TECHNICAL SPECIFICATION

ISO/TS 17574

Second edition
2009-09-15

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 17574:2009(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In other circumstances, particularly when there is an urgent market requirement for such documents, a technical committee may decide to publish other types of document:

— an ISO Publicly Available Specification (ISO/PAS) represents an agreement between technical experts in an ISO working group and is accepted for publication if it is approved by more than 50 % of the members of the parent committee casting a vote;

— an ISO Technical Specification (ISO/TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

An ISO/PAS or ISO/TS is reviewed after three years in order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn. If the ISO/PAS or ISO/TS is confirmed, it is reviewed again after a further three years, at which time it must either be transformed into an International Standard or be withdrawn.

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.

ISO/TS 17574:2009 was prepared by the European Committee for Standardization (CEN) Technical Committee CEN/TC 278 *Road Transport and Traffic Telematics* in collaboration with Technical Committee ISO/TC 204, *Intelligent transport systems*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This second edition cancels and replaces the first edition (ISO/TS 17574:2004) which has been technically revised.

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 Technical Specification to prepare their own EFC/PP, as security requirements should be described from the standpoint of the operators and/or operators', organizations.

It should be noted that this Technical Specification is of a more informative than normative nature and it cannot be used without also using the ISO/IEC 15408 series. Most of the content of this Technical Specification 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 and used 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 standard on security service framework and EFC/PP is based on the ISO/IEC 15408 series. ISO/IEC 15408 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, 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 Technical Specification provides a **guideline** for 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. By a Protection Profile (PP) is meant 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 (OBEs) to be used in an EFC system.

This Technical Specification should be read in conjunction with the underlying standards ISO/IEC 15408 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, in particular A.4 and A.5, require that the reader be familiar with ISO/IEC 15408. 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.

Figure 1 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.

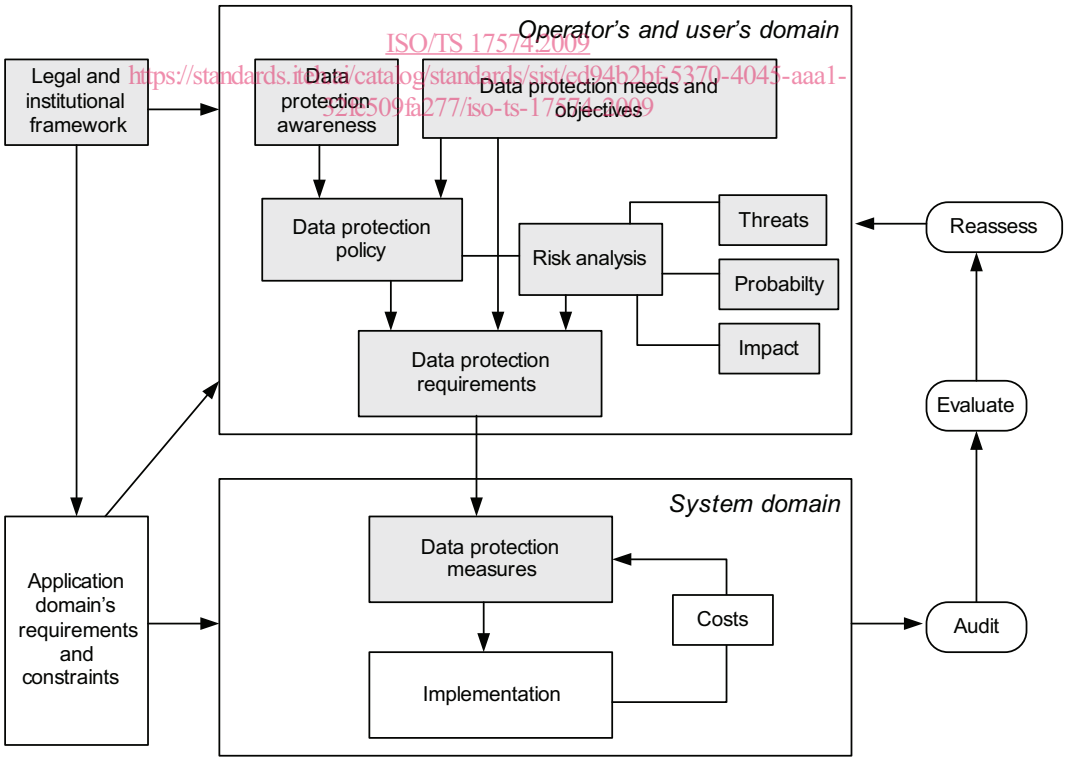

Figure 1 — Overall view of security architecture

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 2 (in line with the contents described in Clause 5).

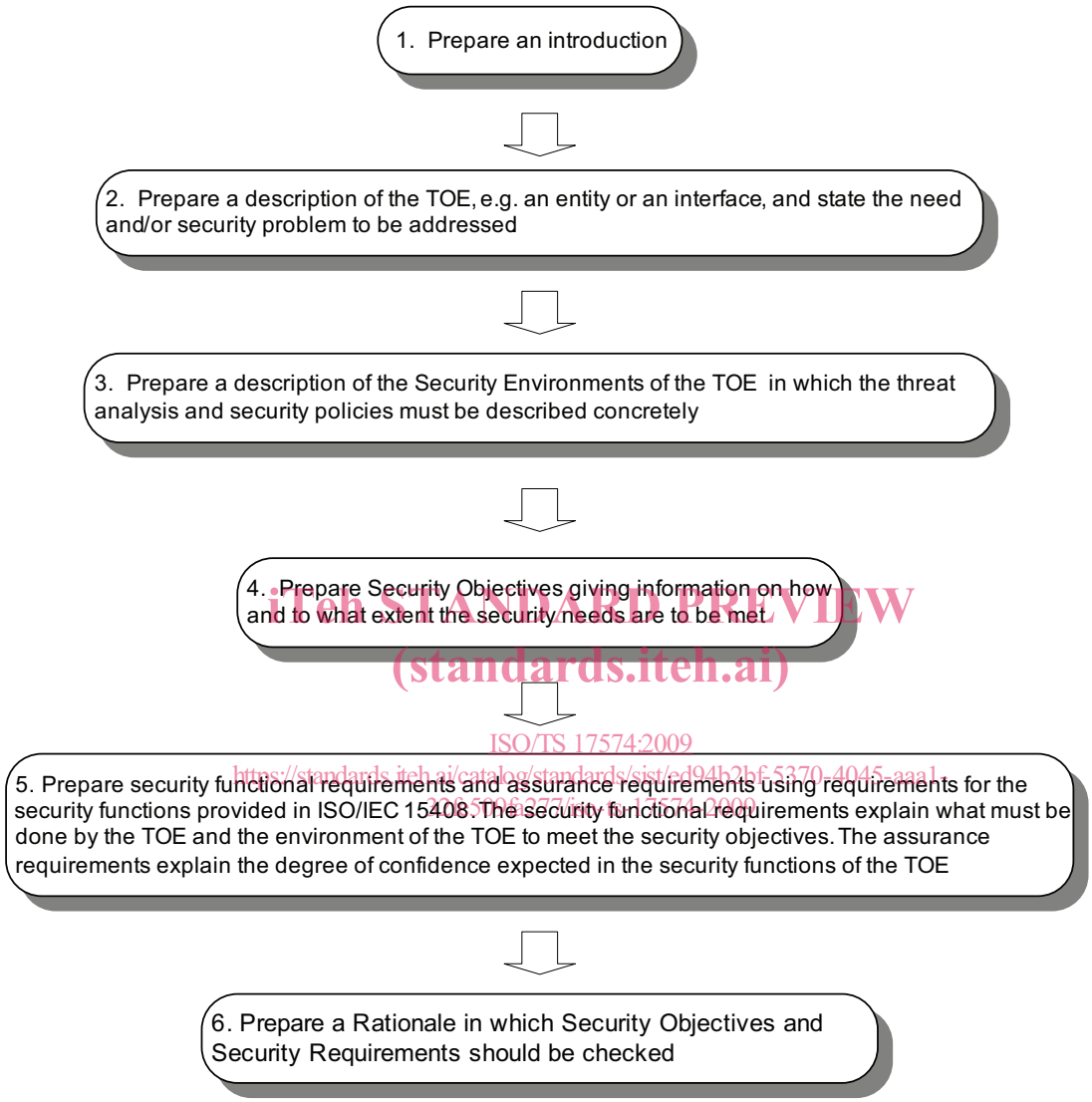

Figure 2 — The process of preparing a Protection Profile for EFC equipment

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.

By a Security Target (ST) is meant 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 operator 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 3 shows a simplified picture and example of the relationships between the EFC operator, the EFC equipment supplier and an evaluator. For an international registry organization, i.e. Common Criteria Recognition Arrangement (CCRA) and current registered PPs, please refer to Annex D.

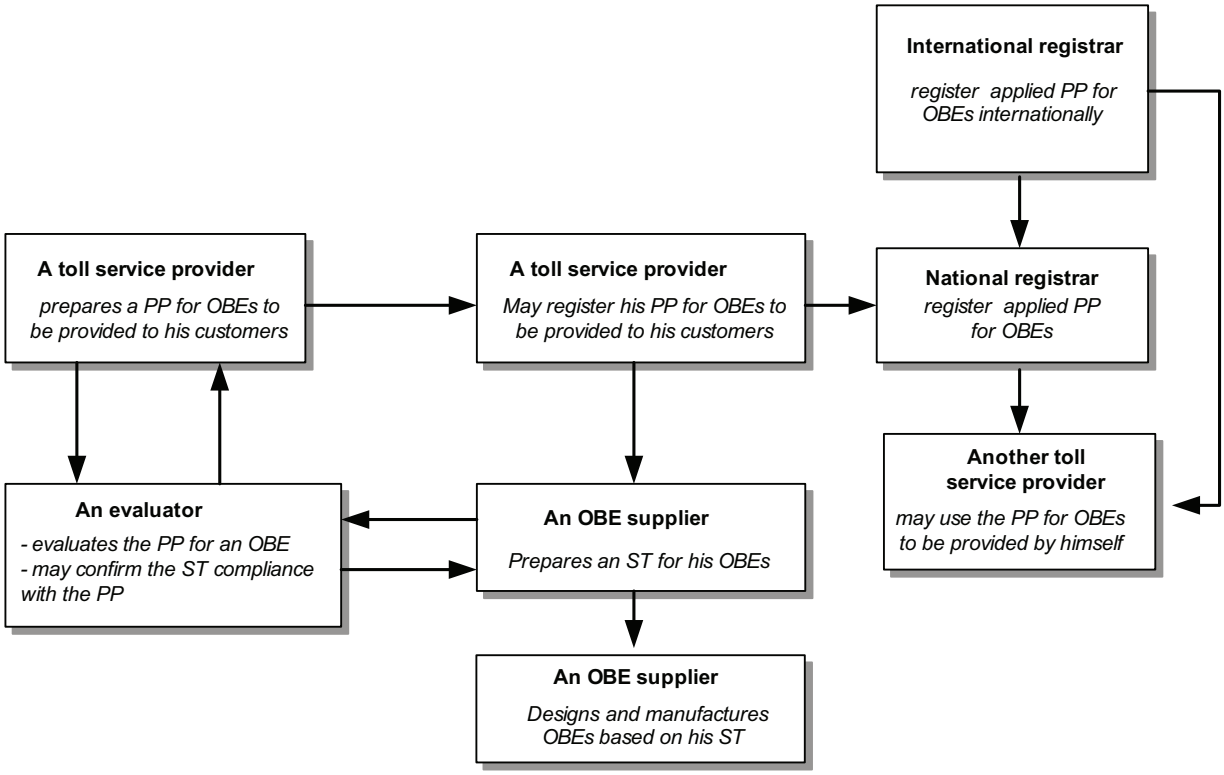

Figure 3 — Relationships between operators, suppliers and evaluators

The ST is similar to the PP, except that it contains additional implementation-specific information detailing how the security requirements are realised 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 4.

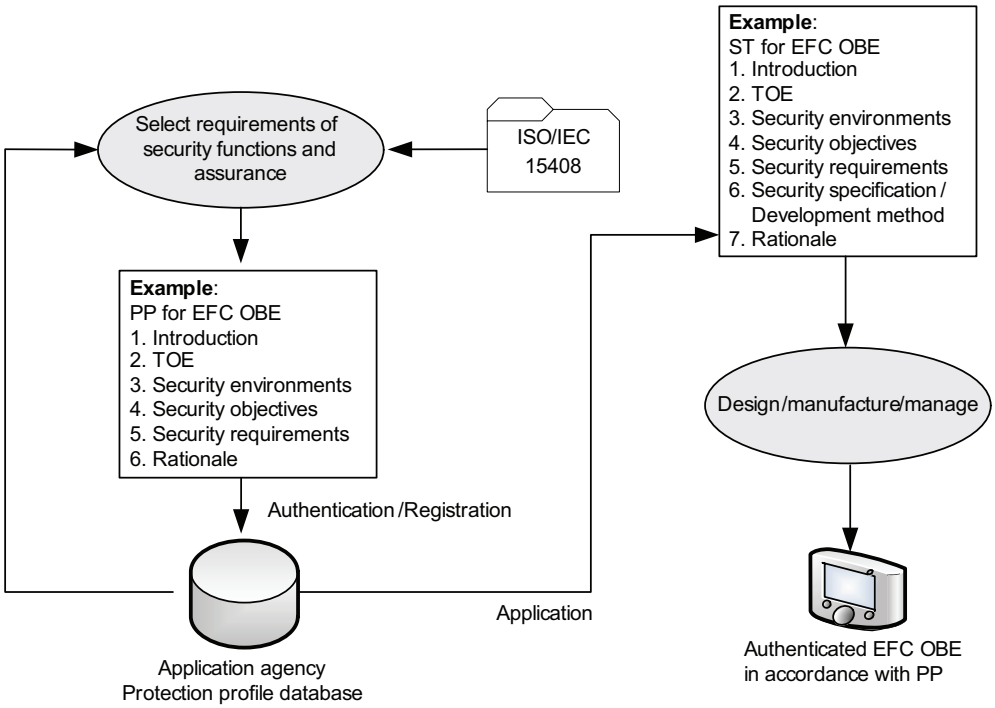

Figure 4 — Example of design based on a PP

TOE for EFC is limited to EFC specific roles and interfaces shown in Figure 5. 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.

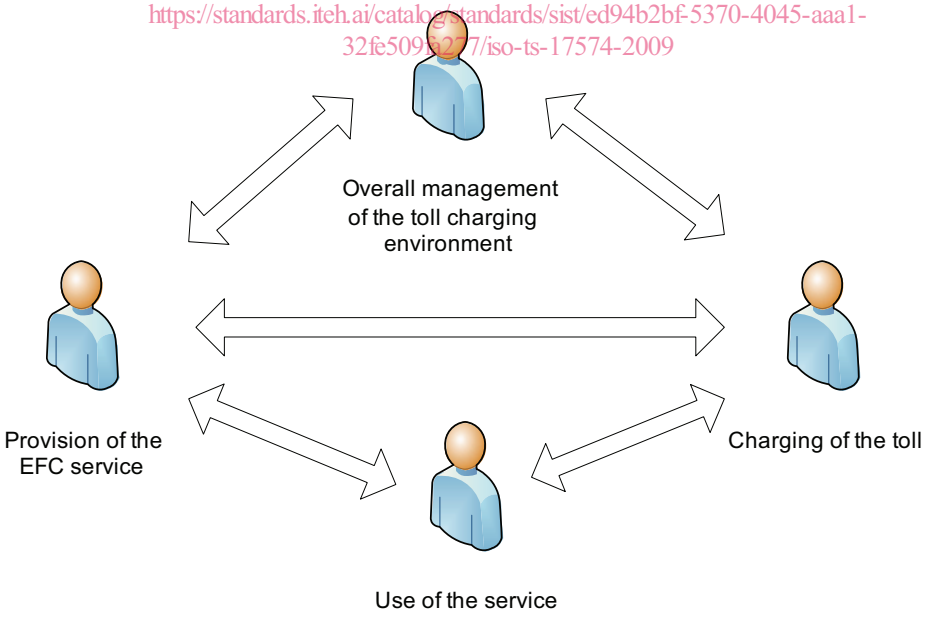

Figure 5 — Scope of TOE for EFC

The security evaluation is performed by assessing the security related properties of roles, entities and interfaces defined in STs, as opposed to assessing complete processes which often are distributed over more entities and interfaces than those covered by the TOE of this CEN/ISO Technical Specification.

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.

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

2 Normative references

The following referenced documents are indispensable for the application 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, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements*

ISO/IEC 15408-3:2008, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements*

3 Terms and definitions

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

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

3.2
audit
recognising errors such as illicit systems and/or illicit access and recording and analysing information related to security relevant activities and events in order to attain proper security control in accordance with security policy

3.3
availability
dependability with respect to readiness for usage and a measure of correct service delivery based on the alternation of correct and incorrect service

3.4
Central Communication Unit
part of the central equipment serving as a mobile communication interface to the OBE

3.5
central equipment
system components at fixed centralized locations

NOTE Central equipment is not the same as central system. Central equipment is used in the GNSS/CN based EFC system.

3.6
certification
action by a third party, demonstrating that adequate confidence be provided that a duly identified product, process or service is in conformity with a specific standard or other normative document

3.7
confidentiality
prevention of information leakage to non-authenticated individuals, parties and/or processes

3.8
customer
〈of a toll service provider〉 person or legal entity that uses the service of a toll service provider

NOTE Depending on the local situation the customer may be the owner, lessor, lessee, keeper, (fleet) operator, holder of the vehicle's registration certificate, driver of the vehicle, or any other third person.

3.9
Evaluation Assurance Level
EAL
assurance levels to evaluate securities for products and systems

3.10
functional requirement
security requirements to determine the security functions, which are required for systems and/or products

3.11
integrity
property that information (data) has (have) not been altered or destroyed in an unauthorized manner

3.12
international registrar
company authorized to register Protection Profiles at an international level

3.13
Key Management
Encryption Key Control
generation, distribution, storage, application and deletion of encryption keys

3.14
On-Board Equipment
OBE
equipment fitted within or on the outside of a vehicle and used for toll purposes

NOTE The OBE does not need to include payment means.

3.15
personalization card
set-up card
IC card to transcribe individual data such as vehicle information into On-Board Equipment

3.16
privacy
right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

3.17
protection
act of protecting, or the state of being protected

EXAMPLE Preservation from loss, theft, damage or unauthorized access.

3.18
rationale
verification
process determining that a product of each phase of the system life cycle development process fulfils all the requirements specified in the previous phase

3.19
reliability
attribute of any system that consistently produces the same results, preferably meeting or exceeding its specifications

3.20
responsibility
state of being responsible, accountable or answerable, as for an entity, function, system, security service or obligation

3.21
road side equipment
RSE
equipment located at a fixed position along the road transport network, for the purpose of communication and data exchanges with the On-Board Equipment of passing vehicles.

3.22
secure application module
SAM
physically, electrically and logically protected module intended to contain algorithm(s), related keys, security procedures and information to protect an application in such a way that unauthorized access is not possible

3.23
security policy
set of rules that regulate how to cope with security threats or to what degree of security levels should be kept

3.24
security threat
potential action or manner to violate security systems

3.25
security target
ST
set of security requirements and specifications to be used as the basis for evaluation of an identified TOE

3.26
target of evaluation
TOE
information security product or system for the subject of security evaluation

3.27
toll charger
legal entity charging a toll for vehicles in a toll domain

NOTE In other documents the terms operator or toll operator can be used.

3.28
toll service provider
legal entity providing to his customers toll services on one or more toll domains for one or more classes of vehicle

NOTE 1 In other documents the terms issuer or contract issuer might be used.

NOTE 2 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 The toll service provider is responsible for the operation (functioning) of the OBE.

3.29
validity
quality or state of being valid; having legal force

4 Abbreviations

— 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 Outlines of Protection Profile

5.1 Structure

The content of a Protection Profile for a part or interface of an EFC system is shown in Figure 6.

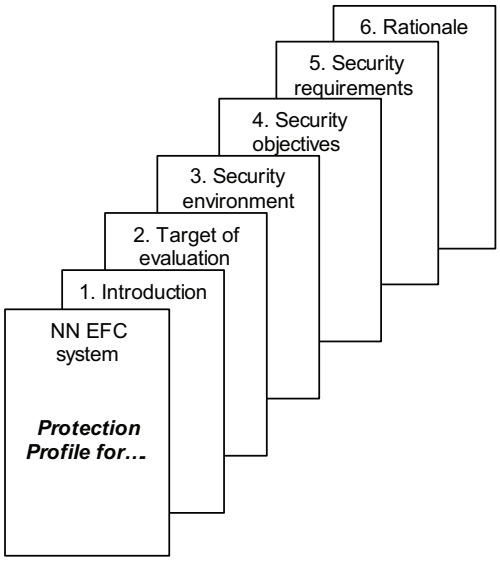

Figure 6 — Content of a Protection Profile

5.2 Context

Guidelines for preparing PP are as follows:

a) Introduction (See Clause A.1).

b) Target of Evaluation (TOE, See Clause A.2).

The scope of the TOE shall be specified.

c) Security environments (See Clause A.3).

Development, operation and control methods of the TOE are described in order to clarify the working/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.

d) Security objectives (See Clause A.4).

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

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

Operational/control policy is defined as personnel and physical objectives in the status for which the TOE is used or operated. The operational/control policy includes control and operational rules for operators.

e) Security requirements (See Clause A.5).

In accordance with the security objectives defined in Clause A.4, concrete security requirements for security threats stated in Clause A.3 are specified. The security requirements consist of functional requirements (technical requirements) and assurance requirements for security quality.