PD CEN ISO/TS 19299:2015

BSI Standards Publication

Electronic fee collection — Security framework

urrently in preview, click buy full vers

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of CEN ISO/TS 19299:2015. It supersedes PD CEN/TS 16439:2013 which is withdrawn.

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

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

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

© The British Standards Institution 2015.
Published by BSI Standards Limited 2015

ISBN 978 0 580 87862 6
ICS 03.220.20; 35.240.60

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

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 October 2015.

Amendments/corrigenda issued since publication

Date	Text affected

urrently in preview, click buy full versi

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN ISO/TS 19299

October 2015

ICS 35.240.60; 03.220.20

Supersedes CEN/TS 16439:2013

English Version

Electronic fee collection - Security framework (ISO/TS 19299:2015)

Perception de télépéage - Cadre de sécurité (ISO/TS 19299:2015)

Elektronische Gebührenerhebung - Sicherheitsgrundstruktur (ISO/TS 19299:2015)

This Technical Specification (CEN/TS) was approved by CEN on 26 June 2015 for provisional application.

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

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

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

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

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

© 2015 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. CEN ISO/TS 19299:2015 E

Currently in preview, click buy full version

Contents

Page

European foreword **3**

urrently in preview, click buy full versi

European foreword

This document (CEN ISO/TS 19299:2015) has been prepared by Technical Committee ISO/TC 204 "Intelligent transport systems" in collaboration with Technical Committee CEN/TC 278 "Intelligent transport systems" the secretariat of which is held by NEN.

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

This document supersedes CEN/TS 16439:2013.

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

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

Endorsement notice

The text of ISO/TS 19299:2015 has been approved by CEN as CEN ISO/TS 19299:2015 without any modification.

urrently in preview, click buy full versi

Contents

Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **2**
3 Terms and definitions **4**
4 Symbols and abbreviated terms **9**
5 Trust model **10**
5.1 Overview 10
5.2 Stakeholders trust relations 10
5.3 Technical trust model 11
5.3.1 General 11
5.3.2 Trust model for TC and TSP relations 11
5.3.3 Trust model for TSP and service user relations 13
5.3.4 Trust model for Interoperability Management relations 13
5.4 Implementation 13
5.4.1 Setup of trust relations 13
5.4.2 Trust relation renewal and revocation 14
5.4.3 Issuing and revocation of sub CA and end-entity certificates 14
5.4.4 Certificate and certificate revocation list profile and format 15
5.4.5 Certificate extensions 15
6 Security requirements **17**
6.1 General 17
6.2 Information security management system 18
6.3 Communication interfaces 18
6.4 Data storage 19
6.5 Toll charger 19
6.6 Toll service provider 21
6.7 Interoperability Management 23
6.8 Limitation of requirements 23
7 Security measures — countermeasures **24**
7.1 Overview 24
7.2 General security measures 24
7.3 Communication interfaces security measures 25
7.3.1 General 25
7.3.2 DSRC-EFC interface 26
7.3.3 CEC interface 27
7.3.4 LAC interface 28
7.3.5 Front End to TSP back end interface 28
7.3.6 TC to TSP interface 29
7.3.7 ICC interface 30
7.4 End-to-end security measures 30
7.5 Toll service provider security measures 32
7.5.1 Front end security measures 32
7.5.2 Back end security measures 33
7.6 Toll charger security measures 34
7.6.1 RSE security measures 34
7.6.2 Back end security measures 34
7.6.3 Other TC security measures 35
8 Security specifications for interoperable interface implementation **35**
8.1 General 35
8.1.1 Subject 35

Currently in preview, click buy full version

8.1.2 Signature and hash algorithms ... 35
8.2 Security specifications for DSRC-EFC ... 36
8.2.1 Subject ... 36
8.2.2 OBE ... 36
8.2.3 RSE ... 36

9 Key management ... 36
9.1 Overview ... 36
9.2 Asymmetric keys ... 36
9.2.1 Key exchange between stakeholders ... 36
9.2.2 Key generation and certification ... 37
9.2.3 Protection of keys ... 37
9.2.4 Application ... 37
9.3 Symmetric keys ... 38
9.3.1 General ... 38
9.3.2 Key exchange between stakeholders ... 38
9.3.3 Key lifecycle ... 39
9.3.4 Key storage and protection ... 40
9.3.5 Session keys ... 41

Annex A (normative) **Security profiles ... 42**
Annex B (normative) **Implementation conformance statement (ICS) proforma ... 46**
Annex C (informative) **Stakeholder objectives and generic requirements ... 64**
Annex D (informative) **Threat analysis ... 68**
Annex E (informative) **Security policies ... 124**
Annex F (informative) **Example for an EETS security policy ... 131**
Annex G (informative) **Recommendations for privacy-focused implementation ... 133**
Annex H (informative) **Proposal for end-entity certificates ... 135**
Bibliography ... 136

urrently in preview, click buy full versi

 © ISO 2015 – All rights reserved

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.

Currently in preview, click buy full version

© ISO 2015 – All rights reserved

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.

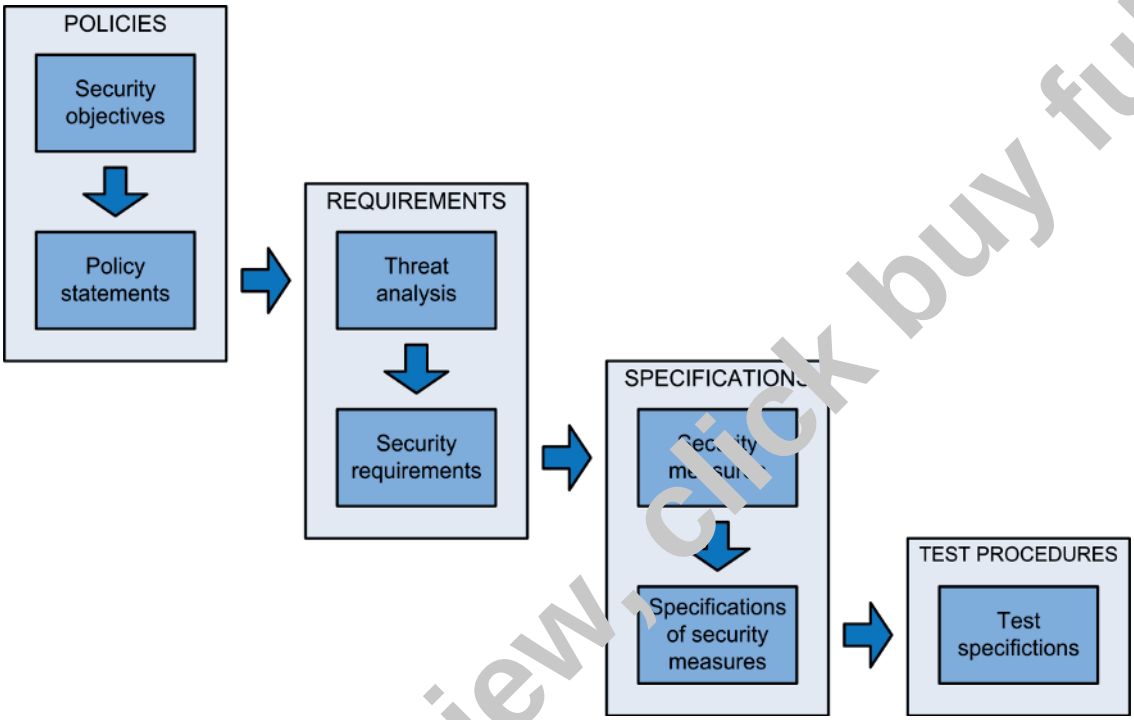

Figure 1 — Development path for the security documents

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.

currently in preview, click buy full version

 © ISO 2015 – All rights reserved

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

Currently in preview, click buy full version

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).

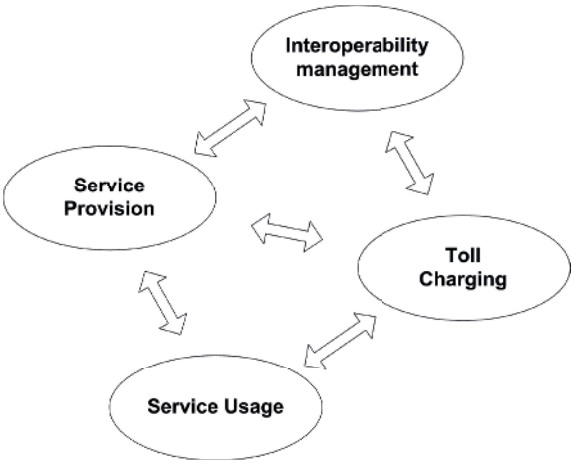

Figure 2 — The role model underlying this Technical Specification

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

 © ISO 2015 – All rights reserved

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.

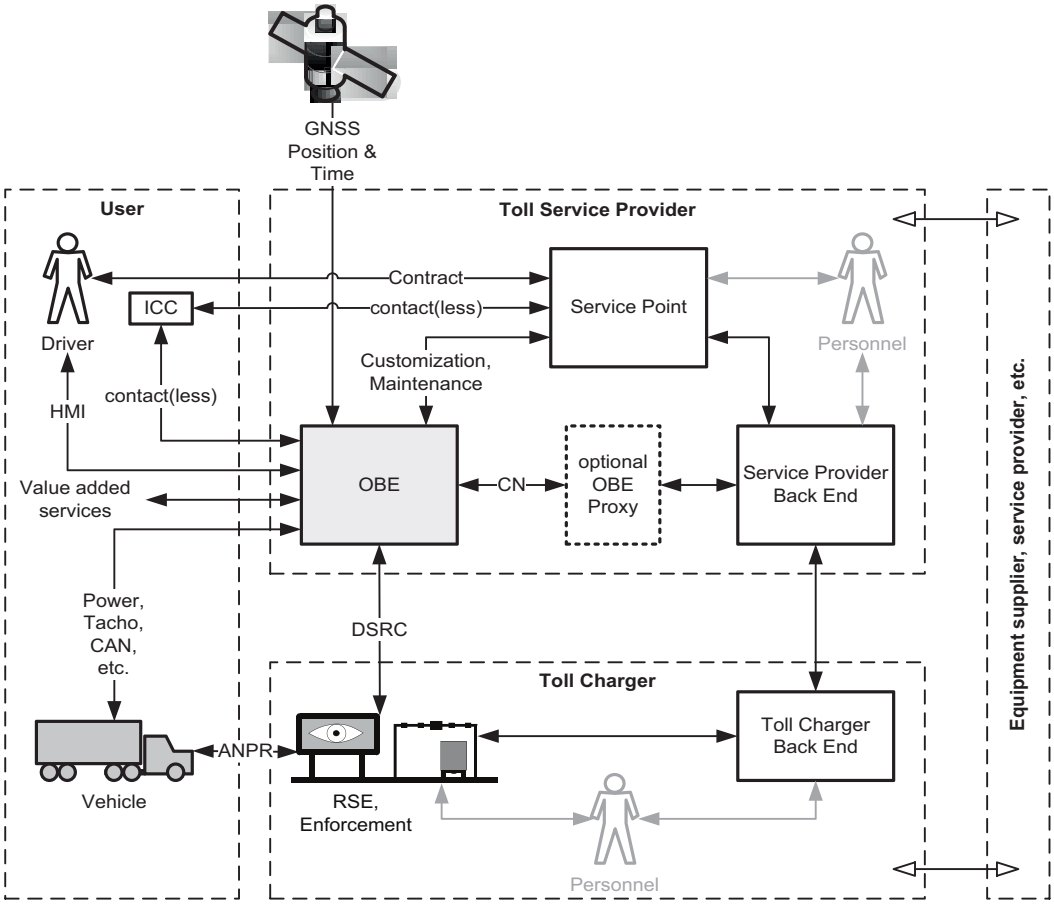

Figure 3 — EFC system model of the EFC Security framework

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.

© ISO 2015 – All rights reserved

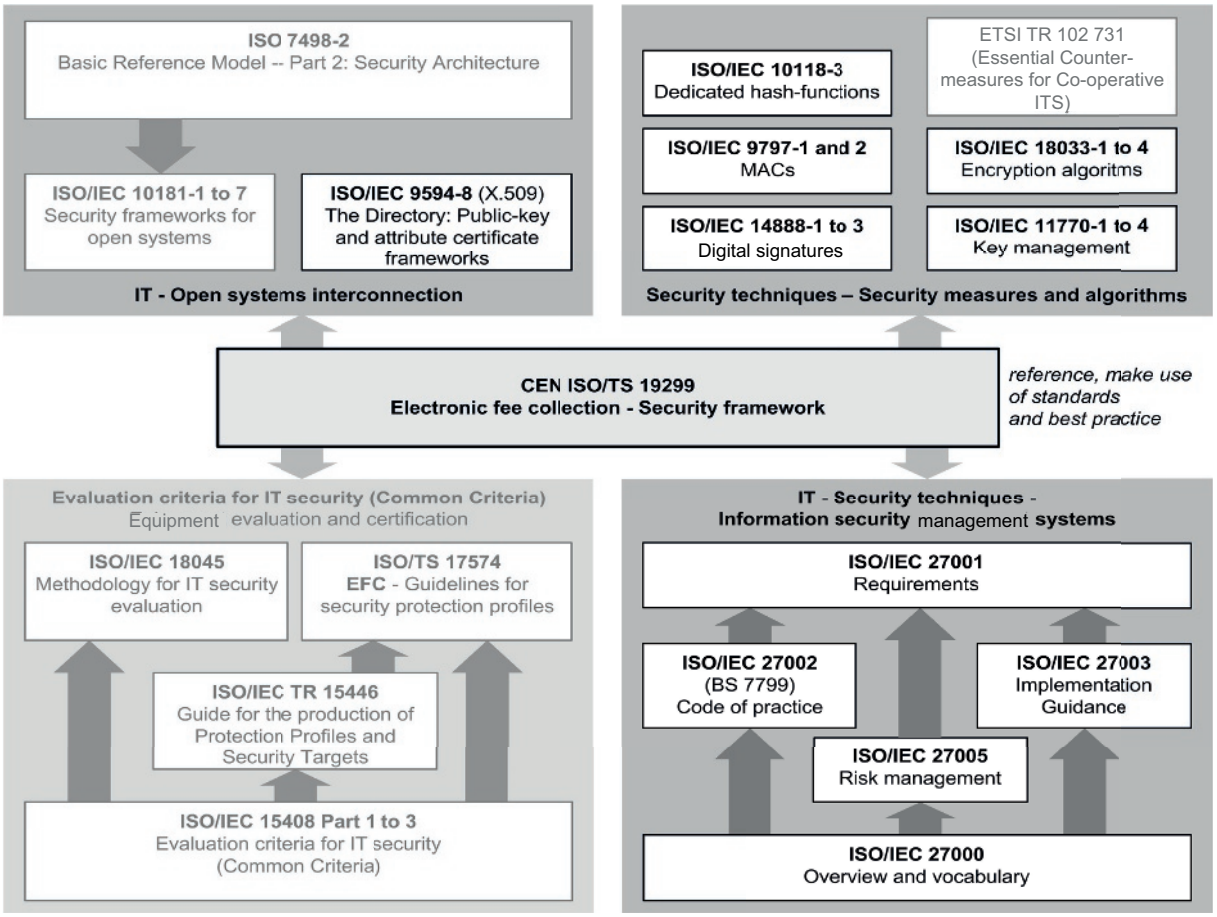

Figure 4 — Relevant security standards in the context of the EFC — Security framework

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.

 © ISO 2015 – All rights reserved

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

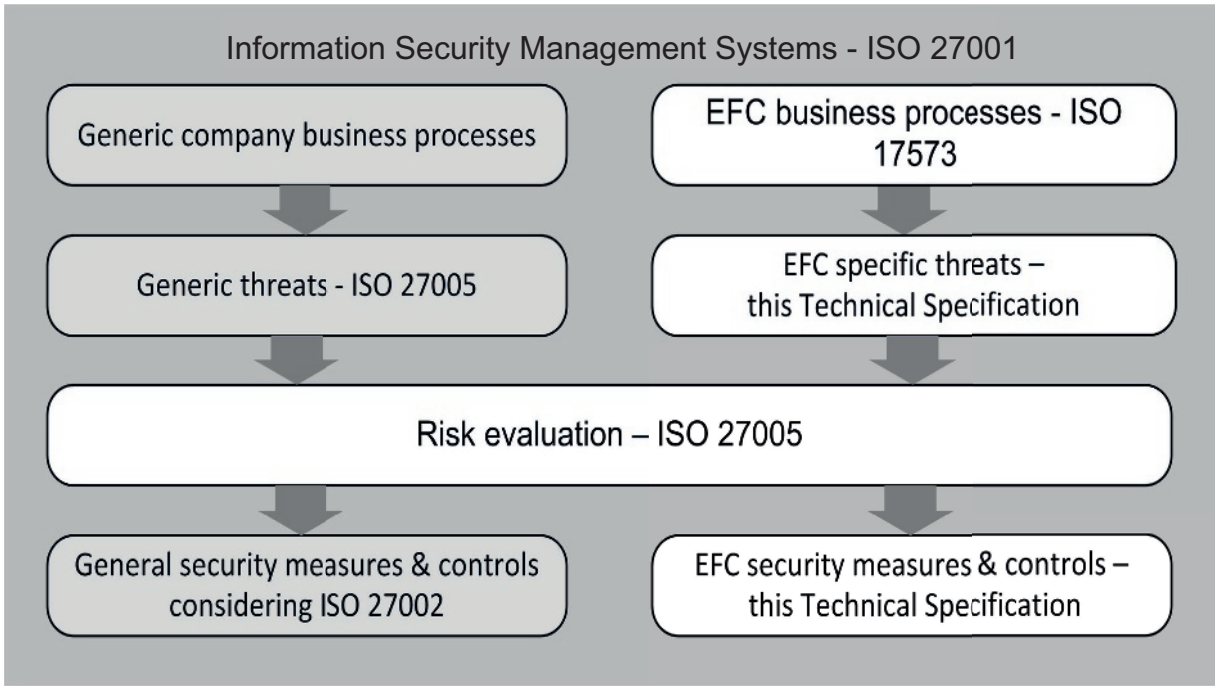

Figure 5 — Scope in relation to the Information Security Management System

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)].

© ISO 2015 – All rights reserved

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).

© ISO 2015 – All rights reserved