International Standard

ISO 17574

Electronic fee collection — Requirements for security protection profiles

Perception de télépéage — Exigences relatives aux profils de protection de sécurité

First edition
2026-09

Reference number
ISO 17574:2026(en)

COPYRIGHT PROTECTED DOCUMENT

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 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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 the third edition (ISO/TS 17574:2017), which has been technically revised.

The main changes are as follows:

— Clause 3 has been updated and ISO 17573-2 has been made the primary source for terms and definitions;

— requirements have been updated to reflect the latest edition of the ISO/IEC 15408 series.

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

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 are countered with various types of security measures linked to specified security requirements.

It is recommended that EFC operators prepare their own EFC protection profile (PP) according to this document, as security requirements should be described from the operator's point of view.

A protection profile (PP) refers to a set of safety requirements for a category of products or systems that meet specific needs. A typical example is a PP for on-board equipment (OBE) to be used in an EFC system. However, the requirements in this document are superseded if a PP already exists for the subsystem in question.

The target of evaluation (TOE) for EFC is limited to EFC specific roles and interfaces as shown in Figure 1. Figure 1 shows the relationships and interactions among the entities related to the TOE of the EFC. As shown in this figure, entities are overall management of the toll charging environment, EFC service provider, toll charger and user of the service. 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.

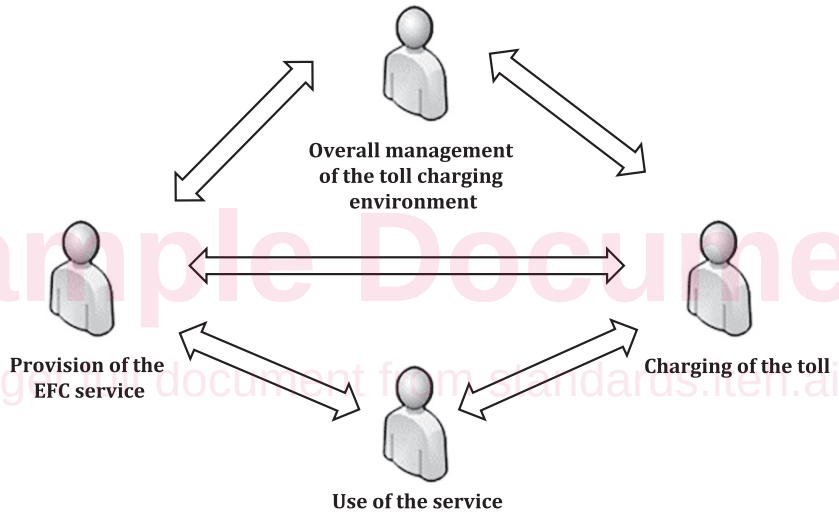

Figure 1 — Scope of TOE for EFC

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 complementary approach, which can be beneficial to apply when evaluating the security of a system.

It should be noted that the requirements provided in this document are intended to be read in conjunction with the ISO/IEC 15408 series. Annex A provides an example of how to prepare the security requirements for EFC equipment, in this case, a dedicated short-range communication (DSRC)-based OBE with an integrated circuit(s) card (ICC) containing data needed for the EFC. The example refers to a Japanese national EFC system and should only be regarded as an example.

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

This document on security service framework and PP for EFC is based on the ISO/IEC 15408 series. The ISO/IEC 15408 series includes a set of requirements for the security functions and assurance of IT-relevant products and systems. Operators, organizations or authorities defining their own PP for EFC can use these

requirements. The different PPs for EFC defined by operators, organizations or authorities will be similar to the different PPs registered by several financial institutions, e.g. for payment instruments like IC cards (ICCs).

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

Electronic fee collection — Requirements for security protection profiles

1 Scope

This document specifies electronic fee collection (EFC) requirements for the preparation and evaluation of security requirements specifications, referred to as protection profiles (PP) in the ISO/IEC 15408 series and in ISO/IEC TR 15446.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15408-1:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components*

ISO/IEC 15408-4:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities*

ISO/IEC 15408-5:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements*

ISO 17573-2, *Electronic fee collection — System architecture for vehicle related tolling — Part 2: Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 17573-2 apply.

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

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

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

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

ICC integrated circuit(s) card

IT information technology

OBE on-board equipment

PP protection profile

RSE roadside equipment

SAM secure application module

SFP security function policy

SFR security functional requirement

ST security target

TOE target of evaluation

TSF target of evaluation 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 ISO/IEC 15408 series and ISO/IEC TR 15446. Although a reader unfamiliar with the standards can read the first part of the document to have an overview on how to prepare a PP for EFC equipment, the annexes, in particular Annexes A.4 and A.5, require the reader to be familiar with the ISO/IEC 15408 series. This 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 procedure for preparing PP for EFC is illustrated, which is described by using an OBE as an example of EFC equipment. 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 illustrates the position of this document within the broader context of the EFC security architecture, highlighting the relationships between related domains and information dependencies. The shaded boxes are the aspects mostly related to the preparation of PPs for EFC systems.

Regarding the security design framework, there are five domains. Functionality of these domains are described as below.

— Operator domain defines the data protection requirement of the TOE as PP.

— System domain develops the ST based on the requirement. For development of the ST, threat and risk assessment are done with balancing the cost and effect of the security measures.

— Legal domain defines the relevant regulations and standards.

— Application domain defines the requirement and constraints of the TOE.

— Audit domain conducts the audit and evaluation of validities of design of implementation for data protection measures. As the feedback of the audit and evaluation, reasons are reported to System domain and Operator domain.

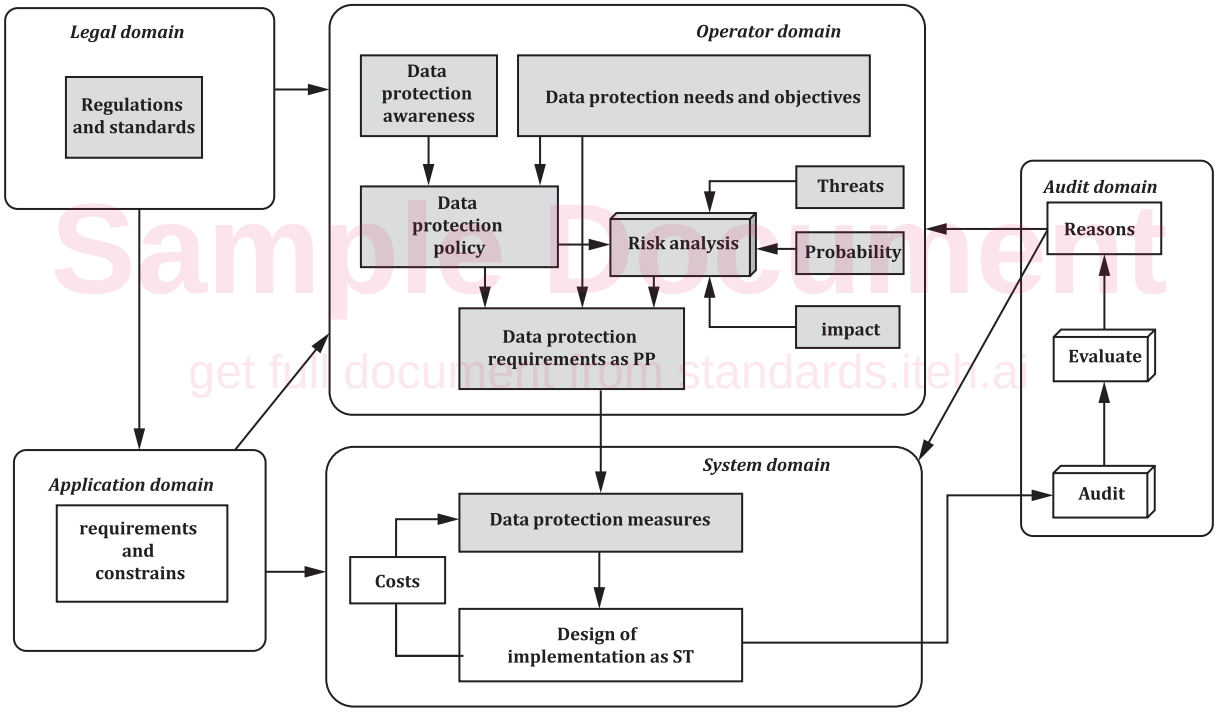

Figure 2 — Overall view of security design framework

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 for each of the threats identified by 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 PP for EFC consists of the steps shown in Table 1, according to the contents described in Clause 6.

For the first step, a general outline of TOE is prepared as overview. As the second step, features, interface of TOE and its use case are defined and in the third step, security environment and its security policies are defined. As the fourth step, security objectives are defined. Based on this preparation, the security functional requirements and the assurance requirements are defined based on the requirements in ISO/IEC 15408. As the 6th step, rationale of the defined functional and assurance requirements are checked.

Table 1 — Process of preparing a protection profile for EFC equipment

Step	Description prepared by Toll service provider	Contents
1	Overview	Overview of the description
2	Descriptions of the TOE	An entity, an interface and necessity, security problems to be addressed
3	Descriptions of the security environment	Threat analysis and security policies must be described concretely
4	Security objectives	How and what extends the security needs are to be met
5	Security functional and assurance requirements using requirements for the security functions provided in ISO/IEC 15408.	The security functional requirements explain what must be done by the TOE and the environment of the TOE to meet the security objectives. The assurance requirements explain the degree of confidence expected in the security functions of the TOE
6	Rationale	Security Objectives and Security Requirements should be checked.

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

5.4 Relationship between actors

A security target (ST) represents a set of security requirements and specifications to be used as the basis for evaluation of an identified TOE. While the PP can be looked upon as the EFC toll service provider's requirements, the ST can be looked upon as the relevant equipment's supplier documentation for the compliance of TOE with the PP (e.g. an OBE as the TOE).

Figure 3 shows a simplified picture and example of the relationships among toll service provider, the EFC equipment supplier and an evaluator. The toll service provider prepares the PP and provides it to OBE supplier to specify the security target to design and manufacturing the OBE. The PP is registered to National Register for the future use for development of a new OBE. The OBE supplier prepares the ST and submits this to the evaluator. The evaluator confirms the ST with the PP. After the evaluation, the OBE supplier designs and manufactures the OBE.

NOTE The Common Criteria Recognition Arrangement [4] includes provision for an international registrar.

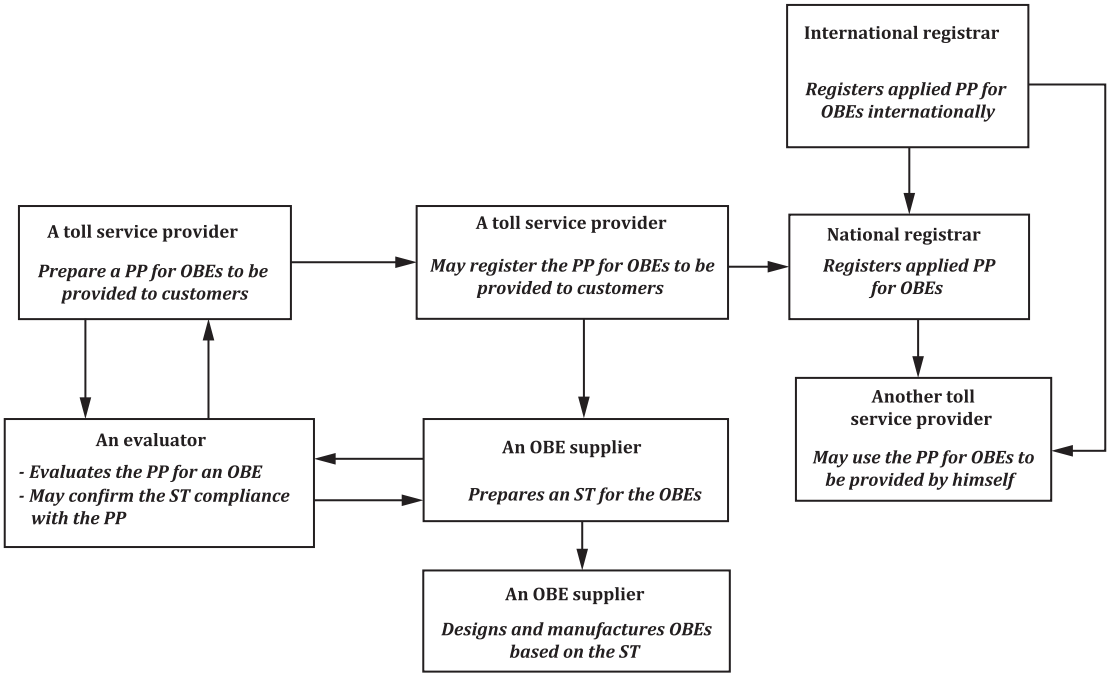

Figure 3 — Relationships among operators, suppliers and evaluators

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 present in a PP:

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

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

— a justification 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 4). The PP is prepared by referring to ISO/IEC 15408 or the PP database. A new PP is registered in the PP database. The ST of the OBE is prepared referring to the PP stored in the database.

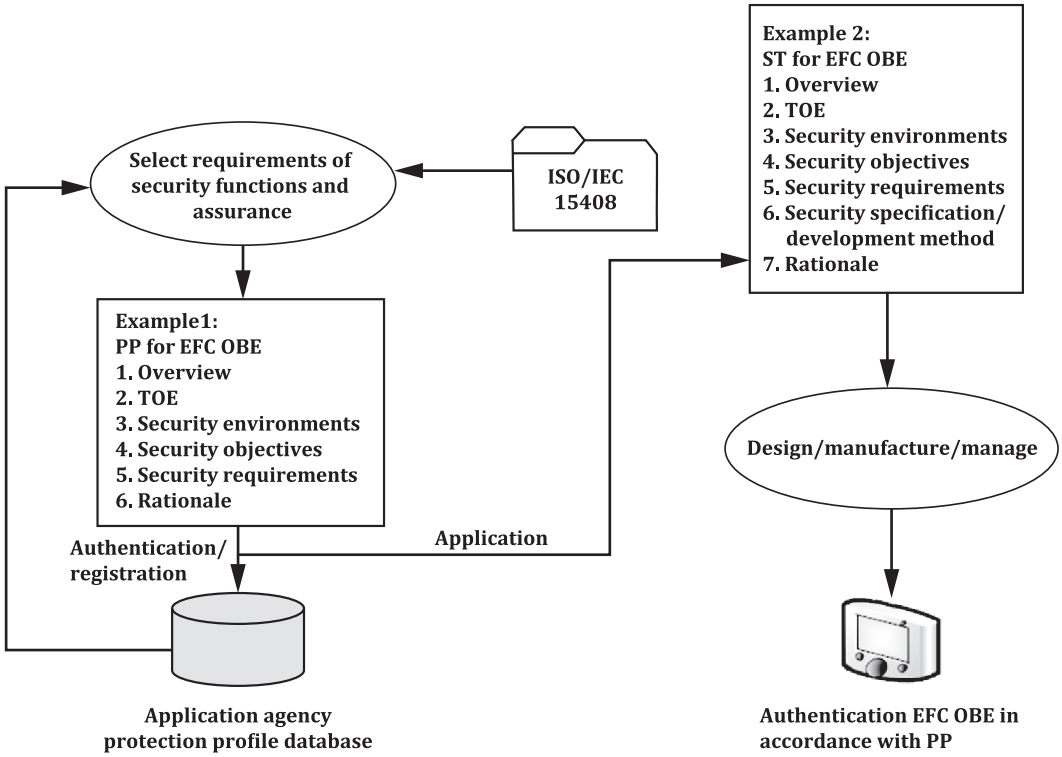

Figure 4 — Example of design based on a PP

6 Outline of protection profile (PP)

6.1 Structure

The content of a PP for a part or interface of an EFC system shall be in accordance with ISO/IEC 15408-1:2022, Clause 10. An example is provided in Annex B.

a) Top page for title

b) Overview

c) Target of Evaluation

d) Conformance

e) Security Environment

f) Security Objectives

g) Security Requirements

h) Rationale

6.2 Context

Guidelines for preparing PP are as follows:

a) Overview (see A.1)

b) Target of evaluation (TOE, see A.2)

The scope of the TOE shall be specified.

c) Conformance

The conformance claims of PPs shall be specified.

d) Security environment (see A.3)

Development, operation and control methods of the TOE are described to clarify the working and operation requirements. Regarding these requirements, IT assets, for which the TOE must be protected, and the security threats to which the TOE is exposed, shall be specified.

e) Security objectives (see A.4)

Security policies for threats to the TOE are determined. The policies are divided into technical, operational and control policy.

Security objectives should be consistent with the operational aim or product purpose of the TOE.

Operational and control policies are defined as personnel and physical objectives applicable to the status, in which the TOE is used or operated. The operational and control policy include control and operational rules for operators.

f) Security requirements (see A.5)

In accordance with the security objectives specified in A.4, specific security requirements for security threats stated in A.3 are specified. The security requirements consist of functional requirements and assurance requirements for security quality.

Functional requirements are provided, selecting necessary requirements from ISO/IEC 15408-2 and determining parameters, which shall be in accordance with ISO/IEC 15408-2:2022, Clause 6 to Clause 18.

Regarding assurance requirements, assurance requirements specified in ISO/IEC 15408-3 are adopted by determining evaluation levels for assurance requirements, which shall be in accordance with ISO/IEC 15408-3:2022, Clause 5 to Clause 15.

The evaluation method and activities are included in the security requirements, which shall be in accordance with ISO/IEC 15408-4:2022, Clauses 5 and 6.

The evaluation assurance levels are included in the security requirements, which shall be in accordance with ISO/IEC 15408-5:2022, Clause 4.

g) Rationale of justification and effectiveness (see A.6)

The content of PP is checked when necessary and covers security requirements for the TOE. The checked items are as follows:

— all security environments needed are covered;

— security objectives should completely meet the security environments;

— security requirements should implement security objectives.

Annex A
(informative)

Procedure to prepare the protection profile

A.1 Overview

A.1.1 General

A general outline of the protection profile (PP) is described in this annex.

This annex provides an example of how to prepare the security requirements for EFC relevant equipment, in this case, an OBE with an ICC containing data needed for EFC.

A.1.2 Identification information

Identification information for the document with example is as follows:

a) document title

EXAMPLE 1 document title: OBE Security protection profile

b) version or release number

EXAMPLE 2 reference or version number: 1.0

c) preparation date

EXAMPLE 3 preparation date: 2002-10-20

d) name of the person responsible for preparing the PP document

EXAMPLE 4 prepared by: ABC Association

A.1.3 Target of evaluation (TOE) description

TOE in the prepared PP contains the following:

a) product

EXAMPLE 1 product: EFC OBE

b) version or release number

EXAMPLE 2 version or release number: 1.0

c) developer

EXAMPLE 3 developer: ABC Co., Ltd

A.1.4 In accordance with ISO/IEC 15408 (all parts)

The prepared PP according to ISO/IEC 15408 (all parts) and the edition of ISO/IEC 15408 are stated explicitly.

The PP shall be prepared according to the ISO/IEC 15408 series and its relation to the ISO/IEC 15408 series shall be stated in the PP. The statement of conformance includes conformance to each part of the ISO/IEC 15408 series and state the relevant edition used.

An example of conformance statement according to ISO/IEC 15408 (all parts) is shown as follows:

EXAMPLE

— ISO/IEC 15408-1:2022(Edition 4)

— ISO/IEC 15408-2:2022 (Edition 4)

— ISO/IEC 15408-3:2022 (Edition 4)

— ISO/IEC 15408-4:2022 (Edition 1)

— ISO/IEC 15408-5:2022 (Edition 1)

A.1.5 Outline of TOE

A.1.5.1 Type of TOE

For users of security PP a type of TOE described in PP is described explicitly to help them determine the application.

EXAMPLE

Type of TOE: EFC OBE

A.1.5.2 TOE functional outline

For users of security PP, a type of device described in PP is described explicitly to help them determine the application. Examples are as follows:

EXAMPLE

TOE functional outline of an OBE

a) EFC function:

   1) mutual authentication with ICC;

   2) transcription (caching) of ICC data to OBE;

   3) encryption of radio communication with RSE;

   4) assurance of message integrity;

   5) mutual authentication with RSE;

   6) storage of secured information (encryption key) used in OBE during EFC transaction.

b) Set-up function:

   1) authentication of set-up card;

   2) caching of vehicle information from ICC to OBE.

c) HMI function:

   1) report of EFC billing results to users;

   2) guidance of EFC lane.