INTERNATIONAL STANDARD

ISO 19299

First edition
2020-08

Electronic fee collection — Security framework

Perception de télépéage — Cadre de sécurité

Reference number
ISO 19299:2020(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
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*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/TC 278 *Intelligent transport systems*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This first edition cancels and replaces 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 into account the European Union's new General Data Protection Regulation (i.e. Directive 2016/679/EC).

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.

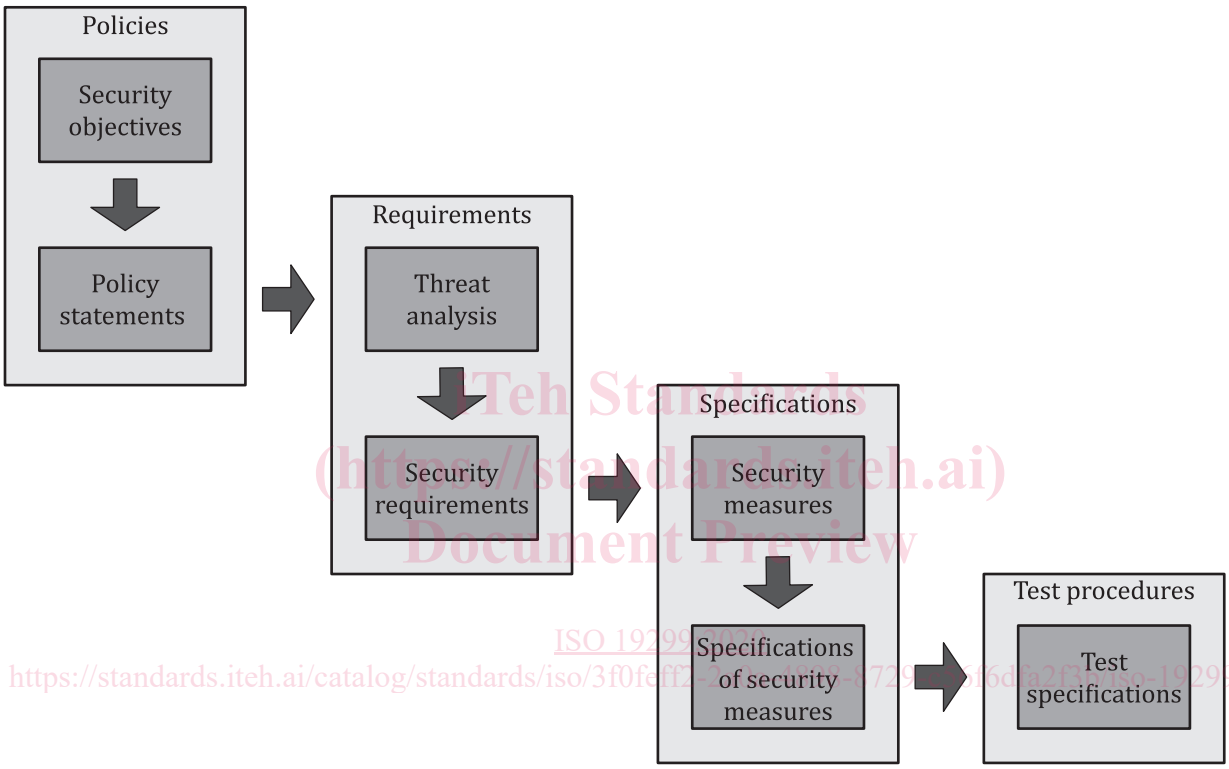

Figure 1 — Development path for the security documents

Each actor in an existing EFC system implements the defined security measures and supervises their effectiveness. When a security measure is found not working properly, an improvement process is started. The development of the EFC security framework follows this approach, with the following limitations:

— No standard security policy exists, nor can it be defined: 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 standard risk assessment is possible: Risk assessment compares possible losses to stakeholders with the required resources (e.g. equipment, knowledge, time) 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 an extensive (but non-exhaustive) toolbox of requirements and security measures.

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. An application independent security framework for such system parts and interfaces, an information security management system (ISMS), can be found, for example, in the ISO/IEC 27000 series.

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, such as 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 (e.g. keys, certificates, certificate revocation lists) to support security services like confidentiality, integrity, authenticity, and non-repudiation. This section of the document covers the (initial) setup of key exchange between stakeholders and several operational procedures, such as key renewal, certificate revocation.

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 should 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).