

PD CEN/TS 16439:2013



BSI Standards Publication

Electronic fee collection — Security framework

bsi.

...making excellence a habit.
AVA Documents™
Document Sharing Hub

National foreword

This Published Document is the UK implementation of CEN/TS 16439:2013.

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

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

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

© The British Standards Institution 2013.

Published by BSI Standards Limited 2013

ISBN 978 0 580 78694 5

ICS 35.240.60

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

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 28 February 2013.

Amendments issued since publication

Date	Text affected
------	---------------

TECHNICAL SPECIFICATION
SPÉCIFICATION TECHNIQUE
TECHNISCHE SPEZIFIKATION

CEN/TS 16439

January 2013

ICS 35.240.60

English Version

Electronic fee collection - Security framework

Perception de télépéage - Cadre de sécurité

Elektronische Gebührenerhebung -
Sicherheitsgrundstruktur

This Technical Specification (CEN/TS) was approved by CEN on 27 August 2012 for provisional application.

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

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

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



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

Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

Page

Foreword.....	6
0 Introduction	7
0.1 Reader's guide	7
0.2 EFC role model.....	8
0.3 Relation to other security standards.....	9
1 Scope.....	11
1.1 EFC specific scope	11
1.2 Scope in relation to other security frameworks.....	14
2 Normative references.....	15
3 Terms and definitions	16
4 Symbols and abbreviations	22
5 Trust model	24
5.1 Introduction	24
5.2 Stakeholders trust relations	24
5.3 Technical trust model	25
5.3.1 General	25
5.3.2 Trust model for TC and TSP relations	25
5.3.3 Trust model for TSP and User relations.....	27
5.3.4 Trust model for Interoperability Management relations	27
5.4 Implementation.....	27
5.4.1 Setup of trust relations	27
5.4.2 Trust relation renewing and revocation	27
5.4.3 Issuing and revocation of sub CA and entity certificates	28
5.4.4 Certificate and Certificate Revocation List profile and format.....	28
5.4.5 Certificate extensions	28
6 Security requirements.....	29
6.1 Introduction	29
6.2 Information Security Management System	29
6.3 Communication interfaces.....	30
6.3.1 General	30
6.3.2 Generic interface requirements	31
6.3.3 DSRC profile.....	31
6.3.4 TC to TSP profile	32
6.3.5 Communication provider profile.....	32
6.4 Data storages	33
6.4.1 General	33
6.4.2 OBE data storages	33
6.4.3 RSE data storages.....	33
6.4.4 Back End data storage.....	34
6.5 Toll Charger.....	34
6.6 Toll Service Provider.....	35
6.7 User.....	37
6.8 Interoperability Management	38
6.9 Limitation of requirements	38
7 Security measures - countermeasures	38
7.1 Introduction	38
7.2 General security measures.....	39
7.3 Communication interfaces security measures	39

7.3.1	General	39
7.3.2	DSRC-EFC interface	39
7.3.3	CCC interface	40
7.3.4	LAC interface	40
7.3.5	Front End to TSP Back End interface	41
7.3.6	TC to TSP interface	41
7.4	End-to-end security measures	41
7.5	Toll Service Provider security measures	43
7.5.1	Front End security measures	43
7.5.2	Back End security measures	43
7.6	Toll Charger security measures	44
7.6.1	RSE security measures	44
7.6.2	Back End security measures	44
7.6.3	Other TC security measures	44
8	Security specifications for interoperable interface implementation	45
8.1	General	45
8.1.1	Subject	45
8.1.2	Signature and hash algorithms	45
8.1.3	MAC algorithm	45
8.1.4	MAC key derivation	46
8.1.5	Key encryption algorithm	46
8.1.6	Padding algorithm	46
8.2	Security specifications for DSRC-EFC	46
8.2.1	Subject	46
8.2.2	OBE	46
8.2.3	RSE	47
8.3	Security specifications for CCC	47
8.3.1	Subject	47
8.3.2	OBE	47
8.3.3	RSE	47
8.4	Security specifications for LAC	47
8.4.1	Subject	47
8.4.2	OBE	47
8.4.3	RSE	47
8.5	Security specifications for Front End to TSP interface	48
8.5.1	General	48
8.5.2	ChargeReport message authentication	48
8.6	Security specifications for TC to TSP interface	49
8.6.1	General	49
8.6.2	Secure communication channel	49
8.6.3	Message authentication	49
8.6.4	Proof of message delivery	51
8.6.5	TSP ChargeReport authentication	51
9	Key management	52
9.1	Introduction	52
9.2	Asymmetric keys	52
9.2.1	Key exchange between stakeholders	52
9.2.2	Key generation and certification	52
9.2.3	Protection of Keys	53
9.2.4	Application	53
9.3	Symmetric keys	53
9.3.1	Introduction	53
9.3.2	Key exchange between stakeholders	53
9.3.3	Key lifecycle	54
9.3.4	Key storage and protection	56
9.3.5	Session keys	57
Annex A (normative)	Data type specification	58
Annex B (normative)	Implementation Conformance Statement (ICS) proforma	62

B.1	Guidance for completing the ICS proforma	62
B.1.1	Purposes and structure	62
B.1.2	Abbreviations and conventions.....	62
B.1.3	Instructions for completing the ICS proforma	64
B.2	Identification of the implementation.....	64
B.2.1	General	64
B.2.2	Date of the statement.....	64
B.2.3	Implementation Under Test (IUT) identification	64
B.2.4	System Under Test (SUT) identification	65
B.2.5	Product supplier.....	65
B.2.6	Applicant (if different from product supplier)	66
B.2.7	ICS contact person.....	66
B.3	Identification of the standard.....	67
B.4	Global statement of conformance	67
B.5	Roles	67
B.6	Trust Model functionalities	67
B.7	Profiles	68
B.8	Requirements	68
B.9	Security measures	71
B.10	Specifications for interoperable interfaces security	74
Annex C (informative)	Stakeholder objectives and generic requirements	76
C.1	Introduction	76
C.2	Toll Chargers.....	77
C.2.1	Toll chargers and their main interests	77
C.2.2	Security service requirements for a Toll Charger.....	77
C.3	Toll Service Providers.....	78
C.3.1	Toll service providers and their main interests	78
C.3.2	Security service requirements for a Toll Service Provider.....	78
C.4	Users.....	79
C.4.1	Users and their main interests	79
C.4.2	Users requirements.....	79
C.5	Interoperability Management.....	79
C.5.1	Interoperability management and its main interests	79
C.5.2	Security service requirements for interoperability management.....	80
Annex D (informative)	Threat analysis	81
D.1	General introduction	81
D.2	Attack trees based threat analysis	81
D.2.1	Introduction	81
D.2.2	System model.....	82
D.2.3	Presentation of attack trees.....	83
D.2.4	Attacker class 1: User	84
D.2.5	Attacker class 2: Toll Service Provider	86
D.2.6	Attacker class 3: Toll Charger	89
D.2.7	Attacker class 4: Hacker	91
D.2.8	Attacker class 5: Activist.....	94
D.2.9	Attacker class 6: Communication provider.....	95
D.2.10	Attacker class 7: Enterprise	96
D.2.11	Attacker class 8: Government	99
D.2.12	Attacker class 9: Foreign power.....	101
D.3	Asset based threat analysis	102
D.3.1	General	102
D.3.2	Threatened Assets	102
D.3.3	Compliance matrix	104
D.3.4	Presentation of threats	106
D.3.5	Generic threats.....	107
D.3.6	Asset: Billing details	109
D.3.7	Asset: OBE Charge Report.....	110
D.3.8	Asset: Customisation information	111
D.3.9	Asset: User contract information	111

D.3.10	Asset: Exception List	112
D.3.11	Asset: "Help, info, complain"	112
D.3.12	Asset: OBE	113
D.3.13	Asset: User privacy	115
D.3.14	Asset: RSE	115
D.3.15	Asset: EFC stakeholders image and reputation	116
D.3.16	Asset: TC and TSP central system	117
D.3.17	Asset: Transit information	117
D.3.18	Asset: Trust object	118
D.3.19	Asset: User identification	120
D.3.20	Asset: Context Data	120
D.3.21	Asset: Payment means	121
D.3.22	Asset: Limited autonomy	122
D.3.23	Asset: EFC Schema	122
D.3.24	Asset: Contractual conditions	123
D.3.25	Asset: Operational rules	124
D.3.26	Asset: Complaint	125
D.3.27	Asset: Certification	127
D.3.28	Asset: Operational report	128
Annex E	(informative) Security Policies	129
E.1	Introduction	129
E.1.1	Scope of the annex	129
E.1.2	Motivation for the need of security policies	129
E.2	Example EFC scheme security policy	129
E.2.1	Motivation for information security	129
E.2.2	Purpose of the security policy	130
E.2.3	Scope	130
E.2.4	Policy statements	132
E.3	Development of operators security policies	134
E.3.1	General	134
E.3.2	Interface requirements	135
E.3.3	Data storage requirements	135
Annex F	(informative) Example for an EETS Security Policy	136
F.1	Introduction	136
F.2	Basic laws and regulations	136
F.3	Organisation of EETS Information Security	136
F.3.1	General	136
F.3.2	Steering Committee	136
F.3.3	Trust Model	136
Annex G	(informative) Requirements on privacy-focused implementation	138
G.1	Introduction	138
G.2	Legal basis	138
G.2.1	EU Directive 95/46/EC	138
G.2.2	European data protection supervisor (EDPS)	138
G.3	Users' requirements	139
	Bibliography	140

Foreword

This document (CEN/TS 16439:2013) has been prepared by Technical Committee CEN/TC 278 “Road transport and traffic telematics”, the secretariat of which is held by NEN.

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

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

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

0 Introduction

0.1 Reader's guide

The development process for the security concept and implementation to protect an existing system normally includes several steps as follows: threat analysis with risk assessment, security policy definition, requirements and countermeasures definition followed by the implementation of countermeasures and supervising of their effectiveness. Countermeasures which do not work or work incorrectly need to be improved. The development of the Electronic Fee Collection (EFC) - Security Framework follows this approach as closely as possible, although there is no existing system to analyse. The used methodology needs to consider following limitations:

- 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 existing system.
- No security policy exists. The security policy can only be defined by the responsible stakeholder and its freedom is only limited by laws and regulations. Nonetheless, basic but incomplete examples of possible security policies can be provided.
- No specific system design or configuration exists to be based on. Only the available EFC base standards can be taken as references. Specific technical details of a particular system (e.g. servers, computer centres, de-central elements like road side equipment) need to be taken into consideration in addition to the present 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 the several stakeholders for their system parts. Due to the fact that there is neither an overall valid security policy, nor that the possibility to provide a useful risk assessment exists, the EFC security framework provides a toolbox of requirements and security measures covering as many threats as possible.

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. For such parts however, only requirements and recommendations, no security measures, are provided. 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 as the basic motivation for the security requirements (Annex C).
- 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 threat analysis, definition of requirements and security measures (see Clause 1 and Annex D).
- c) The threats on the EFC system model and its assets are analysed by two different methods: an asset-based analysis and an attack-based analysis. This approach, although producing some redundancy, ensures completeness and coverage of all relevant factors (Annex D).
- d) The requirements specification (Clause 6) is based on the threats identified in Annex D. Each requirement is at least motivated by one threat. At this stage, the specification does not prescribe any concrete implementation of a security requirement.

- e) The definition of security measures (Clause 7) provides a high level description of recommended possible methods to achieve and implement the goal(s) of the fulfilled requirements.
- f) Detailed security measures are only provided for the implementation of the interoperable interfaces (Clause 8) based on the requirements and the high level security measures.
- g) Basic key management requirements that support the implementation of the interoperable interfaces security measures are described in Clause 9.

A general trust model (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 if needed.

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

- 1) Identify the relevant processes, systems and interfaces in the security framework.
- 2) Extract the corresponding security requirements according to his security policy.
- 3) Provide evidence of compliance of its systems, processes and interfaces with the requirements of this specification. Evidence can be provided by a self-declaration, an internal or external audit or other certifications.

0.2 EFC role model

This Technical Specification complies with the role model defined in ISO 17573, *Electronic fee collection — System architecture for vehicle-related tolling*. 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 charges. The Toll Charger is the actor associated with the Toll Charging role; see Figure 1.

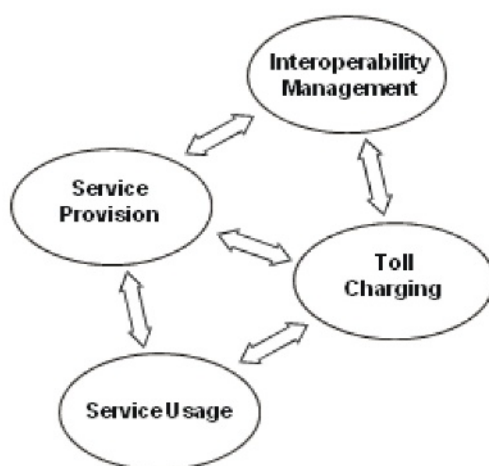


Figure 1 — The role model underlying this standard

Service Providers issue on-board equipment (OBE) to the users of the tolled infrastructure or transport service. Service Providers are responsible for providing the OBE that will be used for collecting data, enabling the Toll Charger to send a claim to the Service Provider for the usage of the infrastructure or transport service. In autonomous systems, each Service Provider delivers toll declarations to several Toll Chargers, as well as each Toll Charger receives toll declarations from more than one Service Provider. In dedicated short-range communication (DSRC) systems, the Toll Charger receives the main toll declarations from its own RSE and only supplementary charging data, if required from the Service Providers. Interoperability Management (IM) in

Figure 1 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 Service Provider compliant to this Technical Specification needs to be able to give evidence of security management as required. Such evidence is the basement of trust relations between the involved entities.

0.3 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 the usability of them for EFC applications. The framework will reference and tailor the security techniques and methodologies from these standards.

Figure 2 illustrates the context of the EFC Security Framework to other security standards. It is not exhaustive description; 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.

Each group of standards in Figure 2 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 the accurate use of them.
- **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 organisations. The standards are well suited for the security solutions of the Back End and other fixed or installed equipment including software of EFC systems.
- **IT - Open system interconnection** – This group of standards provide 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.

In addition, the EFC Security Framework makes use of existing threat analysis methods and also uses existing threat analysis with relations to EFC or ITS, e.g. ETSI TR 102 893 (Intelligent Transport Systems; Security; Threat, Vulnerability and Risk Analysis).

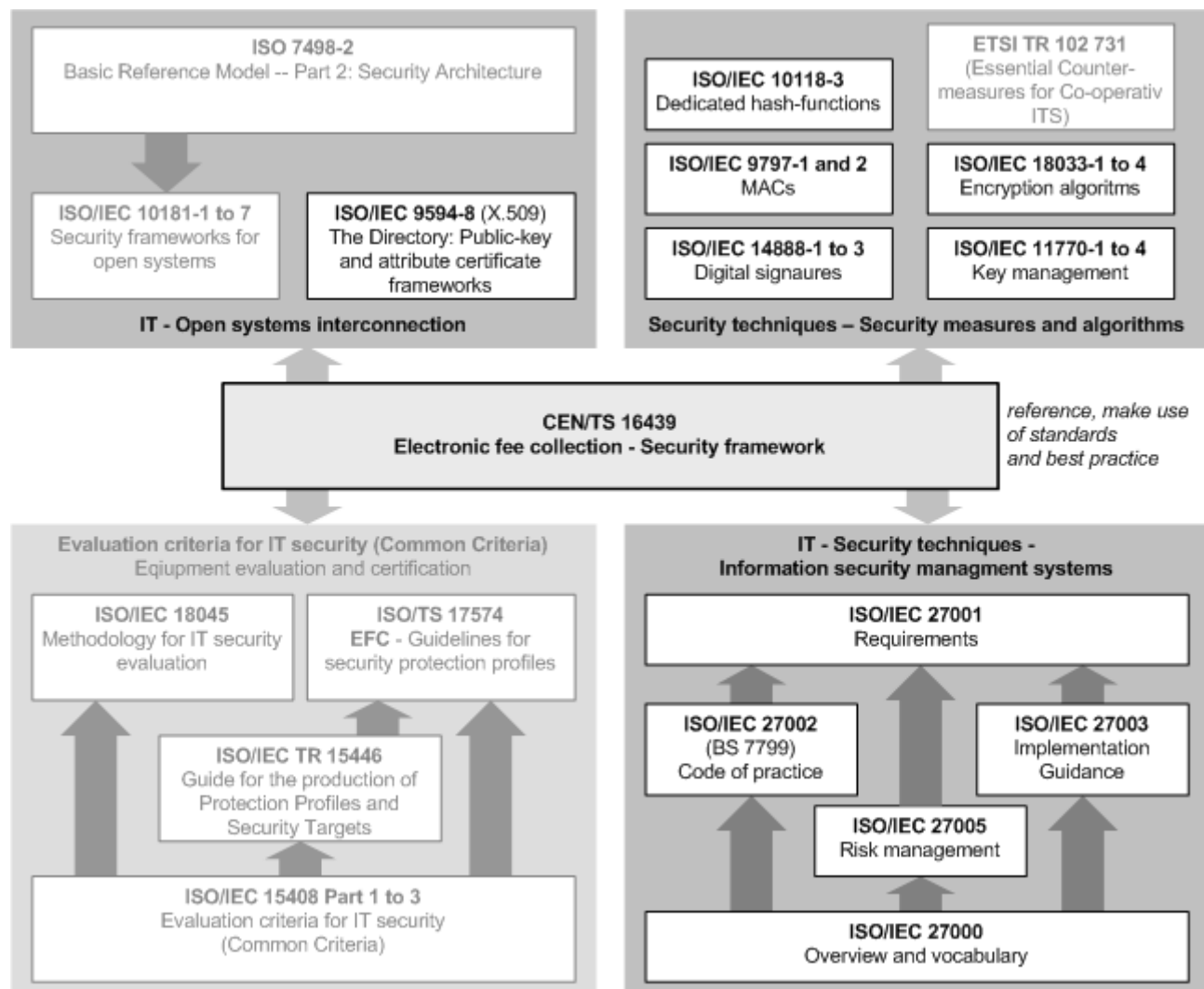


Figure 2 — Relevant security standards in the context of the EFC — Security framework

1 Scope

1.1 EFC specific scope

ISO 17573 defines the roles and functions as well as the internal and external entities of the EFC system environment. Based on the system architecture defined in ISO 17573, the security framework describes a set of requirements and security measures for stakeholders to implement and operate their part of an EFC system as required for a trustworthy environment according to its basic information security policy. In general, the overall scope is an information security framework for all organisational and technical entities and in detail for the interfaces between them.

Figure 3 below illustrates the abstract EFC system model used to analyse the threats, define the security requirements and security measures of 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 (called in-vehicle ITS Stations) used to host the EFC application.

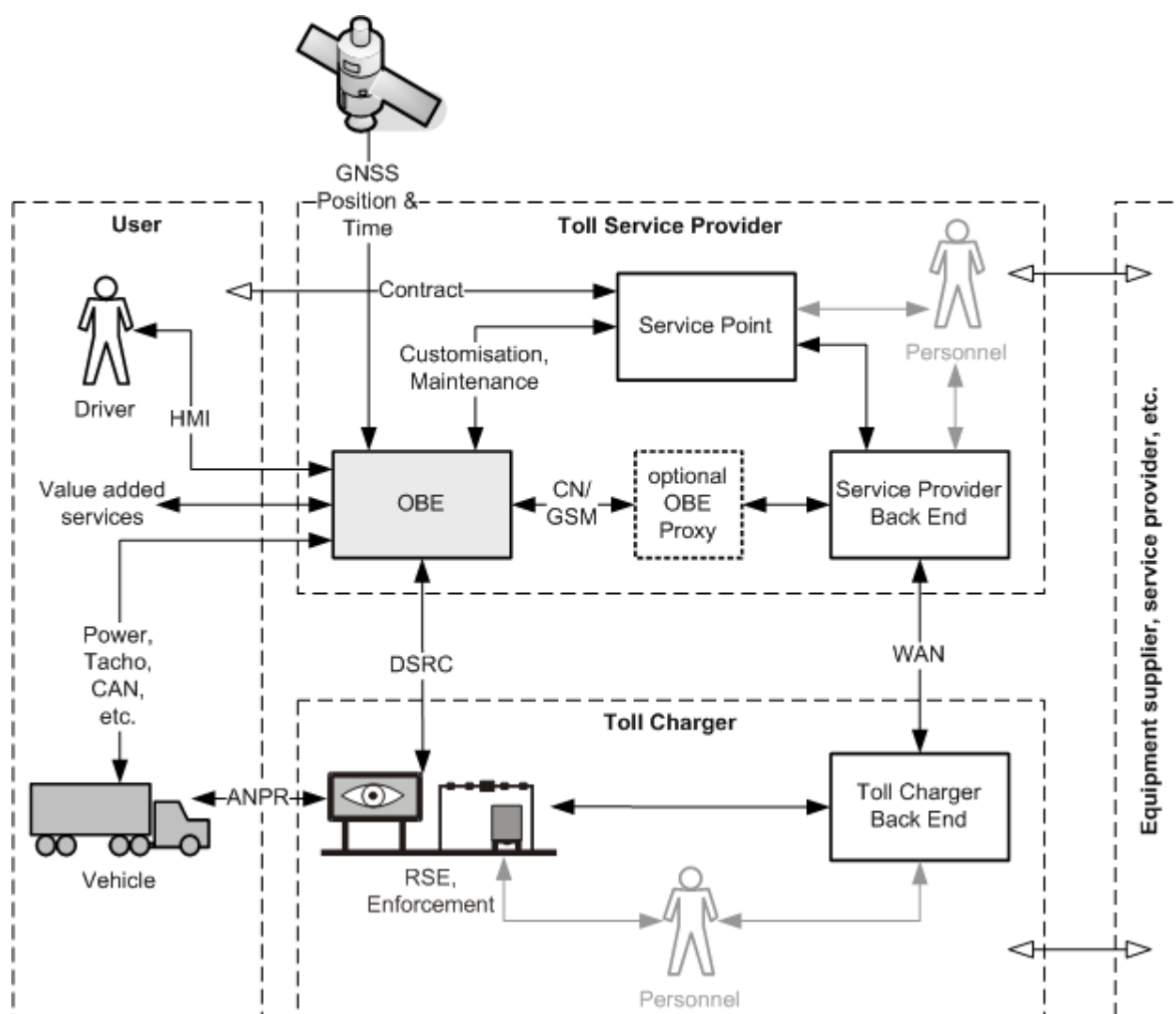


Figure 3 — EFC system model of the EFC Security Framework

The scope of this security framework comprises the following:

- general information security objectives of the stakeholders;
- threat analysis;
- definition of a trust model;
- security requirements;
- security measures – countermeasures;
- security specifications for interface implementation;
- key management;
- security policies;
- privacy-enabled implementations.

The following is 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 will be covered in a CEN Technical Report on "Guidelines for EFC-applications based on in vehicle ITS Stations" that is being developed at the time of publication of this document.

- entities and interfaces of the interoperability management role;
- the technical trust relation of the model between TSP and User;
- a complete specification and description of all necessary security measures to all identified threats;
- 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.

The detailed scope of the bullet points and the clause with the corresponding content is given below:

- General information security objectives of the stakeholders (informative, Annex C)

To derive actual security requirements and define implementations, it is crucial to gain a common understanding of the possible different perspectives and objectives of such stakeholders of a toll charging environment.

- Threat analysis (informative, Annex D)

The threat analysis is the basis and motivation for all the security requirements resulting in this framework. The results from two complementary approaches will be combined in one common set of requirements. 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).

- Definition of a trust model (normative, Clause 5)

The trust model comprises all basic assumptions and principles for establishing trust between the stakeholders. The trust model forms the basis for the implementation of cryptographic procedures to ensure confidentiality, integrity, authenticity and partly non-repudiation of exchanged data.

— Security requirements (normative, Clause 6)

Based on the threat analysis, security requirements are defined (e.g. for organisational and technical entities, interfaces, information etc) from which a system operator can draw its own applicable set according to the actual security policy. No concrete implementation specifications will be given as they are strongly dependent on the actual context of the toll charging environment and the relations between the stakeholders. A basic risk analysis of the interfaces shown in Figure 4 introduces the minimum set of security requirements for the protection of these interfaces.

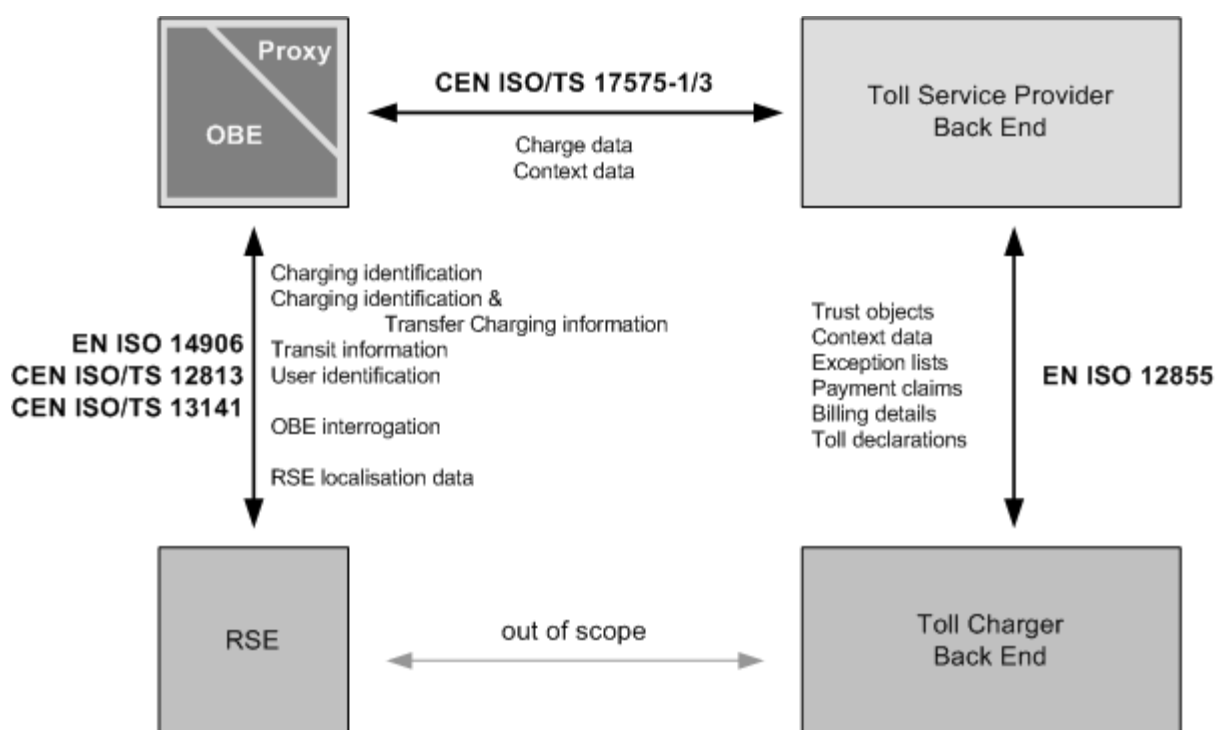


Figure 4 — Scope of EFC security framework for secure communication

— Security measures - countermeasures (normative, Clause 7)

A set of security measures mainly for data protocol layer of interfaces according to Figure 4 based on the requirements is defined to support actual EFC system implementations and as a base for the security specifications for interoperable interface implementation.

— Security specifications for interface implementation (normative, Clause 8)

To support the future implementation of (interoperable) toll charging environments, this specification provides precise implementation specifications for the interfaces, e.g. the detailed definition of message authenticators. These specifications represent an add-on for security to the corresponding standards. Figure 4 shows the relevant interfaces and the corresponding standards which need to be enhanced by proper security provisions.

— Key management (normative, Clause 9)

The toll charging environment uses cryptographic elements (keys, certificates, revocation lists etc) to support security services like confidentiality, authenticity, integrity 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.

- Implementation conformance statement (ICS) proforma (Annex B)

Annex B defines the implementation conformance statement proforma to be used by an equipment supplier, a system implementation or an actor of a role declaring his conformity to this Technical Specification.

- Security policies (informative, Annex E and Annex F)

As an aid for using this Technical Specification to build up a secure system, some examples are provided of what security policies could look like for a concrete interoperability framework (including European electronic toll service).

- Privacy-enabled implementations (informative, Annex G)

Respecting privacy is crucial for the implementation of every toll charging environment. However, different Toll Chargers may have different requirements on the level of privacy. This Technical Specification supports implementations with respect to privacy, but does not mandate one specific implementation. Therefore, it summarises the general requirements and conditions in relation to data privacy.

1.2 Scope in relation to other security frameworks

In general the overall scope is an information security framework for all organisational and technical entities of an EFC environment and in detail for the interfaces between them. This Technical Specification covers only the EFC specific aspects and not general IT security aspects. A general and complete IT security guideline, the Information Security Management System, is provided in the ISO 2700x family of standards.

A corresponding ISO/IEC 27001 certification of a TC or Toll Service Provider (TSP) organisation 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 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 shows 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.

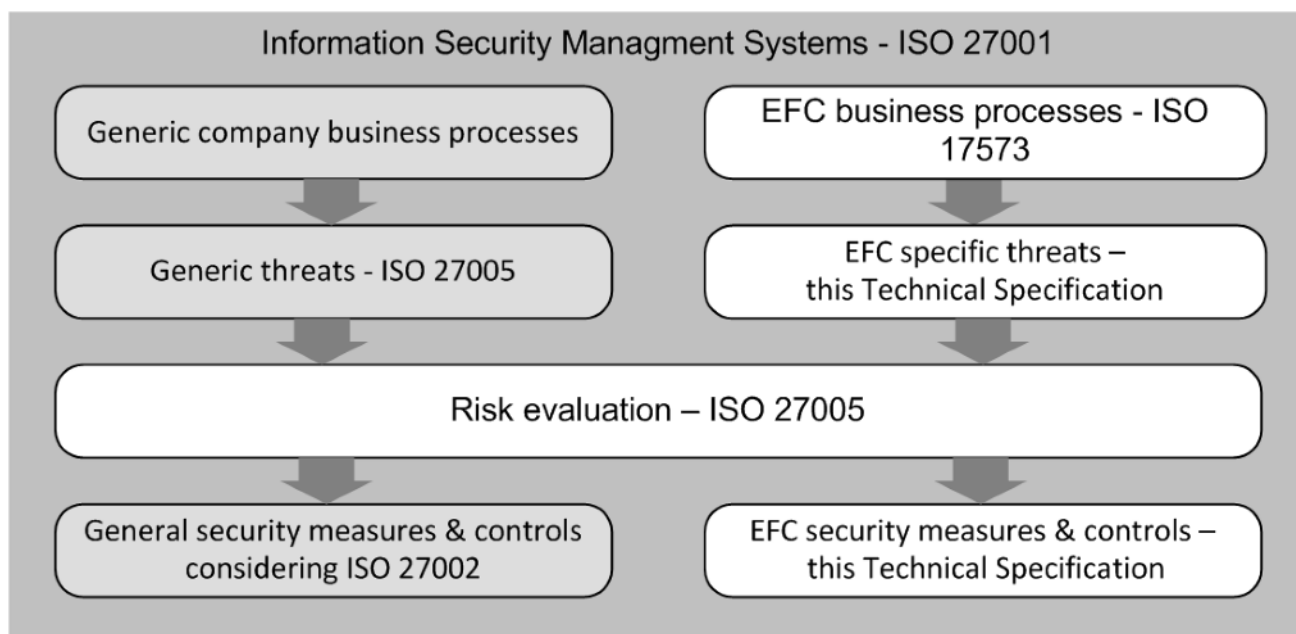


Figure 5 — Scope in relation to the Information Security Management System

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.

EN 15509:2007, *Road transport and traffic telematics — Electronic fee collection — Interoperability application profile for DSRC*

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

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

CEN ISO/TS 13141:2010, *Electronic fee collection — Localisation augmentation communication for autonomous systems (ISO/TS 13141:2010)*

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

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

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

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

ISO/IEC 9594-8:2008, *Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks*

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

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

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

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

ISO/IEC 14888-2:2008, *Information technology — Security techniques — Digital signatures with appendix Part 2: Integer factorization based mechanisms*

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

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

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

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

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

IETF Request for Comments (RFC) 4301:2005-10, *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*

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]

3.2

activist

especially active, vigorous advocate of a cause, especially a political cause, who may or may not use violence to achieve his goals

3.3

asset

anything of value of an EFC system stakeholder

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

3.4

attack

attempt to destroy, expose, alter, disable, steal or gain unauthorised access to or make unauthorised use of an asset

[SOURCE: ISO/IEC 27000:2009, 2.4]

3.5

authenticity

property that an entity is what it claims to be

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

3.6

availability

property of being accessible and usable upon demand by an authorised entity

[SOURCE: ISO/IEC 27000:2009, 2.7]

3.7

Back End

generic name for the computing and communication facilities of the Service Provider and/or the Toll Charger

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

3.8

business continuity

processes and/or procedures for ensuring continued business operations

[SOURCE: ISO/IEC 27000:2009, 2.8]

3.9

certificate revocation list

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

[SOURCE: ISO/IEC 9594-8:2008, 3.4.12]

3.10

certification authority

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

Note 1 to entry: Optionally the Certification Authority may create the users' keys.

[SOURCE: ISO/IEC 9594-8:2008, modified]

3.11

communication provider

provider of communication services used for the transmission of information

3.12

confidentiality

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

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

3.13

customer (of a Toll Service Provider)

person or legal entity that uses the service of a Toll Service Provider

[SOURCE: ISO 17573:2010, 3.2]

3.14

data protection commissioner

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

3.15

data subject's consent

freely given specific and informed written indication of his wishes by which the data subject signifies his agreements to personal data relating to him being processed by the EFC Service Provider and Toll Charger

3.16

driver

person who drives a vehicle

Note 1 to entry: The driver is assumed to operate (use / serve) the OBE.

3.17

electronic fee collection

EFC

toll charging by electronic means via a wireless interface

[SOURCE: ISO 17573:2010, 3.4]

3.18

enforcement

process of compelling observance of a law, regulation, etc.

[SOURCE: ISO 17573:2010, 3.5]

Note 1 to entry: In this context: the process of compelling observance of a toll regime.

3.19

enterprise

company organised for lawful or unlawful commercial purposes

3.20

foreign power

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

3.21

government

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

3.22

Front End

part(s) of the toll system where road usage data for an individual road user are collected, processed and delivered to the Back End. The Front End comprises the on-board equipment and an optional proxy

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

3.23

hacker

computer user who attempts to gain unauthorised access to a proprietary computer system or exploit vulnerabilities in such a system

3.24

impact

adverse change to the level of business objectives achieved

[SOURCE: ISO/IEC 27000:2009, 2.17]

3.25

information asset

knowledge or data that has value to the organisation

[SOURCE: ISO/IEC 27000:2009, 2.18]

3.26

information security

preservation of confidentiality, integrity and availability of information

[SOURCE: ISO/IEC 27000:2009, 2.19]

Note 1 to entry: In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.

3.27

information security incident

single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

[SOURCE: ISO/IEC 27000:2009, 2.21]

3.28

integrity

property of protecting the accuracy and completeness of assets

[SOURCE: ISO/IEC 27000:2009, 2.25]

3.29

interface

abstraction of the behaviour of an object that consists of a subset of the interactions of that object together with a set of constraints on when they may occur

3.30

interoperability

ability of systems to provide services to and accept services from other systems and to use the services so exchanged to enable them to operate effectively together

[SOURCE: ISO 17573:2010, 3.7]

3.31
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 9797-1:2011, 3.9]

3.32
non-repudiation

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

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

3.33
on-board equipment
OBE

equipment fitted within or on the outside of a vehicle and used for toll purposes

[SOURCE: ISO 17573:2010, 3.9]

3.34
personal data

information relating to an identified or identifiable natural person (data subject)

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

3.35
policy

overall intention and direction as formally expressed by management

[SOURCE: ISO/IEC 27000:2009, 2.28]

3.36
privacy

right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

[SOURCE: CEN ISO/TS 17574:2009, 3.16]

3.37
processing of personal data

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

3.38
processor (privacy)

natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller

3.39

roadside equipment

RSE

equipment located along the road transport network, for the purpose of communication and data exchanges with on-board equipment

[SOURCE: ISO 17573:2010, 3.12]

3.40

security policy

set of rules that regulate how to cope with security threats or to what degree of security levels should be kept

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

3.41

security service

service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers

[SOURCE: ISO 7498-2:1989]

3.42

signature

one or more data elements resulting from the signature process

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

3.43

threat

potential cause of an unwanted incident, which may result in harm to a system, organisation or person

[SOURCE: ISO/IEC 27000:2009, 2.45]

3.44

threat analysis

systematic detection, identification, and evaluation of threats

3.45

threat agent

entity that has the intention to act adversely on an asset

3.46

toll

charge, tax, fee, or duty in connection with using a vehicle within a toll domain

[SOURCE: ISO 17573:2010, 3.15]

3.47

toll charger

TC

legal entity charging toll for vehicles in a toll domain

[SOURCE: ISO 17573:2010, 3.16]

3.48

toll declaration

statement to a Toll Charger that confirms the presence of a vehicle in a toll domain in a format agreed between the Toll Service Provider and the Toll Charger

[SOURCE: ISO 17573:2010, 3.17]

3.49

toll domain

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

[SOURCE: ISO 17573:2010, 3.18]

3.50

toll service

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

[SOURCE: ISO 17573:2010, 3.22]

3.51

toll service provider

TSP

legal entity providing to his customers toll services on one or more toll domains for one or more classes of vehicles

[SOURCE: ISO 17573:2010, 3.23]

3.52

toll system

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

[SOURCE: ISO 17573:2010, 3.24]

3.53

trusted third party

TTP

security authority or its agent that is trusted with respect to some security-relevant activities (in the context of a security policy)

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

3.54

user

generic term used for the customer of a Toll Service Provider, one liable for toll, the owner of the vehicle, a fleet operator, a driver etc. depending on the context

[SOURCE: ISO 17573:2010, 3.29]

3.55

vulnerability

weakness of an asset or control that can be exploited by a threat

[SOURCE: ISO/IEC 27000:2009, 2.46]

4 Symbols and abbreviations

AC_CR Access Credentials (EN 15509)

ADU	Application Data Unit
AES	Advanced Encryption Standard (ISO/IEC 18033-3:2010)
CA	Certification Authority
CCC	Compliance Check Communication (CEN ISO/TS 12813)
CN	Cellular Network (for example GSM)
CRL	Certificate Revocation List
DES	Data Encryption Standard
DSRC	Dedicated Short-Range Communication (EN ISO 14906)
DTLS	Datagram Transport Layer Security
ECC	Elliptic Curve Cryptography
EETS	European Electronic Toll Service
EFC	Electronic Fee Collection (ISO 17573)
GNSS	Global Navigation and Satellite System (ISO 17573)
HTTP	HyperText Transfer Protocol
HTTPS	HTTP over Secure socket layer
ICS	Implementation Conformance Statement (CEN ISO/TS 14907-2)
IETF	Internet Engineering Task Force
IM	Interoperability Management
IPsec	Internet Protocol Security
ISMS	Information Security management system (ISO/IEC 27000)
LAC	Localisation Augmentation Communication (CEN ISO/TS 13141)
MAC	Message Authentication Code
MAC_NR	DSRC Message Authentication guaranteeing Non-Repudiation to the Toll Charger
MAC_TC	DSRC Message Authentication Code for Toll Charger
MAC_TSP	DSRC Message Authentication Code for Toll Service Provider
OBE	On-Board Equipment (EN ISO 14906)
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 (EN ISO 14906)
SC	Steering Committee
SHA-1	Secure hash algorithm (ISO/IEC 10118-3)
SM	Security Measure (countermeasure)
SMTP	Simple Mail Transfer Protocol
SU	Service User
TC	Toll Charger (ISO 17573)
TE	Trusted Element
TLS	Transport Layer Security
TSP	Toll Service Provider
TTP	Trusted Third Party
UDP	User Datagram Protocol
VPN	Virtual Private Network
VST	Vehicle Service Table (EN ISO 14906)
WAN	Wide Area Network
XER	XML Encoding Rules (ISO/IEC 8825-4)

5 Trust model

5.1 Introduction

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 User) and the technical trust model between the IT infrastructure of the TC and TSP. The technical trust relation of the model between TSP and User is outside the scope of this Technical Specification.

The trust model is based on the assumption that no initial trust 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. These are the peer to peer trust relations:

- between Toll Charger and Toll Service Provider;
- between Toll Service Provider and User; and
- Toll Charger or Toll Service Provider and Interoperability Management.

There is no direct trust relation between Toll Charger and User, as is illustrated in Figure 6. 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.

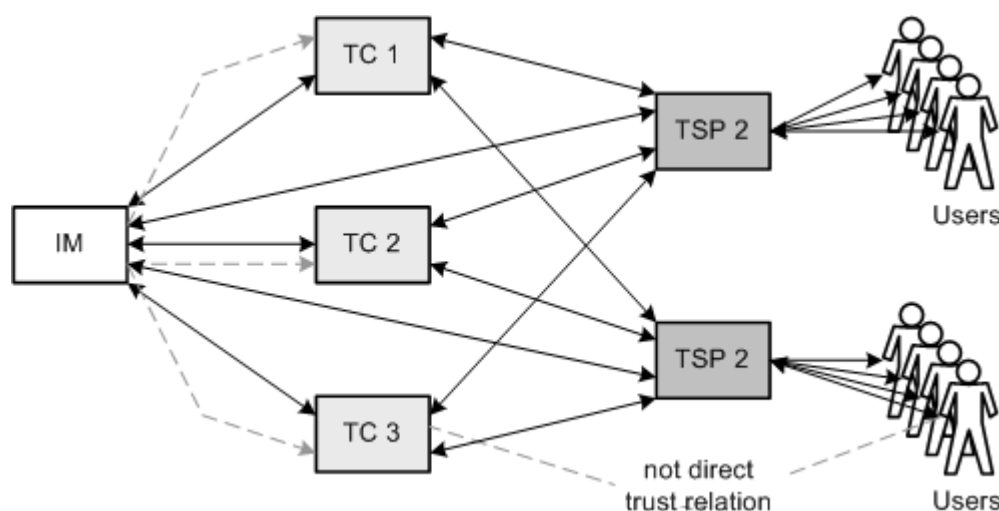


Figure 6 — Stakeholder trust relations

The Interoperability Management may be a single organisation or a construct of several entities performing the different tasks. Issuing laws, regulations and general User information by the Interoperability Management (IM) is done using a trust relation outside of the scope of this specification (dotted arrows). Trust relations between IM and TC or TSP inside the scope are among others used for certification of organisation or equipment and in case of TTP functions.

TC and TSP could possibly agree to use a Trusted Third Party (TTP) (e.g. for issuing public-key certificates). Such a TTP supported trust relation may include the IM relations. In this case, the TTP should be seen as a part of the Interoperability Management.

This Technical Specification does not require a mandatory TTP but supports the use of it.

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 assure 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 7 illustrates an example of a trust model approach, which is supported by this specification.

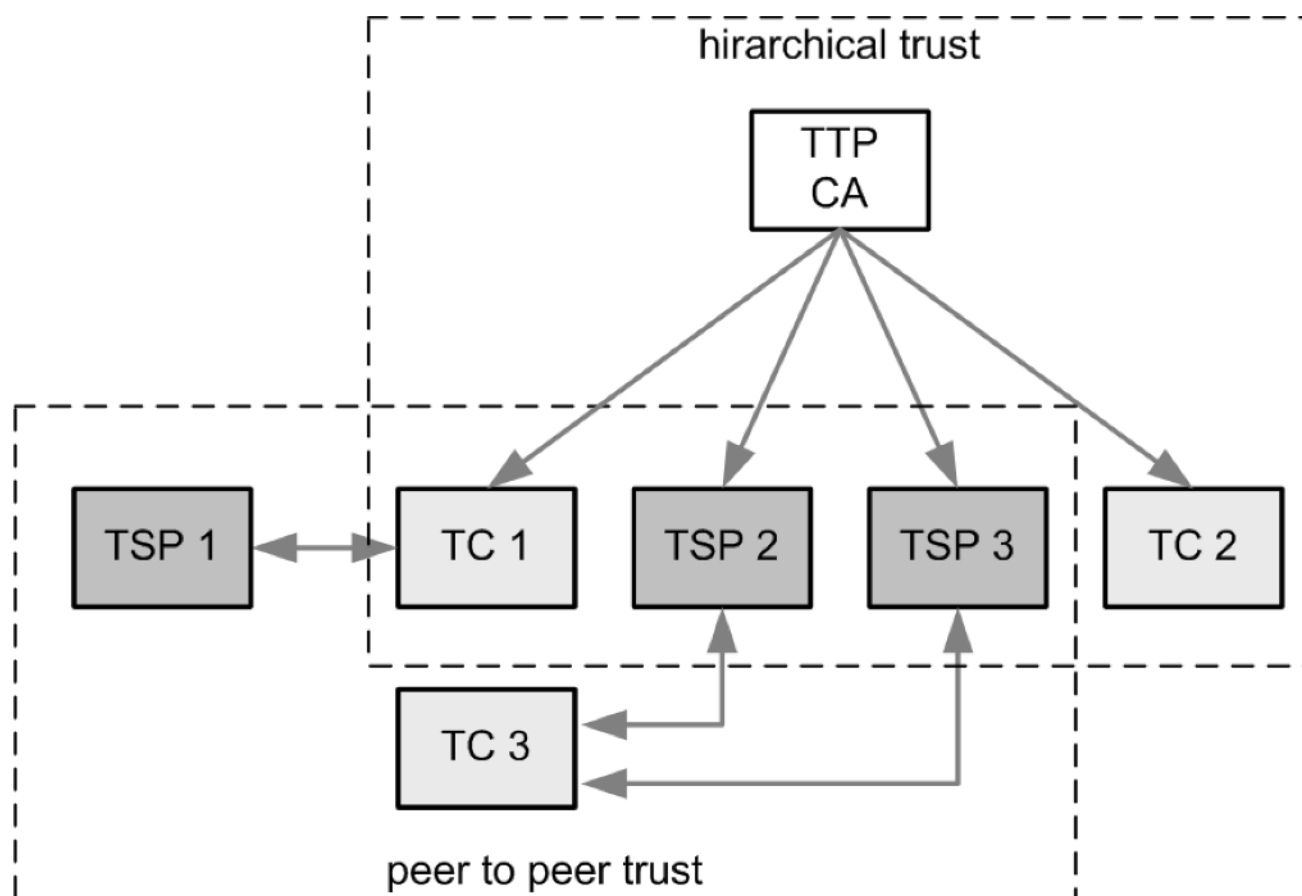


Figure 7 — Example of a mixed trust model environment

Figure 7 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 TTP as a CA issuing certificates for each entity based on its self-signed root certificate imported by the entities. 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 import both the TTP CA and the connected peer to peer trust partner 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 should be limited (see 5.4.3).

The used type and structure of the model for the trust relation between two stakeholders is a decision of their contractual framework.

Large scale interoperable systems like EETS should use a TTP with a CA function if this is available. In contrast, bilateral or small size interoperable systems may prefer a peer to peer trust model to avoid the need for a TTP. An example for EETS can be found in Annex F.

5.3.3 Trust model for TSP and User relations

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

5.3.4 Trust model for Interoperability Management relations

The Interoperability Management may issue laws, regulations and standards for the EFC system via public recognised channels. Communication between IM and TC or TSP (e.g. for certification of organisations or equipment) may 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 if bidirectional electronic data exchange channels are required, the same technical trust model as defined in 5.3.2 shall be used.

The preferred IM function in the trust model should be the role of a TTP with CA functionality.

5.4 Implementation

5.4.1 Setup of trust relations

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

The initial step for the setup of the trust relation is the import of a root self-signed certificate. This may be either a self-signed root certificate of an agreed TTP acting as a CA or a self-signed root certificate of the TC or TSP. The purpose and usage of the certificate (e.g. TC to TSP communication) shall be defined by the Extended Key Usage extension in the ISO/IEC 9594-8 certificate.

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 11770-3:2008, Clause 12 (Public key transport). In case of public key transport mechanism 2, the key token verification shall be done using fingerprint of the root certificate based on the algorithms defined in 8.1.2.

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.

5.4.2 Trust relation renewing and revocation

The self-signed root certificate shall have a validity limited to the recommended time of use of the key length of the respective private key. A self-signed root certificate may also be revoked by its issuer before the expiry of the validity for any reason. The replacement of the self-signed root certificate shall be done as defined in 5.4.1. All issued entity certificates of this root certificate shall be renewed according to the process of 5.4.3.

The revocation of a self-signed root certificate without replacement shall be done by a procedure similar to the early termination of the contract. Certificates issued by the revoked root certificate are included in the revocation and are no longer valid and trustworthy.

The revocation message for a self-signed root certificate shall be signed by the respective private key. The message signature shall be verified with the public key of the originally imported self-signed root certificate.

Reaching the date of expiry or a prior revocation of a self-signed root certificate without issuing a new certificate shall result in a termination of the trust relation.

5.4.3 Issuing and revocation of sub CA and entity certificates

The self-signed root certificates shall have a key length recommended for the use during the planned contract duration between TC and TSP. The corresponding private-key of the self-signed root certificate shall only be used for signing entity or sub CA certificates.

The implementation of the certificate verification process shall support a certificate chain starting from root certificate and at least up to four certificate levels signed by a sub CA or entity private key.

Each entity shall have at least three different certificates used for secure communication channels, for message signing and for message and/or key encryption purposes. These certificates shall have a validity period of not longer than two years.

The information about revocation of entity and self-signed root certificates shall be distributed issuing a Certificate Revocation List (CRL) defined in ISO/IEC 9594-8 signed by the self-signed root certificates private-key.

Exchange of certificates and CRLs is defined in Clause 9, Key management.

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. A compliant implementation to this specification to import and use the certificates and CRLs shall at least support all possible critical certificate and CRL extensions as defined in IETF RFC 5280 profile.

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

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

The certificate and the CRL shall have a fingerprint in hexadecimal format based on the algorithms defined in 8.1.2.

5.4.5 Certificate extensions

The entity certificates shall use the certificate extensions listed below:

- a) Basic Constraints;
- b) CRL Distribution Points;
- c) Key Usage;
- d) Extended Key Usage with object identifier (OID) for:
 - 1) TC to TSP interface certificate;
 - 2) Front End to TSP Back End interfaces certificate.
- e) Subject Information Access.

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

6 Security requirements

6.1 Introduction

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

- Generic information technology security requirements may be found in ISO Information Security Management System family of standards (e.g. in ISO/IEC 27001 [12]).
- Security requirements for the protection of payment card data may be found in the Payment Card Industry Data Security Standard (PCI DSS, see [10]), 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 or at least a defined subset thereof, in accordance with the applicable security policy.

Table 1 explains the notation and relations of the requirements defined in this clause.

Table 1 — Notation of requirements

No.	Unique number for every requirement to enable a later matching with the security measures.
Requirement	Definition of the requirement or recommendation.

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 organisations operating EFC systems, by performing a comprehensive risk analysis according to ISO/IEC 27005.

In order to effectively assure information security in a holistic approach, TCs and TSPs shall establish, implement, operate, monitor, review, maintain and 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 Specification shall be used while defining and implementing the controls for minimising the impact of the identified risks.

The ISMS should also consider the generic companies business processes as part of its scope. Control objectives and controls should be identified in accordance with ISO/IEC 27002 to fulfil and monitor the treatment of risks.

Table 2 lists the requirement reference for threats to be dealt with in the ISMS framework.

Table 2 — ISMS requirements

No	Requirement
RQ.ISMS.1	Establish, implement, operate, monitor, review, maintain and improve an Information Security Management System (ISMS) according to ISO/IEC 27001
RQ.ISMS.2	Threat requires a security measure or security control defined by the ISO/IEC 27002 standard.

6.3 Communication interfaces

6.3.1 General

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. Subclause 6.3.2 lists all requirements driven by the threat analysis whereas the three Subclauses 6.3.3 to 6.3.5 define the recommended requirement profiles for the main EFC system interface types based on a simplified risk assessment.

The following pattern for the profile definition is used:

Risk assessment: Simplified risk assessment description.

Requirement profile: Defines the requirements to be fulfilled for profile compliance. Requirements in brackets are only recommendations.

6.3.2 Generic interface requirements

Table 3 — Generic interface requirements

No	Requirement
RQ.IF.01	Data exchange shall be done using an authenticated channel that shall guarantee data integrity, confidentiality and non-repudiation (proof of origin and delivery).
RQ.IF.02	Data exchange shall be done using transmission channels with reliable availability.
RQ.IF.10	Data exchange shall guarantee data confidentiality.
RQ.IF.11	Data exchange shall guarantee data integrity.
RQ.IF.12	Data exchange shall guarantee the authenticity of the data originator.
RQ.IF.13	Data exchange shall guarantee non-repudiation with proof of origin.
RQ.IF.14	Data exchange shall guarantee non-repudiation with proof of delivery.
RQ.IF.20	Data exchange shall only be done between authenticated entities for the respective data exchange.
RQ.IF.21	Data exchange shall be done using an authenticated channel that shall guarantee data integrity and confidentiality.
RQ.IF.30	Data exchange shall allow the detection of resent messages (protection against reply attacks).

6.3.3 DSRC profile

The DSRC profile includes the requirements for the charging, the compliance check (CCC) and the localisation (LAC) transaction.

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 User notice. This requires authentication of 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 User may deny a certain road use (charging or CCC event). A faked LAC event may be used to proof deny or a claimed 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 User, vehicle or RSE. Confidentiality is not required.

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

6.3.4 TC to TSP profile

The profile covers the not-secured communication between TC and TSP for data according to EN ISO 12855.

Risk assessment: Profile A: Communication eavesdropping and interception by third parties on a not 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 User data is also an issue. Message confidentiality, integrity and authenticity shall be assured.

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

A Back End interface shall protect against replay attacks.

Profile B (extends profile A): 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.

<i>Requirement profile A:</i>	Mandatory	RQ.IF.13 + RQ.IF.21 + RQ.IF.30
	Recommended	RQ.IF.02

<i>Requirement profile B:</i>	Mandatory	RQ.IF.13 + RQ.IF.14 + RQ.IF.21 + RQ.IF.30
	Recommended	RQ.IF.02

NOTE The implementation of requirement profile A is defined in 8.6.2 and the extensions for profile B in 8.6.3 and 8.6.4.

6.3.5 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:

- TC to RSE communication;
- TSP to OBE communication;
- internal Back End WAN communication.

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

Risk assessment: Standard communication channels offered by communication providers may 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 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.

<i>Requirement profile:</i>	Mandatory	RQ.IF.21
	Recommended	RQ.IF.02

6.4 Data storages

6.4.1 General

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

Table 4 — Data storage requirements

No	Requirement
RQ.DS.01	Access to stored data shall only be granted after authorisation.
RQ.DS.02	Access to store data shall only be granted via defined interfaces and defined procedures.
RQ.DS.03	Stored data shall have an independent backup storage.
RQ.DS.05	Data storage shall guarantee data integrity.
RQ.DS.06	Data storage shall guarantee data confidentiality.
RQ.DS.07	Data storage shall guarantee non-repudiation with proof of origin for applicable data. Proof of origin authenticators shall be stored together with the data received.
RQ.DS.08	Data storage shall guarantee non-repudiation with proof of delivery for applicable data. Proof of delivery authenticators shall be stored together with the data delivered.

6.4.2 OBE data storages

This profile considers an OBE in the User environment, i.e. a personalised OBE mounted into a vehicle.

Risk assessment: Not allowed manipulation of data stored in the OBE may result in lower charge for the user and loss of income for TC and TSP. Not authorised read out of data stored in the OBE may result in a privacy violation to the 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.01 is fulfilled for the HMI. An existing GSM or DSRC interface requires additional access credentials.

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

6.4.3 RSE data storages

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

Risk assessment: Not allowed manipulation of data stored in the RSE (before transmitted to the TSPs Back End) may result in loss of income for TC and TSP. Not authorised read out of data stored in the RSE (e.g. enforcement data) may result in a privacy violation to the user and/or loss of reputation of the TC. Change of the data originator identity (i.e. OBE identity) may result in charging a wrong user.

<i>Requirement profile:</i>	Mandatory	RQ.DS.01 + RQ.DS.02 + RQ.DS.05 + RQ.DS.07 + RQ.DS.06 if applicable (e.g. for keys)
	Recommended	-

6.4.4 Back End data storage

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 kind of data.

<i>Requirement profile:</i>	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	-

6.5 Toll Charger

The following clauses list requirements for protection of the Toll Charger's asset. This leads to requirements to both Toll Service Providers and Toll Chargers.

Table 5 — Toll Charger requirements (1 of 2)

No	Requirement
RQ.TC.01	The Toll Charger shall determine if factual road usage is represented by a corresponding set of toll declarations (enabled by RQ.TSP.51).
RQ.TC.02	The Toll Charger shall be able to determine if a toll declaration is based on correct and complete road usage data (enabled by RQ.TSP.52).
RQ.TC.03	The TC shall determine, in a spot check, if an OBE is in an OK operational state.
RQ.TC.04	The TC shall check the integrity and authenticity of the received data as compared to the data sent from the Front End.
RQ.TC.05	The TC shall determine if toll declarations are based on data originating from a legitimate Front End and/or TSP Back End (enabled by RQ.TSP.55).
RQ.TC.06	The Toll Charger shall periodically audit invoices to customers for tolls of his toll domain (enabled by RQ.TSP.56).
RQ.TC.07	The TC shall assure that the TSPs Front End is acceptable for use in the system.
RQ.TC.08	The TC shall check the model and make of OBE during a vehicle check (enabled by RQ.TSP.58).
RQ.TC.09	The TC shall provide evidence that the repudiation of the toll declaration is legal and correct.
RQ.TC.11	The TC shall detect faked or cloned OBEs (for DSRC systems) and inform the TSP to black list the detected OBEs (enabled by RQ.TSP.61).
RQ.TC.20	The TC shall detect RSE damaging and recover the RSE functionality.
RQ.TC.21	The TC shall detect theft of RSE parts and recover the RSE functionality by a replacement of the stolen part.

Table 5 (2 of 2)

No	Requirement
RQ.TC.22	The TC shall implement RSE authentication measures for DSRC communication.
RQ.TC.23	The TC shall detect RSE malfunction and correct the malfunctioning RSE functionality.
RQ.TC.24	The RSE shall not allow unauthorised access to software and data.
RQ.TC.90	The Toll Chargers 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).
RQ.TC.91	The TC shall provide non-repudiation with proof of origin for distributed EFC context data and shall oblige TSPs receiving this EFC context data to provide non-repudiation with proof of delivery.
RQ.TC.92	The TC shall only accept an OBE after detecting if an OBE belongs to a trusted Service Provider and if the Service provider guarantees payment for that specific OBE (enabled by RQ.TSP.62).
RQ.TC.93	The TC shall oblige the TSP to deliver protection against repudiation by users of invoices and CCC events.
RQ.TC.94	Received Exception List shall only be accepted after verification of non-repudiation with proof of origin. The TC shall also provide for the exception list non-repudiation with proof of delivery to the TSP.
RQ.TC.95	The TC shall be responsible for the availability of his interfaces according to agreed service levels.

6.6 Toll Service Provider

Table 6 lists requirements for the protection of the Toll Service Provider's asset. This leads to requirements to both Toll Service Providers and Toll Chargers.

Table 6 — Toll Service Provider requirements (1 of 3)

No	Requirement
RQ.TSP.01	The Toll Service Provider shall determine if factual road usage is represented by a corresponding set of toll declarations. NOTE This means that toll declarations are not altered and completely transmitted.
RQ.TSP.02	The Toll Service Provider shall determine if a toll declaration is based on correct and complete road usage data. NOTE This means that tolling related events are correctly collected.
RQ.TSP.04	The TSP shall check the integrity and authenticity of the received data as compared to the data sent from the Front End.
RQ.TSP.05	The TSP shall determine if toll declarations are based on data originating from a legitimate Front End.
RQ.TSP.06	An OBE shall prevent or at least detect illegal modification of parameters through its external interfaces. Illegal modification shall result in "NOT OK" OBE state.
RQ.TSP.07	An OBE shall not allow the User to modify fixed vehicle parameters.

Table 6 (2 of 3)

No	Requirement
RQ.TSP.08	TSP shall detect duplicate (also false) OBE identities and black list such duplicated OBE identities.
RQ.TSP.09	The TSP shall notify the driver if the OBE is not working correctly.
RQ.TSP.10	The TSP shall determine if billing details are based on correct and complete road usage data.
RQ.TSP.11	The TSP shall determine if factual road usage is represented by a corresponding set of billing details.
RQ.TSP.12	The TSP shall verify the calculation of amounts in the billing details.
RQ.TSP.13	The TSP shall accept only distributed EFC context data having non-repudiation with proof of origin.
RQ.TSP.14	The TSP shall oblige the TC to guarantee that distribution of exception lists features non-repudiation with proof of delivery.
RQ.TSP.15	The TSP shall oblige the TC to enable the TSP to determine the correctness and relevance of a CCC event via the corresponding record.
RQ.TSP.16	The OBE shall detect signal input inconsistencies and in such case signal not OK to the User and send an indication to TSP.
RQ.TSP.19	The TSP shall provide the TC with the means to identify the stolen OBEs.
RQ.TSP.20	The TSP shall manage stolen OBEs.
RQ.TSP.21	The TSP shall detect cloned OBEs and black list the detected OBEs.
RQ.TSP.22	TSP shall avoid exaggerate loss of OBE caused by Users.
RQ.TSP.23	The TSP shall validate the User contract information.
RQ.TSP.30	The TSP shall validate payment means of a User.
RQ.TSP.31	The TSP shall monitor the validity of payment means.
RQ.TSP.40	The OBE shall not allow change of internal data via the user interface, except the data allowed to be changed.
RQ.TSP.41	The OBE shall only present intended data by the User interface.
RQ.TSP.42	The Toll Service Providers implementation of the Front End and gathering and processing of data should be in compliance with the privacy requirements.
RQ.TSP.50	The TSP shall assure that only authenticated Users have access to systems that manage their personal data.
RQ.TSP.51	The TSP shall enable the TC to determine if factual road usage is represented by a corresponding set of Toll Declarations (required to enable RQ.TC.01).
RQ.TSP.52	The TSP shall enable the TC to determine if a toll declaration is based on correct and complete road usage data (required to enable RQ.TC.02).

Table 6 (3 of 3)

No	Requirement
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).
RQ.TSP.56	The TSP shall enable the TC to audit invoices to customers for tolls of his toll domain (required to enable RQ.TC.06).
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 These 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 OBU models and makes."
RQ.TSP.61	The TSP shall provide measures to the TC to detect faked or cloned OBEs (required to enable RQ.TC.11).
RQ.TSP.62	The TSP shall enable the TC to detect if an OBE belongs to the TSP (required to enable RQ.TC.92).
RQ.TSP.90	The Toll Service Providers 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).
RQ.TSP.91	The data communication between Front End (OBE) and Back End (TSP) Back End 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).
RQ.TSP.92	Customisation of OBE shall be done in a secure way.
RQ.TSP.93	The Toll Service Provider shall implement monitoring procedures to detect any non-compliant behaviour.
RQ.TSP.94	The TSP shall implement technical and organisational measures to prevent that billing details are revealed to unauthorised parties.
RQ.TSP.95	The TSP shall guarantee the availability of its interfaces according to agreed service levels.

6.7 User

Table 7 lists the requirements of the User to protect his assets. The User requirements lead to requirements for the TSP and TC.

Table 7 — User requirements

No	Requirement
RQ.SU.01	The TSP and TC shall enable the User to check the correctness of an invoice.
RQ.SU.02	The TSP shall publish his procedures of collecting and processing customer data.
RQ.SU.03	The TC shall publish his procedures of collecting and processing customer data.

6.8 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
RQ.IM.01	The Interoperability Management shall issue an EFC scheme security policy in collaboration with the involved stakeholders. NOTE Examples explaining the content of such a security policy are given in Annex E and Annex F.
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.

6.9 Limitation of requirements

The following qualified requirements are included to document the limitation of security measures against some threats. This means that either no required security measure exists to prevent from the threat or the security measure is not really feasible because it is much too expensive.

Table 9 — Denial of service and hardware integrity threats

No	Requirement
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.
RQ.XX.02	Prevent manipulating equipment hardware; especially prevent OBE from HW manipulation. Such a requirement can only be fulfilled by developing a tamper resistant OBE which is not cost efficient feasible. This is out of scope of this Technical Specification.

7 Security measures - countermeasures

7.1 Introduction

Based on the security requirements, this section provides recommended security measures (or countermeasure requirements, specifications) to be implemented to fulfil the related requirements.

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

Table 10 — Notation and relations of the security measures

No.	Unique number for every security measure.
Security measure	Description of the security measure (countermeasure).
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

Table 11 — General security measures

No	Security measure	Fulfilled RQ
SM101	A data protection commissioner or delegate shall have the possibility to audit the system for compliance with data privacy regulations	RQ.SU.02
SM102	Certification and audits shall be used to proof the implementation concept.	RQ.TSP.42
SM103	Contracting parties of communication providers shall have proper privacy protection agreements in place to prevent illegal tracking of users.	RQ.TSP.42

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	Security measure	Fulfilled RQ
SM200	Contracting parties of communication providers should have proper service levels agreed and monitoring procedures in place that are able to detect any non-compliant behaviour of the communication provider.	RQ.IF.02

7.3.2 DSRC-EFC interface

Table 13 — DSRC-EFC interface security measures (1 of 2)

No	Security measure	Fulfilled RQ
SM210	The RSE shall request the OBE to calculate and provide a DSRC Message Authentication Code for Toll Charger (MAC_TC) over at least the EN ISO 14906 attributes PaymentMeans, using a key known only to the Toll Charger and the Toll Service Provider	RQ.IF.11 RQ.IF.12 RQ.TSP.19

Table 13 (2 of 2)

No	Security measure	Fulfilled RQ
SM211	The RSE shall request the OBE to calculate and provide a DSRC Message Authentication Code for Toll Service Provider (MAC_TSP) over at least the EN ISO 14906 attributes PaymentMeans, using a key known only to the Toll Service Provider	RQ.TSP.02
SM212	The OBE shall implement an access control mechanism for EFC commands addressing its data attributes. The RSE shall implement the calculation of the corresponding access codes.	RQ.TSP.06 RQ.TC.22
SM213	The RSE shall read, increment and write a transaction counter to the OBE. The OBE shall support this.	RQ.TSP.02 RQ.TSP.08 RQ.TSP.21

7.3.3 CCC interface

Table 14 — CCC interface security measures

No	Security measure	Fulfilled RQ
SM220	The RSE shall request the OBE to calculate and provide a (MAC_TC) over at least the PaymentMeans attribute, using a key known only to the Toll Charger and the Toll Service Provider. The OBE shall respond accordingly.	RQ.IF.11 RQ.IF.12 RQ.TC.92 RQ.TSP.19 RQ.TSP.62
SM221	The RSE shall request the OBE to calculate and provide a DSRC Message Authentication guaranteeing Non-Repudiation to the Toll Charger (MAC_NR) over at least the PaymentMeans attribute, using a key known only to the Toll Service Provider. The OBE shall respond accordingly.	RQ.TC.93
SM222	The OBE shall implement an access control mechanism for EFC commands addressing its data attributes. The RSE shall implement the calculation of the corresponding access codes.	RQ.TSP.06 RQ.TC.22
SM223	The OBE shall provide an undeniable proof of correct registration of usage data for the given location and moment in time of the CCC transaction.	RQ.TC.01 RQ.TSP.51

7.3.4 LAC interface

Table 15 — LAC interface security measures

No	Security measure	Fulfilled RQ
SM230	The RSE shall provide a MAC_TC over the LAC data send to the OBE calculated with a key known only to the Toll Charger and the IACtime.	RQ.IF.11 RQ.IF.12 RQ.TC.02 RQ.TSP.02
SM231	The OBE shall implement an access control mechanism for EFC commands addressing the LAC data attributes. The RSE shall implement the calculation of the corresponding access codes.	RQ.TSP.06 RQ.TC.22

7.3.5 Front End to TSP Back End interface

Table 16 — Front End to TSP Back end interface security measures

No	Security measure	Fulfilled RQ
SM240	The authenticator in the ChargeReport shall guarantee its authenticity and integrity.	RQ.TC.04 RQ.TSP.04
SM241	The bidirectional Front End to TSP Back End communication shall be implemented using a secure virtual private network connection.	RQ.IF.21

7.3.6 TC to TSP interface

Table 17 — TC to TSP interface security measures

No	Security measure	Fulfilled RQ
SM250	The bidirectional TC to TSP communication shall be implemented using a secure virtual private network connection.	RQ.IF.21
SM251	The Toll Charger shall link the billing details to a set of toll declarations provided by the Toll Service Provider or include the associated event data for those toll declarations which have been acquired by himself.	RQ.TSP.10
SM252	The Toll Charger shall provide the tariff table and all EFC Context data to the Service Provider to allow him to calculate the amount given in the Billing Details.	RQ.TSP.12
SM253	Distribution of EFC context data shall be undeniably signed by the Toll Charger, and confirmed by the Toll Service Provider in an agreed time frame with an authenticated response.	RQ.TSP.13 RQ.TC.91 RQ.IF.13 RQ.IF.14
SM254	Distribution of the exception list shall be undeniably signed by the Toll Service Provider, and confirmed by the Toll Charger in an agreed time frame with an authenticated response.	RQ.TSP.14 RQ.TC.94 RQ.IF.13, RQ.IF.14
SM255	The Front End and/or the TSP Back End shall undeniably sign charge reports and/or toll declarations.	RQ.TSP.55
SM256	The originator of a Trust Object shall undeniably sign it.	RQ.IF.12 RQ.IF.13
SM257	The Toll Service Provider shall provide data underlying a specific toll declaration acquired through his system, on demand of the Toll Charger (ChargeReport and/or more detailed road usage data).	RQ.TSP.51 RQ.TSP.52

7.4 End-to-end security measures

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

Table 18 — End-to-end security measures

No	Security measure	Fulfilled RQ
SM310	The Front End shall be designed as a clearly distinguished entity with a defined interface to the TSP Back-office. The Front End's functionality shall be tested to guarantee its functionality and it shall be auditable according to a procedure agreed between Toll Charger and Toll Service Provider.	RQ.TC.01 RQ.TC.02 RQ.TSP.51 RQ.TSP.52
SM311	The correct and trustworthy Front End functionality shall be periodically audited by the Toll Service Provider and optionally by the Toll Charger or an independent entity on his behalf. NOTE An audit process can compare charge data of sample vehicles equipped with the OBE with known independent trip data.	RQ.TC.01 RQ.TC.02 RQ.TSP.51 RQ.TSP.52
SM312	The Toll Charger and/or Toll Service Provider shall perform plausibility and completeness checks on toll declarations acquired by the Toll Service Provider. Those checks comprise the verification of the physical feasibility of trips on the Toll Domain compared with the actual toll declarations.	RQ.TC.02 RQ.TSP.02 RQ.TSP.52
SM313	The Toll Charger shall compare the toll declarations with his own observations, in accordance with privacy regulations.	RQ.TC.01
SM314	The Toll Charger shall verify if toll declaration(s) acquired by the Toll Service Provider correctly correspond(s) to ChargeReport(s) and/or usage data.	RQ.TC.02 RQ.TSP.52
SM316	The Toll Charger shall determine if the ChargeReport has been produced by a trusted Front End by a message authentication code (MAC) or signature.	RQ.TC.01 RQ.TC.02 RQ.TC.04 RQ.TC.05
SM317	The Toll Charger shall verify the integrity of the ChargeReport based on the Front End MAC or signature.	RQ.TC.01 RQ.TC.02 RQ.TC.04 RQ.TC.05
SM318	The registration of usage data by the Toll Service Provider shall be based on a minimum set of functions in the Front End trusted by both the Toll Service Provider and the Toll Charger. These functions shall directly or indirectly ensure the integrity of the toll declarations including non-repudiation with proof of origin.	RQ.TC.01 RQ.TC.02 RQ.TSP.51 RQ.TSP.52
SM319	The Toll Service Provider shall provide an undeniable proof of correct registration of usage data for a defined location and moment in time, or for a defined range of time, on demand to the Toll Charger.	RQ.TSP.51
SM320	The Toll Charger shall compare the proof of correct registration of usage data with his own observations, in accordance with privacy regulations.	RQ.TC.01
SM321	In case the Toll Service Provider supports the Toll Charger in handling CCC events, the Toll Charger shall forward him a complete compliance check record.	RQ.TSP.15 RQ.TC.93