TECHNICAL SPECIFICATION

ISO/TS 17574

Third edition
2017-03

Electronic fee collection — Guidelines for security protection profiles

Perception de télépéage — Lignes directrices concernant les profils de protection de la sécurité

Reference number
ISO/TS 17574:2017(E)

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

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 on 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 the following URL: www.iso.org/iso/foreword.html.

The committee responsible for this document is ISO/TC 204, *Intelligent transport systems*.

This third edition cancels and replaces the second edition (ISO/TS 17574:2009), which has been technically revised. This edition includes the following significant changes with respect to the previous edition:

— Clause 1 has been redrafted and shortened;

— Clause 3 has been updated with harmonized terms;

— requirements updated as to reflect the latest version of the ISO/IEC 15408 series;

— a new Clause 5 has been added, comprising much of the text from the Scope of the previous edition.

Introduction

Electronic fee collection (EFC) systems are subject to several ways of fraud both by users and operators but also from people outside the system. These security threats have to be met by different types of security measures including security requirements specifications.

It is recommended that EFC operators or national organizations, e.g. highway authorities or transport ministries, use the guideline provided by this document to prepare their own EFC/protection profile (PP), as security requirements should be described from the standpoint of the operators and/or operators' organizations.

It should be noted that this document is of a more informative than normative nature and it is intended to be read in conjunction with the underlying international standards ISO/IEC 15408 (all parts). Most of the content of this document is an example shown in Annex A on how to prepare the security requirements for EFC equipment, in this case, a DSRC-based OBE with an IC card loaded with crucial data needed for the EFC. The example refers to a Japanese national EFC system and should only be regarded as an example.

After an EFC/PP is prepared, it can be internationally registered by the organization that prepared the EFC/PP so that other operators or countries that want to develop their EFC system security services can refer to an already registered EFC/PP.

This EFC-related document on security service framework and EFC/PP is based on ISO/IEC 15408 (all parts). ISO/IEC 15408 (all parts) includes a set of requirements for the security functions and assurance of IT-relevant products and systems. Operators, organizations or authorities defining their own EFC/PP can use these requirements. This will be similar to the different PPs registered by several financial institutions, e.g. for payment instruments like IC cards.

The products and systems that were developed in accordance with ISO/IEC 15408 (all parts) can be publicly assured by the authentication of the government or designated private evaluation agencies.

Electronic fee collection — Guidelines for security protection profiles

1 Scope

This document provides guidelines for preparation and evaluation of security requirements specifications, referred to as Protection Profiles (PP) in ISO/IEC 15408 (all parts) and in ISO/IEC TR 15446.

By Protection Profile (PP), it means a set of security requirements for a category of products or systems that meet specific needs. A typical example would be a PP for On-Board Equipment (OBE) to be used in an EFC system. However, the guidelines in this document are superseded if a Protection Profile already exists for the subsystem in consideration.

The target of evaluation (TOE) for EFC is limited to EFC specific roles and interfaces as shown in Figure 1. Since the existing financial security standards and criteria are applicable to other external roles and interfaces, they are assumed to be outside the scope of TOE for EFC.

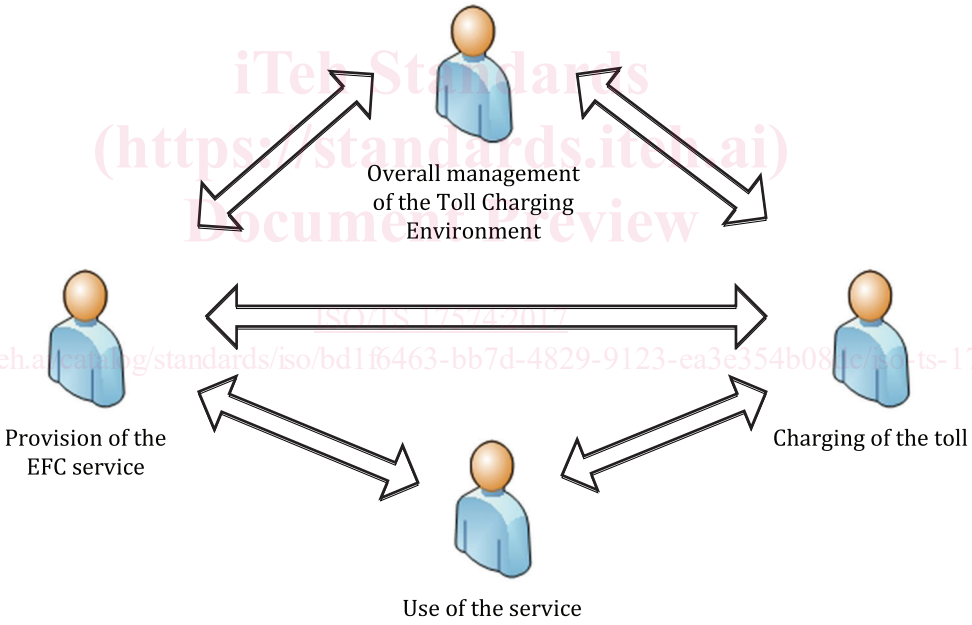

Figure 1 — Scope of TOE for EFC

The security evaluation is performed by assessing the security-related properties of roles, entities and interfaces defined in security targets (STs), as opposed to assessing complete processes which often are distributed over more entities and interfaces than those covered by the TOE of this document.

NOTE Assessing security issues for complete processes is a complimentary approach, which may well be beneficial to apply when evaluating the security of a system.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

3.1
assurance requirement
security requirements to assure confidence in the implementation of functional requirements

3.2
audit
independent review and examination in order to ensure compliance with established policy and operational procedures and to recommend associated changes

3.3
availability
property of being accessible and usable upon demand by an authorized entity

[SOURCE: ISO/TS 19299:2015, 3.6]

3.4
certification
procedure by which a party gives written assurance that a product, process, or service conforms to specified requirements

[SOURCE: ISO/TS 14907-1:2015, 3.3]

3.5
confidentiality
prevention of information leakage to non-authenticated individuals, parties, and/or processes

[SOURCE: ISO/TS 19299:2015, 3.11]

3.6
data privacy
rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure and disposal of personal information

[SOURCE: ISO/TS 19299:2015, 3.32]

3.7
Evaluation Assurance Level
EAL
set of assurance requirements, usually involving documentation, analysis and testing, representing a point on a predefined assurance scale, that form an assurance package

3.8
functional requirement
requirement for a function that a system or system component is able to perform

3.9
integrity
property that data have not been altered or destroyed in an unauthorized manner

3.10
international registrar
organization authorized to register protection profiles at an international level

3.11
key management
generation, distribution, storage, application and revocation of encryption keys

3.12
On-Board Equipment
OBE
required equipment on-board a vehicle for performing required EFC functions and communication services

Note 1 to entry: The OBE does not need to include payment means.

3.13
personalization card
set-up card
IC card to transcribe individual data such as vehicle information into On-Board Equipment

3.14
rationale verification
process determining that a product of each phase of the system lifecycle development process fulfils all the requirements specified in the previous phase

3.15
reliability
ability of a device or a system to perform its intended function under given conditions of use for a specified period of time or number of cycles

[SOURCE: ISO/TS 14907-1:2015, 3.17]

3.16
road side equipment
RSE
equipment located along the road, either fixed or mobile

3.17
secure application module
SAM
physical module that securely executes cryptographic functions and stores keys

[SOURCE: ISO/TS 19299:2015, 3.35]

3.18
security policy
set of rules that regulate how to handle security threats or define the appropriate security level

[SOURCE: ISO/TS 19299:2015, 3.36]

3.19
security target
ST
set of security requirements and specifications to be used as the basis for evaluation of an identified TOE

3.20
security threat
potential action or manner to violate the security of a system

3.21
target of evaluation
TOE
set of software, firmware and/or hardware possibly accompanied by guidance

[SOURCE: ISO/IEC 15408-1:2009, 3.1.70]

3.22
threat agent
entity that has the intention to act adversely on an asset

[SOURCE: ISO/TS 19299:2015, 3.40]

3.23
toll charger
entity which levies toll for the use of vehicles in a toll domain

Note 1 to entry: In other documents, the terms operator or toll operator can be used.

[SOURCE: ISO 17573:2010, 3.16, modified]

3.24
toll service provider
TSP
entity providing toll services in one or more toll domains

Note 1 to entry: In other documents, the terms issuer or contract issuer might be used.

Note 2 to entry: The toll service provider can provide the OBE or might provide only a magnetic card or a smart card to be used with an OBE provided by a third party (like a mobile telephone and a SIM card can be obtained from different parties).

Note 3 to entry: The toll service provider is responsible for the operation (functioning) of the OBE.

[SOURCE: ISO 17573:2010, 3.23, modified]

4 Abbreviated terms

CC Common Criteria

CCRA Common Criteria Recognition Arrangement

CN cellular networks

DSRC dedicated short-range communication

EAL Evaluation Assurance Level

EFC electronic fee collection

GNSS global navigation satellite systems

HMI human machine interface

I/F interface

ICC integrated circuit(s) card

IT information technology

OBE On-Board Equipment

PP Protection Profile

RSE road side equipment

SAM secure application module

SFP security function policy

SOF strength of function

ST security target

TOE target of evaluation

TSF TOE security functions

5 EFC security architecture and protection profile processes

5.1 General

This clause gives an overview of the context and use of this document in terms of the EFC security architecture and protection profile processes.

This document is intended to be read in conjunction with the underlying standards ISO/IEC 15408 (all parts) and ISO/IEC TR 15446. Although a layman could read the first part of the document to have an overview on how to prepare a Protection Profile for EFC equipment, the annexes, particularly A.4 and A.5, require that the reader be familiar with ISO/IEC 15408 (all parts). The document uses an OBE with an integrated circuit(s) card (ICC) as an example to describe both the structure of the PP, as well as the proposed content.

In Annex A, the guideline for preparing EFC/PP is described by using an OBE as an example of EFC products. The communication link (between the OBE and the RSE) is based on DSRC.

Annex B gives an example of how a threat analysis can be done, while Annex C provides an overview of the relevant security standards in the context of the EFC, which provides the background of EFC roles and interfaces.

5.2 EFC security architecture

Figure 2 shows how this document fits in the overall picture of EFC security architecture. The shaded boxes are the aspects mostly related to the preparation of PPs for EFC systems.

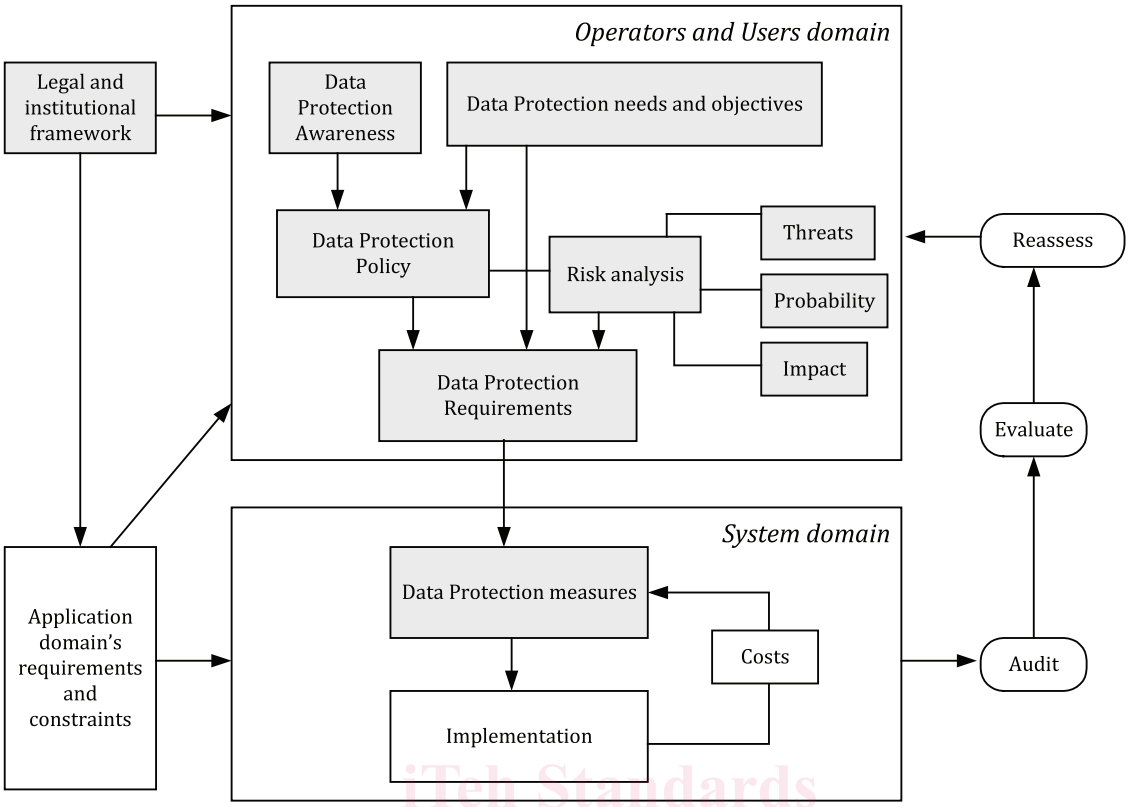

Figure 2 — Overall view of security architecture

5.3 Protection profile preparatory steps

The main purpose of a PP is to analyse the security environment of a subject and then to specify the requirements meeting the threats that are the output of the security environment analysis. The subject studied is called the target of evaluation (TOE). In this document, an OBE with an ICC is used as an example of the TOE.

The preparatory work of EFC/PP consists of the steps shown in Figure 3 (in line with the contents described in Clause 6).

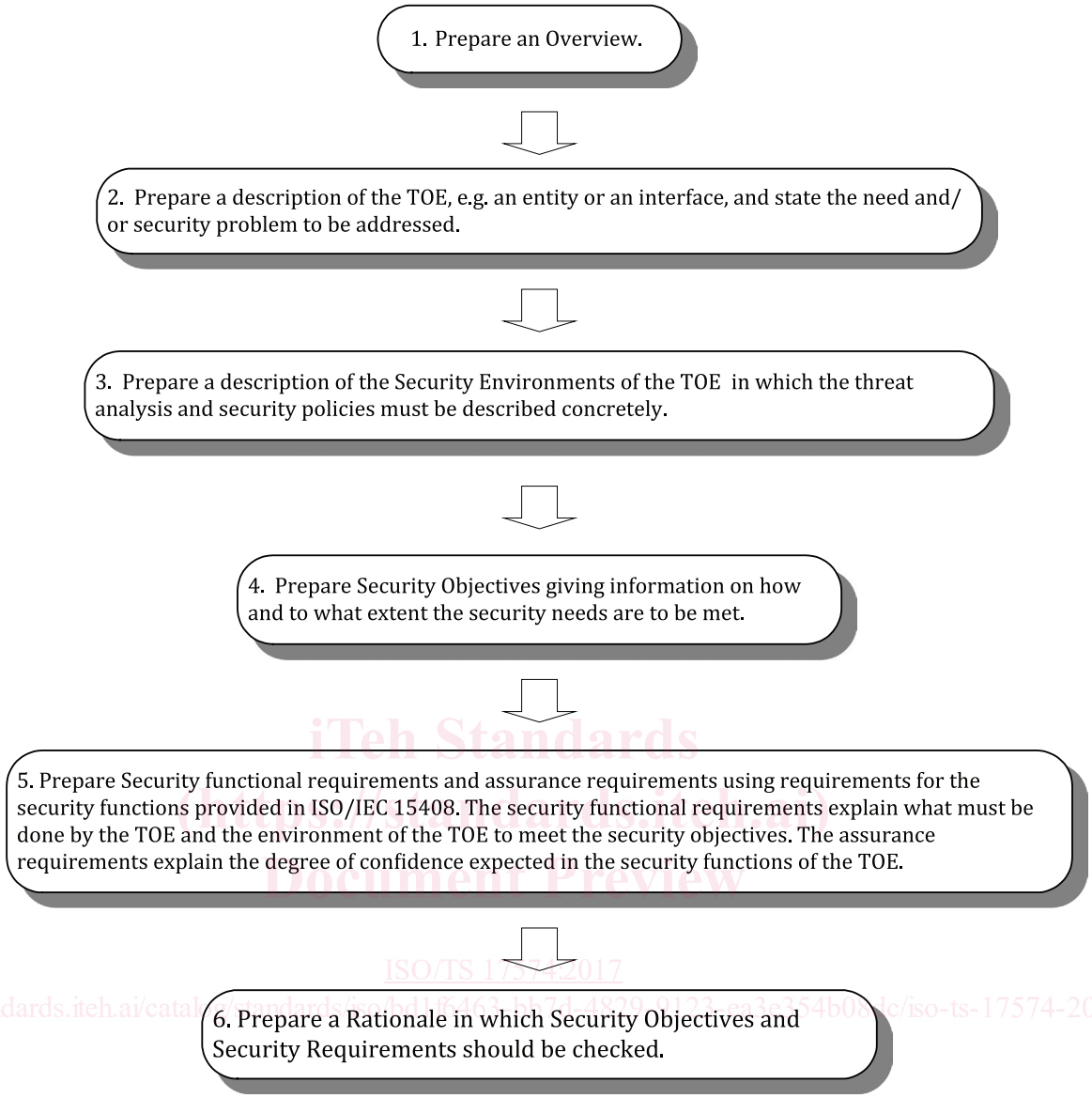

Figure 3 — Process of preparing a Protection Profile for EFC equipment

A PP may be registered publicly by the entity preparing the PP in order to make it known and available to other parties that may use the same PP for their own EFC systems.

5.4 Relationship between actors

By security target (ST), it means a set of security requirements and specifications to be used as the basis for evaluation of an identified TOE. While the PP could be looked upon as the EFC toll service providers' requirements, the ST could be looked upon as the documentation of a supplier as for the compliance with and fulfilment of the PP for the TOE, e.g. an OBE.

Figure 4 shows a simplified picture and example of the relationships between toll service provider, the EFC equipment supplier and an evaluator. For an international registry organization, i.e. Common Criteria Recognition Arrangement (CCRA) and current registered PPs, refer to Annex D.

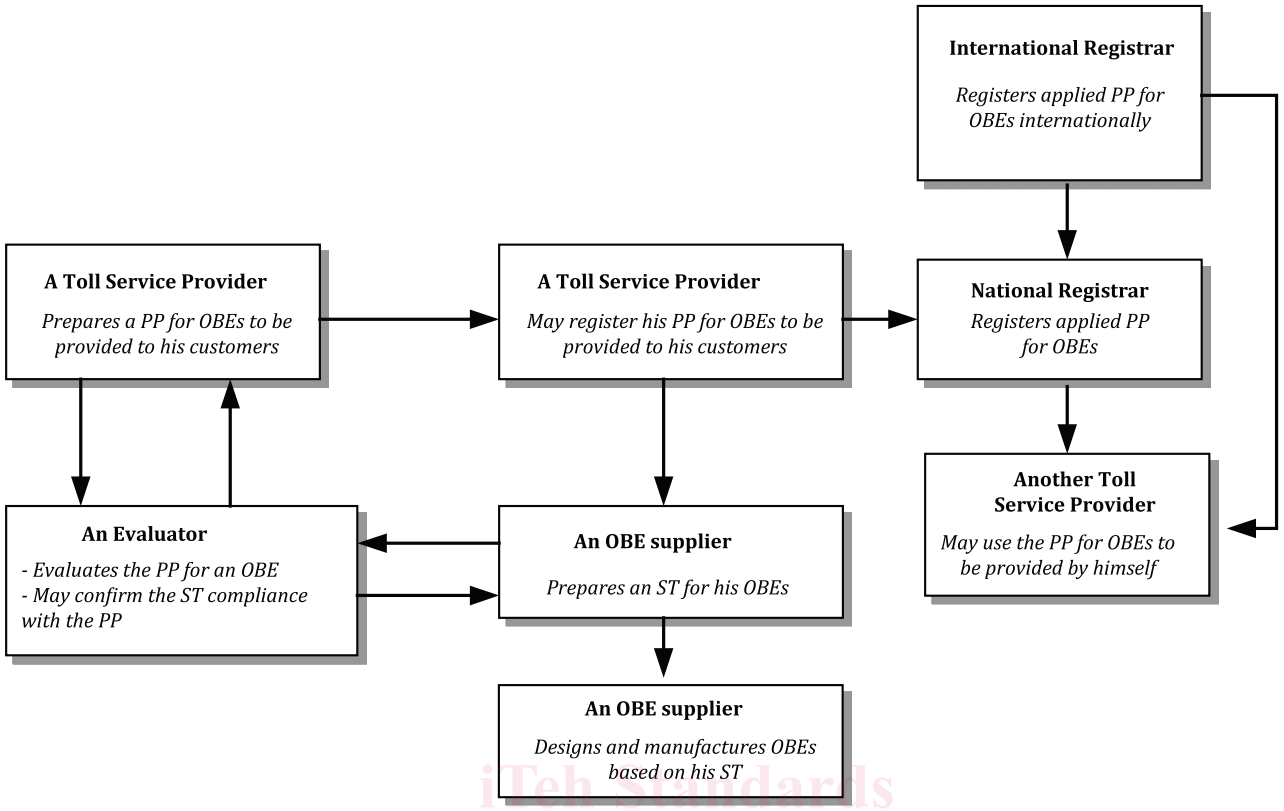

Figure 4 — Relationships between operators, suppliers and evaluators

The ST is similar to the PP, except that it contains additional implementation-specific information detailing how the security requirements are realized in a particular product or system. Hence, the ST includes the following parts not found in a PP:

— a TOE summary specification that presents the TOE-specific security functions and assurance measures;

— an optional PP claims the portion that explains PPs with which the ST is claimed to be conformant (if any);

— a rationale containing additional evidence establishing that the TOE summary specifications ensure satisfaction of the implementation-independent requirements and that claims about PP conformance are satisfied;

— actual security functions of EFC products will be designed based on this ST (see example in Figure 5).