SLOVENSKI STANDARD
oSIST prEN ISO 19299:2019

01-december-2019

Elektronsko pobiranje pristojbin - Varnostni okvir (ISO/DIS 19299:2019)

Electronic fee collection - Security framework (ISO/DIS 19299:2019)

Elektronische Gebührenerhebung - Sicherheitsgrundstruktur (ISO/DIS 19299:2019)

Perception de télépéage -- Cadre de sécurité (ISO/DIS 19299:2019)

Ta slovenski standard je istoveten z: **prEN ISO 19299**

ICS:

35.240.60	Uporabniške rešitve IT v prometu	IT applications in transport

oSIST prEN ISO 19299:2019 **en,fr,de**

DRAFT INTERNATIONAL STANDARD

ISO/DIS 19299

ISO/TC **204**

Secretariat: **ANSI**

Voting begins on:
2019-09-18

Voting terminates on:
2019-12-11

Electronic fee collection — Security framework

Perception de télépéage — Cadre de sécurité

ICS: 35.240.60; 03.220.20

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

Reference number
ISO/DIS 19299:2019(E)

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

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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 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 of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems*.

This edition cancels and replaces the first edition of ISO/TS 19299:2015, which has been technically revised.

The main changes compared to the previous edition are as follows:

— added requirements and security measures for the use of common payment media according to ISO/TS 21193;

— updated data protection considerations in Annex G, in order to take the European Union's new General Data Protection Regulation (i.e. Directive 2016/679/EC) into account.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Context of this document

The development process for a security concept and implementation to protect any existing electronic fee collection (EFC) system normally includes several steps as follows (see Figure 1):

— 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.

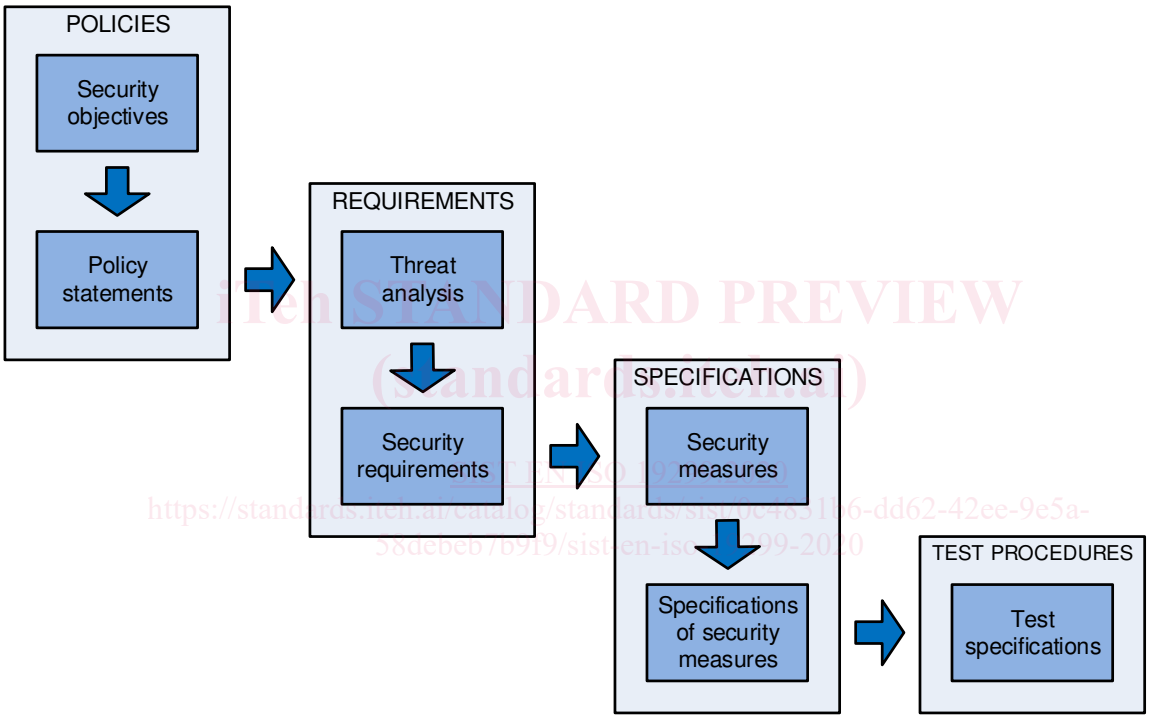

Figure 1 — Development path for the security documents

Each actor in an existing EFC system has to implement the defined security measures and supervise the effectiveness. Security measures which do not work properly need to be improved. The development of the EFC security framework follows this approach as closely as possible, with the following limitations:

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

— No risk assessment possible: Risk assessment compares the possible loss for the stakeholder and the required resources (e.g. equipment, knowledge, time, etc.) to perform an attack. In a real system, risk assessment is based on the evaluation of the costs and benefits of each countermeasure.

— No specific system design or configuration was deemed as universally applicable. Only the available EFC base standards were taken as references. Specific technical details of a particular system (e.g. servers, computer centres, and de-centralised elements like roadside equipment) need to be additionally taken into consideration when implementing security measures.

Selection of requirements and 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 no overall valid security policy, nor is there 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.

Having stated that, in order to be compliant to this document, if a requirement is selected, the associated security measure(s) have to be implemented.

To understand the content of this document, the reader should be aware of the methodological assumptions used to develop it. 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 document 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 a 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 17573-1), 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 several threat scenarios from the perspective of various attackers. The second approach looks in depth on threats against the various identified assets (tangible and intangible). This approach, although producing some redundancy, ensures completeness and coverage of a broad 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 each threat is covered by at least one requirement.

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

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

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

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

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

— define a security policy for the EFC scheme (may involve more than one stakeholder in an interoperable EFC scheme). Some examples for a security policy and its elements are provided (in Annex E and Annex F) as an aid 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 document. Evidence can be provided by a self-declaration, an internal or external audit, or other certifications.

EFC role model

This document complies with the role model defined in ISO 17573-1. 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).

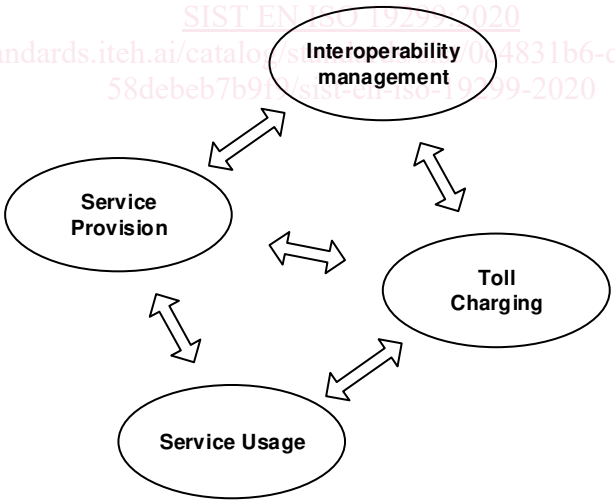

Figure 2 — The role model underlying this document

Toll service providers (TSP) issue on-board equipment (OBE) to the users of the tolled infrastructure or transport service. The OBE 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. 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 OBEs. 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 document is based on the role model summarized 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 TC or TSP compliant to this document 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 document. This document assumes an OBE that is dedicated to EFC purposes only and does not consider value added services based on EFC OBE, nor more generic OBE platforms (also called in-vehicle ITS Stations) which could be used to host the EFC application. The OBE may either be connected to a central account or use a payment medium such as integrated circuit cards (ICC) or mobile payment for on-board-account EFC system. Any financial transactions are out of scope of this document.

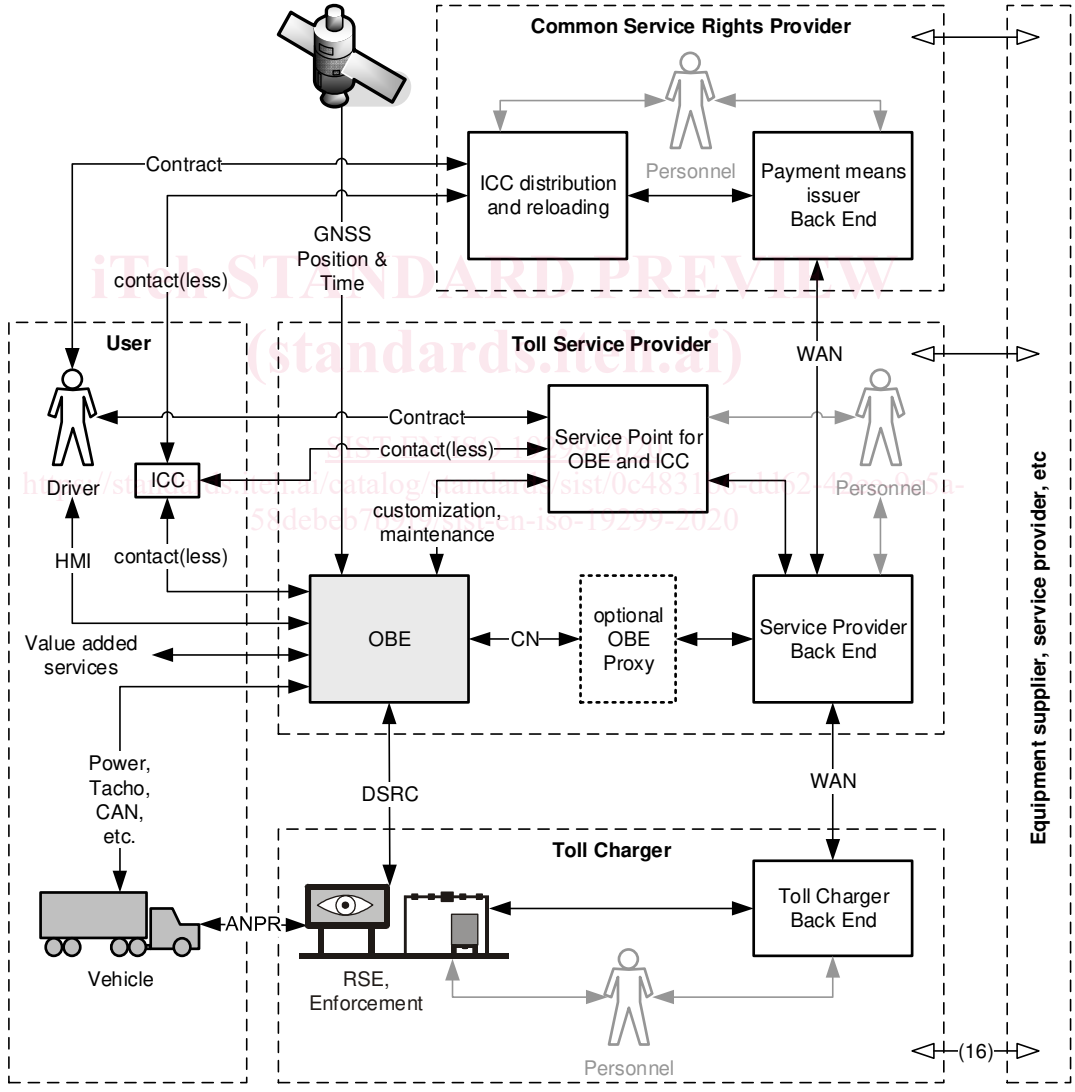

Figure 3 — EFC system model of the EFC Security framework

Relation to other security standards

Several generic and specific standards and technical reports concerning security issues for information technology already exist. This document uses these existing standards and expands their usability for

EFC applications. This framework references and adapts security techniques and methodologies from these standards.

Figure 4 shows the context of the EFC security framework to the most relevant security standards that gave input to this document. Standards that are directly used and referenced are highlighted in black.

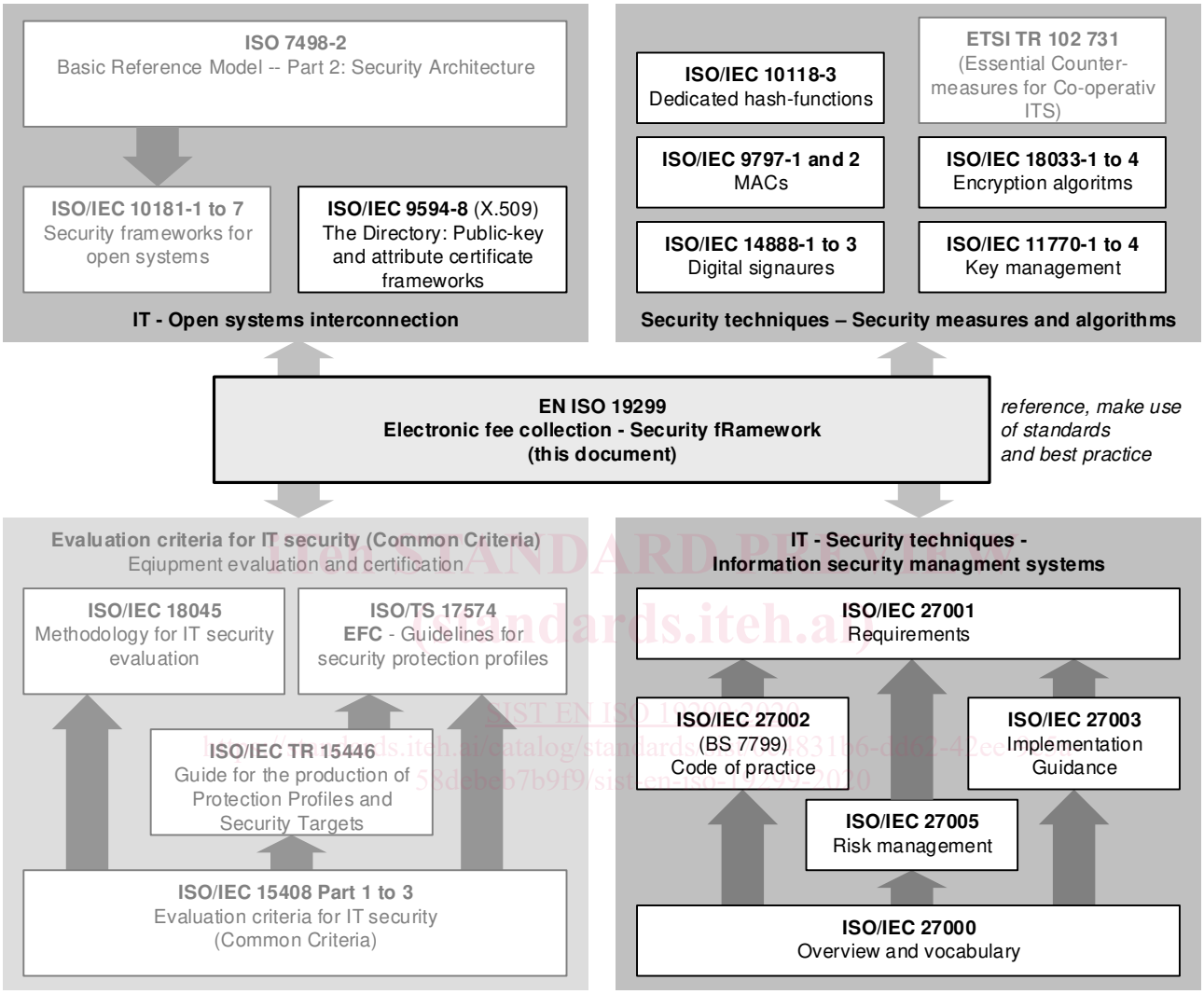

Figure 4 — Relevant security standards in the context of the EFC — Security framework

Standards shown in Figure 4 are grouped in the following categories, where arrows inside each group indicate which standard provides input to other standards:

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

— **IT — Open system interconnection**: This group provides mechanisms for the secure communications between open systems. These 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 group defines methodologies and processes for the security evaluation and certification for most categories of products used in the EFC environment.

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

An ISO/IEC 27001 certification of a TC or TSP organization may be used to demonstrate compliance to this document, provided that the scope and the Statements of Applicability (SoA) include the EFC business processes specified in ISO 17573-1 and that security requirements and their associated security measures provided by this document 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 two parallel paths. The first step of both paths is analysing the business processes, which is then followed by a threat analysis. A common risk analysis combines the generic and the EFC related analysis and results in the respective security measures and controls.

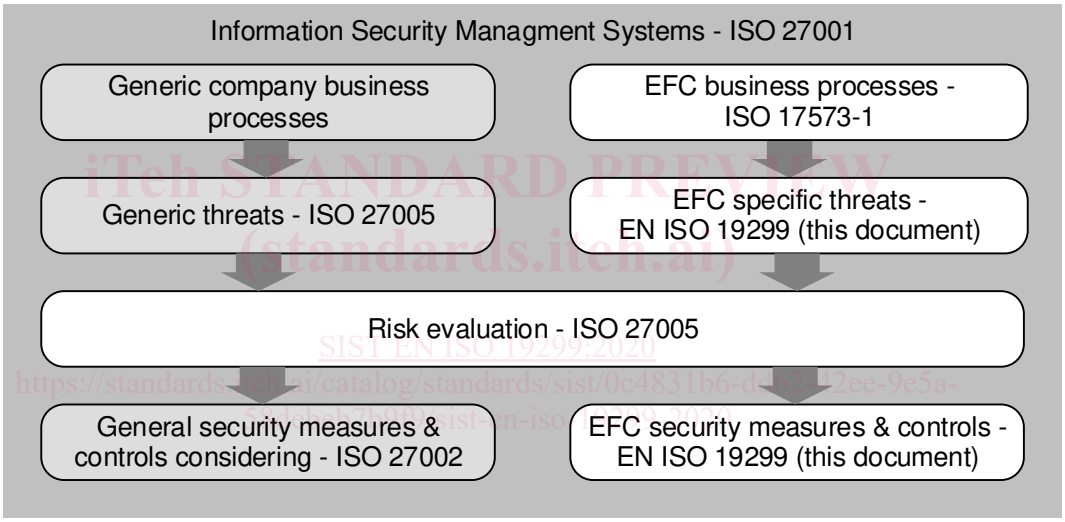

Figure 5 — Scope in relation to the Information Security Management System

In addition, the EFC security framework makes use of existing threat analysis methods and uses existing threat analysis with relation to EFC or ITS, such as ETSI/TR 102 893.