This is a free page sample. Access the full version online.

Standard Recommendation
S.R. CEN/TS 16439:2013

Electronic fee collection - Security framework

© CEN 2013 No copying without NSAI permission except as permitted by copyright law.

This is a free page sample. Access the full version online.

S.R. CEN/TS 16439:2013

Incorporating amendments/corrigenda/National Annexes issued since publication:

The National Standards Authority of Ireland (NSAI) produces the following categories of formal documents:

I.S. xxx: Irish Standard – national specification based on the consensus of an expert panel and subject to public consultation.

S.R. xxx: Standard Recommendation - recommendation based on the consensus of an expert panel and subject to public consultation.

SWiFT xxx: A rapidly developed recommendatory document based on the consensus of the participants of an NSAI workshop.

This document replaces:

This document is based on:
CEN/TS 16439:2013

Published:
21 February, 2013

This document was published
under the authority of the NSAI
and comes into effect on:
21 February, 2013

ICS number:
35.240.60

NSAI
1 Swift Square,
Northwood, Santry
Dublin 9

T +353 1 807 3800
F +353 1 807 3838
E standards@nsai.ie

W NSAI.ie

Sales:
T +353 1 857 6730
F +353 1 857 6729
W standards.ie

Údarás um Chaighdeáin Náisiúnta na hÉireann

This is a free page sample. Access the full version online.

S.R. CEN/TS 16439:2013

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

© 2013 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. CEN/TS 16439:2013: E

This is a free page sample. Access the full version online.

Contents

Page

This is a free page sample. Access the full version online.

This is a free page sample. Access the full version online.

This is a free page sample. Access the full version online.

This is a free page sample. Access the full version online.

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.

This is a free page sample. Access the full version online.

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.

This is a free page sample. Access the full version online.

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.

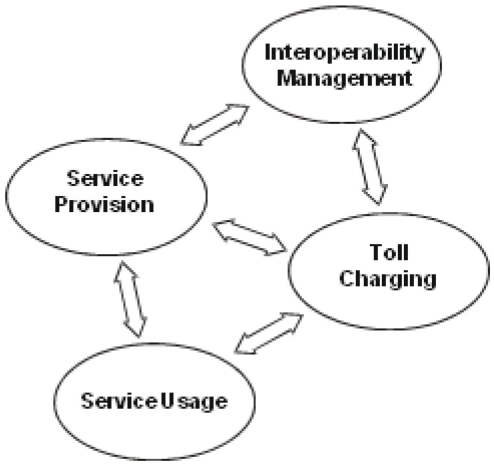

Figure 1 — The role model underlying this standard

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

This is a free page sample. Access the full version online.

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).

This is a free page sample. Access the full version online.

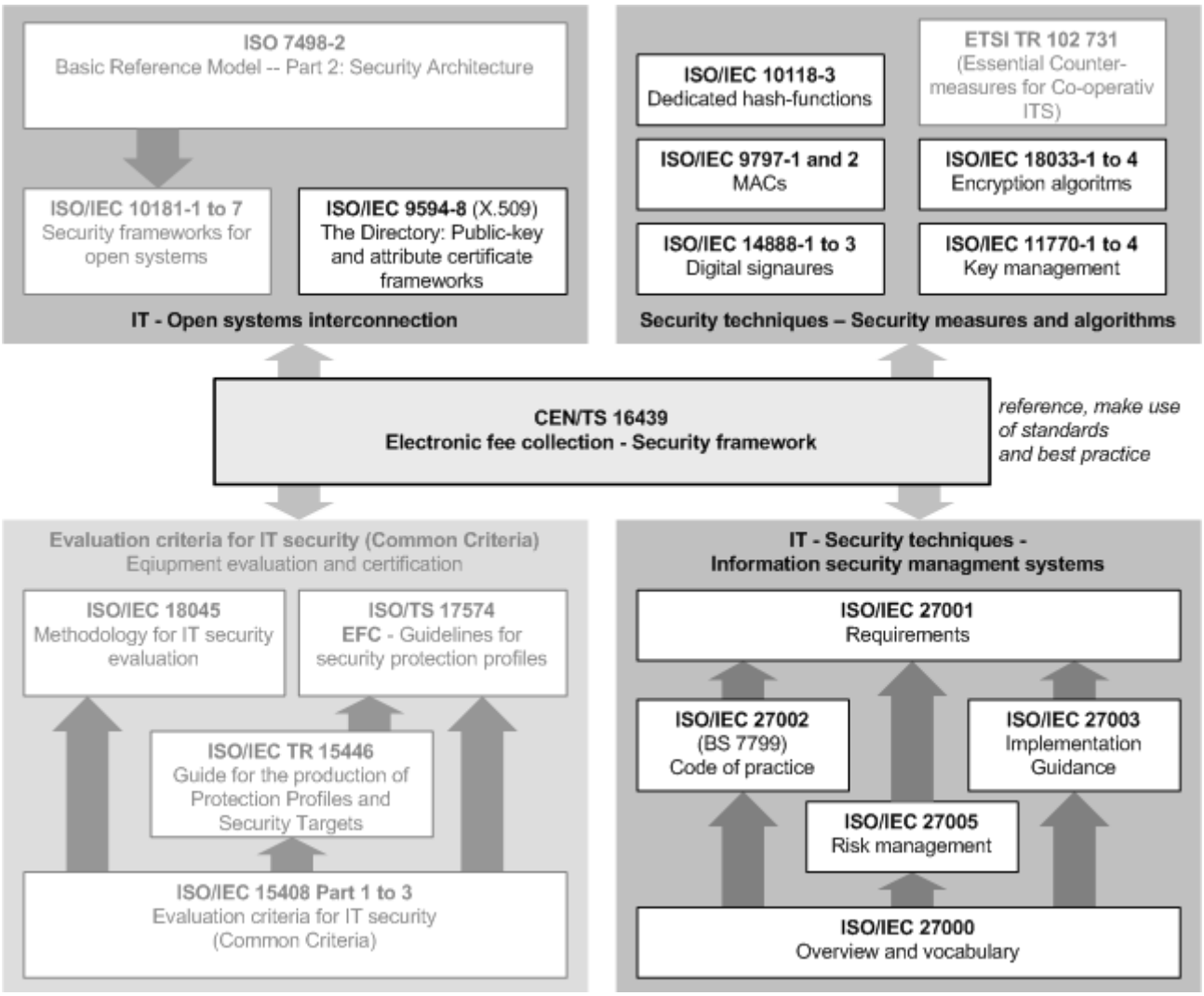

Figure 2 — Relevant security standards in the context of the EFC — Security framework

This is a free page sample. Access the full version online.

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.

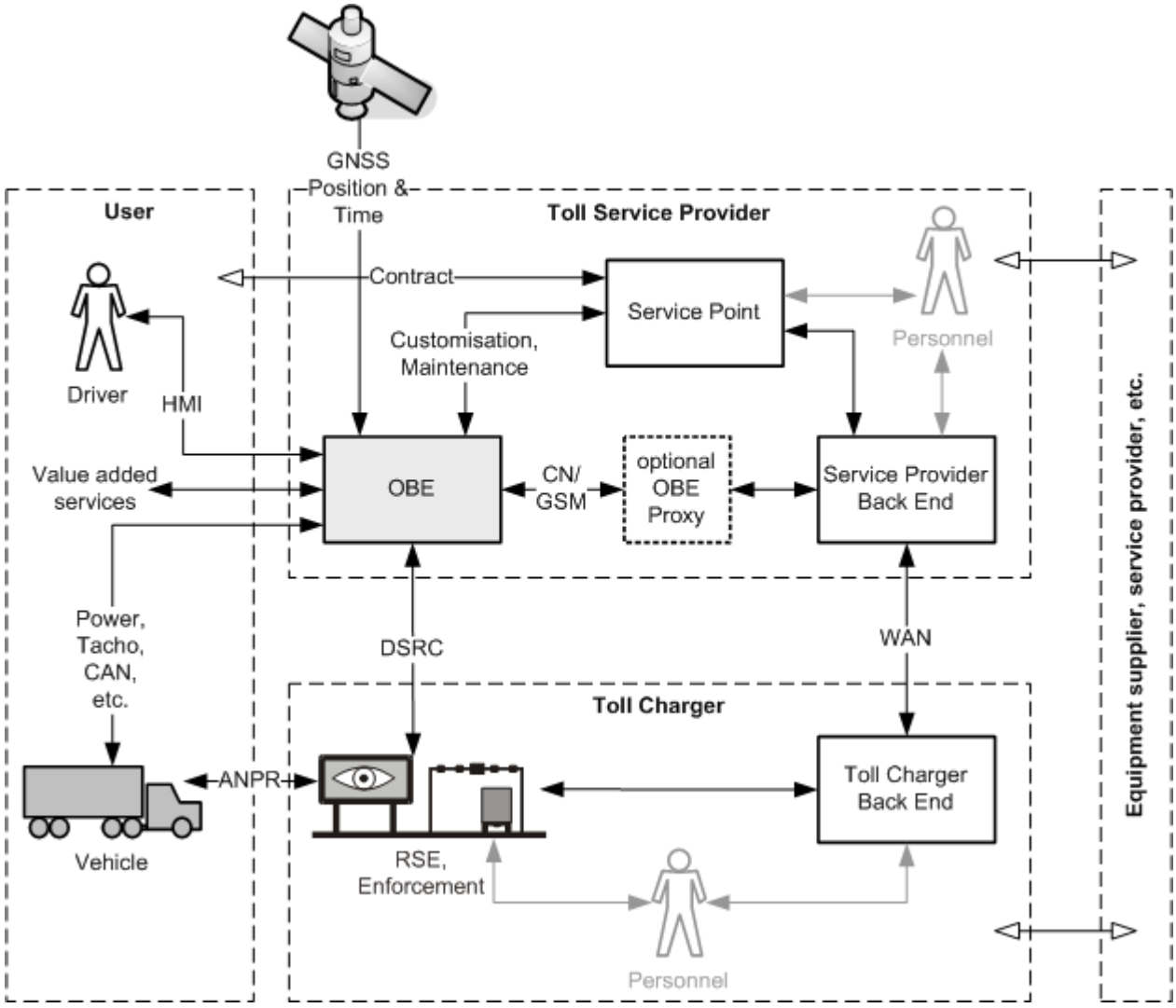

Figure 3 — EFC system model of the EFC Security Framework

This is a free page sample. Access the full version online.

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)

This is a free page sample. Access the full version online.

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.

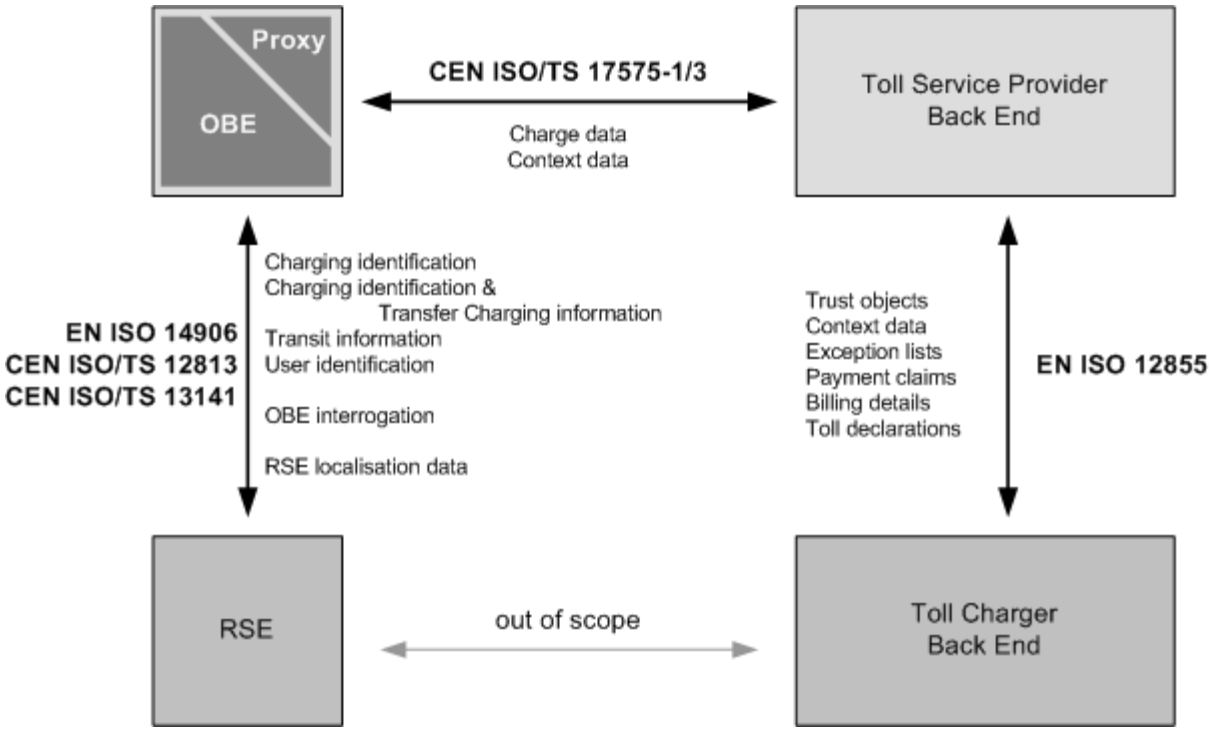

Figure 4 — Scope of EFC security framework for secure communication

— 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

This is a free page sample. Access the full version online.

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.

This is a free page sample. Access the full version online.

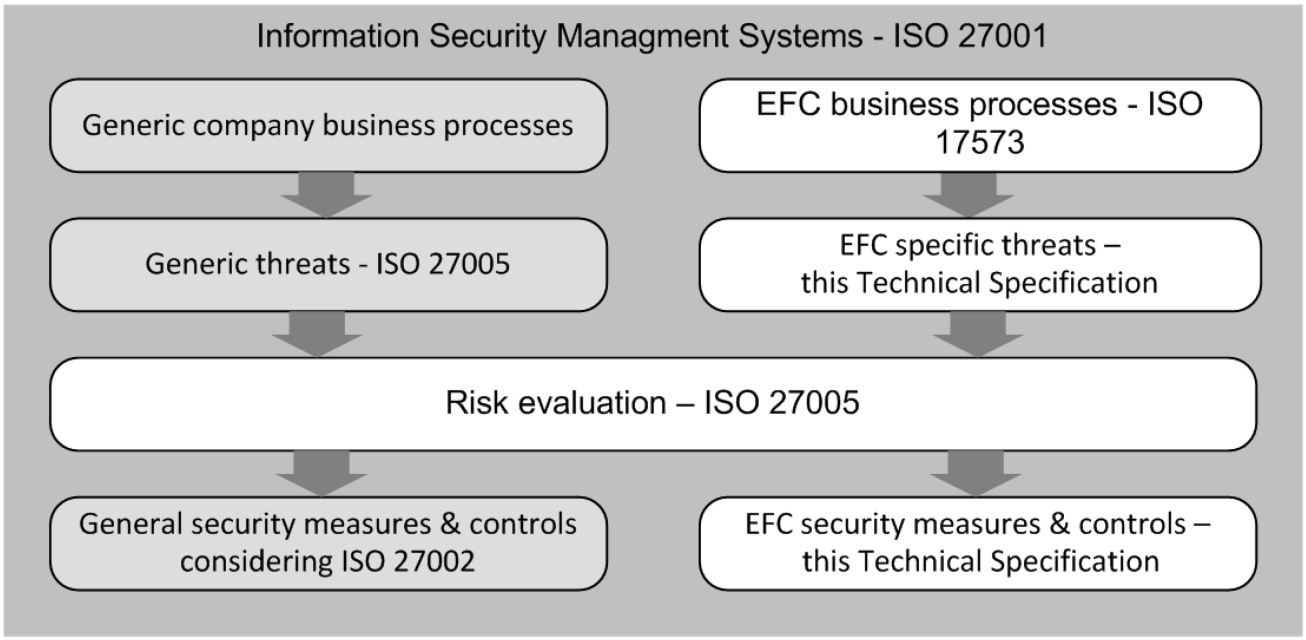

Figure 5 — Scope in relation to the Information Security Management System

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*

SAI GLOBAL

This is a free preview. Purchase the entire publication at the link below:

Product Page

Looking for additional Standards? Visit Intertek Inform Infostore

Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation