negatively affect billing processes; — violate service levels agreed with the TC.	X	X
		RQ.ISMS.2 RQ.TC.95	
TH.OUT.203.06 TH.TSP.203.06	The authenticity of sent billing details cannot be proven and/or its origin is repudiated. Possible damage: — no end-to-end security and therefore no acceptance of the billing details for further processing and billing.	X	X
		RQ.IF.13 RQ.IF.14	

D.3.7 Asset 204: OBE Charge Report

Table D.41 — Threats to OBE charge report

No.	Threat	DSRC	GNSS
		Related RQ	
TH.DT.204.01	A charge report could be changed during transmission between front end and TSP back end. Possible damage: — charge report data no longer usable for billing the service user; — wrong data could lead to wrong invoices and TC claims.	n.a.	X
		RQ.IF.11	
TH.IT.204.02 TH.OUT.204.02 TH.SU.204.02	A charge report could be transmitted to an unauthorized party. Possible damage: — undermine trust in the toll charging environment; — violation of service users privacy; — loss of charge report for further processing and billing.	n.a.	X
		RQ.IF.20	
TH.IT.204.03 TH.OUT.204.03	A charge report could be sent from an unauthorized party. Possible damage: — undermine trust in the toll charging environment; — charging the service user for non-existing usage of the toll domain.	n.a.	X
		RQ.IF.20	
TH.IT.204.04 TH.OUT.204.04 TH.SU.204.04	The content of a charge report could be revealed to an unauthorized party during transmission. Possible damage: — undermine trust in the toll charging environment; — violation of service users privacy	n.a.	X
		RQ.IF.10	
TH.DT.204.05 TH.IT.204.05 TH.OUT.204.05 TH.SU.204.05	The transmission of charge reports could be disturbed and delayed. Possible damage: — undermine trust in the toll charging environment; — denial of service; — negatively affect billing processes; — violate service levels agreed with the TC.	n.a.	X
		RQ.TSP.01	

Table D.41 *(continued)*

No.	Threat	DSRC	GNSS
		Related RQ	
TH.OUT.204.06 TH.SU.204.06	The authenticity of sent charge reports cannot be proven and/or its origin is repudiated. Possible damage: — no end-to-end security and therefore no acceptance of the charge report for further processing and billing.	n.a.	X
		RQ.IF.13 RQ.IF.14	

D.3.8 Asset 205: Customization information

Table D.42 — Threats to customization information

No.	Threat	DSRC	GNSS
		Related RQ	
TH.DT.205.01 TH.SU.205.01	Changing all or parts of the customization information (e.g. service user contract, tariff classes, etc.) during transmission to the OBE. Possible damage: — wrong or no service user is invoiced for the road usage; — loss of income for TSP because no service user can be invoiced (payment guarantee to TC until user/OBE is on exception list); — loss of income caused by wrong tariff class.	X	X
		RQ.IF.10 RQ.IF.11 RQ.TSP.92	
TH.IT.205.02 TH.SU.205.02	Changing or deleting all or parts of the customization information stored in the OBE. Possible damage: — violation of data integrity (loss of income).	X	X
		RQ.DS.01 RQ.DS.02 RQ.DS.05	
TH.DT.205.03 TH.IT.205.03 TH.SU.205.03	Changing all or parts of the customization information sent by the OBE.	X	X
		RQ.IF.10 RQ.IF.11	
TH.DT.205.04 TH.IT.205.04 TH.SU.205.04	Prevent OBE from updating customization information.	X	X
		RQ.XX.01	
TH.TSP.205.05 TH.TC.205.05	Change of fee relevant customization information over the air. The personalization data in a GNSS OBE can be changed over the air causing a sudden change of data transmitted to the RSE from one charging point to the next. Possible damage: — this could lead to negative effects in normal operation (e.g. enforcement, fraud detection, etc.) if not properly agreed and tested between TSP and TC (e.g. sudden change of vehicle group or Euro emission category settings); — in a failure condition, this could jeopardize tolling if the TSP transmits wrong data to the OBE(s).	X	X
		RQ.TC.12 RQ.TSP.97	

D.3.9 Asset 206: Service user contract information

Table D.43 — Threats to service user contract information

No.	Threat	DSRC	GNSS
		Related RQ	
TH.DT.206.02 TH.IT.206.02 TH.OUT.206.02 TH.SU.206.02	Change of contract information during transmission (contract agent to the TSP) or storage in TSP back end. Possible damage: — wrong or no service user is invoiced for the road usage; — loss of income for TSP because no service user can be; invoiced (payment guarantee to TC until user/OBE is on exception list); — loss of income caused by wrong tariff class.	X	X
		RQ.DS.01 RQ.DS.02 RQ.DS.05 RQ.DS.07 RQ.IF.10 RQ.IF.11	
TH.DT.206.03 TH.OUT.206.03	Loss of contract information during storage in TSP back end. Possible damage: — TSP loses income and may be no longer able to operate its service	X	X
		RQ.DS.03 RQ.DS.05	
TH.DT.206.04 TH.IT.206.04 TH.TSP.206.04	Contract details are revealed to unauthorized third parties. Possible damage: — infringement of service user privacy; — service user loses money by non-genuine and unauthorized debiting based on his contractual account information.	X	X
		RQ.DS.01 RQ.DS.02 RQ.DS.06 RQ.IF.10 RQ.IF.11	

D.3.10 Asset 207: Exception list

Any problems regarding the exchange of exception lists has direct effects on the shift of risk between TC and TSP and can thus have significant economic consequences.

The following threats can cause different types of damage to the different stakeholders in an EFC system. These damages could be grouped into four main groups, namely,

— loss of reputation and personal integrity for the user,

— economical loss for the service user,

— loss of reputation and credibility for the operators, and

— economical loss for the operators.

Table D.44 — Threats to exception list

No.	Threat	DSRC	GNSS
		Related RQ	
TH.DT.207.01 TH.IT.207.01 TH.TSP.207.01 TH.TC.207.01	Loss/change of exception list during transmission from TSP to TC. Possible damage: — requested locking does not take effect; — wrong OBE gets locked; — contractual consequences.	X	X
		RQ.DS.07 RQ.IF.11 RQ.IF.14 RQ.TC.99	
TH.DT.207.02 TH.IT.207.02 TH.OUT.207.02 TH.TC.207.02	Loss/change of exception list during transmission from TC CS to RSE. Possible damage: — requested locking does not take effect; — wrong OBE gets locked; — contractual consequences.	X	X
		RQ.IF.11 RQ.IF.14	
TH.OUT.207.03 TH.TSP.207.03 TH.TC.207.03	Transmission of exception list to unauthorized party. Possible damage: — loss of privacy.	X	X
		RQ.DS.08 RQ.IF.20 RQ.TC.99 RQ.TSP.18	
TH.OUT.207.04 TH.TSP.207.04 TH.TC.207.04	Placement of OBE on exception list by unauthorized party. Possible damage: — wrong OBE gets locked.	X	X
		RQ.IF.20	
TH.DT.207.05 TH.IT.207.5 TH.TSP.207.05 TH.TC.207.05	Delay of exception list transmission. Possible damage: — delay in requested locking; — contractual consequences.	X	X
		RQ.TC.99 RQ.TSP.18 RQ.XX.01	

D.3.11 Asset 208: Customer service

Customer service data can be information about the SUs personal data or information about the OBE used by the SU which can be contract, payment, and vehicle or usage data. The information is exchanged between the SU and TSP.

Table D.45 — Threats to customer service

No.	Threat	DSRC	GNSS
		Related RQ	
TH.OUT.208.01	The service user can be impersonated by a fraudulent person getting access to the service users personal data. Possible damage: — violation of privacy; — undermine trust in the TSP operation of the toll charging environment. EXAMPLE An attacker can give the impression that he is the service user and requires a printout of all stored user information, e.g. payment means and toll transactions.	X	X
		RQ.TSP.50	
TH.OUT.208.02	The service user can be impersonated by a fraudulent person giving false information or complaints. Possible damage: — violation of privacy, e.g. incorrect enforcement; — undermine trust in the TSP operation of the toll charging environment. EXAMPLE An attacker can give the impression that he is the service user and reports an OBE stolen asking for it to be blocked.	X	X
		RQ.TSP.50	

D.3.12 Asset 209: OBE

Table D.46 — Threats to OBE

No.	Threat	DSRC	GNSS
		Related RQ	
TH.IT.209.01 TH.OUT.209.01 TH.SU.209.01	Manipulation of stored data. Due to manipulation, the correct functionality of the OBE is no longer guaranteed. Possible damage: — creation of wrong charging or enforcement records with the goal to pay less toll; — instability of the OBE due to bogus data; — undermine trust in the toll charging environment.	X	X
		RQ.DS.01 RQ.DS.02 RQ.DS.05	
TH.TSP.209.02	Violation of data privacy requirements. Possible damage: — violation of privacy laws; — collect and store more data than needed; — violation of the service users privacy; — undermine trust in the toll charging environment.	X	X
		RQ.TSP.42	

Table D.46 *(continued)*

No.	Threat	DSRC	GNSS
		Related RQ	
TH.DT.209.03 TH.IT.209.03 TH.OUT.209.03 TH.SU.209.03	Eavesdropping of OBE communication connection (CN or DSRC). Possible damage: — reveal confidential data to unauthorized parties; — gain knowledge of internal data transmission; — undermine trust in the toll charging environment.	X	X
		RQ.IF.10 RQ.IF.11	
TH.DT.209.04 TH.OUT.209.04 TH.SU.209.04	Prevention of communication. An attacker tries to prevent the working of communication channels (CN, DSRC), e.g. by covering the antennas. Possible damage: — prevention of correct toll event detection; — less stability of the OBE operations.	X	X
		RQ.TC.01 RQ.TC.02 RQ.TSP.01 RQ.TSP.09 RQ.TSP.51	
TH.OUT.209.05 TH.SU.209.05 TH.TC.209.05	Change of configuration data. An attacker tries to manipulate any configuration data on the OBE (e.g. communication end points, retry limits, etc.). Possible damage: — less stability of the OBE operations; — creation of wrong charging or enforcement records with the goal to pay less toll; — prevention of correct toll event detection; — undermine trust in the toll charging environment.	X	X
		RQ.TSP.40	
TH.OUT.209.06 TH.SU.209.06 TH.TC.209.06	Inspection of configuration data. An attacker can gain an advantage from inspecting configuration data on the OBE. Possible damage: — undermine trust in the toll charging environment; — prepare efficient attacks on the system using this specific knowledge.	X	X
		RQ.TSP.41	
TH.OUT.209.07 TH.SU.209.07	An attacker tries to change the compliance check attributes inside the OBE to a proper value for an enforcement authority. Possible damage: — undermine trust in the toll charging environment; — creation of incorrect charging and enforcement records in order to pay less toll.	n.a.	X
		RQ.TSP.40	
TH.OUT.209.08 TH.SU.209.08	Internal knowledge on the OBE design. An attacker tries, using technical and organizational measures (such as social engineering), to get internal or confidential knowledge about the OBE. Possible damage: — instability of the OBE; — prevention of correct toll event detection; — creation of incorrect charging and enforcement records in order to pay less toll; — undermine trust in the toll charging environment.	X	X
		RQ.ISMS.2	
TH.OUT.209.09 TH.SU.209.09	An attacker tries to manipulate or exchange hardware components to pay lower toll. Possible damage: — prevention of correct toll event detection.	X	X
		RQ.XX.02	

Table D.46 *(continued)*

No.	Threat	DSRC	GNSS
		Related RQ	
TH.DT.209.11 TH.IT.209.11 TH.TSP.209.11	Mass failure of OBE after update over the air. Mass failure of a significant number of OBE after an update over the air. This could be caused by — insufficient tests by the TSP, — malfunction due to IT problems, or — change of SW during transmission to OBE over the air. Possible damage: — undermine trust in the toll charging environment; — no or incorrect tolling; — loss of income; — additional cost to the TC by providing local OBE.	X	X
		RQ.TSP.70 RQ.TSP.71	
TH.DT.209.12 TH.IT.209.12 TH.TSP.209.12	Bad performance of a whole production charge or OBE type. Bad communication performance of a whole production charge or OBE type. This could affect a pure DSRC OBE or the DSRC part of a GNSS OBE while communicating with the RSE. This could be caused by — insufficient charge testing by TSP, — short lived components in OBE, or — bad quality of internal antenna. Possible damage: — undermine trust in the toll charging environment; — no or incorrect tolling; — loss of income; — additional cost to the TC by providing local OBE.	X	X
		RQ.TSP.80	

D.3.13 Asset 210: Service user privacy

Table D.47 — Threats to service user privacy

No.	Threat	DSRC	GNSS
		Related RQ	
TH.TSP.210.01 TH.TC.210.01	Collection of personal data. This could be caused by — not necessary for toll collection, — use of data for other purpose, — other data than consented to by the service user (data subject), or — provides data to third parties. Possible damage: — violation of privacy; — undermine trust in the toll charging environment.	X	X
		RQ.TC.50 RQ.TC.51 RQ.TSP.59	
TH.TSP.210.02 TH.TC.210.02	Collected personal data not handled according to data protection laws and regulations. This could be caused by — change, loss, or too long storage of data, — providing no access to collected service user data, or — no agreements between data controller and data processor/assistant. Possible damage: — violation of privacy; — undermine trust in the toll charging environment.	X	X
		RQ.TC.50 RQ.TC.51 RQ.TSP.59	
TH.TC.210.03	An organization identifies the service user in cases where there is no violation of the EFC system. Possible damage: — violation of privacy.	X	X
		RQ.TSP.59 RQ.TC.50 RQ.TC.51 RQ.TSP.59	
TH.TSP.210.04 TH.TC.210.04	A service user is subject to enforcement due to lack of crucial data availability or improper data processing (e.g. no updated exception list in a charging point). Possible damage: — undermine trust in the toll charging environment.	X	X
		RQ.TC.51 RQ.TSP.59	

D.3.14 Asset 211: RSE

Table D.48 — Threats to RSE

No.	Threat	DSRC	GNSS
		Related RQ	
TH.OUT.211.01	Vandalism on the RSE, e.g. shooting with guns on antennas, using explosives on RSE cabinets or cutting cables. Possible damage: — no or incorrect tolling; — instability of the RSE; — prevention of correct toll event detection.	X	X
		RQ.TC.20	
TH.SU.211.02	Traffic accidents damaging charging points. Possible damage: — loss of income.	X	X
		RQ.TC.20	

Table D.48 *(continued)*

No.	Threat	DSRC	GNSS
		Related RQ	
TH.OUT.211.03	Theft of RSE. Possible damage: — no tolling; —disclosure of sensitive information like security keys.	X RQ.TC.21	X
TH.OUT.211.04	Faking an RSE. Possible damage: — reading of data from all OBE passing the fake RSE for later use, e.g. OBE impersonation or violation of privacy; — undermine trust in the toll charging environment.	X RQ.TC.22	X
TH.OUT.211.05	Prevention of communication. An attacker tries to prevent the working of communication channels, e.g. by covering the antennas or by jamming the DSRC link. Possible damage: — no or incorrect tolling.	X RQ.TC.23	X
TH.OUT.211.06	Modification or alteration of RSE software. Possible damage: — incorrect tolling.	X RQ.TC.24	X
TH.OUT.211.07	Internal knowledge on the RSE design. An attacker tries, using technical and organizational measures (such as social engineering) to get internal or confidential knowledge about RSE. Possible damage: — undermine trust in the toll charging environment.	X RQ.ISMS.2	X
TH.DT.211.08 TH.IT.211.08 TH.OUT.211.08	Enforcement interface at RSE unavailable. An OBE is not able to communicate with the enforcement equipment of the TC. This could be caused by — broken antenna, — misdirected antenna, — no power supply to RSE, or — IT failure in RSE station. Possible damage: — undermine trust in the toll charging environment; — no or wrong enforcement of service user(s) — loss of income — additional cost to the TSP for customer service.	X RQ.TC.96	X

D.3.15 Asset 212: EFC stakeholder image and reputation